UNIVERSITÉ DU QUÉBEC À MONTRÉAL

CYBERESPACE, RELATIONS INTERNATIONALES ET PAYS ÉMERGENTS : ÉVOLUTION OU RÉVOLUTION?

MÉMOIRE
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN SCIENCE POLITIQUE

PAR SAMUEL RAGOT

OCTOBRE 2015

REMERCIEMENTS

Mes remerciements les plus chaleureux vont à mon directeur, le professeur Ting-Sheng Lin pour son encadrement et ses nombreux apports à la présente recherche.

Je tiens également à remercier mes parents pour leur soutien constant et leur inébranlable confiance dans mon travail et dans les différentes implications qui m'ont été possibles de vivre tout au long de mon cheminement universitaire. Sans leur précieux soutien, il est certain que le présent mémoire n'aurait pas été écrit.

Mes remerciements vont aussi à ma meilleure amie et partenaire de vie, Mme Gaëlle-Mauve Lapostolle, qui m'a accompagnée pendant de nombreuses années d'écriture et d'implication universitaire. Son dévouement et sa présence ont été essentielles à la réussite du présent projet d'études.

N'oublions pas le soutien et l'écoute constante de Mme Lysa Brunet, assistante des programmes de cycles supérieurs au Département de science politique. Sans son aide et ses tours de magie, il est probable que la machine administrative eu tôt fait de me faire abandonner le présent mémoire.

Enfin, je tiens à remercier différentes personnes ayant à un moment donné ou un autre pu me soutenir à travers différentes épreuves dans les dernières années. Mentionnons M. Philippe Ducharme, le Dr.Frederique Van Den Eynde, Mme Valérie Lafrance ; et tous les camarades d'études et de lutte que j'ai pu côtoyer et qui m'ont alimenté tant intellectuellement, politiquement que socialement depuis de nombreuses années.

DÉDICACE

À mes parents,
À mes amis et amies,

À toutes les personnes pouvant vivre avec des problématiques de santé mentale,

qui se voient encore et toujours stigmatisées dans le milieu universitaire,

ensemble nous pouvons réussir et dépasser les préjugés.

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES iv

RÉSUMÉ vi

CHAPITRE I
INTRODUCTION ET CADRE D'ANALYSE 1
1. Question et intérêt de la recherche 1
2. Questions secondaires de recherche et structure de la recherche 2
3. Cadre d'analyse 3
3.1 Méthodologie 3
3.2 La « crise d'intelligibilité » liée au cyberespace 4
3.3 Cadre d'analyse utilisé 6
3.4 Conclusion sur le cadre d'analyse 13

CHAPITRE II
STRUCTURE DU CYBERESPACE 14
1. Le cyberespace et ses principales caractéristiques 14
1.1 Un espace nouveau et omniprésent des activités humaines, basé sur la technologie 15
1.2 Un espace poreux 23
1.3 Un espace facile d'accès 26
1.4 Les risques liés au cyberespace 30
1.5 Conclusion sur la structure du cyberespace 37
2. Acteurs en présence et intérêts 37
2.1 Les États 39
2.2 Les groupes terroristes et autres *hackers* 40
2.3 Cybercriminels et cybercriminalité 42
2.4 Les acteurs civils 43
3 Conclusion partielle sur la structure du cyberespace et les acteurs en présence 45

CHAPITRE III
CYBERESPACE ET RELATIONS INTERNATIONALES 46

1. Un espace nouveau des relations internationales 46
2. La projection de la force dans le cyberespace 48
2.1 Souveraineté dans le cyberespace 49
2.2 L'information au cœur du cyberespace 50
2.3 Le cyberpouvoir 52
3. Cyberattaques, cyberguerre, cyberdéfense, attaques informatiques et autres menaces dans le cyberespace 56
3.1 Les cyberattaques 57
3.2 La cyberguerre, nouvelle forme de conflit dans le système international 61
3.3 Stratégies de cyberdéfense 65
3.4 Espionnage électronique et industriel 72
4. La gouvernance dans le cyberespace 75
4.1 La présence historique de l'hégémon américain 75
4.2 Un modèle contesté : revendication sur le cyberespace et puissances émergentes 80
5. Conclusion 82

CHAPITRE IV
COMMENT DES PAYS ÉMERGENTS AYANT ORIENTÉ LEURS POLITIQUES ÉDUCATIVES VERS LA MISE À DISPOSITION D'UNE MAIN-D'OEUVRE TECHNOLOGIQUEMENT QUALIFIÉE POURRAIENT-ILS TIRER PROFIT DE LA MISE EN PLACE DE CYBERSTRATÉGIES? 83
1. Politiques éducatives et projections de force dans le cyberespace 84
2. Exemples d'utilisation des technologies du cyberespace par des pays émergents dans le système international 93
2.1 Diplomatie et renseignement 95
2.2 Cyberguerre et appui aux conflits classiques 107
2.3 Espionnage industriel 117
3. Conclusion 127

CHAPITRE V
L'UTILISATION PAR DES ACTEURS NON DOMINANTS DE TECHNOLOGIES DANS LE CYBERESPACE PRÉSENTE-T-ELLE VRAIMENT

UN RISQUE DE RENVERSEMENT DU SYSTÈME INTERNATIONAL ? 130
1. Un espace révolutionnaire?.....131
1.1 Un nouvel espace des activités humaines 131
1.2 Cyberespace et système international 133
1.3 Un potentiel de guerre totale à ne pas négliger 137
1.4 Les États réussissent-ils à assurer leur sécurité? 144
2. Pourquoi n'y a-t-il pas encore eu de cyberguerre ou d'utilisation des outils présents dans le cyberespace par des pays du sud ? 146
2.1 La question de la dissuasion.....147
2.2 Dépendance nord-sud, développement économique et politique étrangère dans le cyberespace 151
2.3 La désorganisation actuelle des pays du sud contrairement à la période des « non alignés » 154
2.4 Autres acteurs dans le cyberespace.....160

CONCLUSION.....165
1. Cybercrime et espionnage industriel : la plus grande menace? 166
2. L'industrie de la sécurité 169
3. Le cyberespace a déjà tout changé et va continuer de tout changer.....173

BIBLIOGRAPHIE 180

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

APL	Armée population de libération (Chine)
APT	*Advanced Persistent Threat*
BRICS	Brésil, Russie, Inde, Chine, Afrique du Sud
CIA	*Central Intelligence Agency*
DEA	*Drug Enforcement Agency*
FAI	Fournisseur d'accès Internet
FBI	*Federal Bureau of Investigation*
FIRST	*Forum of incident response and security teams*
GCHQ	*Government Communications Headquarters*
GSD (APL)	*General Staff Department* de l'APL
IBSA	Inde, Brésil, Afrique du Sud
ICANN	*Internet Corporation for Assigned Names and Numbers*
IDE	Investissements directs à l'étranger
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
ITU	*International Telecommunication Union*
IRIS	Institut de recherche et d'informations socio-économiques
IXP	*Internet exchange point*
NASA	*National Aeronautics and Space Administration*
NSA	*National security agency*

OTAN	Organisation du Traité de l'Atlantique Nord
OCDE	Organisation de coopération et de développement économiques
ONU	Organisation des Nations-Unies
OSCE	*Organization for security and Co-operation in Europe*
PCC	Parti communiste Chinois
RPDC	République populaire démocratique de Corée
SCADA	*Supervisory Control And Data Acquisition*
STEM	*Science, Technology, Engineering and Math Education*
UE	Union Européenne
WGIG	Working Group on Internet Governance

RÉSUMÉ

La présente recherche a pour but d'étudier les potentielles utilisations de technologies présentes dans le cyberespace par différents acteurs du système international.

Afin de bien comprendre les différents paramètres de notre objet d'étude, nous procéderons à un examen de ce qu'est le cyberespace et de son rôle dans les sociétés occidentales modernes. Cette approche nous permettra d'évaluer l'importance de ce nouvel espace dans les relations humaines.

Par la suite, nous nous pencherons sur l'importance que le cyberespace a pris dans les relations internationales. Nous étudierons notamment les différentes formes de pouvoir qui peuvent exister dans cet espace afin de vérifier si des acteurs non dominants du système international pourraient bénéficier de l'utilisation de ces nouvelles formes de projection de la force.

De façon plus précise, nous étudierons le cas des pays émergents ayant développé des politiques éducatives visant la massification de l'éducation supérieure. Nous tacherons de comprendre en quoi ces politiques publiques pourraient être un avantage stratégique important dans le cadre du développement de capacités de projection de la force dans le cyberespace.

Enfin, nous essaierons de comprendre les enjeux plus larges liés aux évolutions que le cyberespace amène dans nos vies ainsi que dans le système international.

MOTS-CLÉS : cyberespace, cybersécurité, cyberguerre, cyberattaques, cyberpouvoir, cyberinfluence, APL, massification de l'éducation, système international, Internet, théories du droit international, théories de la guerre, sécurité informatique.

CHAPITRE I

INTRODUCTION ET CADRE D'ANALYSE

1. Question et intérêt de la recherche

Notre travail s'intéresse aux questions liées au cyberespace comme nouvel espace d'interactions et de projection de force dans les relations internationales, tant pour les acteurs étatiques que non étatiques.

Notre problématique est axée sur le questionnement visant à savoir si le cyberespace pourrait changer les règles d'engagement dans le système international et ainsi provoquer une révolution dans les relations internationales en permettant à des acteurs non dominants de mener de nouvelles formes de guerres ou de diplomatie. Nous nous intéresserons à des pays d'Asie de l'Est (avec une attention particulière pour le cas de la Chine), ainsi qu'à la Russie. Ces pays ayant développé des politiques publiques de massification de l'éducation nous essaierons, de comprendre en quoi de telles orientations pourraient être un avantage dans l'engagement dans le cyberespace.

Notre thèse est que les pays émergents ayant axé leur développement économique et industriel autour des technologies de l'informatique et des télécommunications et ayant adopté des politiques de massification de l'éducation ont une capacité accrue à utiliser les technologies présentes dans le cyberespace afin de mener des actions politiques pouvant renverser ou déstabiliser le système international, à l'échelle mondiale ou régionale.

L'intérêt de notre recherche est avant tout d'analyser un espace nouveau avec un angle de recherche s'intéressant à des acteurs habituellement négligés, car n'étant pas

dominants dans les relations internationales. En tant que nouvel espace des activités humaines en général, encore mal encadré et maîtrisé, le cyberespace nous semble assez important pour bouleverser les règles du système international et son fonctionnement. Il y a donc un intérêt pour le domaine de la science politique dans l'exploration de ces questions nouvelles et potentiellement majeures pour l'évolution du système international.

2. Questions secondaires de recherche et structure de la recherche

Au fil du présent exercice, nous nous pencherons sur différents sujets d'intérêt pour la vérification de notre hypothèse et pour la compréhension des dynamiques en présence. Les différents chapitres représentent tous autant de questions secondaires de recherche que des explorations utiles à la compréhension et à la vérification de notre hypothèse de recherche.

En premier lieu, nous nous intéresserons aux caractéristiques du cyberespace puisqu'il s'agit de l'espace dans lequel se situe notre recherche. Afin de bien comprendre ce que l'on entend par cyberespace, nous présenterons un ensemble de visions et d'enjeux y étant liés.

Par la suite, nous tâcherons de comprendre comment le cyberespace peut être considéré comme un nouvel espace des relations internationales, mais aussi de la guerre, au même titre que la terre, l'eau, l'espace ou l'air. Nous nous pencherons également sur la question de la nature du cyberespace dans le système international. Nous établirons ainsi la base conceptuelle nécessaire pour traiter de notre problématique de recherche.

Notre quatrième chapitre présentera le concept de massification de l'éducation ainsi

que des cas d'utilisation de technologies du cyberespace dans les relations internationales. À travers des cas d'études, nous nous pencherons sur les multiples façons de projeter de la force ou de l'influence dans le cyberespace pour les pays émergents ou en voie de réindustrialisation.

Enfin, nous tenterons de vérifier la validité de notre hypothèse de recherche. Nous procéderons également à l'ouverture d'un certain nombre de questions de recherche n'ayant pas pu être traitées dans le présent exercice.

3. Cadre d'analyse

La question du cadre d'analyse est épineuse lorsqu'il s'agit d'appréhender notre objet de recherche. En effet, il s'agit d'un domaine assez récent dans la science politique et donc assez peu abordé au point de vue théorique. Nous avons donc opté pour un cadre d'analyse relativement hybride, inspiré d'autres cadres d'analyse existants.

3.1 Méthodologie

Au niveau de la méthodologie nous avons abordé la situation du cyberespace et de ses caractéristiques de manière empirique. Il s'agit entre autres d'évaluer la possibilité d'utiliser différents outils par certains acteurs dans le but de modifier, influencer les relations internationales.

Afin de mener nos recherches, nous nous sommes appuyés sur différentes sources. La majorité de notre matériel de recherche est issue de documents officiels (doctrines militaires, documents de politiques publiques, rapports à différentes institutions étatiques ou chambres de représentants, rapports d'organisations internationales,

rapports militaires) ou de livres traitant de la question de la cyberguerre et plus généralement du cyberespace. Un autre des aspects particuliers des recherches sur le cyberespace est qu'un grand nombre de publications et de rapports viennent d'entreprises privées spécialisées en sécurité informatique. Si nous avons une critique relative au rôle de ces sociétés dans la création - souvent artificielle - d'une menace omniprésente, visant à agrandir le marché de la sécurité, il reste toutefois que de nombreux rapports produits par ces entreprises sont tout de même pertinents à titre informatif ou de complément. Compte-tenu de la nouveauté de notre objet d'étude, nous avons également intégré des articles de périodiques ou de revues afin d'illustrer certains cas d'étude ou d'actualité. D'autres documents proviennent d'ouvrages de référence des théories des relations internationales ou de la science politique en général.

Dans notre réflexion sur le cyberespace nous nous sommes également inspirés d'autres technologies civiles et militaires récentes telles que les drones employés par différentes armées. Cette comparaison, notamment grâce à l'excellent ouvrage de Chamayou, *Théorie du drone*, a permis de mieux cerner certaines évolutions importantes dans la façon d'analyser les relations internationales et les conflits entre acteurs du système international.

La diversité des sources sur lesquelles nous nous appuyons permet d'avoir un aperçu assez général des enjeux liés au cyberespace, et ce malgré la relative nouveauté de cet objet de recherche.

3.2 La « crise d'intelligibilité » liée au cyberespace

Tout comme les drones, le cyberespace crée des **« crises d'intelligibilité »** (Chamayou 2013, 26) dans les théories des relations internationales et les théories de

la guerre. Il est donc difficile de l'aborder avec un cadre d'analyse précédant son existence.

La première difficulté que nous avons rencontrée a été de trouver un cadre d'analyse qui puisse convenir à l'objet de nos recherches. Les enjeux entourant les activités militaires et civiles dans le cyberespace n'ont en effet pour le moment fait l'objet que de trop peu d'écrits scientifiques. De plus, les quelques analyses académiques se limitent souvent à des ouvrages relativement descriptifs, sans être analytiques ou présenter un cadre d'analyse clair. En ce sens, nous avons essayé de puiser dans différents cadres d'analyses existants afin de réussir à bien analyser nos problématiques de recherche. De prime abord, il est important de mentionner que ces « emprunts » dans les différents cadres d'analyse ne sont pas mutuellement exclusifs entre eux. Ainsi, si l'on peut considérer, par exemple, que le cadre d'analyse réaliste n'est pas particulièrement adapté aux paramètres du cyberespace, nous ne l'avons pas pour autant rejeté de manière catégorique puisque certains éléments sont tout de même pertinents. Il en va de même pour les autres cadres d'analyse abordés dans nos recherches.

De façon générale, et bien que notre cadre d'analyse s'appuie sur différentes théories, nous avons fait le choix de nous orienter généralement vers les études critiques de la sécurité (« critical security studies »), avec de clairs emprunts au constructivisme et aux néoréalistes (notamment sur la projection de la force). Les analyses critiques de la sécurité se distinguent notamment des analyses plus classiques parce qu'elles n'ont pas nécessairement pour seul objet l'État comme acteur prépondérant (Macleod 2004). Le cyberespace étant caractérisé par son caractère poreux entre domaines civil et militaire, les analyses critiques de la sécurité permettent d'élargir le spectre des objets d'étude.

Par ailleurs, concernant la projection de la force dans le cyberespace, nous avons

préféré nous orienter vers les cadres d'analyses néoréalistes, mais surtout constructivistes. En effet, même si la force militaire classique des États reste importante dans le système international, le cyberespace se caractérise notamment par la facilité d'accès (en termes physiques et financiers) aux moyens d'attaque, de riposte et de dissuasion. Il en résulte alors qu'il devient difficile de classer la force des pays uniquement en fonction de leur force militaire classique (comme le feraient les réalistes) tant celle-ci ne se trouve pas nécessairement projetée dans le cyberespace. Nous retiendrons plutôt des critères tels que la capacité à mobiliser du capital humain ou à innover et contrôler les technologies de l'information et des télécommunications.

Une autre des raisons de s'orienter vers différents cadres d'analyses est la difficulté pour les analyses classiques de prendre en compte le caractère transnational et presque illimité du cyberespace. Ces nouvelles frontières majoritairement dématérialisées forcent donc à explorer différents cadres d'analyse afin de clarifier la question de la souveraineté, mais aussi de la territorialité du cyberespace dans les relations internationales.

3.3 Cadre d'analyse utilisé

Pour mener notre recherche nous avons donc choisi de nous inspirer largement du constructivisme et des analyses critiques de la sécurité. Partant du postulat que toute réalité est socialement construite (Macleod et O'Meara 2007, 184), les constructivistes tentent de comprendre les acteurs du système international et la façon dont ils agissent en fonction de leurs structures idéationnelles, de leurs perceptions et de leurs structures identitaires. Ainsi, le seul discours conditionne-t-il parfois un grand nombre des actions des acteurs en présence, en cela qu'il crée une réalité énoncée et qu'un ensemble de conséquences pourraient advenir s'il devait être suivi

d'actes concrets.

Cette analyse trouve un écho particulier dans le cyberespace où les capacités propres à chaque État et acteur sont difficilement mesurables et font l'objet de beaucoup de spéculations. Ces objets sont généralement évalués en fonction d'analyses intersubjectives des capacités des autres acteurs se basant autant sur les renseignements militaires que sur le discours de puissance des différents acteurs. La puissance est donc un phénomène soumis à interprétation et est relative à l'identité perçue et projetée des différents acteurs. Il en va de même pour la construction sociale des armes et de leur utilisation, qui relève bien plus de l'idée que l'acteur s'en fait que de la nature réelle de l'arme.

Dans ce cadre, analyser les dynamiques entre acteurs est plus complexe. En effet, les difficultés d'attribution des attaques ou menaces, elles-mêmes basées sur les perceptions des différents acteurs, deviennent importantes puisqu'elles peuvent mener à des crises entre acteurs en cas d'attaque massive attribuée de façon erronée (le mauvais acteur est visé par les accusations ou les représailles de la victime ou de ses alliés). L'aspect furtif des opérations dans le cyberespace représente également un autre problème à la recherche puisque l'évaluation de la force se fait majoritairement sur des réalités empiriques. En l'absence de traces ou de preuves d'opérations dans cet espace, il est plus difficile de déterminer la capacité d'un acteur à projeter de la force ou de l'influence.

Par ailleurs, le constructivisme nous permet de prendre une distance critique quant aux concepts généraux de système international et des relations internationales (Battistella 2003). Si ces concepts sont acceptés de façon assez large, ils restent toutefois des constructions sociales venant de discours d'acteurs et d'universitaires dominants. Dans le cadre de notre analyse, nous n'aurons d'autre choix que de réutiliser en partie ces construits sociaux puisqu'ils permettent une compréhension

générale des faits que nous articulons. Il reste toutefois que nous prendrons nos distances par rapport à ces concepts dans certains cas, afin de mettre en lumière des dynamiques *invisibilisées* par les discours dominants dans les champs d'études des relations internationales. Par exemple, selon nous, il n'existe pas qu'un seul système international, mais bien une multiplicité de systèmes s'enchevêtrant et entrant en collision. Ainsi, quand nous utiliserons l'expression « système international », nous entendrons avant toute chose la structure systémique dans laquelle différents acteurs rentrent en conflit ou en dialogue à l'échelle internationale. Ce système est lui-même un mélange de différents systèmes existant simultanément. Il existe par exemple des systèmes internationaux locaux comme les alliances des pays arabes ou encore les organisations de coopérations régionales comme l'Organisation du traité de sécurité collective (OTSC) qui agissent dans des zones d'influence précises.

De plus, étant une construction sociale comme une autre, le système international tel que nous venons de le présenter est relativement instable. Dans le cadre où ce sont les acteurs qui définissent le système et participent à sa construction idéologique et intellectuelle, la stabilité n'est liée qu'à la bonne volonté de ces acteurs et à leurs actions. Il n'existe donc pas selon nous une permanence du système international, qui permettrait de valider les résultats ou les hypothèses de notre recherche de façon définitive ou figée dans le temps et l'espace. Nous sommes donc dans une démarche d'exploration des questions de recherche afin de valider à un instant précis si nos hypothèses sont exactes ou non.

Un autre cadre d'analyse fournissant de nombreux outils pour étudier les relations internationales et la question du cyberespace est l'ensemble du champ des études critiques de la sécurité. Ces études sont grandement influencées par le constructivisme au niveau méthodologique et conceptuel. Toutefois, comme leur nom l'indique elles s'attardent plus sur la question de la sécurité et ses différentes formes dans les relations internationales. En tant qu'études critiques, elles visent à remettre

en question une partie des paradigmes classiques afin d'aborder de nouvelles dimensions et d'étudier de nouvelles questions (voir par exemple Krause et Williams 1997; Vaughan-Williams 2010).

En effet, la sécurité n'est pas qu'une affaire militaire : elle peut aussi être politique, économique, environnementale et sociétale. Il s'agit de prendre en compte d'autres facteurs et éléments entrant dans l'équation de la sécurité, et de remettre en question la seule place de l'État dans ces conceptions et théories (Buzan, Wæver et Wilde 1998, 1). C'est ce que les chercheurs en études critiques de la sécurité qualifient de sécurité « élargie » (*widen*) par rapport à la sécurité plus « étroite » (*narrow*) des analyses plus classiques. Les études critiques de la sécurité proposent ainsi un certain nombre d'outils analytiques profilant la sécurité comme objet multiforme et recoupant différents objets d'analyse sur différents niveaux d'analyse (système international, sous-systèmes, unités et sous-unités et individus), secteurs d'analyse (économie, militaire, sociétal, environnemental, etc.) ainsi que régions d'analyse. D'autres concepts comme la sécurisation ou encore les différents types de sécurité (objective ou intersubjective) sont pertinents dans notre étude puisqu'ils peuvent permettre de donner une orientation particulière à notre recherche et pourraient mettre en lumière certaines tendances dans le cadre du cyberespace.

Un des concepts clés des études critiques de la sécurité est la « sécurisation » (Wæver 2011). La sécurisation est un processus politique généré par le discours des différents acteurs du système international, visant le plus souvent à énoncer la présence d'une menace ou d'un enjeu de sécurité pesant sur un domaine ou un objet en particulier. La sécurisation cherche notamment à rendre légitime toute riposte à la menace dans le cadre du système international. Elle peut également avoir un rôle dissuasif en nommant une menace et en annonçant les représailles potentielles.

Dans le système international (et national), toute problématique peut être non-

politique (l'État ne s'en mêle pas et n'intervient pas), politique (l'État prend part à la problématique et éventuellement régule ou intervient) ou objet de sécurisation (situation dans laquelle existe une menace existentielle qui demande des mesures urgentes et qui justifie l'action étatique en dehors des normes établies).

> Security is the move that makes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics. Securization can thus be seen as a more extreme version of politicization (Buzan, Wæver et Wilde 1998, 23).

Afin de déterminer dans quelle catégorie se situe la problématique visée, il faut s'arrêter à la perception de la sécurité par les États (et d'autres acteurs, le cas échéant) et les systèmes de valeurs qui leur sont propres. Ainsi, la sécurisation vise à établir l'existence d'une menace existentielle (et d'un discours qui s'articule autour de cette menace) contre un objet à sécuriser; à établir la réponse urgente et extraordinaire à y apporter; puis enfin à déterminer l'effet sur les autres acteurs du système en fonction de la violation des règles normales. Dans le cadre du cyberespace, la sécurisation est un concept qui mérite d'être utilisé puisque comme nous l'avons mentionné, les perceptions des projections de force sont extrêmement subjectives. La création d'un objet de sécurisation revêt alors un caractère encore plus politique et lié au champ des relations internationales entre acteurs.

Dans le cyberespace, l'« objet référent » (l'objet visé par une menace existentielle et qui aurait un droit légitime à la survie) est parfois plus difficile à définir puisque les différents réseaux et infrastructures sont très dépendants les uns des autres. Par ailleurs, les « acteurs sécurisateurs », qui sont les acteurs qui sécurisent des objets en déclarant qu'ils sont menacés, sont encore moins clairs que dans le reste des autres domaines : il n'existe pas d'institution internationale forte régulant les relations dans le cyberespace, et les États sont hésitants à intervenir de façon marquée dans toute une partie du cyberespace gérée par des entreprises privées. Enfin les « acteurs

fonctionnels » : des acteurs qui auront une influence importante dans le processus de sécurisation, sans pour autant être l'acteur sécurisateur ou l'objet à sécuriser, sont également plus difficiles à identifier dans le cyberespace puisque de nombreux acteurs non étatiques sont présents et qu'il n'existe pas de réelle institution visant à réguler les rapports dans le cyberespace.

La sécurisation dans le cyberespace se fait avant tout grâce au « *speech act* », soit le fait de procéder par le langage à la construction d'un objet de sécurisation (Buzan, Wæver et Wilde 1998, 26). Le *speech act* est d'autant plus important qu'il conditionne de façon très forte la réaction des acteurs fonctionnels dans le cyberespace. En effet, en l'absence d'une capacité d'attribution fiable pour les attaques ou les menaces entre acteurs, le *speech act* prend une grande place dans le processus de légitimation d'une action par un acteur sécurisateur contre un éventuel ennemi qu'il suspecte être la source d'attaques ou de menaces. Cette construction de la menace pourrait avoir un aspect fondamental en cas de riposte : afin de pouvoir légitimement riposter, il faudra que l'acteur sécurisateur prouve au reste de la communauté que l'objet visé par la sécurisation était sous le coup d'une menace existentielle. Cette démonstration se fera avant tout par la mise en place d'un *speech act* et d'une mise en exergue de concepts philosophiques susceptibles de frapper l'imaginaire, puisque le cyberespace est avant tout dématérialisé et rend donc difficile la présentation d'une menace comme un objet concret dans la sphère matérielle des États et autres acteurs.

Par ailleurs, la sécurité étant une construction subjective des acteurs, il importe de mentionner qu'elle peut prendre différentes formes et différents niveaux d'analyse. Par exemple, dans certains cas on admet que certains objets sont *de facto* des objets de sécurisation (sécurité nationale, défense nationale, lutte contre le terrorisme, etc.) alors que dans d'autres cas c'est carrément le politique qui peut devenir objet de sécurisation (dans des régimes plus autoritaires ou militaires). Ces distinctions et

discours sont pratiquement absents dans le cyberespace dans la majorité des États occidentaux, Il en résulte que de nombreux aspects capitaux dans les stratégies de défense et de sécurité des États sont vulnérables (comme les infrastructures essentielles)

Il faut toutefois noter que, comme le décrit Ally Butler dans son essai *Security and the « Smokeless war », A critical look at « security as Speech Act » Theory via Internet security in China* (Butler 2010), les études critiques de la sécurité ne sont pas exemptes de problèmes et de contestations quand vient le temps de les appliquer à Internet et au cyberespace en général. Si Internet lui-même peut devenir un objet de sécurisation, il reste que de nouvelles problématiques sont à prendre en compte dans l'analyse du cyberespace. Notamment, la multitude des acteurs en présence dans le cyberespace rend difficile la dénomination des acteurs fonctionnels et plus généralement la communauté appelée à justifier ou non l'objet de la sécurisation (Butler 2010, 115 - 117).

Par ailleurs, avec l'arrivée des plateformes de partage et de communication massive, les acteurs pouvant donner leur avis se sont multipliés et la construction de la prise de parole devient plus complexe tant de nombreuses influences nouvelles peuvent se faire sentir et prendre part aux débats face aux États (ce que l'auteure appelle « the voices of bandwith », « les voix de la bande passante »).

Ainsi, si de nombreux domaines peuvent être concernés par l'arrivée d'Internet et la massification du cyberespace, il devient plus difficile de discerner efficacement qui intervient dans les processus de sécurisation et comment cela se produit. Ces critiques sont donc à prendre en compte dans un espace où la prise de parole est facilitée, en dehors notamment des espaces publics classiques.

3.4 Conclusion sur le cadre d'analyse

Afin de conclure sur le cadre d'analyse, il nous semble évident que la question de l'élaboration d'un cadre d'analyse formel pour traiter du cyberespace est un exercice périlleux tant de nombreuses sphères de l'activité humaine entrent en jeu (et pas seulement militaires). Par la complexité des enjeux à aborder, nous ne nous rangerons donc derrière aucun cadre d'analyse limitatif et formel.

Notre cadre d'analyse s'appuiera donc avant tout sur des analyses critiques, méthodologiquement et intellectuellement plus proches des constructivistes, tout en se basant en grande majorité sur des documents officiels et sur des faits observables. Les différents emprunts, notamment aux néoréalistes, nous permettent de compléter un cadre d'analyse plus adapté aux questions du cyberespace puisqu'il s'agit d'une sphère nouvelle de la science politique et qui mérite d'être abordée comme telle.

CHAPITRE II

STRUCTURE DU CYBERESPACE

Afin de bien comprendre quel est notre objet d'étude, il importe de définir ce que l'on entend par cyberespace. Nous aborderons dans ce chapitre un ensemble de questions permettant de dresser un portrait de cet espace et de son importance dans les activités humaines.

1. Le cyberespace et ses principales caractéristiques

L'origine du Cyberespace se retrouve dans des activités militaires. Le projet *Darpanet*, ancêtre de l'Internet, est par exemple une source importante pour comprendre l'émergence du cyberespace. Toutefois, il s'agit maintenant d'un espace majoritairement investi par les civils et dans lequel se déroule un ensemble d'activités commerciales et privées. Il y a donc eu un croisement entre les différentes vocations du cyberespace où se sont jointes activités militaires et civiles. En peu de temps, le cyberespace a acquis une place stratégique dans la majorité des activités humaines.

Comme nous le verrons au fil du présent chapitre, une des principales caractéristiques du cyberespace est qu'il s'agit d'un *espace* d'échanges et d'affrontements entre acteurs. De nombreuses activités par une multitude d'acteurs tant civils que militaires, s'y déroulent : commerce électronique, information, échanges entre personnes, etc. En son sein, les acteurs peuvent utiliser différents *outils* basés sur les différentes *technologies* qui constituent la base opérationnelle de cet espace, majoritairement dématérialisé. Parmi ces différents outils, l'Internet est le plus connu. Il ne faut

toutefois pas confondre Internet et cyberespace, puisque ce dernier englobe un nombre bien plus important de dispositifs et de technologies.

Dans le cyberespace, les infrastructures et technologies employées étant majoritairement les mêmes quel que soit le secteur d'activité, il s'en suit une difficulté de différenciation entre ces types d'activités. Cette interdépendance des réseaux amène donc elle-même un ensemble de problématiques que nous étudierons.

1.1 Un espace nouveau et omniprésent des activités humaines, basé sur la technologie

Le cyberespace est un produit des sociétés modernes, basé sur un ensemble de technologies relativement nouvelles. Il s'agit d'un espace encore jeune, marqué par une forte temporalité, qui ne ressemble à rien de connu dans l'histoire de l'humanité. Cette temporalité est importante puisqu'elle permet de comprendre pourquoi tant de questions restent inexplorées dans notre champ d'intérêt.

L'apparition du cyberespace est intimement liée à l'avènement et à la généralisation des nouvelles technologies de l'information et des communications. Depuis la fin des années 1980, un nouvel espace physique dématérialisé (électromagnétique) et social s'est créé et a transformé l'activité humaine dans presque toutes ses sphères. Le cyberespace, et Internet en particulier, n'en est que la dernière occurrence, la plus développée et la plus tentaculaire, mais elle aussi amenée à évoluer dans le futur (certains en appellent d'ailleurs déjà à son remplacement par des nouvelles technologies, McMillan 2014b).

Le cyberespace et les technologies de l'information sur lesquelles il se base sont maintenant partout dans nos vies quotidiennes. La « révolution » numérique à

laquelle le monde a fait face dans les trente dernières années s'accélère et ne laisse que peu de sphères d'activité intouchées. Qu'il s'agisse de l'utilisation des ordinateurs ou des cellulaires, ou encore des compteurs d'électricité 'intelligents' ou bien des réseaux d'approvisionnement en eau potable, de nombreux dispositifs sont raccordés dans le cyberespace. Seules quelques sphères d'activité humaine ne sont pas encore totalement connectées, du fait de leur importance ou d'un manque d'investissement dans ces activités, telles que les communications pour les services d'urgence (ondes radio), ou les feux de circulation (systèmes mécaniques avec minuteur), par exemple.

La pénétration des technologies liées au cyberespace dans nos vies est telle qu'il est difficile de les ignorer. Cette hyper-présence peut être problématique à certains égards. Il ne s'agit pas ici de faire une critique de la technologie ou de la place que nous lui accordons dans nos vies, puisque ces avancées se sont trouvées être d'excellents moteurs de développement économique et social, permettant un meilleur accès à l'information, une plus grande liberté d'expression et d'échange, etc. Il faut toutefois se souvenir que cet espace omniprésent est également un terrain d'affrontement et d'opportunités pour des acteurs mal intentionnés. En effet, les vulnérabilités qui apparaissent avec l'utilisation de ces technologies augmentant beaucoup plus vite que leur nombre d'utilisations, cette situation pourrait créer un ensemble de problématiques nouvelles.

Afin de bien comprendre en quoi le cyberespace est important pour un large spectre des activités humaines, nous nous attarderons ici à différentes définitions et analyses. Nous aborderons tant les questions civiles que militaires, puisqu'elles sont souvent interconnectées et présentées ensembles dans les différentes doctrines et publications gouvernementales.

Dans sa Stratégie de cybersécurité, le Canada définit le cyberespace comme étant un

espace touchant l'ensemble des activités humaines. De façon concrète, il s'agit du :

> monde électronique créé par des réseaux interconnectés formés de systèmes de technologie de l'information et de l'information qui se trouve sur ces réseaux. Le cyberespace est un bien commun reliant plus de 1,7 milliard de personnes qui échangent des idées et des services et qui tissent des liens d'amitié (Gouvernement du Canada [Sécurité publique Canada] 2010, 2).

Si cette définition est un peu limitée par son aspect assez vague, il est intéressant de constater que pour le Canada, un acteur qui était historiquement assez pacifique et peu orienté vers le militarisme, le cyberespace semble avant tout un espace d'échanges et de contacts, avant d'être un espace militaire. Cela n'empêche toutefois pas le gouvernement du Canada de se doter de moyens importants afin de surveiller les activités de ses citoyens dans le cyberespace (sur la surveillance généralisée du Centre de la sécurité des télécommunications, on pourra aller consulter le reportage du magasine Vice par Braga 2015; ou encore l'article de Ryan Gallagher et Glenn Greenwald du site The Intercept : Gallagher et Greenwald 2015).

De même, pour les auteurs du rapport *Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use* (United States Government Accountability Office 2011), si le cyberespace se définit de façon assez proche de celle du gouvernement du Canada, il comporte toutefois une dimension industrielle fondamentale, ainsi qu'une importance liée aux infrastructures critiques et à leur prise en compte dans l'étude de la cybersécurité (dimension face à laquelle l'inaction du gouvernement a été vertement critiquée par le Vérificateur général du Canada en 2012, Office of the Auditor General of Canada 2012). Cette définition est notamment celle avancée de façon classique par les militaires de la *US Air Force* (United States Air Force 2011; United States Government Accountability Office 2011, 53) :

Dans la même veine, la stratégie du Royaume-Uni (*The UK Cyber Security Strategy,*

Protecting and promoting the UK in a digital world) définit quant à elle le cyberespace comme un espace propice au commerce et à la croissance économique. On y verrait donc plus un intérêt commercial, propre à l'histoire impériale et capitaliste du Royaume-Uni qu'un avantage stratégique militaire. Ainsi, et bien que le Royaume-Uni se soit illustré récemment pour ses pratiques intrusives pour la liberté de la presse (Ball 2015) et la vie privée (MacAskill et al. 2013) – allant même jusqu'à surveiller des avocats (Bowcott 2014) ou des organisations non gouvernementales comme Amnistie internationale (McLaughlin 2015) - le cyberespace serait un important espace pour le développement et la création de richesses (Cabinet Office, United-Kingdom Government 2011). Il serait donc nécessaire de le rendre sécuritaire et propice à un commerce plus paisible. L'Internet et les technologies de l'information, au cœur du cyberespace, auraient également permis des améliorations des procédés de gestion et de production pour l'industrie, mais aussi pour les services rendus aux citoyens par les gouvernements (Cabinet Office, United-Kingdom Government 2011, 12). Paradoxalement, bien que le Royaume-Uni espionne de façon assez importante ses propres citoyens et le reste du monde, pour ce gouvernement le cyberespace serait également un élément de renforcement des libertés en tant qu'il permet l'échange libre et la diffusion du savoir (Cabinet Office, United-Kingdom Government 2011, 12).

Également intéressée par l'importance du cyberespace, l'Organisation de coopération et de développement économique (OCDE) estime que certaines composantes du cyberespace, dont l'Internet, sont d'une importance vitale pour le développement économique et les relations entre acteurs du système international. Dès 2008, dans la *Déclaration de Séoul sur le futur de l'économie Internet*, les pays signataires sont allés jusqu'à élever Internet et les technologies présentes dans le cyberespace au niveau d'un élément omniprésent sur lequel reposent un grand nombre d'activités humaines et économiques (Organisation for Economic Co-operation and

Development 2008, 4- 5).

Ainsi, pour l'OCDE, Internet est un espace d'échanges économiques vital, et non plus seulement une seule plateforme technologique permettant l'échange d'information entre militaires ou réseaux scientifiques :

> The Internet began as a way of linking different computers over the phone network, but it now connects billions of users worldwide from wherever they happen to be via portable or fixed devices. People with no access to water, electricity or other services may have access to the Internet from their mobile phone. The Internet is a multi-billion dollar industry in its own right, but it is also a vital infrastructure for much of the world's economy (Organisation for Economic Co-operation and Development 2012).

Selon l'OCDE, Internet serait également un moteur de développement économique et social pour des pays émergents ou des populations marginalisées. Dans son rapport d'étape sur la Déclaration de Séoul (Organisation for Economic Co-operation and Development 2013), l'organisation note que certains pays émergents et certains secteurs commerciaux ou d'activités ont su utiliser les technologies présentes dans le cyberespace afin de se développer ou de briser l'isolement (Organisation for Economic Co-operation and Development 2013, 176).

Pareillement, une présentation d'un rapport prochainement publié (fin 2015) par la Banque mondiale (Deichmann et Mishra 2014) laisse entendre qu'Internet et le cyberespace en général sont d'une grande importance dans un contexte où les marchés des économies occidentales sont de plus en plus saturés, par exemple en ouvrant de nouvelles opportunités commerciales, notamment dans les pays émergents. Il y aurait donc des avantages partagés selon la Banque mondiale à ce que ces pays entrent dans le cyberespace et participent au 'libre marché'. D'une part, cela favoriserait le développement économique et social, d'autre part les puissances économiques pourraient profiter de ces nouveaux marchés pour se maintenir et continuer leur expansion.

En plus d'être un espace d'échange d'idées, le cyberespace aurait donc une fonction économique et industrielle, qui dans un monde connecté et 'globalisé' aurait une importance fondamentale pour les acteurs économiques et politiques. Du fait de cette place centrale au capitalisme, le cyberespace est également devenu un espace où de nouvelles formes de pouvoir sont apparues et sont utilisées. Avec l'émergence d'une importance économique, s'est aussi développée une importance diplomatique et politique au niveau des différents sous-systèmes internationaux composant le grand système international (tel qu'on le conçoit de façon classique).

Jean-Marie Bockel, sénateur français et rapporteur pour la Commission des affaires étrangères, de la défense et des forces armées du Sénat (France) considère que le cyberespace a un volet fondamentalement militaire et stratégique. Dans son rapport *La cyberdéfense : un enjeu mondial, une priorité nationale*, M. Bockel affirme ainsi :

> le cyberespace constitue un nouveau milieu, qui se superpose aux milieux traditionnels (terre, mer, air), à l'espace et au nucléaire, ce qui n'implique pas pour autant qu'il domine les autres ou que la 'cyberguerre' constitue à elle seule un milieu autonome de la guerre (Bockel 2012, 36).

Pour M. Bockel, le cyberespace est notamment caractérisé par une absence de gouvernance globale et un système particulièrement anarchique (Bockel 2012, 5), l'OTAN et les organisations transnationales comme l'Union européenne ou l'ONU n'ayant codifié qu'un nombre relativement limité de règles ou conventions, plus ou moins respectées selon les intérêts particuliers des différentes parties prenantes dans le cyberespace.

Cette vision stratégique du cyberespace comme nouvel espace est également partagée par un des acteurs principaux pour notre étude, l'Armée populaire de libération

(APL), en Chine. Dans leur rapport '*Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*' (Krekel, Adams et Bakos 2012), présenté à la '*U.S.-China Economic and Security Review Commission*', Krekel, Adams et Bakos affirment que la Chine a identifié le cyberespace comme étant semblable aux autres sphères de la guerre (Krekel, Adams et Bakos 2012, 14). On voit donc ici une certaine continuité dans la prise en compte du cyberespace comme une des sphères stratégiques de la diplomatie et de la guerre.

Les différentes façons d'appréhender et de définir le cyberespace sont intimement liées aux intérêts stratégiques et aux priorités des acteurs du système international. Autant les Français et les Chinois semblent y voir une importance stratégique et militaire, autant les pays anglo-saxons semblent être dans une lignée protestante (voir Max Weber, *L'éthique protestante et l'esprit du capitalisme*), valorisant l'apport du cyberespace au travail et au marché en général. Malgré tout, même un pays comme le Royaume-Uni, qui définit le cyberespace comme étant un champ de liberté, a décidé de créer des unités spécialisées de l'armée afin d'intervenir sur Facebook et d'autres médias électroniques (« British army creates team of Facebook warriors », MacAskill 2015).

Cette synergie est d'ailleurs visible dans les visions étatiques du cyberespace présentées dans les différentes politiques et livres blancs. En effet, si différentes politiques publiques (France, États-Unis, Chine) soulignent l'aspect stratégique du cyberespace comme espace diplomatique et politique, d'autres mettent davantage en avant les échanges entre acteurs privés ou encore l'importance économique du cyberespace (comme celles du Royaume-Uni ou du Canada). Dans une analyse constructiviste, on peut donc constater que l'importance donnée au cyberespace et les activités qui y sont encouragées varient donc selon le discours et les intérêts des différents acteurs en présence. Cela peut avoir un impact important dans les relations internationales dans la mesure où l'objet de sécurisation peut varier selon les acteurs,

tout un ayant un impact important sur toutes les autres activités se déroulant, ou non, dans le cyberespace. Par exemple, si le Royaume-Uni considère que le secteur économique présent sur Internet doit être un objet de sécurisation, toute attaque contre cette sphère d'activité pourrait être sujette à riposte et avoir des conséquences tant sur d'autres activités dans le cyberespace qu'à l'extérieur de cet espace. La construction de la menace et les actions posées dans le système international pourraient donc changer selon l'importance que donnent les acteurs aux différentes activités dans le cyberespace.

Les chercheurs de la *National Defense University* avancent quant à eux que le cyberespace est caractérisé avant tout par ses aspects techniques :

> [cyberspace is] an operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and Internetted information systems and their associated infrastructures (Kramer, Starr et Wentz 2009, 4).

Dans son ouvrage concernant la cyberguerre *Cyber war: the next threat to national security and what to do about it* (Clarke et Knake 2010), Clarke souligne que n'importe quel ordinateur peut faire partie du cyberespace, n'importe quel immeuble qui semble sans intérêt peut héberger des infrastructures stratégiques, n'importe quel câble sous terre peut avoir une importance cruciale, le cyberespace étant partout où il peut y avoir de l'électronique et un contact avec l'extérieur (Clarke et Knake 2010, 70). De cette conception technique, il résulte que le cyberespace est un espace relativement malléable, contrairement à la terre ou à la mer ou encore l'air et l'espace (Kramer, Starr et Wentz 2009, 256).

Des attaques les plus complexes aux plus simples, visant tout autant des infrastructures civiles (pour affaiblir les États), que les réseaux militaires (pour paralyser les troupes dépendantes d'informations relayées par des réseaux

électroniques), les stratégies sont donc multiples. Le cyberespace serait en fait « un champ de bataille où les serveurs informatiques tiennent lieu de places fortes et où les routes et les ponts sont remplacés par des maillages de fibre optique ou de liaisons haut débit » (Arpagian 2009a, 26). Dans le cyberespace « tous les supports concernés ne sont plus seulement les ordinateurs, mais bien tous les appareils dotés de fonctionnalités de communication » (Arpagian 2009a, 66). On pensera ici notamment à tous les appareils '*intelligents*', aux systèmes de contrôle et d'acquisition de données dans tous types de dispositifs, aux serveurs de télécommunications, etc. L'ensemble du spectre électronique est potentiellement relié au cyberespace d'une façon ou d'une autre, même les appareils non reliés à l'Internet pouvant être la cible d'attaques (voir *N.S.A. Devises Radio Pathway Into Computers,* Sanger et Shanker 2014). Des chercheurs ont par exemple créé un dispositif de la taille d'un pain pita, pouvant capter et décoder les ondes émises par les processeurs d'ordinateur et ainsi extraire des données sans y être connecté physiquement (Greenberg 2015b).

Cette pénétration du cyberespace dans les autres espaces d'activités humaines est importante puisqu'il se crée une certaine interdépendance entre les dimensions matérielles et dématérialisées des activités humaines. Toute vulnérabilité dans le cyberespace peut alors avoir un impact direct sur le cours des activités qui en dépendent.

1.2 Un espace poreux

Puisque les technologies de base utilisées dans le cyberespace sont généralement les mêmes, quelles que soient les applications et les acteurs, cet espace est très poreux. Les connexions entre serveurs et systèmes informatiques, par exemple, se font essentiellement par le biais des mêmes réseaux et par les mêmes routes, quel que soit le trafic qui les emprunte. Contrairement à d'autres espaces où la configuration

physique des lieux ou les types d'activités permettent un certain cloisonnement (il est par exemple assez rare de croiser des véhicules de l'armée dans la rue, ou encore de mettre les pieds dans une bourse mondiale, et que dire d'un parlement), le cyberespace tend à rassembler toutes les activités humaines sur des réseaux interreliés.

Sur les réseaux se retrouvent donc autant les requêtes de navigation des internautes que les informations relevant de systèmes de contrôle et d'acquisitions de données (SCADA) permettant la surveillance à distance de systèmes informatiques aussi variés que les compteurs d'électricité, les systèmes liés au réseau électrique, les réseaux d'approvisionnement en eau, les canalisations de gaz ou de pétrole, ainsi qu'un ensemble d'autres données liées à des infrastructures industrielles; ou encore une partie du trafic militaire et étatique. Une commande de contrôle d'un drone dans une zone de guerre transitant dans le cyberespace peut donc se retrouver au milieu d'un ensemble de données liées au commerce en ligne, par exemple. Ou encore, les données de contrôle d'une centrale électrique pourraient être sur le même réseau et passer par les mêmes routeurs et fibres optiques que l'appel que vous passez sur un logiciel de discussion vidéo. Cette interconnexion de nombreuses activités est une nouveauté importante par rapport aux autres sphères de la guerre ou des relations internationales.

La grande diversité d'utilisation de ces technologies est une richesse et une grande vulnérabilité dans la mesure où une attaque massive ne ferait que peu de différence entre les multiples activités, du fait même de leur '*backbone*' commun. Nous pouvons ainsi affirmer que le cyberespace est un ensemble poreux : toutes les activités qui s'y déroulent emploient les mêmes technologies, et peuvent avoir des impacts les unes sur les autres en cas de perturbation ou de problème logiciel ou physique.

Il en ressort que, contrairement aux conflits classiques, les attaques dans le

cyberespace ont un potentiel de confusion et de discorde à propos notamment des ripostes à y apporter. Ainsi, le flou entre les sphères d'activité et leur interdépendance crée de nouvelles problématiques dans les relations internationales. Comme le souligne Arpagian, « que vous soyez puissant ou misérable, la porosité informatique ne connait pas les barrières sociales... » (Arpagian 2009b, 73) et est donc susceptible de faire que toutes les sphères d'activité présentes dans le cyberespace soient touchées par une attaque ou une perturbation du réseau.

Un des autres problèmes importants induit par l'interdépendance des activités dans le cyberespace est la difficulté de distinguer combattants et non-combattants dans un cadre de conflit. Cette distinction fondamentale dans les conflits armés, notamment adoptée dans différents traités internationaux (dont les protocoles additionnels de la Convention de Genève, voir : International Committee of the Red Cross (ICRC)) est presque inexistante dans le cyberespace. L'utilisation de moyens offensifs génère un ensemble de problèmes de droit international, de classification des conflits et de légitimité des ripostes à apporter dans ces cas. Si Chamayou voyait une zone d'ombre dans l'utilisation du drone comme arme supprimant le conflit (Chamayou 2013, 204), les moyens d'attaques dans le cyberespace poussent probablement à leur paroxysme ces problèmes conceptuels et juridiques.

Dans ce cadre, la construction de la menace et des objets de sécurisation sera alors plus importante qu'avant. Il sera en effet difficile pour des acteurs sécurisateurs de valider ou non la menace et les secteurs d'activité touchés par une attaque. De plus, considérant les importantes difficultés d'attribution des attaques dans le cyberespace, il est clair que la construction de l'identité de la menace prendra un poids encore plus considérable que dans d'autres types de conflit. Avec l'incapacité de définir clairement qui est à la source d'une attaque, les discours des différents acteurs du système international risquent de prendre une place encore plus grande pour légitimer les actes de riposte ou de représailles.

La porosité et l'interdépendance des réseaux dans le cyberespace créent « une dimension supplémentaire qui doit être prise en compte pour envisager la sécurité nationale », (Arpagian 2009a, 78) mais aussi celle d'autres acteurs comme les entreprises privées ou les organisations internationales, ou encore tout bonnement celle des civils. Cette préoccupation de certains acteurs concernant la sécurité ne se retrouve étrangement que rarement dans les politiques publiques dédiées par exemple aux infrastructures essentielles, le secteur privé étant trop peu soumis à des régulations assurant la sécurité de ses activités (sur ce sujet, voir notamment Quiggin, Queen's University (Kingston et Centre for International and Defence Policy 2012).

1.3 Un espace facile d'accès

> L'un des principes classiques de la guérilla est de se fournir en armes dans le camp d'en face. Cette règle vaut également aujourd'hui pour la composante électromagnétique de l'arsenal. (Chamayou 2013, 113)

Une caractéristique importante des technologies employées dans le cyberespace est qu'elles sont majoritairement faciles d'accès. Ces technologies sont généralement disponibles pour le grand public et ont une base documentaire assez importante, permettant à quiconque intéressé d'en apprendre sur leur fonctionnement. Une personne bien formée peut donc rapidement devenir spécialiste dans le domaine. Les coûts d'entrée et d'acquisition du matériel sont également très bas.

Par ailleurs, un des outils le plus important du cyberespace, Internet, n'a pas été créé pour être sécuritaire. Tant les logiciels gérant les données échangées que les protocoles de base permettant son existence sont des technologies assez anciennes sur l'échelle des technologies de l'information et des télécommunications (White 2007) et n'ont pas été développées pour l'utilisation massive que nous en faisons

actuellement (certains allant jusqu'à affirmer que l'infrastructure d'Internet doit être complètement repensée. voir McMillan 2014c). Malgré l'évolution des logiciels et dispositifs de communication utilisés dans un certain nombre d'activités, la base technologique permettant l'échange des données sur le réseau est restée presque la même depuis près de quarante ans (permettant même l'interception directe par des tiers des données transitant par les différents réseaux, van Beijnum 2010).
Par ailleurs, il est également relativement peu onéreux d'opérer dans le cyberespace. Pour Arpagian, il s'agit d'« une arme largement accessible aux plus démunis » (Arpagian 2009b, 69). En effet, « la constitution de telles armadas numériques est une activité fort peu couteuse puisqu'il suffira de débourser quelques centaines d'euros pour une attaque en déni de service un peu conséquente et au maximum quelques milliers pour l'envoi d'un virus considéré comme dérangeant pour ces destinataires » (Arpagian 2009b, 69). Ou encore : « un rapport de l'OCDE (Organisation for Economic Co-operation and Development 2009) [...] estimait que la mise à disposition d'un de ces ordinateurs contaminés pouvait être facturée 33 cents de dollar l'unité » (Arpagian 2009b, 69).

Il existe ainsi un véritable marché du piratage dans lequel des individus vendent des informations volées (Violet Blue 2015). Dans ce marché noir se trouvent autant des outils permettant de voler l'identité de victimes que d'outils permettant de mener des attaques massives contre des serveurs ou des dispositifs électroniques. Des listes complètes de logiciels et de services (représentant un vrai marché du service de pirate, voir InfoSec Institute 2013 et InfoSec Institute 2015) sont ainsi disponibles sur ce marché, à des prix variables. Les numérisations de passeport se vendaient par exemple entre un et deux dollars fin 2014 (Wueest 2014), alors que les numéros de carte de crédit en 2013 se vendaient entre quatre et dix-huit dollars américains (Clarke 2013). Des informations confidentielles comme la date de naissance étaient disponibles moyennant entre onze et vingt-cinq dollars. Des informations bancaires complètes (pour des comptes ayant entre 70 000 et 150 000 dollars en banque) étaient

achetables pour environ trois-cents dollars. Des outils permettant l'infiltration dans des systèmes informatiques se vendaient quant à eux entre 50 et 250 dollars. Les services de perturbation offerts par des groupes de pirates se vendaient entre trois dollars et 1800 dollars selon la durée de l'attaque (Lillian Ablon, Martin C. Libicki et Andrea A. Golay 2014, 23). Les lots de 1000 ordinateurs infectés se vendaient quant à eux vingt dollars, alors que des lots de 15 000 se vendaient pour environ deux-cent cinquante dollars. Il en coutait entre trente et quatre cents dollars pour louer les services d'un pirate afin de prendre le contrôle ou de s'infiltrer dans un compte d'ordinateur personnel ou dans un compte courriel (Lillian Ablon, Martin C. Libicki et Andrea A. Golay 2014, 12).

Le marché noir regorge également de pirates cherchant à revendre des vulnérabilités encore inexploitées, des « zero-day vulnerabilities ». Ces vulnérabilités, jamais publiques, permettent aux pirates de s'infiltrer dans des systèmes ne pouvant pas détecter les intrusions. Les prix passent alors à des échelles supérieures, allant en général de 200 à 300 000 dollars américains (Lillian Ablon, Martin C. Libicki et Andrea A. Golay 2014, 26). Ce marché est d'ailleurs particulièrement florissant pour les pirates puisque les compagnies de sécurité n'offrent en général que de minces fractions de ces prix sur les marchés réguliers. HP et Verisign offrent par exemple chacun 10 000$ pour chaque vulnérabilité signalée. Parallèlement, les agences étatiques ont également commencé à négocier dans le marché de la sécurité et de l'achat de vulnérabilités (Greenberg 2012), offrant presque les mêmes prix que sur le marché noir.

Ces coûts d'opération sont donc extrêmement faibles comparés aux coûts générés par l'acquisition de matériel militaire ou de haute technologie, tout en permettant des opérations en général extrêmement efficaces. Pour Arpagian, « ce faible coût d'entrée explique également que les acteurs de ces guerres informatiques peuvent être des États, mais aussi, et surtout des groupes d'activistes militants. Ou des particuliers »

(Arpagian 2009b, 69).

La perpétuelle évolution du cyberespace fait également qu'il est bien plus difficile de saisir les limites de cet espace et d'y corriger des problèmes rapidement (on se référera notamment à l'article de Bilge et Dumitras sur les vulnérabilités « zero-day » dans lequel les auteurs estiment qu'il faut environ trois-cents jours avant que ces vulnérabilités ne soient corrigées. Bilge et Dumitras 2012).

De plus, la quasi-omniprésence des systèmes connectés dans le cyberespace offre également un anonymat beaucoup plus important que bien d'autres formes d'action politique. Les attaques dans le cyberespace sont donc très profitables, tout acte en son sein devenant « moins risqué, moins couteux et beaucoup plus discret, l'identification de son auteur étant extrêmement difficile » (Bockel 2012, 11). Le fait que les moyens d'influence et de pouvoir dans le cyberespace soient facilement accessibles est donc particulièrement intéressant pour des acteurs disposant de moins de moyens que les forces dominantes dans le système international et dans les sous-ensembles régionaux ou nationaux. Il y a un intérêt pour des acteurs comme les pays émergents (ou encore comme les compagnies privées, les groupes politiques ou terroristes, etc.) à se doter de capacités opérationnelles importantes dans cet espace. C'est d'ailleurs majoritairement dans ces pays, ainsi que dans l'ensemble des BRICS (acronyme anglais désignant *Brazil, Russia, India, China, South Africa*), que se sont installés les marchés noirs de la sécurité informatique, dont l'étendue et l'importance varient avec le temps (voir par exemple le cas du marché noir en Russie avec les deux rapports de recherche de Max Gonchakov : Goncharov 2014; Goncharov 2012). Ces marchés en expansion constante représentent une manne financière importante pour différents types d'acteurs dans le milieu (Lillian Ablon, Martin C. Libicki et Andrea A. Golay 2014).

Rajoutons à cela que la majorité des infrastructures utilisées dans le cyberespace appartiennent au secteur privé, sans réel contrôle des États ou d'autres organisations.

Dans un mode de production capitaliste où le secteur privé cherche avant tout le profit plutôt que la sécurité à long terme, ces infrastructures sont particulièrement vulnérables. Cela a pour effet de rendre ces systèmes « plus vulnérables, car ils peuvent être infectés plus facilement par des pirates malintentionnés, avec de possibles effets en cascade aux conséquences certainement dommageables » (Arpagian 2009a, 70).

1.4 Les risques liés au cyberespace

Avec l'utilisation généralisée des technologies présentes dans le cyberespace et leur importance dans les activités humaines, s'est créé un ensemble de nouveaux risques. Dans les sociétés modernes, « de la dématérialisation des flux financiers au fonctionnement en réseau des feux de signalisation d'une grande métropole, tout est régi par les technologies de l'information et de la communication » (Arpagian 2009a, 70). Par conséquent, tout devient une cible potentielle et un risque pour la sécurité.

L'utilisation massive que nous faisons de technologies datées et d'infrastructures vieillissantes - en plus des erreurs humaines présentes dans les logiciels - crée un ensemble de problèmes de sécurité et de capacités de fonctionnement (il ne reste, par exemple, que peu de temps avant que les capacités physiques de transmission de l'information par la fibre optique ne soient atteintes, voir Aron 2015). La « révolution technétronique » (Brzezinski 1982), mêlant technologie et électronique dans une « société aux éléments extraordinairement enlacés » (Arpagian 2009a, 123) amènerait donc un ensemble de problématiques et de vulnérabilités nouvelles.

Parmi la longue liste des attaques et vulnérabilités répertoriées dans les dernières années, on remarque les piratages de centrales nucléaires (Brandom 2014), des attaques contre des compagnies pétrolières (Hammouche 2012), contre le système

financier ou encore contre les systèmes informatiques de la justice aux États-Unis, paralysant le fonctionnement des tribunaux sur de plus ou moins longues périodes (Fung 2014).

Des failles sont également présentes dans des objets de la vie courante. Dès 2010, des chercheurs avaient réussi à contrôler des automobiles récentes ayant des systèmes embarqués présentant des vulnérabilités (Markoff 2010; Agence France-Presse 2015a), ou encore à déverrouiller d'autres autos (Greenberg 2014b; Atmani 2011). Cela ne devrait qu'empirer avec la propagation des systèmes embarqués reliés à Internet ou ayant des technologies sans fil. Le cas des voitures sans conducteur qui devraient arriver sur le marché d'ici peu (Knapton 2014) pourrait également devenir une source de vulnérabilités à exploiter. Plus récemment, des chercheurs ont réussi à contrôler des systèmes embarqués dans des avions (Finkle 2014), leur permettant par exemple d'envoyer des commandes de navigation afin de changer la trajectoire ou l'altitude des aéronefs en question (Zetter 2015a).

Les transports ne sont pas le seul secteur majeur où la menace d'attaques contre des dispositifs connectés dans le cyberespace pourrait avoir des effets dévastateurs. Des rapports concernant les dispositifs médicaux connectés ont souligné les vulnérabilités que ces technologies présentent. Il serait par exemple possible de pirater un pancréas artificiel (O'Keeffe et al. 2015) ou des robots utilisés lors des chirurgies (Bonaci et al. 2015) par le biais d'ondes radio et de dérégler les fonctions de ces dispositifs afin de porter atteinte gravement à la santé de la personne visée.

D'autres chercheurs ont démontré qu'il était possible de détruire des objets du quotidien avec une simple radio (Greenberg 2014c), tout comme tous les dispositifs liés à ce que l'on appelle « the Internet of things » (sur la question, voir notamment Schneier 2014; et McMillan 2014a). Afin de mieux comprendre de quoi il s'agit, nous nous référerons à la définition qu'en fait Hermann Koptez dans son ouvrage

Real-time systems. Design Principles for Distributed Embedded Applications (on se rapportera notamment à l'excellent chapitre 13 de son ouvrage, où l'auteur analyse en longueur les dynamiques liées à cette question. Voir Kopetz 2011). Pour le chercheur, il s'agit d'un système de synergies de l'information récoltée à travers différents dispositifs 'intelligents' permettant de dépasser les seules capacités d'un objet non connecté au restant du cyberespace (Kopetz 2011, 307).

Cette dynamique de propagation rapide des dispositifs liés à l'*Internet of things* accélère elle aussi le nombre de vulnérabilités dans le quotidien et pour les sociétés développées dans leur ensemble. Par exemple, près de quatre-vingts pour cent des appareils testés par HP en 2014 montraient des problématiques de sécurité allant de mineures à majeures, mettant en péril les données confidentielles récoltées (Fortify, H.P 2014, 4). 100% des dix systèmes anti intrusion de domicile les plus populaires sur le marché avaient quant à eux de graves lacunes en termes de sécurité et de protection de la vie privée, pouvant aller jusqu'à permettre à des intrus de contrôler ces dispositifs (HP Fortify 2015). Afin de prendre la mesure des risques que ces appareils peuvent créer, mentionnons que d'ici à 2020, il devrait y avoir près de vingt-six milliards de ces dispositifs à travers le monde (Fortify, H.P 2014, 6). D'autres outils de notre quotidien comme les clés USB sont également sur la sellette à cause de failles de sécurité importantes (voir Greenberg 2014a).

Ces vulnérabilités ne sont pas uniquement présentes dans des dispositifs destinés au grand public. En décembre 2014, l'espace aérien londonien a dû être fermé après qu'une panne informatique eut rendu tous les systèmes de navigation et de suivi du trafic inopérants (Kastrenakes 2014). Un incident informatique a également paralysé les activités d'une compagnie aérienne polonaise au début de l'année (Osborne 2015). Au mois de juillet 2015, *United airlines* a également victime d'une panne logiciel ayant forcé l'interruption de tous ces vols aux États-Unis pendant près de 24h. Le secteur financier a aussi été victime de ces attaques, dont les cas du NASDAQ à New

York (Riley 2014) ou encore de banques américaines (Lauer 2014; Nakashima 2012). Le complexe militaro-industriel a lui aussi été ciblé à plusieurs reprises, dont le spectaculaire piratage de l'entreprise de défense Lockheed Martin en 2011 (Schneier 2011) où des plans secrets auraient été volés ainsi qu'un ensemble d'autres données; ou encore le piratage d'ordinateurs appartenant à l'OTAN par le groupe Anonymous en 2011 (*Le Monde* 2011).

Les gouvernements sont également visés par ces attaques de plus en plus fréquentes. Le gouvernement du Canada en a fait les frais dans les dernières années, avec par exemple le piratage des sites Internet de la Cour suprême et la police d'Ottawa (ICI.Radio-Canada.ca 2014), de sites du gouvernement du Québec au plus fort de la grève étudiante de 2012 (Teisceira-Lessard 2012), du site du Service de Police de la Ville de Montréal (Renaud 2012; de Pierrebourg 2013; Lasalle 2015), ou encore en étant une des cibles d'un réseau d'espionnage découvert en 2011 (Alperovitch 2011). Aux États-Unis on a même pu voir des cas de piratage viser des systèmes informatiques utilisés dans des prisons, conduisant à l'ouverture de cellules dans des ailes à sécurité maximale (Zetter 2013).

Il est également important de considérer les infrastructures physiques sur lesquelles repose le cyberespace comme étant elles-mêmes à risque. Internet comme principal ensemble de technologies utilisées dans le cyberespace repose sur différentes couches complémentaires. Kramer et al. présentent notamment quatre couches à cet espace (Kramer, Starr et Wentz 2009, 118) : le cyber qui est composé de toutes les données, et des informations de l'Internet; le réseau logique composé des appareils de communication et d'information permettant de naviguer sur Internet ou de communiquer; le réseau physique qui sert à acheminer les signaux électriques et électroniques; et enfin la 'base' qui est composée des câbles, des équipements radio, etc.

De façon synthétique, Internet, comme d'autres technologies, fonctionne grâce à un ensemble de serveurs informatiques connectés entre eux par des fibres optiques (une carte répertoriant tous les câbles sous-marins dans le monde a été préparée par TeleGeography, voir : TeleGeography 2015) transmettant l'information d'un serveur à l'autre. Tout au long du chemin qu'emprunte l'information se trouvent d'autres systèmes servant à diriger le flot d'informations par différentes routes. Les premiers systèmes d'échanges de données sont ceux des fournisseurs d'accès Internet (FAI / *ISP, Internet service provider*) qui traitent l'information des ordinateurs vers d'autres serveurs de routage régionaux. Ces seconds serveurs sont généralement mis en place par les opérateurs de transit IP et servent à échanger de façon globale les données entre les différents FAI. Les échanges des données des FAI ont lieu dans des nœuds d'interconnexion, que l'on appelle des points d'interconnexion Internet (IXP, *Internet exchange point*). Ce sont essentiellement des infrastructures physiques (serveurs, fibre optique, routeurs, alimentation électrique, sécurité) présentes au sein de ce que l'on appelle souvent des « *data center* ». Une fois l'information échangée entre fournisseurs d'accès Internet et opérateurs de transit IP, elle arrive au serveur auquel l'utilisateur faisait sa demande initiale, puis est renvoyée par le même biais qu'à l'aller (pour plus de références et de détails sur ce sujet, voir par exemple van Beijnum 2010).

Bien qu'Internet ait été créé pour être un réseau des réseaux, permettant une continuité des activités en cas de problèmes sur un des nœuds de connectivité, il n'en reste pas moins qu'un ensemble de vulnérabilités existe. Il n'y avait par exemple en 2014 qu'une centaine (102) de points d'interconnexion Internet permettant l'échange de données entre fournisseurs d'accès Internet en Amérique du Nord (dont seulement 14 au Canada); environ 190 (186) en Europe; une cinquantaine (56) pour l'Amérique du Sud et les Caraïbes; une trentaine (34) pour le continent africain et enfin 89 pour l'Asie; pour un total de 467 points d'interconnexion Internet dans le monde entier (European Internet Exchange Association 2015).

Ces différentes infrastructures sont vulnérables aux pannes, aux coupures d'électricité ou encore aux attaques informatiques ou physiques. Une récente panne (mécanique et logicielle) chez l'opérateur de transit IP Bloomberg a par exemple fortement perturbé le fonctionnement des marchés financiers, entrainant la paralysie temporaire de bourses dans le monde (Titcomb 2015). Une autre panne début juillet 2015, a également perturbé le fonctionnement de la bourse de New-York (CBC News 2015). Des incidents ont également fréquemment eu lieu directement dans les « data center » faisant fonctionner les IXP, entrainant des coupures de services très importantes. Par exemple, en 2013 un incident a mis hors service pendant plusieurs jours le système de paye des contractants de l'État français (Sayer 2013), alors qu'en 2014, une coupure de courant avait rendu inaccessible un ensemble de services du gouvernement provincial du Nouveau-Brunswick, allant des services d'urgences aux systèmes informatiques du réseau de la santé (Gilbert 2014). En France en 2011, une pelleteuse avait quant à elle coupé un câble de fibre optique lors de travaux, paralysant de nombreux sites internet (Col 2011).

D'autres incidents ont eu lieu lorsque des câbles sous-marins ont été endommagés par des pêcheurs (Cuthbertson 2015), des explorateurs d'épaves sous-marines (Arthur 2013), des bateaux s'étant ancrés sur des câbles par mégarde (Cooper 2012), des tremblements de terre comme en Asie en 2006 (Matis 2012, 2), des accidents maritimes (Moore 2012) ou encore parfois à cause de requins (Gibbs 2014; ce n'est d'ailleurs pas si surprenant puisque le New York Times le rapportait déjà en 1987 : Lewis 1987). Dans tous ces cas, des perturbations significatives du trafic d'Internet ont eu lieu, faisant chuter les capacités de transmission de l'information parfois de près de 90% de leur capacité normale. Ces incidents ont conduit de plus en plus d'acteurs du système international à considérer que les câbles sous-marins sont des infrastructures critiques pour la sécurité des réseaux, mais aussi pour celle des États (Woodall 2013).

D'autres problèmes de taille sont en train de se manifester, comme l'atteinte des capacités maximales des câbles de fibre optique transmettant l'information (Spencer 2015), poussant des compagnies à investir dans leurs propres câbles sous-marins. Google a ainsi décidé d'investir 300 millions de dollars américains pour poser de nouveaux câbles de la côte est des États-Unis jusqu'au Japon (Chowdhry 2014) alors que Microsoft a annoncé qu'elle investirait dans de nouvelles liaisons sous-marines avec différents pays d'Asie de l'Est (Lardinois 2015). Le nombre maximum d'adresses IP est également en phase d'être atteint dans les standards actuels (IPv4), empêchant toute nouvelle connexion Internet pour un ensemble d'appareils (Williams 2012). Ces problèmes logiciels et matériels ont plus ou moins tous des solutions en cours de développement, mais représentent des coûts faramineux pour l'industrie qui doit les mettre en application par la suite.

Pris de façon séparée, ces incidents et problèmes techniques peuvent sembler anecdotiques, mais il s'agit ici de tenter de prendre mesure du tableau plus large qui se dessine avec l'adoption des technologies utilisées dans le cyberespace. Dans toutes les sphères d'activité humaine, la technologie est présente et porte en son sein des vulnérabilités pouvant menacer le bon déroulement des activités.

Enfin, il est important de noter que ces vulnérabilités créent un marché de la sécurité de plus en plus important. À mesure que les failles sont répertoriées et que le nombre d'incidents augmente, les compagnies de sécurité, voire les marchands d'armes (Associated Press 2013), offrent davantage de produits et de services afin de protéger leurs clients. Ce marché représentait déjà près de soixante-dix-neuf milliards de dollars en 2014, et pourrait voir sa valeur passer à près de cent cinquante-cinq milliards de dollars en 2019 (Cybersecurity ventures 2015), soit, à titre d'exemple, près de la moitié de la valeur totale de l'industrie pharmaceutique (World Health Organization 2015). Il y a ici un intérêt à se questionner sur l'identité des acteurs

créant le discours de la sécurité et des besoins qui y sont liés dans le cyberespace. Autant les États peuvent bénéficier d'une bonne partie du discours sur la sécurité dans un ensemble de sphères des relations internationales, autant il nous semble ici que les compagnies privées de sécurité ont une tendance lourde à générer un discours alarmiste afin de pouvoir vendre leurs produits.

1.5 Conclusion sur la structure du cyberespace

Le cyberespace se caractérise avant tout par l'ensemble des réseaux informatiques, électromagnétiques, connectés entre eux à diverses fins, qu'elles soient militaires, économiques ou civiles. Il s'agit en quelque sorte d'un réseau des réseaux, permettant à une multitude d'acteurs de communiquer, d'échanger et faire transiter de l'information. Qu'il s'agisse des activités boursières; d'informations militaires (en partie seulement); ou encore de structurer les communications des forces de l'ordre, tous utilisent les mêmes protocoles de communication entre serveurs, ainsi que les mêmes câbles de fibre optique que n'importe quelle vidéo YouTube ou page Facebook. Il est donc fondamental de retenir que tout dans le cyberespace est interrelié et qu'une attaque contre une partie de cet espace peut avoir de grandes répercutions sur les autres activités.

2. Acteurs en présence et intérêts

Par sa grande flexibilité technique et les possibilités qu'il a ouvertes, le cyberespace regroupe en son sein un ensemble d'acteurs différents ayant des intérêts qui leur sont propres. Si les États restent parmi les acteurs les plus importants, les institutions

internationales, les individus, les groupes politiques, terroristes et *hacktivistes* sont également à étudier puisqu'ils peuvent avoir un impact considérable quand ils mènent des opérations dans le cyberespace. Ces acteurs peuvent profiter des facilités d'accès au cyberespace, tant en termes financiers que technologiques, afin de prendre une place importante dans la société et dans les relations internationales ainsi que pour acquérir une certaine autonomie face aux États.

Tout comme la question de la nature des acteurs en présence, la question de l'intérêt de ces acteurs est à élargir. Si les États ont encore la sécurité et la souveraineté de leur territoire au cœur de leurs préoccupations, ce ne sont plus les seules questions qui les motivent à agir. Il en va de même pour les autres acteurs. Il semble clair que dans un mode de production capitaliste avancé, tous les acteurs ont des intérêts économiques et stratégiques qu'ils cherchent à atteindre. Sur cette question, nous nous rapprochons plus des néoréalistes et néolibéraux, puisque ceux-ci ne se limitent pas qu'aux intérêts militaires et sécuritaires. Il importe donc de se questionner sur des domaines proches des études critiques de la sécurité, tels que la sécurité de l'État (militaire, notamment), la sécurité économique, mais aussi la sécurité de la société civile en tant que composante dépendante du cyberespace et visée directement par des attaques dans cet espace. Il s'agit notamment de comprendre comment des pays qui n'étaient qu'« objets subalternes » (Ayoob) et non « sujets » lors de la guerre froide et dans les processus de décolonisation peuvent bénéficier de l'utilisation des technologies liées au cyberespace afin d'accomplir pleinement ce changement de paradigme identitaire et international.

Nous tenterons donc ici d'aborder quelques-uns des acteurs principaux dans le cyberespace en nous basant notamment sur la *Stratégie de cybersécurité du Canada* (Gouvernement du Canada [Sécurité publique Canada] 2010) qui dresse un portrait assez large de la question.

Ce travail de distinction des différents acteurs en présence est toutefois rendu compliqué dans les situations réelles puisque l'attribution des attaques est difficile. Les acteurs civils peuvent en effet servir d'écran de fumée aux États, tout comme les groupes criminels ou nationalistes. De même, des groupes de pirates peuvent utiliser des technologies ressemblant à celle des États afin de brouiller leurs traces. Dans ce cadre, la formulation et l'énonciation de la menace par les acteurs sécurisateurs est d'autant plus importante, puisque les preuves tangibles sont rarement totalement fiables.

2.1 Les États

Pour le gouvernement du Canada, il est clair que les États sont les premiers acteurs à étudier. Dans le cyberespace, les cas de « cyberespionnage et activités militaires parrainés par des États » seraient parmi les attaques et opérations les plus courantes. En effet, puisque les États ont théoriquement de grandes ressources à leur disposition et ont un appui logistique considérable, « les services militaires et du renseignement étranger sont à l'origine des cybermenaces les plus évoluées » (Gouvernement du Canada [Sécurité publique Canada] 2010, 5).

Il est important de noter que les buts de ces opérations sont variés et correspondent à un ensemble d'enjeux liés à une conception élargie de la sécurité (Buzan, Wæver et Wilde 1998), allant « d'obtenir des avantages politiques, économiques, commerciaux ou militaires » (Gouvernement du Canada [Sécurité publique Canada] 2010, 5) à des attaques contre des structures civiles ou militaires.

> Les programmes de cyberattaques de ces États sont habituellement conçus pour saboter les infrastructures et les communications d'un adversaire, ou appuyer des attaques électroniques contre le matériel et les opérations militaires d'un adversaire. Les cyberattaques qui perturbent les systèmes d'intervention d'urgence et de santé publique peuvent mettre des vies en danger » (Gouvernement du Canada [Sécurité publique Canada] 2010, 5)

Il y a donc un ensemble large de préoccupations ou d'enjeux poussant ces États à projeter de la force de différentes façons dans le cyberespace. Ces opérations seraient autant de nature d'espionnage militaire ou industriel que de complément à des moyens de guerre conventionnels. Les cibles dans le cyberespace peuvent être autant civiles, commerciales que militaires, et en cela, la guerre dans le cyberespace vient bousculer des normes importantes du droit de la guerre ainsi que du commerce international. Il est ainsi clair que « le Canada et ses alliés savent qu'ils doivent moderniser leur doctrine militaire pour affronter ces risques ». Cela a notamment poussé l'OTAN et d'autres organisations à se doter de doctrines stratégiques sur la question (Myrli 2009; Organisation du traité de l'Atlantique nord 2011).

Comme nous le verrons, les pays émergents ou en voie de réindustrialisation ne sont pas en reste. Ces derniers mènent notamment dans le cyberespace un ensemble d'opérations pouvant leur permettre de renforcer leurs capacités d'influence et favoriser leur développement économique.

2.2 Les groupes terroristes et autres *hackers*

Compte tenu de la facilité d'accès aux technologies du cyberespace, les groupes non étatiques peuvent également y mener des actions de différentes natures (attaques, propagande, recrutement, financement, etc.). Même s'il n'y a pas réellement eu d'actions terroristes à proprement parler dans le cyberespace, et bien que la majorité des doctrines ou documents officiels omette cette catégorie d'acteurs, le gouvernement du Canada est un de ceux qui mettent l'accent sur une utilisation potentielle du cyberespace par des groupes terroristes :

> Les réseaux terroristes ont également commencé à intégrer les cyberopérations

> à leur doctrine stratégique. Ils utilisent entre autres Internet pour recruter des membres, recueillir des fonds et faire de la propagande. (Gouvernement du Canada [Sécurité publique Canada] 2010, 5)

Ces groupes seraient ainsi « conscients que la dépendance des pays occidentaux à l'égard des cybersystèmes constitue une vulnérabilité à exploiter ». Malgré tout, ces groupes représentent une menace marginale, puisque « les spécialistes soupçonnent que les terroristes n'ont pas actuellement la capacité de causer de graves dommages aux moyens de cyberattaques » (Gouvernement du Canada [Sécurité publique Canada] 2010, 5).

Pour le moment, ces groupes (par exemple *Daech*, qui fait une utilisation intensive des réseaux sociaux et d'Internet) ont eu tendance à investir le cyberespace afin de se financer (voir par exemple : *How the Terrorists Got Rich*, Zarate et Sanderson 2014) ou d'attaquer des médias étrangers (voir notamment, *Syrian Electronic Army hacks Washington Post Web site*, Farhi et Tsukayama 2013) ou diffuser de la propagande (Farwell 2014).

Pour certains gouvernements, la menace vient aussi des différents groupes de *hackers* (voir par exemple, FBI adds five new hackers to cyber most wanted list Gibbs 2013). Bien qu'il existe différents types de *hackers* (« *white hats* » : hackers travaillant pour les compagnies de sécurité informatique; « *grey hats* » : hackers professionnels ou amateurs cherchant à souligner l'existence de failles sans les utiliser ou nuire ; « *black hats* » : hackers cherchant à utiliser et exploiter des failles informatiques à des fins personnelles ou criminelles (Bockel 2012, 33)), l'amalgame entre ces différents groupes pousse souvent à confondre les menaces et à qualifier d'emblée tout *hacker* comme étant un criminel ou un terroriste. Ce manque de nuances est dommageable si l'on essaie de comprendre les types d'influence différents que ces différents groupes peuvent avoir. Par exemple, certains groupes que l'on ne qualifiera pas de terroristes, mais plutôt de *hacktivistes* (mot valise venant de *hacker* et activistes) comme *Anonymous* ou *LulzSec* ont également un potentiel de perturbation à ne pas négliger.

Ces groupes ont parfois mené à des crises internationales mineures, par exemple en piratant des systèmes en Corée du Nord (Anonymous hacks North Korea's Twitter and Flickr accounts, Whitney 2013) ou encore en intervenant dans la crise en Syrie (Global hacking network declares Internet war on Syria, Holmes 2012) et d'autres conflits (*An Inside Look at Anonymous, the Radical Hacking Collective*, Kushner 2014).

Ces différents groupes peuvent donc avoir des motivations variées, qu'elles soient nationalistes ou plus largement politiques, les poussant à agir de multiples façons avec divers degrés d'intensité. Ces différences montrent qu'il est nécessaire de ne pas mettre tous ces acteurs dans la même catégorie. Il reste tout de même que les potentiels de perturbation par ces acteurs sont importants, ceux-ci n'étant généralement pas sous un quelconque contrôle des États, et échappant aux classifications typiques des relations internationales. Il importe donc de prendre en compte ces acteurs utilisant les technologies dans le cyberespace afin de faire avancer leurs intérêts stratégiques et par le fait même, gagner une place plus prépondérante dans les relations internationales.

2.3 Cybercriminels et cybercriminalité

Les groupes criminels (autres que terroristes) ont également profité de l'ère du tout numérique afin de moderniser leurs secteurs d'activités. Du vol d'identité aux sites frauduleux ou alimentant le trafic de drogue en ligne, l'éventail de leurs activités est grand. Contrairement aux groupes terroristes, les cybercriminels n'ont en général pas de visées politiques ou sociales particulières, cherchant plutôt à s'enrichir par le biais d'activités illégales. La prolifération de leurs activités dans le cyberespace n'est en quelque sorte qu'une extension logique et naturelle de leurs activités classiques.

La question de la cybercriminalité est notamment au centre des préoccupations de bien des forces de police *(voir par exemple A report on cybercrime in Canada,* Deloitte 2008) et il est clair qu'elle deviendra une priorité dans un futur proche. Pour certains auteurs, il s'agirait même d'une question de sécurité élargie à différents secteurs économiques et sociaux, devant faire l'objet d'une prise en charge plus complète par les États (Kramer, Starr et Wentz 2009, 436).

Il y a donc dans la cybercriminalité d'importants enjeux économiques et sociaux, dont on estimait le coût à quatre cent quarante-cinq milliards de dollars américains en 2014 (Nakashima et Peterson 2014; Center for Strategic and International Studies 2014), alors que le marché de la sécurité représentait quant à lui un maigre soixante-et-onze milliards en 2014 (Cybersecurity ventures 2015).

2.4 Les acteurs civils

S'il existe une grande variété d'acteurs pouvant avoir une influence importante dans le cyberespace, il ne faudrait pas oublier la catégorie la plus importante numériquement : la société civile. Avec la propagation des technologies de l'information et le développement de l'utilisation du cyberespace pour un ensemble d'activités, les citoyens ont massivement intégré le cyberespace dans leur vie courante. Il est d'ailleurs remarquable que leur présence ne se retrouve jamais dans les documents de doctrine autrement que comme étant un simple paramètre dans les stratégies de sécurité. Pourtant, les citoyens pourraient être les premiers concernés en cas de cyberattaque puisque les activités civiles dans les sociétés occidentales reposent grandement sur cet espace.

Par ailleurs, les populations civiles pourraient se trouver au centre de stratégies offensives dans le cyberespace. De plus en plus d'acteurs avancent ainsi la possibilité

de développer de nouvelles formes de conscription ou de service militaire par le biais de la technologie. Notamment, la conscription électronique (le fait, par exemple, de forcer les populations civiles à dédier une partie de la puissance de calcul de leurs ordinateurs à des activités militaires) pourrait amener un ensemble de nouvelles façons de mener la guerre et de concevoir l'implication des civils dans les conflits (voir notamment Brenner et Clarke 2010).

Parmi les acteurs de la société civile, se trouvent également les entreprises privées. Ces dernières contrôlent d'ailleurs généralement les infrastructures sur lesquelles repose le cyberespace. Dans cette optique, certains comme Bockel, en appellent à une plus grande supervision du secteur privé et à une plus étroite collaboration entre ces entreprises et les services de l'État chargé de veiller à la sécurité des infrastructures du cyberespace, mais aussi de la sécurité d'infrastructures physiques ou d'autres sphères d'activités humaines. En effet, la coopération avec le secteur privé est généralement limitée et peu contraignante, et devrait être accentuée. À des fins de sécurité informatique au niveau des infrastructures essentielles, mais aussi afin de lutter contre l'espionnage industriel et le vol de secrets.

Parmi certaines mesures possibles pour accentuer cette coopération, dans le cas de la France, Bockel propose notamment le fait d'instaurer une « déclaration obligatoire (et confidentielle) des entreprises en cas d'attaque importante sur leurs systèmes d'information » (Bockel 2012, 108). Cela aurait le bénéfice de permettre à l'État de mesurer l'ampleur des attaques ainsi que d'accompagner ces entreprises en cas de problème.

Notons enfin que le manque de collaboration ne viendrait pas seulement des entreprises, mais aussi des structures de l'État qui ne sont pas toujours à même de prendre en charge les demandes du secteur privé.

3 Conclusion partielle sur la structure du cyberespace et les acteurs en présence

Le cyberespace est donc l'ensemble du domaine électronique créé par les nouvelles technologies de l'information et leur utilisation intensive partout dans les sphères de l'activité humaine. Cet espace est également un lieu de pouvoir et d'affrontements entre puissances et acteurs politiques.

L'omniprésence du cyberespace dans les activités humaines, combinée à son caractère fondamentalement poreux, fait que toute opération qui y est menée, est susceptible de toucher des populations civiles ainsi que des systèmes essentiels au fonctionnement de la société. Il s'agit probablement de la première fois dans l'histoire qu'un tel niveau de synergie, tous secteurs confondus, existe et qu'un tel partage égal des risques de sécurité est aussi manifeste.

Le cyberespace a également permis à des groupes plus marginaux de se projeter dans l'arène internationale afin de faire valoir leurs points de vue et opinions. La facilité d'action, en plus du coût limité des opérations dans le cyberespace, fait que de nombreux acteurs pourraient utiliser ces technologies afin de faire avancer leurs politiques ou de sécuriser leurs intérêts. Il est particulièrement important de prendre en compte ce point puisqu'il s'agit à notre avis d'une opportunité gigantesque pour les pays émergents de devenir des « sujets » à part entière du système international. Il pourrait également s'agir d'un moyen efficace de défense contre des guerres impérialistes.

Enfin par ses origines et la façon dont il est structuré, et contrairement à d'autres espaces, le cyberespace est un domaine mouvant pouvant être modifié selon la volonté de ses acteurs. Les analyses que nous formulons ici sont donc nécessairement

amenées à évoluer avec le temps.

CHAPITRE III

CYBERESPACE ET RELATIONS INTERNATIONALES

1. Un espace nouveau des relations internationales

Le cyberespace en tant que nouvel espace d'interactions entre différents acteurs, est également un espace de diplomatie, d'affrontement et de guerre. Il est, comparable et vient se superposer aux espaces classiques comme l'air, l'espace, la mer ou encore la terre. Si l'utilisation des technologies présentes dans le cyberespace et utilisées pour y mener des opérations est une pratique assez nouvelle dans le système international, les États et le domaine militaire ont tout de même rapidement investi cet espace.

Rappelons que le système international est avant tout une construction conceptuelle visant à regrouper sous un seul nom générique un ensemble d'acteurs (et leurs interactions) et de sous-systèmes politiques et géographiques. Selon nous, le système international ne se limite pas aux seuls acteurs étatiques, puisqu'il comprend un ensemble d'autres groupes susceptibles d'intervenir dans les questions locales, régionales et internationales. Quand nous utilisons le concept de système international, il faut donc se souvenir que cette construction langagière et conceptuelle est avant tout une idée mise en avant par les États et certains chercheurs en science politique afin de rendre plus simple une réalité trop complexe (et formuler la perception de leurs intérêts et de leurs besoins). Dans ce contexte, notre utilisation de ce concept relève avant tout d'une recherche d'intelligibilité pour les lecteurs que d'une réelle adhésion au terme.

Notre vision du système international est donc marquée par différents cadres

d'analyse et tente de répondre aux besoins de notre recherche. Tout comme les néoréalistes (Waltz), nous pensons que le système international est marqué par une certaine forme d'anarchie (au sens des relations internationales et non de la philosophie politique) : il n'existe pas réellement de pouvoir de contrainte supranational ni de structures fédérant et régissant les activités des États. Si les États-Unis sont un hégémon partiel, leur influence a tendance à diminuer de plus en plus. Cette érosion des puissances dominantes au XXe siècle se fait généralement au profit de l'apparition de nouvelles puissances émergentes (tant économiquement que militairement ou diplomatiquement). De même, s'il existe des régimes juridiques et internationaux marqués par l'influence de cet hégémon partiel, il ne s'agit pas d'une domination intégrale.

Dans le cyberespace, cette anarchie relative se trouve renforcée, puisqu'il n'existe pas d'hégémon ou encore d'institution de coercition et de régulation supranationale. Si les États peuvent contrôler une partie des infrastructures physiques dans le cyberespace, l'absence de vraie capacité de contrôle sur les autres acteurs en présence est une problématique importante. L'autonomisation des individus, groupes, sociétés privées, etc. rend difficile l'application d'un ensemble de régimes techniques (et juridiques dans certains ensembles régionaux) visant à réguler les activités entre acteurs dans cet espace. Il semble donc que la stabilité et l'existence du cyberespace se basent plus pour le moment sur la coopération entre les différents acteurs publics et privés (qui se voient délégués un ensemble de pouvoirs et de responsabilités) que sur le respect de régimes juridiques ou encore sur le contrôle par un hégémon. Si les néolibéraux affirment que des régimes internationaux de droit (« un ensemble de principes, de normes, de règles et de processus décisionnels implicites ou explicites autour desquels les attentes d'acteurs convergent dans un domaine spécifique des relations internationales », Macleod et O'Meara 2007, 114) peuvent stabiliser les relations entre États et autres acteurs et favoriser leur collaboration, nous verrons que dans le cyberespace cela se limite à des questions assez techniques.

Le cyberespace est donc une sphère nouvelle d'activités humaines, y compris militaires, politiques et diplomatiques, mais aussi un espace venant en appui aux activités classiques des acteurs présents dans le système international, ou dans les systèmes régionaux ou locaux. Une des premières utilisations des moyens informatiques du cyberespace a notamment été la conduite d'opérations de guerre pour l'information afin de rendre les activités classiques plus efficaces (Kramer, Starr et Wentz 2009, 284).

2. La projection de la force dans le cyberespace

Dans le cyberespace, la façon dont les acteurs peuvent projeter de la force est différente des espaces plus traditionnels. Comme nous l'avons vu précédemment, le cyberespace est très accessible et les moyens d'action et d'attaque sont peu onéreux tout en étant efficaces.

Comme les néoréalistes, nous pensons que la force – ou la puissance - est foncièrement l'alliance des « capacités militaires, économiques et technologiques des États » (Gilpin 1981, 13) et autres acteurs. Cette force permet aux différents acteurs d'« appliquer [ses] capacités dans une tentative de changer le comportement d'un autre de certaines manières » (Waltz 1979, 191) de façon offensive ou défensive (Aron 1984). Dans le cyberespace, c'est notamment la guerre de l'information qui vient prendre une nouvelle dimension et devient capitale pour la conduite des opérations.

Comme le mentionne Chamayou dans son ouvrage sur les drones (Chamayou 2013), l'arrivée de nouvelles technologies ouvre la porte à une reconfiguration des formes de guerre et d'affrontement. Dans le cyberespace, la projection de la force, ce que l'on

appellera le cyberpouvoir, est différente des cadres réalistes et classiques puisqu'il n'existe pas fondamentalement de façon de mesurer une force militaire dans cet espace grandement dématérialisé. Le cyberpouvoir peut en fait prendre des formes multiples et variées, parfois diffuses. En l'absence de conflit, cette force de pouvoir est donc une interprétation intersubjective des différents acteurs, et non une mesure précise de la force armée de ces derniers. Dans cet espace, la fameuse formule de Staline, « Le Pape, combien de divisions ? » devient ainsi caduque.

2.1 Souveraineté dans le cyberespace

La notion de souveraineté dans le cyberespace amène de nouvelles difficultés épistémologiques. Il est en effet difficile de concevoir une souveraineté étatique dans un espace majoritairement dématérialisé, mais servant de superstructure à un vaste ensemble d'activités humaines qui se déroulent à l'échelle locale.

Si comme dans les autres espaces, la protection des infrastructures essentielles (réseaux électriques, distribution de l'eau, etc.) et la continuité des services de l'État et de l'armée peuvent légitimement être des questions de souveraineté, dans le cyberespace cette question recoupe également celle de la sécurité élargie. Ainsi, la souveraineté peut se situer au niveau des infrastructures physiques et électroniques permettant le fonctionnement de l'État, mais aussi des secteurs économiques et de l'Internet. Il serait possible d'étendre ce spectre à la protection contre l'espionnage industriel ou contre l'espionnage massif des communications diplomatiques ou civiles par d'autres États.

Du fait de la porosité entre sphères civiles et étatiques, ou militaires, il y a une nécessité d'interpréter de façon plus large la problématique de la souveraineté. Par exemple, des menaces contre une sphère d'activité du cyberespace peuvent avoir un

impact sur un ensemble d'autres activités et engager une réplique étatique visant à garantir la souveraineté. L'interconnexion des systèmes et réseaux fait que la souveraineté et sa sauvegarde deviennent plus complexes à aborder. Dans la mesure où les menaces évoluent, « il n'y a aucun doute que la fréquence et la gravité des cybermenaces vont en augmentant » (Gouvernement du Canada [Sécurité publique Canada] 2010, 6) et que la protection des différentes activités dans le cyberespace (commerciales, civiles, administratives, etc.) sera un élément clé de la sécurité nationale dans le futur.

Il est également intéressant d'étudier la question du 'speech act' des États concernant le cyberespace et sa sécurisation. Malgré les déclarations de principes, il est rare que des éléments vulnérables et soumis à des attaques répétées soient réellement sécurisés par les pouvoirs publics ou les autres acteurs du cyberespace. Ainsi, l'énonciation de la menace et de l'importance de ces secteurs est parfois plus liée aux préoccupations de politique interne ou internationale qu'à de réelles questions de souveraineté.

Enfin, un autre aspect de la souveraineté dans le cyberespace est la capacité des acteurs (majoritairement étatiques dans ce cas) à neutraliser les infrastructures physiques qui permettent son fonctionnement. Si par exemple couper Internet dans un territoire donné (par le biais de l'interruption des transferts de données par les fibres optiques internationales) peut être un geste de souveraineté d'un acteur étatique, ces actions peuvent avoir des répercussions sur d'autres acteurs puisque l'ensemble des infrastructures est partagé entre les États. S'agit-il alors de l'exercice de la souveraineté étatique, d'une attaque ou d'un acte remettant en cause la stabilité du système international ?

2.2 L'information au cœur du cyberespace

Bien avant l'apparition du cyberespace, une des ressources les plus importantes pour la conduite de la guerre a toujours été l'information. Afin de viser les bonnes cibles ou de faire les bonnes manœuvres militaires, il était déjà nécessaire de posséder de l'information.

La pénétration des technologies du cyberespace dans nos sociétés a créé un nouveau type de dépendance à l'information, l'élevant au rang de valeur la plus importante des sociétés modernes (voir notamment Crowell 2010). Dans cet espace, tout devient d'une façon ou d'une autre, une bribe d'information dématérialisée, convertie en signaux électriques ou lumineux, acheminée d'un système à l'autre. Il s'agit en fait de la denrée la plus abondante et à la fois la plus rare : il existe une énorme masse de données dans laquelle des informations pertinentes et stratégiques se trouvent noyées dans un amas de vidéos d'animaux (de chats par exemple) et autres phénomènes liés à la culture Internet. À travers ce flot de signaux électriques et de faisceaux lumineux, il importe pour les différents acteurs en présence de protéger leurs données sensibles ou de tenter d'accéder à celles des autres de diverses façons. Si la guerre pour l'information n'est pas une pratique nouvelle pour les militaires, elle revêt un aspect crucial dans le cyberespace. Il s'agit de combiner l'information et les moyens conventionnels afin de mener la guerre, mais aussi ouvrir de nouveaux champs d'opérations inconnus jusqu'à présent. Cette mutation technologique et technique serait « une remise en cause de l'organisation hiérarchique telle qu'elle datait de Napoléon » (Arpagian 2009a, 119) puisqu'elle viendrait chambouler entièrement la façon dont la guerre est menée.

Il y aurait donc, dans le cadre de conflits ou d'affrontements entre pays développés (ou d'autres acteurs) une nouvelle pratique de la guerre qu'il ne faut pas négliger et que nous étudierons plus en détail par la suite.

L'information peut également concerner les entreprises privées et autres acteurs économiques, les secrets et procédés industriels pouvant se retrouver au cœur des

stratégies de différents acteurs. Cela est également vrai dans le cadre d'affrontements commerciaux entre pays ou entre sociétés privées. L'information étant un élément clé de l'innovation technologique, se prémunir contre l'espionnage industriel deviendrait une priorité. Il s'agit là d'ailleurs d'une des formes de guerre de l'information la plus développée actuellement dans le cyberespace, parfois érigée en véritables politiques publiques structurant la présence dans cet espace, mais aussi le développement industriel (comme dans le cas de la Chine, par exemple).

Dans le cyberespace, l'information est donc une des clés du pouvoir et une ressource à protéger contre les attaques d'autres acteurs. Cette considération nous mène nécessairement à nous intéresser au cyberpouvoir et à ses composantes.

2.3 Le cyberpouvoir

Dans le cyberespace, la projection de la force et de la diplomatie entre États et autres acteurs se voit également transformée. Élément clé de ces mutations, le « cyberpouvoir » s'est développé et a pris de nombreuses formes, en fonction des différents acteurs et de leurs besoins. Le cyberpouvoir dépasse d'ailleurs souvent le seul cadre du cyberespace pour pénétrer d'autres espaces et d'autres formes de pouvoir, entrainant une évolution de ces dernières (Kramer, Starr et Wentz 2009, 3).

De façon simple, le cyberpouvoir peut être défini comme étant la capacité à utiliser des outils dans l'environnement du cyberespace afin de manipuler de l'information de façon stratégique (Kramer, Starr et Wentz 2009, 48).

L'importance du cyberespace et des opérations qui s'y déroulent a notamment eu pour conséquence que la majorité des acteurs étatiques se sont dotés de cyberstratrégies (de défense et/ou d'attaque), en plus des stratégies militaires

conventionnelles. D'autres acteurs se sont également dotés de stratégies de défense (par exemple contre l'espionnage industriel ou la fraude) afin de faire face aux menaces pouvant surgir dans cet espace. De façon générale, ces stratégies visent notamment à créer des politiques publiques encadrant la vision globale des interventions dans le cyberespace ainsi que la façon de projeter la force dans cet espace (Kramer, Starr et Wentz 2009, 48).

Cette vision du cyberpouvoir, comme étant transversale aux autres sphères d'exercice du pouvoir et de la force, est par exemple présente dans la doctrine du Royaume-Uni :

> cyberspace has now grown to become a domain where strategic advantage – industrial or military – can be won or lost.[...] Any reduction in trust towards online communications can now cause serious economic and social harm to the UK (Cabinet Office, United-Kingdom Government 2011, 15).

C'est aussi la vision que Kramer et al. mettent en avant lorsqu'ils évoquent le caractère complémentaire du cyberespace à d'autres sphères de l'activité militaire, diplomatique et économique. Il faut ainsi prendre en compte de nouveaux acteurs, indépendants des États et organisations internationales, en tentant de mesurer et de comprendre comment le cyberespace peut avoir un impact sur d'autres formes de pouvoir (Kramer, Starr et Wentz 2009, 286).

Partant de ce constat, il est alors possible de développer un concept proche du cyberpouvoir, transposé à des questions de politiques extérieures et internationales, mais aussi d'influence politique et culturelle : la cyberinfluence. Certains acteurs, comme les États-Unis ou Israël auraient ainsi un intérêt assez fort à utiliser cet outil de propagande et d'influence afin, par exemple, de justifier leurs exactions lors des guerres qu'ils ont menées dans la dernière décennie. On pensera également aux groupes terroristes qui utilisent Internet comme un outil de diffusion de leurs idées (et crimes) ou encore comme vecteur de recrutement. La cyberinfluence peut donc être

une des formes du cyberpouvoir dans le cadre du système international, mais aussi dans des ensembles régionaux ou locaux. Il est intéressant de noter que le cyberespace, par sa facilité d'accès, offre à moindres coûts un vecteur d'influence à des acteurs qui n'auraient pu autrement accéder à une telle tribune.

Dans une analyse constructiviste de ce phénomène, il est clair que le cyberespace est en train de prendre une place majeure dans la perception du discours et la construction des menaces et actions dans le système international, mais aussi dans la légitimité que les différents acteurs ont à répliquer (Kramer, Starr et Wentz 2009, 19).

La cyberinfluence est également importante pour les entreprises privées. Ces dernières bénéficient largement de cette capacité d'influence dans le cyberespace afin de faire la promotion de leurs idées ou de leurs produits. Nommons par exemple la puissance politique que représentent des compagnies comme Google, Apple ou Microsoft. Ces entreprises bénéficient non seulement d'une influence commerciale importante, mais peuvent aussi édicter des standards technologiques et culturels pour l'ensemble du marché (notamment par le biais de l'imposition de choix technologiques. Voir l'ouvrage « The Social shaping of technology » par MacKenzie et Wajcman 1999). Ces entités ont aussi un pouvoir politique puisqu'elles peuvent parfois influencer des prises de décisions des pouvoirs publics. Google est par exemple une influence significative à Washington (Hamburger et Gold 2014), notamment grâce à des dépenses de lobbying plus importantes que toute autre compagnie américaine (Ollstein 2014).

L'instantanéité d'Internet et des technologies du cyberespace en général oblige également les différents acteurs en présence à modifier leurs stratégies de riposte et de réplique en cas d'attaque ou de piratage. En effet, la vitesse à laquelle fonctionne le cyberespace est un élément important, puisqu'une attaque peut avoir des conséquences désastreuses même si elle n'est menée que pendant quelques

minutes, laissant peu de temps pour répliquer ou se protéger (Kramer, Starr et Wentz 2009, 267).

Aussi bien que les États, des groupes terroristes ou des individus peuvent en profiter pour mener leurs opérations et changer un rapport préexistant lors d'un conflit ou simplement projeter une forme efficace de cyberinfluence.

> Nonstate actors will seek to make cyberspace a medium where guerrilla campaigns, orchestrated dispersal, and surreptitious disruption make large land, sea, and air forces fighting decisive battles irrelevant (Kramer, Starr et Wentz 2009, 268)

Cette instantanéité ouvre de plus des questions quant aux règles d'engagement et de riposte dans un espace où il est difficile de cibler l'origine des attaques et d'y répondre suffisamment rapidement.

Dans le cyberespace, la mesure des capacités d'influence est d'autant plus difficile qu'il est facile de se dissimuler et de bluffer. Ce sont donc en général les acteurs eux-mêmes qui vont tenter de projeter une forme de cyberpouvoir par le discours ou par la mise en avant de politiques publiques ou de doctrines militaires. Il faut donc considérer d'une part l'aspect construit des menaces entre acteurs et d'autre part la projection de la force par le discours et par la construction d'une identité politique et militaire.

Si le cyberpouvoir permet de projeter de la force dans le cyberespace, il peut également passer par le *soft power*, soit la capacité d'attirer ou de susciter la coopération plutôt que l'affrontement (Nye 2004). Sur ce point, les constructivistes ont un avantage certain tant la formulation de la menace peut devenir elle-même l'objet de la riposte. Par exemple, la construction sociale de la menace d'un acteur, notamment des armes et de leur utilisation, relève bien plus de l'idée que l'acteur

menacé s'en fait que de sa nature réelle. Ainsi, comme les constructivistes le soulignent, la construction de la menace peut suffire à projeter de la force dans le cyberespace. Cette force, composée de différentes sphères militaires, sociales et économiques, peut alors prendre d'autres formes comme la capacité à procéder à de l'espionnage industriel ou civil à grande ampleur. Cette forme renouvelée de guerre économique qui pousse les États à entrer silencieusement en conflit est importante à prendre en compte dans la force des États et autres acteurs tant elle peut avoir des impacts sur d'autres secteurs et sphères d'activités (industrielles, diplomatiques, etc.).

Si la projection de la force dans le cyberespace est avant tout une structure idéationnelle intersubjective qui dépend foncièrement des acteurs et de leurs systèmes de valeurs, il est doublement intéressant de se questionner sur les changements que cela peut amener dans le système international et dans les relations entre acteurs présents dans le cyberespace. Car si comme pour le drone, il y a possibilité de « projeter du pouvoir sans projeter de vulnérabilité » (Chamayou 2013, 22), il y a là un changement radical dans la façon dont les acteurs vont se comporter : on pourrait maintenant « éliminer ses ennemis en toute sécurité et à distance » (Chamayou 2013, 134) et ainsi rompre avec la façon de mener la guerre (« la guerre, d'asymétrique qu'elle pouvait être, se fait absolument unilatérale » (Chamayou 2013, 24). Et contrairement au drone, il est nécessaire de noter que les États pourraient en être les victimes les plus directes puisqu'ils dépendent des technologies de l'information et sont plus vulnérables à ce type d'attaques qu'à des attaques militaires classiques.

À notre avis, le cyberpouvoir et la façon dont il peut être mis en œuvre créent de nouvelles possibilités pour tous les acteurs en présence. Les difficultés d'attribution en comparaison avec les facilités d'accès aux outils présents dans le cyberespace créent également un ensemble de nouvelles dynamiques internationales.

3. Cyberattaques, cyberguerre, cyberdéfense, attaques informatiques et autres

menaces dans le cyberespace

Le fait que le cyberespace soit extrêmement poreux crée non seulement des problèmes de différenciation entre cibles et victimes collatérales, mais fait aussi que les attaques (et à *fortiori* la cyberguerre) se trouvent à la croisée des chemins entre guerre de l'information et guerre classique. Ces attaques se situent dans un espace qui vise avant tout les réseaux technologiques et d'informations, tout en ayant un impact sur le reste des activités militaires ou civiles. Comme le mentionne Arpagian :

> la technologie fait de moins en moins la différence entre les univers civils et militaires. À part les armes à proprement parler, les systèmes de communication et les différents dispositifs de sécurisation des réseaux informatiques sont globalement les mêmes dans ces deux mondes (Arpagian 2009a, 133)

Le cyberpouvoir peut en conséquence se décliner d'un grand nombre de façons et toucher de nombreuses activités humaines, civiles ou militaires. Nous aborderons ici les distinctions entre cyberattaques, cyberguerre (une forme particulière de projection de la force et de conflit dans le cyberespace) et les autres menaces pouvant résulter de l'utilisation offensive de technologies présentes dans le cyberespace. Ces formes répondent à des besoins et des visées différentes, qu'elles soient politiques, commerciales ou simplement liées au crime. Nous aborderons également la question de la réponse des différents acteurs à ces phénomènes.

3.1 Les cyberattaques

Une des premières formes d'exercice du cyberpouvoir passe par ce que l'on qualifie de cyberattaques (aussi désignées par le terme « attaques informatiques »). De façon générale, les cyberattaques sont caractérisées par une utilisation d'outils ou de

technologies afin de perturber, saboter, intercepter, détruire ou encore modifier des données informatisées ou des systèmes électroniques ou matériels présents dans le cyberespace. Les cyberattaques peuvent toucher toutes les sphères d'activité et peuvent être déployées par la grande majorité des acteurs en présence, contrairement aux attaques armées classiques. Un individu peut donc cibler un État, un État peut cibler une entreprise privée et ainsi de suite.

Le gouvernement américain définit notamment les cyberattaques comme des attaques visant à perturber l'utilisation des technologies présentes dans le cyberespace par différents acteurs.

> A "cyber attack" is further defined as an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or destroying the integrity of the data or stealing controlled information (United States Government Accountability Office 2011, 53).

Les cyberattaques peuvent avoir différentes intensités et différents niveaux de gravité, engageant des réponses différentes. Sur ce point, il existe de nombreux débats, puisque le droit international et le droit de la guerre ne sont foncièrement pas adaptés aux réalités du cyberespace (Gouvernement du Canada [Sécurité publique Canada] 2010, 3).

Ces attaques sont, dans la majorité des cas, de courte durée (plusieurs heures ou plusieurs jours au maximum, exception faite des cas d'espionnage industriel et des actes s'apparentant à la cyberguerre) et n'occasionnent que des dégâts temporaires comme le fait de rendre indisponibles des réseaux de communications ou de traitement de l'information. On recense des dizaines de milliers d'attaques de ce genre chaque jour (McAfee en recensait près de 200 par minutes en 2013 et les chiffres ont grimpé en 2014 - Intel Security 2014a), avec plus ou moins d'impacts selon les cas. La majorité du temps, les impacts les plus concrets sont financiers,

puisque les systèmes d'information sont indispensables dans les milieux de travail et que toute interruption coute donc aux entreprises ou aux individus les utilisant.

En elles-mêmes, les attaques sont possibles en visant des systèmes mal conçus ou en se concentrant sur des utilisateurs peu sensibilisés aux questions de sécurité informatique (*social engeenering*). D'autres attaques visent les réseaux physiques des technologies du cyberespace. Que ce soit en installant des mouchards ou des virus dans les infrastructures de routage des données, il est possible de perturber ou capter un ensemble de données transitant par ces voies. Cette malléabilité du cyberespace crée ainsi de nombreuses opportunités d'avancées technologiques tout en créant un ensemble de vulnérabilités et de possibilités d'espionnage ou de perturbations.

Dans le cas des attaques visant l'altération ou le vol de données, différentes méthodes sont utilisées. Que ce soit par le *social engeenering* ou l'intervention de personnes à l'intérieur des organisations ciblées, ou encore le vol de matériel physique, les attaquants ont un arsenal complet à leur disposition. Il est important de retenir que « la caractéristique de ces techniques d'intrusion est leur furtivité, qui les rend difficilement décelables » (Bockel 2012, 28). Que ce soit en piratant des ordinateurs appartenant au réseau visé, ou à des sous-traitants (souvent vu dans le cas de piratages de grandes entreprises ou d'armées) ou en volant des accès, les attaques peuvent être variées et avoir des impacts importants. C'est notamment cette furtivité qui permet de mener à bien des opérations d'espionnage industriel ainsi que de renseignement militaire ou diplomatique. Toutes les attaques ne sont donc pas nécessairement visibles ou perturbatrices immédiatement.

Les attaques sont d'ailleurs souvent rendues possibles par l'utilisation importante de logiciels ou équipements grands publics dans des systèmes qui devraient normalement être plus sécurisés. Le choix est généralement fait d'utiliser de tels logiciels ou infrastructures physiques pour augmenter la compatibilité entre systèmes

informatiques ou parce qu'ils sont les seuls disponibles sur le marché, ainsi que de procéder à des économies importantes, le tout au détriment de la sécurité. Comme l'avance Bockel à titre d'exemple, les attaques contre des systèmes essentiels ou militaires pourraient causer de grands dégâts, que ce soit pour la population civile ou l'État en tant que tel. Malgré l'importance de ces réseaux, ces derniers sont souvent mal protégés (voir notamment la présentation de McNabb 2010). Les réseaux de distribution de l'eau, de l'électricité ou encore de pétrole pourraient ainsi être corrompus de l'extérieur (Bockel 2012, 31), ce qui pourrait avoir d'importantes conséquences (un pipeline turque avait par exemple été visé en 2008, voir Robertson et Riley 2014).

Les buts visés par les auteurs de ces attaques sont également variés, allant de la perturbation à la destruction de systèmes d'information. Les attaques peuvent également viser à acquérir de l'information sensible auprès de personnes ou d'organisation détenant des renseignements intéressants pour des pirates ou des puissances étrangères. Qu'il s'agisse d'informations liées à la sécurité nationale, à des brevets ou des cas d'espionnage industriel, cette tendance est lourde et a un impact important sur les systèmes politiques et économiques nationaux et internationaux (Bockel 2012, 32). Que ce soit pour des raisons diplomatiques ou industrielles, les attaques visant les systèmes peuvent servir à les rendre inopérants ou à retarder le développement de certaines technologies (pensons au virus Stuxnet qui a retardé le programme nucléaire iranien. Voir par exemple Zetter 2014c).

Par ailleurs, les cyberattaques peuvent également servir à augmenter la cyberinfluence d'un ensemble d'acteurs. En cas d'attaque contre un État par exemple, les différentes institutions gouvernementales pourraient être particulièrement ralenties ou rendues inopérantes. Les relations avec la population s'en trouveraient grandement touchées (Bockel 2012, 30). Ces formes de perturbations et d'attaques peuvent en effet faire perdre la confiance de la population dans les États et mener à de

l'instabilité sociale et politique. Il s'agit donc d'un potentiel d'influence non négligeable pour des acteurs poursuivant des objectifs politiques. La menace de l'attaque répétée peut en elle-même devenir un élément de diplomatie et de politique étrangère en général.

Les cyberattaques se situent donc essentiellement dans un espace numérique fondamental pour la guerre à l'ère de l'information. Différents types d'attaques sont possibles, que ce soit par l'interruption du fonctionnement normal des systèmes militaires, que par l'utilisation de brouilleurs (par exemple dans le cas de l'opération « codename Senior Sutter » Clarke et Knake 2010, 7) ou par l'intrusion dans les systèmes informatiques en tant que tels (que ce soit en amont par la corruption du code source logiciel ou en aval par une intrusion dans les systèmes de sécurité, à distance ou par une intervention physique). Les motivations des attaquants sont variées et répondent à des intérêts propres à chaque acteur. Notons enfin que le nombre de cyberattaques est en hausse constante, année après année (voir par exemple le rapport de la compagnie Vérizon pour 2015, Verizon Enterprise Solutions 2015).

3.2 La cyberguerre, nouvelle forme de conflit dans le système international

Afin de vraiment mesurer la portée des dégâts que peuvent entrainer des cyberattaques massives, il est nécessaire de s'intéresser à la cyberguerre. Il s'agit en effet de la forme la plus évoluée et la plus dangereuse des cyberattaques, pouvant mener à des perturbations importantes de toutes les activités humaines ainsi qu'à des destructions massives d'infrastructures et de systèmes informatiques.

Historiquement, les événements précurseurs à la cyberguerre sont liés à la modernisation des armées. Les premières formes d'utilisation de cyberattaques

rudimentaires vinrent avec la première guerre du Golfe et l'utilisation de moyens propres à la guerre de l'information. Les États-Unis avaient alors essayé de saboter les radars de l'armée iraquienne avant l'invasion (Clarke et Knake 2010, 9). C'est également à cette époque que la Chine décida de moderniser son armée afin d'acquérir une supériorité dans la guerre de l'information (Clarke et Knake 2010, 50). La modernisation des armées a généré « une tendance de fond dans l'ensemble des nations à se doter, au cours des toutes dernières années, de services à part entière capables d'organiser la défense, voire d'opérer des attaques, dans le cadre de cette cyberguerre » (Arpagian 2009a, 212). La modernisation vise notamment le transfert d'un type de guerre conventionnelle lourde en coûts humains et en infrastructures à des guerres dématérialisées ou menées à distance, par le biais de robots ou de drones. La cyberguerre n'en est qu'une des nombreuses formes, facilement accessible à un ensemble d'acteurs non-dominants. Comme le souligne Chamayou, il y a ici un vrai changement de paradigme à l'œuvre, tant au niveau de la façon de mener la guerre que d'interpréter le droit international.

> La « guerre sans risque », dont le drone constitue sans doute l'instrument le plus accompli, met en crise les principes métajuridiques constitutifs du droit de tuer à la guerre. Sur fond de cette déstabilisation fondamentale se formulent des projets de redéfinition du pouvoir souverain de vie et de mort. Il s'agit de faire place à un droit d' « assassinat ciblé », quitte à dynamiter, dans l'opération, le droit des conflits armés (Chamayou 2013, 31).

Puisque la cyberguerre est encore avant tout construction intellectuelle, faute de cas observables et pouvant servir de référence, les définitions de ce type d'affrontements varient beaucoup d'une doctrine à l'autre. Nous essaierons donc d'en faire un portrait prenant en compte ces différentes visions.

Dans *Cyber war : The next threat to national security and what to do about it*, Clarke et Knake définissent la cyberguerre comme étant des « actions by a nation-state to penetrate another nation's computers network for the purposes of causing damage or

disruption » (Clarke et Knake 2010, 6). Cette définition centrée sur les États doit être comprise au sens large : un acte de cyberguerre est la mise en œuvre de cyberattaques visant à perturber les réseaux informatiques d'un autre État dans le but de causer des dommages ou de rendre non opérationnels ces réseaux. Le déclenchement de la cyberguerre n'est toutefois pas simplement une affaire de puissances étatiques : des acteurs non étatiques comme des individus, des groupes politiques ou encore des entreprises privées pourraient être à la source de cyberguerres. Le gouvernement du Canada considère par exemple que la cyberguerre vise à « obtenir des avantages politiques, économiques, commerciaux ou militaires » (Gouvernement du Canada [Sécurité publique Canada] 2010, 5).

Pour Arpagian, la cyberguerre serait une « appellation strictement militaire (qui) désigne la conduite d'opérations militaires suivant des principes relatifs aux canaux d'information. Il s'agit donc de détruire ou détourner les systèmes de communication adverses » (Arpagian 2009a, 24). Cette définition plus restrictive fait toutefois l'économie de l'analyse des enjeux de sécurité élargie pour un ensemble d'acteurs.

La cyberguerre est donc une forme de conflit et d'affrontement dont les enjeux sont généralement liés aux systèmes d'information et de renseignement, dans un contexte d'interconnexion des réseaux et des infrastructures. Dans ce type de guerre, « la barrière à l'entrée ne se jauge pas tant en volumes de budgets ou d'effectifs militaires, mais davantage en termes d'imagination » (Arpagian 2009a, 26). Cela favorise donc de nombreux acteurs non étatiques ou n'étant pas nécessairement en position de force dans le système international. Les pays émergents pourraient ainsi utiliser la facilité d'accès au cyberespace et leur imposante population formée afin de mener des cyberattaques massives, voire des actes de cyberguerre.

Les finalités de ces techniques sont diverses : de la déstabilisation à l'espionnage ou le sabotage des capacités opérationnelles (Bockel 2012, 25), ces attaques visent autant

les réseaux Internet que les réseaux privés et militaires qui sont censés être déconnectés ou séparés d'Internet (voir à cet effet les révélations sur le groupe « Equation » qui aurait développé des moyens sophistiqués pour attaquer des infrastructures non-connectées à Internet, Kaspersky Labs' Global Research & Analysis Team 2015b).

Bockel rappelle notamment que ces attaques visant à endommager des systèmes ou les rendre inopérants peuvent se comprendre dans un contexte plus large que la guerre traditionnelle. Il semble pertinent ici de se souvenir que la guerre moderne n'est plus constituée que de la seule question de la sécurité physique (la souveraineté) des États, mais de bien d'autres facteurs, dont la guerre économique. Ainsi, des attaques dans le cyberespace peuvent viser à empêcher certains acteurs de développer des capacités économiques ou encore à voler un ensemble de secrets industriels vitaux à la souveraineté économique nationale.

De façon imagée, la cyberguerre serait donc essentiellement le fait d'attaquer les infrastructures électroniques et électromagnétiques d'un pays dans le cyberespace afin de perturber son fonctionnement et le déroulement de ses opérations militaires, économiques et civiles. La cyberguerre rentre également souvent en ligne de compte dans des conflits plus traditionnels, comme soutien aux autres activités liées à la guerre de l'information. On a par exemple vu des cas où des attaques pouvant être considérées comme de la cyberguerre venaient en appui à des attaques militaires conventionnelles afin de réduire les capacités de communication et de défense des cibles (Irak 2003, Géorgie 2008).

La cyberguerre se trouverait donc à la croisée des chemins : elle se situe dans un nouvel espace qui vise avant tout les réseaux technologiques et d'informations. En ce sens, elle serait donc bien une guerre pour l'information : pour son contrôle, sa diffusion et son éventuelle manipulation.

3.3 Stratégies de cyberdéfense

> Because we are the most developed technologically – we have the most bandwidth running through our society and are more dependent on that bandwidth – we are the most vulnerable (Gardels et McConnell 2009)

La porosité du cyberespace et la facilité avec laquelle il est possible d'y projeter de la force ont poussé certains acteurs à vouloir se doter de stratégies de cyberdéfense. Ces stratégies visent notamment la protection des réseaux étatiques, militaires et civils dans le cyberespace. Il s'agit de limiter les vulnérabilités et de se prémunir contre la perturbation des activités se tenant dans cet espace. Les stratégies de cyberdéfense les plus faciles à observer et à analyser sont celles mises en avant par les États, puisqu'elles sont majoritairement publiques. D'autres acteurs comme les entreprises privées ou les organisations internationales ont également mis en œuvre des cyberstratégies. Ces dernières sont toutefois plus difficiles à évaluer, car elles ne sont généralement pas publiques et que ces acteurs ne publient que rarement de l'information sur les attaques dont ils ont été victimes. Nous étudierons ici le cas de la stratégie de cyberdéfense de l'hégémon états-unien puisqu'elle reflète à la fois la recherche de sécurité mais aussi le désintérêt ou l'incompréhension des décideurs publics sur cette question.

Ce pays est marqué par des capacités développées dans le domaine et une grande utilisation des technologies de l'information et des télécommunications. Cela en fait donc une cible récurrente pour des pays ou organisations ayant des buts politiques contestataires ou voulant profiter des vulnérabilités présentes dans le cyberespace afin de mener des opérations de cyberespionnage. Il s'agit également d'un bon exemple d'échec partiel de la défense du cyberespace par une puissance dominante. Les différentes tentatives d'adoption d'une politique de cyberdéfense ont en effet été des

échecs successifs. Dès le milieu des années 1990, les différentes commissions et comités ont alerté de façon répétitive les pouvoirs publics sur le danger que pouvait représenter Internet pour les infrastructures critiques (Robert T. Marsh 1997; National Research Council (U.S.) 2007). Qu'il s'agisse d'incidents touchant la maison blanche, le secteur privé, le secteur financier ou d'autres sphères d'activité, les piratages aidèrent à faire comprendre que la menace était bien réelle et qu'il fallait agir. Cela n'a pourtant pas mené à des changements significatifs, notamment à cause de la volonté de dérégulation des républicains. Ce n'est finalement que quand le candidat Obama va se présenter aux élections présidentielles américaines de 2008 que la cybersécurité va commencer à être sérieusement mise en avant (Obama ayant lui-même été piraté par la Chine lors de sa campagne, voir Isikoff 2013). Malgré l'importance croissante de la question, Obama n'a toutefois pas non plus régulé de façon stricte cette problématique, notamment face au secteur privé. Ce n'est que début 2015 que des propositions claires ont été présentées, tout en restant encore insuffisantes pour bien des acteurs (Olavsrud 2015).

Ainsi, si les activités informatiques dans le cyberespace sont un atout pour l'armée et la gestion des forces armées et de leurs activités, il y a quand même des raisons de s'inquiéter des vulnérabilités que cela pourrait créer :

> Unintended risks and vulnerabilities, especially the increased dependence of the military on civilian cyberspace capabilities, products, and services, need careful assessment to be effectively managed (Kramer, Starr et Wentz 2009, 285)

Même si la prise en compte d'Internet et des nouvelles technologies liées au cyberespace par les communautés de l'espionnage et les militaires américains a été rapide, elle reste périlleuse (Clarke et Knake 2010). Par exemple, la NSA fut mise dans une position de collecte d'informations et de pénétration de systèmes informatiques, mais pas d'attaque puisque la législation ne le permettait pas. En tant que telle, l'US Air Force qui avait initié la prise en compte de la cyberguerre comme

nouvel espace a donc pris la responsabilité de former et de mettre en place des unités militaires de cyberguerre. Afin de comprendre à quel point ce secteur va être important pour les États-Unis, il suffit d'observer le nombre de personnes travaillant pour la 24^{e} unité de l'USAF, une des branches sous la responsabilité du commandement unifié, qui regroupait en 2010 plus de 8000 militaires et civils spécialisés dans la cyberguerre (Clarke et Knake 2010, 41).

Reste tout de même qu'avant 2009, il manquait historiquement un cadre général de coordination entre les différentes branches de l'armée, la NSA et le Commandement unifié (Clarke et Knake 2010, 43). À partir de 2009, un commandement unifié « US Cyber command » a été mis en place afin de coordonner les unités civiles de la NSA et les forces militaires des différents corps d'armée chargés des attaques informatiques. Ce commandement unifié manque malgré tout de moyens humains (Sternstein 2015b) et financiers (Sternstein 2015a) pour arriver à accomplir sa mission. Cela est d'autant plus important que les États-Unis se sont dotés d'une nouvelle stratégie de défense nationale (Obama et The Executive Office of the President - The White House 2015) où le cyberespace est largement présent et est considéré comme un espace clé pour la sécurité nationale. Malgré ces efforts et volontés politiques, les États-Unis sont encore parmi les victimes du plus grand nombre d'attaques répertoriées. Il reste donc un important travail afin de traduire le *speech act* en actions concrètes, autres que la surveillance mondiale des réseaux Internet qui n'a de toute façon pas fait ses preuves selon le gouvernement américain lui-même (qui a ailleurs été obligé de mentir afin de prolonger ces programmes, voir Waterman 2013).

Clarke et Knake sont par ailleurs d'avis que la stratégie de protection des infrastructures américaines est déficiente. Les deux chercheurs pensent que trop peu de mesures ont été prises pour protéger les secteurs privés et corporatifs contre des attaques alors que la majorité de l'activité économique et sociale s'y trouve

concentrée (Clarke et Knake 2010, 46). Ces multiples vulnérabilités s'expliquent notamment par une stratégie plus axée sur l'offensive et la « domination » du cyberespace que sur la défense (par exemple en développant des logiciels d'attaques complexes et difficilement détectables, comme les programmes « Equation » ou encore « Regin », voir Kaspersky Labs' Global Research & Analysis Team 2015a; Symantec 2014). La nécessité d'agir rapidement dans un espace mouvant et rapidement modifié est un des principaux problèmes pour les militaires. Il s'agit donc d'être capable de se défendre contre les attaques tout en étant capable de faire le premier pas afin de ne pas perdre de capacités opérationnelles liées aux dysfonctionnements des systèmes.

Ces stratégies déficientes (ou carrément absentes) de cyberdéfense sont assez répandues chez les différents acteurs présents dans le cyberespace. Peu de législations utiles ont en effet été adoptées, de peur de brusquer le secteur privé ou pour des raisons de protection de la vie privée. Parfois, c'est tout simplement l'absence de compréhension des risques et le manque de *leadership* des pouvoirs publics sur cette question qui créent ce vide dans les capacités de défense.

La question importante dans le cadre du cyberespace est finalement de savoir quels acteurs sont les mieux protégés, et non nécessairement de savoir qui a la meilleure attaque. Si la grande dépendance aux technologies présentes dans le cyberespace dans les sociétés développées s'accompagne d'un ensemble de vulnérabilités et de problématiques nouvelles en termes de sécurité et de défense (Clarke et Knake 2010, 149), cela n'est toutefois pas le cas pour tous les acteurs.

Certains pays ont par exemple basé leur développement dans le cyberespace aussi bien dans la défense que dans l'attaque. L'APL en Chine a par exemple des unités de défense autant que d'attaque (Clarke et Knake 2010, 146). Le contrôle de l'Internet en Chine est d'ailleurs à ce propos d'une grande facilité puisque le gouvernement

peut agir comme bon lui semble. Le contrôle du trafic, des sites et des courriels permet de bloquer des menaces importantes en cas d'attaque ou de menace.

D'autres puissances, notamment issues des BRICS, se sont dotées quant à elles de politiques de défense dans le cyberespace. L'Inde a, par exemple, été un pays précurseur dans le domaine en se dotant de structures de recherche et de protection dans le cyberespace (voir Saksena 2014 ainsi que ; Ministry of Communications & IT 2013). Des structures efficaces seraient ainsi développées, grâce auxquelles les États seraient à même d'agir dans le cyberespace. En Russie, les dynamiques reliées à la guerre de l'information ont été prises en compte dès le début des années 2000 avec l'adoption de politiques de défense et d'action dans cet espace (Government of the Russian Federation 2000). Les plus récentes politiques officielles concernant les questions de guerre de l'information et de cyberespace font également état d'une grande préoccupation pour ces questions (voir Government of the Russian Federation 2011; Government of the Russian Federation 2013). Par exemple, une des stratégies employées serait de surveiller étroitement les communications Internet entrant et sortant du pays, afin de pouvoir déceler des cyberattaques et les arrêter.

Quant au Canada, le pays a adopté une posture défensive et préventive plutôt qu'offensive. Le Centre canadien de réponses aux incidents cybernétiques est chargé de veiller à la surveillance du réseau et à procurer des réponses en temps.

L'utilisation moins généralisée et moins interdépendante des technologies du cyberespace dans des pays comme l'Iran, la Corée du Nord ou même la Chine les exposent moins à des attaques que les États-Unis ou d'autres puissances ayant une grande dépendance aux technologies du cyberespace. Cela ouvre une porte à l'utilisation des moyens de guerre dans le cyberespace de façon asymétrique : la riposte contre ces acteurs serait diffuse et passerait forcément par d'autres méthodes plus conventionnelles et onéreuses (Clarke et Knake 2010, 146).

Cette situation implique que malgré toutes les capacités d'attaque, les États-Unis et les autres pays développés sont vulnérables comparés à des pays moins développés ou mieux protégés. Cette vulnérabilité a d'importantes répercussions sur toutes les autres sphères d'action.

> As long as our economic and military systems are so obviously vulnerable to cyber war, they will tempt opponents to attack in a period of tensions. Opponents may think that they have an opportunity to reshape the political, economic, and military balance by demonstrating to the world what they can do to America. [...] Unlike in conventional war, a superior offense cannot be certain to find and destroy all of the opponent's offensive capability. (Clarke et Knake 2010, 157)

Il s'agit d'un élément clé de l'utilisation par des acteurs non-dominants de technologies dans le cyberespace puisque la vulnérabilité peut devenir le talon d'Achille de pays développés, les dissuadant d'intervenir dans des conflits locaux ou régionaux, de peur d'être victimes de cyberattaques massives. D'une façon paradoxale, la technologie sensée améliorer le fonctionnement de la société devient en quelque sorte la condition propice à la conduite de guerres asymétriques pouvant être dévastatrices pour les acteurs dominants.

Enfin, notons qu'il est difficile, voire impossible, de trouver de la documentation sur les stratégies de cyberdéfense des acteurs privés comme les entreprises ou des organisations internationales. Soit parce que ces derniers ne se sont pas dotés de stratégies de cyberdéfense, soit parce qu'ils considèrent qu'il s'agit d'éléments devant rester secrets. Quelques documents sont toutefois disponibles dans les cas de l'OTAN ou de l'Union européenne.

Dans le cas de l'OTAN, cette organisation s'est dotée d'une stratégie de cyberdéfense et d'un centre de coopération (le *Cooperative Cyber Defence Centre of Excellence,*

situé à Tallinn en Estonie) après avoir identifié la cyberdéfense comme un domaine clé pour le futur (Rasmussen 2013). Un manuel sur la cybersécurité a également été diffusé aux pays membres afin de les aider à structurer leurs actions dans ce domaine (Klimburg et NATO Cooperative Cyber Defence Centre of Excellence 2012). Un autre manuel, le fameux *Tallinn Manual* (Schmitt et NATO Cooperative Cyber Defence Centre of Excellence 2013), vise à analyser les enjeux liés à la cyberguerre et à son intégration dans le droit international. Enfin, en septembre 2014 les membres de l'OTAN ont décidé de considérer les menaces et attaques dans le cyberespace comme tout autre type de acte de guerre (Organisation du traité de l'Atlantique nord 2014), élargissant *de facto* le droit international à cet espace (dans le discours du moins, puisque l'OTAN n'a aucun pouvoir d'édiction du droit international). Il est toutefois intéressant de noter que l'Article numéro 5 du Traité de l'Atlantique Nord (Organisation du traité de l'Atlantique nord) prévoyant la clause de défense collective (*« une attaque contre un est une attaque contre tous »*) ne serait invoquée qu'au cas par cas et non de façon automatique comme elle serait sensée l'être. Il s'agit d'une condition importante à l'intégration des cas de cyberguerre dans le système international et aux mécanismes de défense de l'OTAN. En édictant cette limite, l'Organisation laisse *de facto* les acteurs visés procéder à un *speech act* visant à convaincre les autres membres de l'organisation que la situation est réelle et sévère et mérite donc une réponse collective. L'OTAN reste donc dans une vision plus locale et nationale des problématiques de cybersécurité : les outils et conseils sont donnés aux pays membres, par le biais d'avis et d'un centre d'expertise, mais il n'y a pas de politique contraignante ou de vision d'ensemble pour l'organisation.

Du côté de l'Union européenne, la situation est relativement semblable. Une politique concernant le cyberespace a été adoptée en 2013 et tarde à être mise en œuvre plus sérieusement (High representative of the European Union for foreign affairs and security policy 2013; European Commission). Cette politique vise notamment à faire appliquer dans le cyberespace les lois et traités de l'Union européenne de la même

façon que dans les autres espaces. Il s'agit également de tenter de réduire le cybercrime, d'améliorer la résilience des infrastructures du cyberespace ainsi que d'améliorer les pratiques collectives de cyberdéfense. Le secteur privé est également concerné par cette politique, puisque l'UE met en avant l'idée d'une collaboration indispensable entre acteurs gouvernementaux et entreprises privées responsables des infrastructures réseau.

Les pays membres de l'UE sont également convenus de la nécessité de se doter de meilleures lois afin de régir les activités dans le cyberespace. Toutefois, la politique ne prévoit pas d'autres outils que les dispositions déjà présentes dans la Convention de Budapest sur la cybercriminalité, adoptée en 2001 (voir Council of Europe). L'accent étant majoritairement mis sur la coopération entre États membres, institutions européennes et acteurs privés, il est possible de se demander si une telle politique débouchera réellement sur une meilleure prise en charge à l'échelle européenne de la question de la cybersécurité.

Les cas de l'OTAN et l'UE laissent penser que même si les organisations internationales peuvent avoir un rôle à jouer, les différents acteurs préfèrent encore largement privilégier des politiques nationales ou leurs propres règles quand il s'agit du cyberespace et des enjeux qui y sont liés. Signe de cette dynamique : l'ONU n'a elle-même pas adopté de réelle politique de cybersécurité ou de cyberdéfense (sur le sujet, voir Mackinnon 2012).

3.4 Espionnage électronique et industriel

Dans la gamme des actions dans le cyberespace, toutes les attaques ne visent pas nécessairement à perturber ou à détruire. C'est par exemple le cas de l'espionnage électronique ou industriel. Ces formes de projection du pouvoir sont par essence

furtives et misent sur leur non-détection. Il s'agit d'ailleurs d'une des raisons pour lesquelles les cyberattaques ne sont généralement pas la source de plus d'inquiétudes dans le secteur privé ainsi que pour les décideurs publics (Clarke et Knake 2010, 122).

Dans leur rapport *Threats Predictions* (McAfee Labs 2015), les experts de la firme de sécurité informatique McAfee identifient notamment la question du cyber espionnage comme étant une des principales menaces pour 2015 et les années à venir. La fréquence des attaques devrait augmenter, notamment avec la massification de l'utilisation des téléphones intelligents ainsi que la pénétration toujours plus grande de ce que l'on appelle « the Internet of thing » (dont les chercheurs estiment que le nombre d'appareils devrait atteindre 50 milliards en 2019). Ces dispositifs allant des caméras de surveillance connectées à Internet en passant par les dispositifs de réglage de thermostats intelligents ou encore les SCADA (systèmes de contrôle et d'acquisition de données) présentent d'importants risques de sécurité pouvant mener à des incidents importants (voir notamment l'étude produite par Fortify, H.P 2014). Cette donne n'est pas nouvelle puisque les systèmes de ce type étaient déjà l'objet d'inquiétudes dans les années 1970 (voir la référence de l'époque dans le domaine, Ware 1979).

Ces formes d'espionnage électronique et industriel sont majoritairement menées par des États (à près de 87%) selon les chercheurs de McAfee. Toutefois, les difficultés d'attribution, en plus du fait que les attaques sont parfois menées sans être détectées pendant de longues périodes, font qu'il est difficile de mesurer ce qu'il en est réellement. Nous avons donc ici un aperçu de ce qui est détecté actuellement, mais pas nécessairement de la situation globale.

Toujours est-il que l'espionnage industriel, mené par des États ou par des entreprises privées représente un « risque persistant pour les compagnies » selon le rapport

Managing cyber risks in an interconnected world Key findings from The Global State of Information Security® Survey 2015 (PricewaterhouseCooper 2014). Il s'agit d'un risque de plus en plus important, touchant toutes les sphères de l'activité commerciale, des compagnies aux consommateurs. Les attaques se déroulent maintenant tant au niveau des entreprises, qu'à celui des bourses mondiales (dont au moins 50% auraient été ciblées par des attaques en 2014). Les infrastructures essentielles comme les réseaux électriques, les centrales nucléaires sont elles aussi touchées tout comme les sociétés de transport (National Cybersecurity and communications integration center 2014).

Des cas massifs d'espionnage ont également été répertoriés, par exemple en France : « les entreprises françaises sont aujourd'hui massivement victimes d'attaques informatiques non détectées » (Bockel 2012, 23). Malgré la difficulté d'avoir un portrait d'ensemble de la situation, « tout laisse à penser que le préjudice subi par ces entreprises, et par voie de conséquence, sur l'économie française dans son ensemble, est considérable, tant en termes financiers et de parts de marchés, que d'emplois » (Bockel 2012, 23). Ces menaces et attaques dans le cyberespace ont donc de grands impacts. Ces attaques seraient par ailleurs souvent ciblées dans des secteurs économiques stratégiques et viseraient des groupes en particulier, souvent des fleurons de l'industrie.

Si les pertes financières liées à l'espionnage industriel s'élèvent déjà à plusieurs milliards de dollars par année, la tendance plus lourde et plus inquiétante est plutôt liée au vol de secrets industriels par des compagnies adverses ou par des États ayant des modèles de développement basé sur l'appropriation technologique afin de structurer leurs secteurs industriels (comme la Chine). Nous étudierons plus en détails comment l'espionnage industriel peut bénéficier à ces acteurs dans le chapitre suivant.

Ces différentes formes de menaces dans le cyberespace sont le résultat de technologies vieillissantes et dépassées, mais aussi d'une absence marquée de cohérence dans la gouvernance du cyberespace. Il est donc nécessaire d'étudier cette question.

4. La gouvernance dans le cyberespace

4.1 La présence historique de l'hégémon américain

Dans le système international tel qu'il existe actuellement et est définit par les acteurs dominants, il n'existe aucune structure supranationale régissant de manière coercitive (ou pacifique) les conflits et différends entre les acteurs. Cette situation est également présente dans le cyberespace. L'absence de superstructure de régulation se ressent d'autant plus fortement dans cet espace où les frontières ont tendance à s'effacer et où il est facile de se dissimuler.

Plusieurs facteurs expliquent cette absence de régulation du cyberespace dans le système international. Premièrement, si l'ensemble de technologies le plus commun dans le cyberespace - l'Internet - a été développé avant tout par des militaires, la gestion du système a rapidement été transférée à des entreprises privées plutôt qu'à des organisations internationales. Ce sont en fait des entreprises majoritairement américaines et ayant des accords avec le seul gouvernement américain (de La Chapelle 2014) qui se sont retrouvées en position de contrôle et de gestion de l'Internet.

Il est à noter que le lien de gestion d'Internet a été récemment détaché du gouvernement américain (Timberg 2014a), les ententes contractuelles entre sociétés de gestion et gouvernement des États-Unis ayant expiré et laissé place à de nouvelles

structures (National Telecommunications & Information Administration 2014). Ainsi, l'Internet est actuellement structuré par l'ICANN, le l'Internet Engineering Task Force (IETF) et le Word Wide Web Consortium, en plus de la International Telecommunication Union (ITU) de l'ONU. Ces organismes complémentaires et indépendants gèrent la majorité du fonctionnement du web tel qu'il existe actuellement (Kramer, Starr et Wentz 2009, 492). Ils ne sont toutefois pas des régulateurs politiques ou militaires de l'Internet ou du cyberespace, mais plutôt des créateurs de normes techniques. Par ailleurs, ces acteurs fonctionnement souvent en vase-clos, rendant plus difficile la concertation et l'élaboration d'un droit positif du cyberespace. L'ONU a d'ailleurs souligné cette caractéristique en définissant la gouvernance de cet espace comme suit :

> élaboration et application – par les gouvernements, le secteur privé et la société civile, chacun à leur place – de principes, normes, règles, procédures de prise de décision et programmes qui façonnent l'évolution et l'utilisation de l'Internet » (Working Group on Internet Governance (WGIG) 2005, 4)

Le rôle de ces différents acteurs est donc avant tout technocratique et non politique dans le système international (même si le développement technologique a une composante profondément politique).

Par ailleurs, si les États-Unis ont historiquement représenté un hégémon partiel dans le cyberespace, cela n'a pas empêché d'autres acteurs du système international de réclamer une responsabilité dans la gestion de cet espace.

Ainsi, des institutions comme l'Union européenne (UE) ont légiféré sur le cyberespace, mais sans nécessairement avoir l'assurance de l'application de ce droit régional. Par différents traités (Convention on Cybercrime Council of Europe; Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union European Commission),

l'UE a tenté de réguler les activités dans cet espace, notamment afin de limiter le cybercrime. Pour Bockel, l'Union européenne ne serait pas assez impliquée dans le cyberespace puisque « malgré l'adoption d'un grand nombre de textes, l'action concrète de l'Union européenne dans ce domaine est restée jusqu'à présent relativement limitée » (Bockel 2012, 62). Les différentes politiques et stratégies n'auraient que peu de mesures concrètes qui permettraient de sécuriser les cyberespaces. Il manquerait ainsi d'une « véritable stratégie globale du cyberespace à l'échelle européenne », combinée à une « dispersion des acteurs » empêchant une action à l'échelle du continent et menaçant directement les infrastructures de l'UE.

Une variété d'autres traités a pu être adoptée, mettant notamment en avant le cyberespace et l'Internet comme des outils de propagation du savoir et de démocratie. Cette vision a par exemple été partagée par plus de cent-soixante-quinze pays lors du Sommet mondial sur la société de l'information, organisé par l'Organisation des Nations Unies et la *International Telecommunication Union*. On y présentait dans la déclaration de principes la définition suivante :

> The Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism (United Nations et International Telecommunication Union 2003).

Le but était alors de faciliter la coopération internationale afin de permettre une gestion collégiale et transparente de l'Internet. Si une partie des cibles a été atteinte ou est en voie de l'être, il reste tout de même que le bilan est mitigé (voir le rapport d'étape produit par l'ONU sur la question. U.N Secretary-general 2012).

D'autres organisations internationales comme l'OTAN, l'Organisation pour la

sécurité et la coopération en Europe (OSCE) ou encore Interpol tardent également à agir pour se doter de structures de commandement et de réseautage, bien que « les cyberattaques sont désormais une menace prise en compte dans le nouveau concept stratégique de l'Alliance atlantique » (Bockel 2012, 58). Même l'OCDE a appelé à « protéger ces infrastructures de l'information, dont la perturbation ou la destruction pourrait avoir un impact grave sur la santé, la sécurité, la sureté et le bien-être des citoyens ou le fonctionnement efficace du gouvernement ou de l'économie » (Directorate for science, technology and industry et Commitee for information, computer and communcations policy 2008). Il s'agirait d'une « priorité de politique nationale qui exige une coordination avec les propriétaires et exploitants d'infrastructures d'information critiques du secteur privé ainsi qu'une coopération transfrontière » (Directorate for science, technology and industry et Commitee for information, computer and communcations policy 2008). Cela n'a toutefois pas été suivi d'actions concrètes de la part de l'organisation ou des pays membres.

Ces différents textes ne visent d'ailleurs pas à énoncer un droit propre au cyberespace et encore moins un droit de la guerre spécifique à cet espace. Le cyberespace reste donc caractérisé par une absence de gouvernance globale et un système relativement anarchique (Arpagian 2009a, 166).

Il s'agirait finalement plus de se doter de « bonnes pratiques » que de cadres légaux difficiles à appliquer (Bockel 2012, 54). Des codes de conduite ainsi qu'un système d'enquête en cas de conflit sont par exemple proposés par Bockel. Ce mode de régulation, lié à la coopération internationale plutôt qu'à l'établissement d'un droit international formel, se retrouve en partie dans des structures comme les forums servant à l'échange entre les équipes d'intervention d'urgence (dont le « Forum of incident response and security teams (FIRST) »). D'autres structures locales existent également, notamment au sein de l'Union européenne avec l'« European Government Computer Security Incident Response Team ». Il ne s'agit toutefois que de forums de

coopération technique sans réelles capacités d'enquête ou de sanction contre les acteurs en présence.

Cette coopération est toutefois difficile à cause des défis techniques présents dans le cyberespace (à quoi bon édicter des lois si techniquement il est impossible de les faire appliquer correctement?) et par les visions contradictoires d'Internet entre acteurs. Les questions de souveraineté nationale viennent également rajouter un niveau de complexité : chaque État tient à contrôler de façon plus serrée l'utilisation du cyberespace tant il s'agit d'un espace stratégique.

La gouvernance multipartite du cyberespace amène elle aussi un ensemble de conflits liés aux intérêts divergents des différents acteurs. Les compagnies privées voient par exemple l'Internet comme étant plus une source de revenus et de commerce que comme un problème de sécurité nationale ou de souveraineté. Ces intérêts divergents combinés avec le fait que la majorité des infrastructures du cyberespace soient sous le contrôle de compagnies privées impliquent que les États se voient théoriquement dépossédés d'une partie de leurs capacités de contrôle et de régulation. Même au niveau national, il est donc parfois difficile d'imposer des formes de régulation dans le cyberespace. Cette capacité de régulation dépend en fait largement des valeurs politiques et économiques des acteurs en présence. Dans certains cas, des États ne se ménagent pas pour mettre au pas les sociétés contrôlant les infrastructures (la Chine et la Russie régulent et surveillent beaucoup dans le cyberespace); alors que dans les sociétés libérales les théories du libre marché conditionnent trop largement les différents acteurs pour que les États interviennent de façon plus directe, même dans des cas de sécurité nationale (c'est notamment le cas du Canada qui favorise une coopération non coercitive avec les entreprises privées).

Notons enfin que parmi les problèmes récurrents se pose notamment la question de la définition et de la qualification (dont leur encadrement juridique) des

actes de guerre et d'espionnage dans le cyberespace (Kramer, Starr et Wentz 2009, 67, 76). Ces activités se voient modifiées dans cet espace et ne répondent plus au droit international ou aux pratiques établies. Il existe en fait un vide juridique dans le droit de la guerre et les conventions internationales concernant le cyberespace. Qu'il s'agisse de cyberattaques perturbant des segments larges du fonctionnement d'un pays ou de l'utilisation de cyberattaques en temps de guerre sans faire de distinctions entre civils et militaires, les encadrements existants ne semblent pas pouvoir être appliqués de façon claire dans le cyberespace. De même, la perturbation des infrastructures essentielles d'un pays serait-elle considérée comme un acte de guerre, ou au moins comme une utilisation abusive de la force? Le principe de proportionnalité est également plus difficile à mettre en œuvre dans le cyberespace puisque chaque cible peut toucher des réseaux civils importants, violant ainsi le droit international (Kramer, Starr et Wentz 2009, 537).

4.2 Un modèle contesté : revendication sur le cyberespace et puissances émergentes

Le système international est de plus en plus considéré comme étant « uni-multipolaire » dans le sens où les États-Unis gardent leur influence alors que des puissances émergentes comblent rapidement leur retard tant militaire qu'économique ou institutionnel (Ebert et Maurer 2014, 276).

En ce début de siècle, la domination américaine provoque encore un ensemble de contestations et d'alliances afin de renverser le contrôle des États-Unis. Notamment le groupe de puissances constitué du Brésil, de la Russie, de l'Inde, de la Chine et de l'Afrique du Sud (BRICS) est perçu comme un ensemble contestataire particulièrement important dans les questions liées à la gouvernance du cyberespace. Ces pays se sont démarqués par leur approche revendicatrice et contestataire de la

gouvernance du cyberespace.

Deux courants principaux sont présents dans la contestation du modèle actuel : l'un souverainiste qui vise la prise en charge locale des questions reliées à l'Internet, mais coordonnée par une organisation intergouvernementale ; alors que le second s'appuie sur des organisations internationales visant à encadrer vraiment le cyberespace et à limiter la puissance américaine.

Au cœur des BRICS, il est possible de voir ces deux courants à l'œuvre. L'Inde, le Brésil et l'Afrique du Sud (IBSA) cherchent par exemple à développer un ensemble de stratégies et de protocoles de coopération en plus d'alliances politiques (Ebert et Maurer 2014). La Russie et la Chine sont quant à eux considérés comme plus opportunistes, jouant à la fois sur les terrains de la collaboration avec d'autres puissances émergentes tout en essayant de faire des gains individuels. Il existe donc de grandes différences d'opinions sur les modèles de gouvernance à adopter dans le cyberespace.

Certains pays comme le Brésil et l'Afrique du Sud ont favorisé l'inclusion de la société civile dans la gouvernance de l'Internet alors que la Chine a maintenu un contrôle strict par l'État et que la Russie a tendance à emprunter une stratégie alliant contrôle et inclusion partielle de tierces-parties. Entre ces groupes de pays, il existe également une tension entre contrôle étatique et liberté économique des marchés dans la gestion et la mise en place de l'Internet. Ces différences rendent plus difficile l'adoption d'une vision commune de ce que devraient être Internet et sa gouvernance (Ebert et Maurer 2014, 283). Le type de régime joue donc un rôle important dans le type de positions concernant la gouvernance du cyberespace (Ebert et Maurer 2014, 287).

Ces distinctions dans les modèles de gouvernance mis en avant par les différents pays

des BRICS créent un double dynamique : il existe une volonté de créer un véritable équilibre des forces face aux États-Unis, mais aussi face à certaines puissances montantes. De façon paradoxale, afin d'atteindre cet équilibre au sein des puissances montantes, certains pays comme l'Inde ou le Brésil ont décidé de signer des accords ou des conventions avec les États-Unis.

Il ne ressort finalement de cette contestation que des résultats mitigés puisque l'hégémon américain reste bel et bien présent et actif. Cette dynamique reste malgré tout assez importante puisque les pays émergents ou émergents pourraient vouloir accentuer leur place dans la gestion du cyberespace et d'Internet afin de satisfaire leurs intérêts. Dans un cadre où ces pays peuvent bénéficier d'une facilité d'accès et de projection de la force, cela n'est pas négligeable pour les questions reliées au cyberespace.

5. Conclusion

Par ses caractéristiques et son importance, le cyberespace est un nouvel espace d'interactions entre États, mais aussi entre acteurs privés et économiques. Il s'agit également d'un espace de guerre (dans le cas de la *cyberguerre*), comparable aux espaces classiques comme l'air, l'espace, la mer ou encore la terre. Certains auteurs vont même jusqu'à affirmer qu'il s'agit d'un espace proprement révolutionnaire pour les théories de la guerre puisqu'il s'agirait d'une révolution ('Revolution in military affairs') dans la manière de mener la guerre et de concevoir la sécurité (en évoquant par exemple des 'guerres postmodernes' où il y aurait « préservation par substitution » (Chamayou 2013, 257) des combattants par des moyens technologiques). Cet espace viendrait d'ailleurs bousculer les théories de la guerre et les stratégies de défense des acteurs en présence.

La question de la cyberguerre est également devenue fondamentale dans le cadre actuel des relations internationales. Les enjeux de développement et d'influence qui y sont liés sont tels qu'ils ne peuvent être négligés ni mitigés. L'absence de gouvernance globale et de régime juridique fiable pour qualifier les actes de cyberguerre sont à notre avis deux données fondamentales pour le développement de ces conflits (à cet effet, voir le très complet ouvrage de Kerschischnig 2012). Il pourrait d'ailleurs s'agir d'une opportunité pour les pays émergents de devenir des « sujets » à part entière du système international, et même de renverser partiellement ou complètement l'ordre du système international. En nous basant sur des cas d'étude, nous tenterons d'identifier dans le chapitre suivant quelles sont les options pour ces pays.

CHAPITRE IV

COMMENT DES PAYS ÉMERGENTS AYANT ORIENTÉ LEURS POLITIQUES ÉDUCATIVES VERS LA MISE À DISPOSITION D'UNE MAIN-D'OEUVRE TECHNOLOGIQUEMENT QUALIFIÉE POURRAIENT-ILS TIRER PROFIT DE LA MISE EN PLACE DE CYBERSTRATÉGIES?

> Small nation states and foreign terror groups will take to cyberspace to conduct warfare against their enemies. They will attack by launching crippling distributed denial of service attacks or using malware that wipes the master boot record to destroy their enemies' networks. At the same time, long-term cyber espionage players will implement better methods to remain hidden on a victim's network, using better and more sophisticated stealth technologies and other means to remain below the operating system and out of sight (Intel Security 2014b, 6).

Puisque le cyberespace est avant tout dématérialisé, facile d'accès et important pour différentes activités humaines, nous nous intéresserons ici aux possibilités d'utilisation des technologies présentes dans cet espace par des acteurs du système international n'étant pas considérés comme dominants. Plus précisément, nous étudierons le cas de pays émergents ou en voie de réindustrialisation (Russie, par exemple) ayant axé leur développement économique et industriel sur la formation d'une main d'œuvre qualifiée et ayant un niveau d'éducation élevé.

Rappelons que notre hypothèse de recherche est centrée sur l'utilisation que certains pays émergents pourraient faire des technologies présentes dans le cyberespace. À

notre avis, les pays émergents ayant axé leur développement économique et industriel autour des technologies de l'informatique et des télécommunications ont une capacité accrue à utiliser les technologies du cyberespace afin de mener des actions pouvant renverser ou déstabiliser le système international, à l'échelle régionale ou mondiale. La projection de la force par ces acteurs dans le cyberespace serait donc une forme d'*empowerment* (le passage du statut d'objet subalterne au sujet à part entière dans les relations internationales) pour ces derniers.

Nous étudierons rapidement en premier lieu quelques cas de politiques éducatives pouvant présenter un intérêt pour notre recherche. Puis, nous verrons comment ces politiques sont souvent couplées à un financement militaire important visant le renforcement des capacités des forces armées des pays en question.

Enfin, nous étudierons trois cas de projection de la force dans le cyberespace par ces pays. Le premier a trait à la diplomatie et au renseignement, le second est lié à la cyberguerre et aux conflits armés traditionnels, le troisième et dernier est le cas de l'espionnage industriel dans cet espace.

1. Politiques éducatives et projections de force dans le cyberespace

Le concept de « massification de l'éducation » est défini comme étant un phénomène de forte croissance de l'accès à l'éducation par les populations. Une mobilité sociale importante, une croissance économique forte et des changements sociétaux profonds font également partie des contextes permettant l'apparition du phénomène de massification. Dans le cas des États-Unis (et en bonne partie de l'Europe), cette massification s'est effectuée après la Seconde Guerre mondiale (GUMPORT et al. 1997). La massification dépasse donc ainsi la seule reproduction d'une élite universitaire formée à des tâches spécifiques et étant restreinte à un petit nombre des

citoyens. Il s'agit d'une forme de démocratisation de l'accès aux études supérieures (Teichler 1998, 19).

Dans les cas que nous étudions, ces mutations sociales sont à l'œuvre et viennent changer la façon dont la société et l'économie fonctionnent. Les pays émergents ont connu dans les dernières décennies de profondes mutations liées à la mondialisation et à la généralisation de la division internationale du travail. L'apparition de technologies comme Internet a également changé rapidement les pratiques et référents culturels dans ces pays (Mok 2012).

Avec en moyenne près de 20% de scolarisation supérieure (contre par exemple plus de 60% pour Hong-Kong, voir Wan 2011), l'Asie de l'est a connu une massification rapide – mais inégale – de l'éducation afin de répondre aux besoins de développement économique des pays de la région. L'éducation primaire et secondaire a également servi à créer un sentiment d'unité nationale (Ramesh 2004, 186) dans différents pays marqués par une indépendance récente. Ce n'est qu'à la fin des années 1990 que l'éducation a été placée au centre des politiques de développement, notamment en lien avec l'adoption d'accords de libre-échange et l'apparition de l'Organisation mondiale du commerce (à ce propos, voir Miyahara 2015).

Cette zone reste toutefois marquée par de profondes disparités. Dans son étude de 2012 sur l'éducation en Asie de l'est (Gropello, Yusuf et Tandon 2012), la Banque mondiale établissait trois sous-groupes de pays en fonction de leur niveau de développement. Hong-Kong, le Japon, la Corée ainsi que Singapour et Taïwan faisaient partie du premier groupe, le plus développé. La Chine, l'Indonésie, la Malaisie, la Mongolie, les Philippines et la Thaïlande faisaient partie du second groupe avec des économies moyennes-inférieures (à l'exception de la Malaisie qui se trouve dans la classe moyenne supérieure). Enfin, le troisième et dernier groupe était composé du Cambodge, du Laos et du Vietnam. Ce groupe de pays connaissant des

processus de modernisation encore en cours (Gropello, Yusuf et Tandon 2012, 7). Si la situation a évolué depuis 2012, ces sous-groupes restent relativement fidèles à la réalité économique. Ces disparités ne sont pas négligeables quand il s'agit d'étudier les questions liées à la montée en puissance de certains pays comme les BRICS. En effet, le niveau de développement et d'intégration dans le système international conditionne grandement les politiques internes et extérieures de ces pays. Certains, profitant plus de la mondialisation ont des intérêts différents d'autres qui sont plus marginalisés ou qui ne tirent pas leur épingle de la division internationale du travail. Il s'agit d'un facteur important pour comprendre comment, pourquoi et à quelles fins ces pays projettent ou non de la force dans le cyberespace.

Comme pour le développement économique, la Banque mondiale a dégagé trois ensembles de pays se distinguant par leur niveau de développement technologique (Gropello, Yusuf et Tandon 2012, 8). Le premier groupe de pays, composé de Hong-Kong, du Japon, de la Corée du sud, de Singapour et de Taïwan, s'est concentré sur une production manufacturière depuis le début des années 1960 puis a orienté son développement vers des industries à concentration plus élevée (technologies, services, etc.). Ce sous-groupe correspond au groupe de pays ayant les revenus supérieurs. Ce développement s'est notamment fait grâce aux innovations ainsi qu'à l'accumulation de capital de façon rapide.

Le second groupe, composé de la Chine, de l'Indonésie, de la Malaisie, des Philippines et de la Thaïlande, est très hétérogène. Certains pays se sont basés sur le développement de la production technologique et de l'électronique (Chine, Malaisie, Philippines et Thaïlande), d'autres dans des industries manufacturières (Indonésie, Philippines) et enfin, d'autres dans des secteurs agroalimentaires (Indonésie). Ces pays ne sont pas pour autant des producteurs de technologie à proprement parler puisqu'ils ne font souvent qu'assembler des pièces conçues ailleurs. Dans chaque sous-groupe existent également des différences importantes en matière de

développement et d'effort mis dans la recherche et l'innovation. La Chine se distingue par exemple des autres pays dans son groupe (Gropello, Yusuf et Tandon 2012, 9), notamment par un important financement étatique de la recherche dans les secteurs des technologies de l'information et des télécommunications mais aussi de la défense.

Le troisième groupe, composé du Vietnam, du Cambodge, du Laos et de la Mongolie est marqué par un faible développement technologique et des économies à faible rendement. Ces pays semblent être plus en retard dans à peu près tous les domaines et ne bénéficient que peu de la division internationale du travail.

Depuis 2012, les dynamiques de formation de la population ainsi que d'investissement technologique se sont accélérées (World Bank 2014; World Bank 2015). Ce développement s'appuierait notamment sur des institutions publiques et des centres étatiques de technologie. Il faut toutefois noter que dans des territoires développés historiquement comme Hong-Kong, de nombreux chercheurs notent un phénomène de post-massification visant à plus encadrer l'accès aux études supérieures et à la formation spécialisée (Jung et Postiglione 2015).

Dans le cas spécifique de la Chine (comme pour Hong-Kong avant elle, voir Post 1996), la transition vers la massification de l'éducation s'est effectuée au début des années 1990 (Hayhoe et al. 2011) sous l'impulsion de Den Xiaoping. Il s'agissait alors de bénéficier d'une main d'œuvre qualifiée afin de favoriser le développement économique. Cette massification s'est notamment effectuée en incitant la population à suivre les valeurs confucéennes dans lesquelles l'éducation est une richesse et un pouvoir (bien que l'enseignement professionnel tende à être en opposition aux principes du confucianisme. Voir Xiong 2011). Entre 1998 et 2008, le taux de scolarisation supérieure est ainsi passé de 9% à 23.3%, soit une accélération plus rapide que ce qu'avait pu vivre les États-Unis ou le Japon sur des périodes bien plus

longues (Hayhoe et al. 2011, 28). La population éduquée de la Chine est également devenue la plus importante en volume dans le monde (Hayhoe et al. 2011, 27).
Le nombre d'institutions d'enseignement supérieur a également explosé pendant cette période, passant de 1022 en 1998 à 2263 en 2008, soit une augmentation de 121,4%. Bien que ces universités et institutions aient largement été encouragées à s'adapter aux besoins locaux, de nombreuses disparités sont apparues entre les différentes provinces et dans le support que l'État central leur a apporté (à ce sujet, voir l'étude de cas très complète par Gong et Li 2010).

Dans le reste des BRICS, le niveau de scolarisation de la population a également vu une augmentation significative (Schwartzman, Pinheiro et Pillay 2015). Entre 1999 et 2007 le Brésil, a vu le taux de formation supérieure passer d'environ 14% à 30% de la population, alors qu'elle s'est maintenue à des taux élevés de près de 75% en Russie (Sheng-jun 2011, 192). La Russie se distingue d'ailleurs des autres pays des BRICS dans la mesure où les politiques de massification de l'éducation ne sont pas nouvelles puisqu'elles faisaient partie des orientations mises en avant par l'Union Soviétique. Toutefois, la dynamique de massification a évolué avec le déclin démographique et les changements structurels s'effectuant dans l'économie russe. Seule l'Inde semble être vraiment aux prises avec un système d'éducation supérieure figé et difficile à réformer.

Si la qualité de la formation est loin d'être uniforme et reconnue par tous, il reste toutefois que par leur importance les BRICS seraient devenus des acteurs clés dans le système international et dans le milieu universitaire (à ce sujet, voir Altbach 2013). À titre d'exemple, la Chine et l'Inde à elles-seules forment plus d'ingénieurs et de travailleurs qualifiés que l'occident (Kramer, Starr et Wentz 2009, 8).

Un autre aspect important de la formation supérieure pour les pays émergents est la grande circulation d'étudiants entre ces pays. La Russie s'est notamment distinguée

en accueillait près de 186 00 étudiants étrangers en 2014 (*The Moscow Times* 2015) et en ayant une de ses universités se plaçant dans le haut du classement des universités des BRICS et pays émergents mis en place par le *Times higher education (Times Higher Education* 2015). La Chine avait quant à elle près de 712 000 de ses étudiants qui menaient des études à l'étranger en 2014 (UNESCO Institute for Statistics 2012). Parmi les destinations préférées des Chinois en 2008-2009 se trouvaient de nombreux pays occidentaux, mais aussi des pays comme Singapour ou la Russie (China Scholarship Council 2009). Il en était de même pour les étudiants sud-africains qui fréquentaient de façon massive des institutions dans des pays émergents (Cuba, Brésil, etc.). Si dans la majorité des cas, les États-Unis recevaient la plus grande partie de ces étudiants en échange, il reste que la mobilité internationale et la coopération universitaire entre ces pays tend à se développer et pourrait représenter un avantage significatif dans la construction d'une alliance ou d'une identité commune.

Il est donc clair que les politiques d'éducation vont encore jouer un rôle important dans le développement économique et la compétitivité de ces pays. Que ce soit en passant par la scolarisation et le développement d'une main-d'œuvre qualifiée, le financement étatique de la recherche, ou encore un meilleur arrimage aux demandes du marché (par exemple dans le cas de Hong-Kong qui est frappé par un important taux de chômage des populations éduquées) ces politiques devraient faire partie des considérations stratégiques pour la projection de la force dans les relations internationales par ces pays. Cette dynamique est d'autant plus remarquable que nombreux sont les pays d'Occident où l'éducation est perçue comme un poids sociétal à assumer et non comme une richesse. La restriction de l'accès à l'éducation dans ces pays semble ainsi être une dynamique contre-productive défiant toute logique.

Rappelons également que dans un espace malléable comme le cyberespace, la

question de la formation de la main d'œuvre est importante puisqu'elle permet d'utiliser à son avantage cette caractéristique. En formant un grand nombre de travailleurs qualifiés et aptes à utiliser les technologies de l'information et des télécommunications, ces pays pourraient en effet développer des avantages dans la conduite d'opérations dans le cyberespace (Kramer, Starr et Wentz 2009, 41).
Il faut toutefois noter que, malgré les politiques de massification de l'éducation supérieure, les universités ne fourniraient pas toujours suffisamment le marché en main-d'œuvre qualifiée. En effet, dans certains cas l'accès à l'éducation serait encore trop limité pour répondre aux besoins d'un développement technologique avancé et permettant une modernisation économique.

> Some countries urgently need to grow their higher education systems in terms of enrollment. In most countries there is scope to enhance equitable access to widen the talent pool, and the share of graduates in science, technology, engineering, and mathematics (STEM) remains too low to support much technological capability (Gropello, Yusuf et Tandon 2012, 59)

Si cette pénurie de main d'œuvre qualifiée peut avoir des conséquences sur la compétitivité internationale et sur le développement économique, la projection de force dans le cyberespace ne semble pas particulièrement affectée. Pour être efficace, il n'est pas besoin d'un grand nombre d'acteurs militaires ou civils. L'espionnage industriel pourrait également être une façon rapide pour ces pays d'utiliser les populations déjà formées et compétentes, sans nécessairement dépendre du développement de centres de technologie ou d'Investissements directs à l'étranger (IDE). Ces deux paramètres sont d'autant plus importants que même si certains pays ne fournissent pas encore assez de diplômés, ils arrivent toutefois à se distinguer sur le plan de l'innovation et de la recherche.

Enfin, soulignons que l'enseignement technologique est souvent accompagné par un investissement marqué dans les secteurs de la recherche et développement, les

gouvernements et militaires en ayant fait un secteur stratégique pour la poursuite de leurs intérêts.

Dans le cas de la Chine, le PCC a notamment mis l'accent sur le financement de la recherche pouvant lui être utile dans le cyberespace et dans la projection de la force dans le système international en général.

> The PRC government actively funds grant programs to support CNO related research in both offensive and defensive in orientation at commercial IT companies and civilian and military universities. A review of PRC university technical programs, curricula, research foci, and funding for research and development in areas contributing to information warfare capabilities illustrates the breadth and complexity of the relationships between the universities, government and military organizations, and commercial high-tech industries countrywide (Kramer, Starr et Wentz 2009, 287).

C'est notamment avec le concours de l'APL (Armée Populaire de Libération), de ses centres de recherche ainsi qu'avec les partenariats entre universités et sociétés d'État que la Chine a pu développer rapidement et de façon organisée des technologies d'attaque et de défense dans le cyberespace et plus largement dans le secteur militaire (Krekel, Adams et Bakos 2012, 59). Que ce soit aux plans électronique, informatique ou même dans la logistique d'armement classique, les universités et centres de recherche aident l'APL à se moderniser de façon rapide, là où ailleurs l'armée aurait fait appel au secteur privé à des coûts beaucoup plus élevés. Il y avait ainsi en 2009 près de 3707 centres de recherche dans tous les domaines faisant travailler près de 32,3 millions de personnes dans le pays (Krekel, Adams et Bakos 2012, 67). Cela faisait alors de la Chine une des premières puissances mondiales en matière de recherche.

En plus d'avoir une collaboration importante avec un grand nombre de centres de recherche et d'universités, l'APL collabore avec des entreprises afin de se doter

d'infrastructures adéquates et limiter sa dépendance aux technologies étrangères. Ainsi, le secteur des technologies de l'information en Chine serait un hybride entre secteur commercial et industrie devant répondre aux besoins militaires nationaux (Krekel, Adams et Bakos 2012, 68).

Cet enchevêtrement du secteur privé et du secteur militaire ferait en sorte que 90% des entreprises spécialisées dans les TI fourniraient l'APL. Des groupes comme ZTE, Huawei ou Datang collaboreraient avec l'APL dans l'approvisionnement en matériel militaire dérivé de productions civiles. Comme le souligne Arpagian, « l'imbrication des sphères économiques et politiques en Chine assure à la classe dirigeante une puissance d'intervention considérable en matière de technologies innovantes » (Arpagian 2009a, 195) et donc une série d'avantages quant à la capacité de projection de force dans le cyberespace. Cette proximité entre sphères militaire et commerciale a notamment mené à l'interdiction de vente pour certaines de ces compagnies aux États-Unis et au Canada, de peur de voir des dispositifs secrets de contrôle être activés en cas de conflit.

Cette imbrication se voit également dans d'autres pays émergents, qui mettent l'accent sur la création d'un complexe militaro-industriel puissant et travaillant de concert avec les armées nationales. Le développement de fleurons industriels dans les secteurs technologiques et dans l'aérospatiale est également important,

Ainsi, il semble clair que la massification de la formation supérieure, même si elle n'a pas forcément livré toutes ses promesses, représente un avantage humain considérable pour les pays émergents. Que ce soit en favorisant l'innovation et la compétitivité internationale ou en permettant le développement d'un secteur de la recherche dynamique, les politiques publiques en éducation et en recherche pourraient permettre à des pays émergents comme les BRICS de projeter de la force dans le cyberespace de façon efficace et peu onéreuse. Afin de comprendre comment

ces stratégies peuvent être exercées, nous nous intéresserons à quelques utilisations des technologies présentes dans le cyberespace.

2. Exemples d'utilisation des technologies du cyberespace par des pays émergents dans le système international

Une des premières caractéristiques partagées par les pays que nous étudions est leur position d'acteur important dans le système international, sans en être dominant. Nous nous pencherons ici sur les cas de la Chine et de la Russie. Ces deux pays sont membres permanents du Conseil de sécurité de l'ONU et sont des pôles de puissance dans leur zone d'influence, mais n'ont pas le titre d'hégémon mondial puisque les cas récents où ces deux puissances ont projeté de la force restent relativement limités pour le moment.

Par ailleurs, même si la Chine profite largement de la division internationale du travail et développe une industrie nationale forte, elle ne pourrait pas se passer de l'Occident pour le moment. Ses capacités industrielles étant majoritairement orientées vers une sous-traitance de la production des entreprises multinationales occidentales et le marché interne étant encore lui-même assez limité, le développement économique de la Chine repose sur son intégration dans le capitalisme mondialisé.

De même, si la Russie est partiellement capable de se passer du commerce international, elle reste liée aux autres États, étant largement dépendante de la vente et de l'exportation de matières premières (carburant, gaz, bois, métaux, etc.). Dans le cas russe, la fragilité économique vient également de la désindustrialisation forcée opérée par l'Occident après la chute de l'URSS. Que ce soit les réformes néolibérales (« thérapie du choc »), les privatisations massives, la libération des prix et des

changes, l'ouverture du commerce extérieur et le démantèlement du complexe industriel, la Russie a vécu une importante destruction de son économie tout au long des années 1990 (Gerber et Hout 1998). Cette destruction du modèle social et économique a également eu des impacts sur la population, en faisant baisser le taux de scolarisation, en augmentant le taux de mortalité et en engendrant un chômage important (Klein et Pomer 2001). Le recul social s'est donc manifesté de façon frappante lors de l'application de la thérapie du choc dès le début des années 1990 (certains sont allés jusqu'à qualifier ces réformes de « génocide économique », voir Bohlen 1992).

Malgré leur place formelle dans le système international, ces deux puissances en particulier ont vu leur rôle fluctuer à la fin de la guerre froide. Ce n'est que depuis quelques années que la Chine et la Russie ont recommencé à s'engager dans des politiques plus militaristes et impérialistes dans leurs zones d'influence. Le cyberespace est notamment devenu un espace de choix pour le pays (voir Limonier 2014).

On a ainsi vu la Russie s'attaquer à des pays comme la Tchétchénie (1999-2009), l'Estonie (2007), la Géorgie (2008), ou encore l'Ukraine (2014 -). Que ce soit de façon directe (par des invasions armées) ou indirecte (par l'allégué piratage et obstruction de services gouvernementaux en Estonie en 2007), la Russie a mené une politique d'annexion et d'expansion dans sa zone d'influence. Par le fait même, elle a également tenté de limiter l'influence de l'OTAN dans la région. Les dernières années ont donc été marquées par une inflation verbale de la rhétorique du conflit et de l'opposition entre Russie et Occident, accompagnée par des excursions menaçantes de l'armée russe dans l'espace aérien et les eaux internationales.

La Chine n'est pas en reste puisqu'elle a aussi pris des mesures pour moderniser son armée et être capable de projeter de la force dans sa zone d'influence étendue (en mer

de Chine et dans le Pacifique, notamment). Que ce soit par l'acquisition et la production de matériel militaire de pointe ou par la politique de construction d'ilots artificiels dans les eaux internationales afin de clamer les droits sur ces zones (Stone Fish et Johnson 2015), la Chine a tenté de marquer son territoire et sa zone d'influence par de nombreux moyens. De nombreux incidents ont également été répertoriés dans l'espace aérien et les eaux internationales (Thornhill et Reuters 2015).

Dans tous ces cas, les technologies du cyberespace peuvent être utilisées afin de projeter de la puissance et tenter d'influencer les autres acteurs en présence. Nous étudierons ici trois utilisations majeures de cyberinfluence et de projection de la force dans le cyberespace. La première concerne les relations diplomatiques et le *soft power*; la seconde est celle de la cyberguerre et du soutien aux autres formes de guerre; et la troisième est liée au cyberespionnage et à l'espionnage industriel dans le cyberespace.

2.1 Diplomatie et renseignement

Une des façons d'utiliser les technologies présentes dans le cyberespace pour des acteurs non dominants dans le système international est la projection de force par le biais de la cyberinfluence.

Ainsi, dans le système international, certains acteurs ont décidé d'intégrer la cyberinfluence à leurs stratégies de politique étrangère et de développement. Plutôt que de passer par des affrontements militaires classiques ou des confrontations directes dans le système international, certains États décident de faire de la propagande ou des campagnes de guerre de l'information dans le cyberespace. Par l'utilisation des technologies présentes dans le cyberespace, ces acteurs espèrent faire avancer leurs idées et gagner du soutien parmi les autres acteurs. Dans cette

utilisation du *soft power*, les populations civiles sont tout autant interpelées que les décideurs politiques et autres acteurs en présence. Ce contact direct peut servir de levier pour convaincre d'autres acteurs de se rallier à une position en particulier. Cette forme d'exercice de la cyberinfluence revêt en partie le même caractère que les campagnes d'influence dans les autres sphères des médias d'information (télévision, radio, presse écrite) ou encore que les manifestations visant à défendre une cause en particulier. Il y a toutefois une individualisation du processus qui permet à des acteurs non étatiques d'exercer cette cyberinfluence et de joindre de larges populations facilement, ce qui n'est pas le cas avec les médias traditionnels, qui sont majoritairement contrôlés par des intérêts capitalistes et plus facilement soumis à la censure.

La grande porosité et l'omniprésence du cyberespace permettent donc à des acteurs étatiques et privés de s'exprimer et de joindre facilement des populations qui étaient autrefois beaucoup plus difficiles d'accès. On peut y voir une prolongation de la diplomatie classique, dans la mesure où le cyberespace sert dans ces cas essentiellement à prolonger des pratiques déjà existantes. Certains cas ont également permis de voir que l'utilisation de moyens discrets dans le cyberespace peut permettre une certaine forme de *soft power*, visant à menacer des acteurs sans nécessairement passer par une projection classique de la force.

2.1.1 Le cas de la Corée du Nord

L'exemple de l'utilisation des technologies du cyberespace par la République populaire démocratique de Corée (RPDC, ci-après, Corée du Nord) est une illustration de projection de cyberinfluence à des fins de politique intérieure et internationale.

Dans les dernières années, la Corée du Nord a fait un usage croissant des technologies du cyberespace afin de mener des opérations de guerre de l'information ou de perturbation des activités de ses adversaires. Par exemple, en 2009 une attaque fut menée contre les États-Unis et la Corée du Sud dans le but de perturber les cérémonies du 4 juillet, ainsi que d'empêcher le fonctionnement normal des institutions économiques majeures (Clarke et Knake 2010, 24). Ces attaques massives, mais peu sophistiquées, n'eurent que peu d'impact, autre que symbolique et qu'un dérangement temporaire de certains services. Il s'agissait toutefois d'une des premières formes d'agression nord-coréenne dans le cyberespace menée à des fins politiques et de propagande. Même si l'attaque n'a pas eu les effets escomptés, l'utilisation de ces événements à des fins de propagande interne a été bénéfique au régime.

Cette cyberattaque était la première d'une longue série se poursuivant jusqu'à maintenant. La Corée du Nord aurait ainsi intégré cette projection de puissance dans ses façons de mener sa diplomatie, notamment face à l'Occident avec lequel elle est en conflit. L'utilisation de ces moyens est intéressante pour un pays comme la Corée du Nord puisque la riposte ne peut être que faible. Il serait par exemple difficile de justifier une réplique militaire contre la Corée du Nord pour de telles cyberattaques, et encore plus difficile de l'attaquer dans le cyberespace puisqu'elle n'a que peu d'infrastructures (Clarke et Knake 2010, 26). L'armée nord-coréenne aurait en fait près de 600 hackers à son service, regroupés en plusieurs unités (Clarke et Knake 2010, 27). Comme pour d'autres régimes comme la Chine, la Corée du Nord aurait également des unités de guerre psychologique se concentrant sur la guerre de l'information. Ces deux pays seraient d'ailleurs étroitement liés dans ces moyens d'actions puisque des unités nord-coréennes utiliseraient régulièrement la Chine comme base pour mener leurs opérations.

La Corée du Nord aurait par ailleurs mis en place un réseau de formation et

d'enrôlement de personnels capables d'agir dans le cyberespace dès le plus jeune âge. Cette formation d'une main d'œuvre qualifiée est conséquente avec les ressources nécessaires dans le cyberespace afin de pouvoir projeter de la puissance, puisqu'il est bien plus intéressant de disposer de capital humain que de matériel militaire ou d'argent dans ces opérations.

Au niveau de la conduite de la politique étrangère nord-coréenne, il y aurait, dans ces attaques, une façon de signifier aux pays occidentaux ou ennemis que, malgré une infériorité militaire évidente, la Corée du Nord pourrait tout de même se défendre ou riposter:

> The message was : I am still in charge and I can make trouble with weapons that can eliminate your conventional superiority (Clarke et Knake 2010, 29).

Ces attaques auraient également pour but de mesurer la capacité de la Corée du Sud à se défendre et de tester la résistance du réseau. La Corée du Nord pourrait par exemple se servir de cyberattaques afin d'isoler les réseaux de communication de la Corée du Sud, qui servent également à l'armée américaine dans la région. En cas d'attaque conventionnelle contre la Corée du Nord, cette dernière pourrait alors potentiellement perturber les opérations ennemies par ce biais. Les cyberattaques menées par la Corée du Nord pourraient également permettre de cibler des infrastructures sensibles au sud, et seraient potentiellement dévastatrices. Ces attaques pourraient servir différents types de politiques étrangères sans avoir besoin de mobiliser trop de ressources militaires conventionnelles.

Plus récemment, le piratage massif de Sony suite à la sortie du film *The Interview* tournant au ridicule la Corée du Nord, a souligné à quel point les cyberattaques pouvaient servir des objectifs de politique étrangère. Ces attaques massives ayant mené à la publication d'une grande quantité de documents internes à la compagnie a

entaché la réputation de cette dernière. Si le rôle de la Corée du Nord n'a jamais été prouvé publiquement (le FBI a affirmé avoir des preuves solides pointant vers la Corée du Nord. Voir Flitter 2015) et que cette dernière a réfuté être à l'origine des attaques (Sang-hun 2014) – allant jusqu'à proposer une enquête conjointe Corée du Nord et États-Unis (D'Orazio 2014a) – un ensemble d'acteurs a désigné le pays comme étant responsable. Une étude d'une firme de sécurité informatique a d'ailleurs évoqué la possibilité que des pirates russes soient responsables de ces attaques (Taia Global 2014; Kopan 2014).

Dans ce cas, la construction de la menace et du discours, qui a été forte pour convaincre le grand public et d'autres acteurs de la responsabilité de la Corée du Nord, a presque mené à une crise internationale majeure. Les États-Unis ont notamment menacé de façon véhémente le « royaume ermite », que ce soit en demandant plus de sanctions contre le pays ou encore un durcissement législatif contre les cyberattaques (Robertson 2014a). Les États-Unis ont également été accusés d'avoir provoqué d'importantes perturbations de l'Internet en Corée du Nord dans les semaines suivant la publication des documents volés (D'Orazio 2014b; Siddique 2015).

Ces différents cas d'utilisation de technologies du cyberespace dans la conduite de la diplomatie sont intéressants afin de comprendre comment ces stratégies pourraient permettre à des acteurs non dominants d'intervenir dans le système international. Notons à cet effet que la Corée du Nord n'est clairement pas le pays le plus actif dans le cyberespace. Utilisées par des pays plus aptes à développer ces types de stratégies, les technologies présentes dans le cyberespace pourraient devenir d'importants leviers politiques et diplomatiques.

2.1.2 L'Estonie – 2007

En plus de l'utilisation de stratégies de cyberinfluence par certains acteurs, le cyberespace a également été investi dans des cas de conflits internationaux entre États sans qu'il y ait une escalade vers un conflit armé.

Dans ces cas, l'utilisation de moyens offensifs dans le cyberespace est souvent assez importante pour perturber de façon efficace un certain nombre d'activités civiles et étatiques, sans nécessairement risquer une réplique militaire classique. En ce sens, ces cyberattaques peuvent servir de représailles ou de moyens de pression dans des conflits où une intervention armée serait difficilement justifiable. Cette utilisation de technologies du cyberespace est particulièrement intéressante pour des pays émergents qui pourraient la mettre en œuvre pour dénoncer ou décourager des acteurs du système international nuisant à leurs intérêts.

Un des exemples les plus frappants de cette utilisation de la cyberinfluence et des cyberattaques dans des questions de politique internationale est le cas de l'attaque contre l'Estonie en 2007. Après que cette dernière eut décidé de déplacer un monument aux morts russes de la Seconde Guerre mondiale, suscitant ainsi une indignation généralisée chez les russophones du pays et de la Russie (qui considère avoir « libéré » l'Estonie à la fin de la guerre), une vague de cyberattaques a commencé à paralyser le pays. Les principaux serveurs qui traitaient les services Internet du gouvernement ainsi que d'entreprises privées ont été l'objet d'attaques de saturation (déni de service) venant de l'extérieur du pays. Des secteurs d'activités comme les services bancaires, les sites d'information et les services gouvernementaux sur Internet ont ainsi été touchés et rendus inutilisables pendant des semaines. Ces attaques de déni de service très efficaces utilisaient des milliers – voire des dizaines de milliers - d'ordinateurs infectés. Par la suite, les attaques évoluèrent vers des serveurs liés à des infrastructures clés comme les réseaux de téléphonie ou de

paiement en ligne.

> Then the botnets started targeting Internet addresses most people would not know, not those of public webpages, but the addresses of servers running parts of telephone network, the credit-card verification system, and the Internet directory. (Clarke et Knake 2010, 15)

Plus d'un million d'ordinateurs « zombies » participaient alors à l'attaque, paralysant la quasi intégralité des services gouvernementaux. Ces cyberattaques à grande échelle ont donc eu un effet important sur un ensemble d'acteurs en Estonie. Il ne s'agissait toutefois pas d'une cyberguerre puisque le but des attaques n'était pas de détruire, mais seulement de paralyser et de déranger le fonctionnement normal des activités présentes dans le cyberespace. Dans ce cas, c'est notamment la dépendance du pays à Internet et aux applications numériques qui a conduit à une utilisation efficace des cyberattaques (Clarke et Knake 2010, 13).
Ce cas de cyberattaques représente bien la vulnérabilité inhérente aux technologies employées dans le cyberespace, ainsi que la pertinence pour certains acteurs d'utiliser ces tactiques de cyberinfluence et de perturbation.

L'enquête sur ces attaques permit de remonter jusqu'en Russie, sans pour autant réussir à prouver l'implication formelle du gouvernement de la Fédération de Russie. Malgré tout, de nombreux acteurs ont souligné la passivité des services de renseignement et des policiers russes dans le cadre de ces attaques. D'autres ont également noté qu'il est peu probable que le gouvernement russe n'ait pas eu connaissance de ces attaques considérant la surveillance qu'il fait des réseaux dans le cyberespace. Par ailleurs, de telles cyberattaques répondaient alors assez bien aux orientations de la politique étrangère russe concernant la crise en Estonie. Qu'il s'agisse de l'œuvre de groupes nationalistes russes ou russophones ou encore des services de renseignement russes, ces cyberattaques ont permis de manifester une forme de puissance dans la zone d'influence de la Russie. Cela a également envoyé

un signal fort sur les capacités de perturbation des différents acteurs en présence afin d'inciter l'Estonie à ne pas récidiver ou d'aller de l'avant avec ses politiques de « *désoviétisation* » et de discrimination envers la population russophone du pays.

Ces formes de cyberinfluence peuvent donc être utilisées dans des cas d'affrontements entre acteurs sur des questions de politique nationale ou internationale, sans nécessairement mener à des interventions armées. Il s'agit à notre avis d'excellents outils à la disposition de pays non dominants dans le système international. Que ce soit pour tenter d'influencer d'autres acteurs ou de poursuivre des buts diplomatiques, ces moyens pourraient favoriser l'émergence de rapports de force plus favorables aux pays émergents face aux puissances occidentales.

2.1.3 Utilisation de la cyberinfluence à des fins de politique internationale ou nationale

Le cyberespace et les vulnérabilités qui y sont inhérentes peuvent également être utilisés par différents acteurs afin d'influencer des questions de société. Cette démocratisation de la parole politique et des enjeux sociétaux sur Internet et dans le cyberespace en général pourrait être un vecteur de changement politique important pour de nombreuses sociétés ainsi que pour le système international dans son ensemble.

Par exemple, en 2009, le « climategate » avait suscité de vives réactions après la publication de courriels et de document dérobés au groupe de recherche sur le climat de la *University of East Anglia* par des pirates informatiques non identifiés (Hickman 2012). Des échanges de courriels et de documents avaient été utilisés par un ensemble d'acteurs climato-sceptiques afin d'influencer les discussions autour du sommet de

Copenhague sur le climat. Des entreprises privées, des groupes d'intérêts et autres acteurs réfutant les théories scientifiques concernant le réchauffement climatique avaient ainsi déployé un ensemble de moyens de cyberinfluence afin de tenter de discréditer les scientifiques travaillant sur ces questions. L'objectif était de convaincre les populations ainsi que les décideurs politiques de ne pas prendre de mesures pouvant réduire l'activité humaine en lien avec les émissions de gaz carbonique.

Si ces stratégies de cyberinfluence se sont révélées inefficaces dans la perception que le public a des changements climatiques (Carrington 2014), ou encore sur le résultat du sommet de Copenhague (Scher 2009), il s'agissait d'un des premiers cas d'attaque orchestrée avec minutie afin de tenter d'influer sur des questions de politique internationale.

D'autres cas ont également été répertoriés dans ce type d'utilisation de la cyberinfluence. Le collectif *Anonymous* s'est par exemple distingué au cours des dernières années par la façon dont il a pu attaquer des acteurs (États, entreprises privés, individus, etc.) perçus comme ayant posé des actes répréhensibles. Un autre collectif, *LulzSec*, s'est quant à lui démarqué par une liste impressionnante de piratages d'entreprises privées et d'organisations gouvernementales avant d'être démantelé par le FBI.

Les opérations de ce type de collectifs peuvent viser un ensemble de sujets et d'acteurs et sont susceptibles de générer des conflits ou des interférences importantes dans le système international. En ce sens, la dématérialisation des frontières et l'émergence d'une culture globale liée à l'Internet a favorisé l'apparition de nouveaux mouvements sociaux ou politiques utilisant les technologies présentes dans le cyberespace afin de diffuser leur point de vue ou appliquer une certaine forme extra-étatique de justice du peuple. En intervenant dans des situations internationales, ces

groupes peuvent également diffuser de façon assez efficace un discours et une construction sociale de la menace ou des acteurs en présence et ainsi influer sur leurs actions et sur l'issue de ces situations.

2.1.4 Renseignement civil et militaire

Le cyberespace est également marqué par une grande utilisation de moyens de surveillance et d'espionnage à des fins de renseignement civil ou militaire. De nombreux acteurs étatiques et non-étatiques (entreprises, alliances militaires, organisation internationales, etc.) utilisent des technologies présentes dans le cyberespace afin d'acquérir de l'information.

Que ce soit la surveillance généralisée des réseaux dans le cyberespace par les États-Unis (notamment révélés par Edward Snowden) ou celle du Canada afin de faire respecter des droits d'auteurs mis en avant par des lobby commerciaux (Gallagher et Greenwald 2015) et « lutter contre le terrorisme » (Braga 2015), ou encore l'espionnage par la Nouvelle-Zélande des différents acteurs présents dans sa zone d'influence (Gallagher 2015), ou même celle de l'Australie envers des journalistes et officiels (Mitchell 2015), le cyberespionnage est un aspect capital du renseignement des États. À tel point que le Royaume-Uni aurait surveillé et « scanné » des pays entiers afin de se procurer de l'information (voir l'article sur le programme « HACIENDA », Kirsch et al. 2014). Ces capacités d'espionnage seraient tellement avancées que les États-Unis et certains de ses alliés auraient pu accéder à un ensemble de dispositifs de communication, qu'ils soient privés ou publics, s'accaparant de précieuses informations parmi une masse diffuse de données (Sottek 2015).

Cette forme de cyberespionnage peut également prendre la forme de la surveillance

d'entreprises privées afin d'obtenir des secrets industriels ou mieux pouvoir pirater les technologies vendues par ces entreprises (comme le cas d'Apple qui a été piraté par la CIA afin de pouvoir mieux surveiller les produits vendus - et ses utilisateurs - par la compagnie. Voir Scahill et Begley 2015). Ce sont d'ailleurs souvent les entreprises produisant des produits technologiques qui sont ciblées en premier, afin de mieux s'introduire dans un ensemble de dispositifs par la suite, tels que les cellulaires (le Canada fait d'ailleurs bonne figure dans ce domaine avec son programme « BADASS », voir Lee 2015), ou encore des opérateurs téléphoniques étrangers (*Le Monde 2014)*.

Cette surveillance généralisée n'est pas le fait des seuls pays occidentaux, même si ceux-ci ont été sur la sellette dans les dernières années. Des pays non dominants mais ayant une certaine influence, comme les BRICS, sont également pointés du doigt pour leurs pratiques de surveillance. La Russie aurait par exemple espionné des gouvernements étrangers pendant des années grâce à des logiciels pirates (Zetter 2014b; Symantec Security Response 2014) alors que la Chine aurait installé des centres de surveillance de l'Internet à Cuba (Clarke et Knake 2010, 58).
Parallèlement à ces réseaux de surveillance, des États (que l'on soupçonne largement être la Chine et la Russie) ont mené des opérations de détournement majeur de données transitant par Internet (à ce sujet, voir l'excellent article technique de Cowie 2013), dans le but d'intercepter des données sensibles et de l'information pertinente pour des opérations de renseignement. De nombreux incidents de ce type ont été répertoriés dans les dernières années, menant parfois au détournement d'informations capitales pour la sécurité nationale et aux activités militaires. Cela a notamment été le cas pour les dispositifs de commande nucléaire du Royaume-Uni en mars 2015 (Griffin 2015) qui ont été redirigées vers l'Ukraine pendant au moins une semaine. D'autres cas ont vu des détournements importants du trafic russe vers la Chine (Madory 2014). Il ne s'agit là que des incidents répertoriés et rendus publics, les détournements plus ciblés et de courte durée étant presque impossibles à détecter.

Le renseignement militaire ou civil peut également se faire par le piratage de réseaux entiers appartenant à des États ou des entreprises. La Chine aurait par exemple réussit à infecter des milliers d'ordinateurs, dont des infrastructures diplomatiques et gouvernementales (Clarke et Knake 2010, 59). Plus récemment, le pays aurait ciblé les États-Unis afin de bâtir des bases de données de fichiers de renseignement portant sur divers sujets (identité de citoyens américains, données publiques, informations se trouvant dans des systèmes gouvernementaux, etc., voir Nakashima 2015). Les bases de données concernant les informations personnelles de tous les employés du gouvernement fédéral américain auraient notamment été compromises (Franceschi-Bicchierai 2015b), tout comme un grand nombre d'informations militaires (Dilanian et Bridis 2015). Ces données pourraient remonter jusqu'en 1985, offrant une grande quantité d'information pour les pirates (Shalal et Spetalnick 2015), forçant même le Département d'État américain à arrêter temporairement de produire des documents de voyage tels que les passeports ou les visas d'entrée sur le territoire (Knibbs 2015). Si l'attribution de ces attaques n'a pas pu être effectuée avec certitude, tous les regards sont tournés vers la Chine. Ces données seraient pertinentes pour un État comme la Chine puisqu'elles permettraient de mieux cibler les sphères de pouvoir et de responsabilités. Il serait également possible pour les pirates responsables du vol de mieux articuler des stratégies de *social engineering* en ayant accès à la liste de tous les employés du gouvernement. Le vol d'identité afin de s'introduire dans des systèmes sensibles serait également rendu plus facile et rapide.

Il est intéressant de noter que dans le cadre du cyberespace, l'espionnage électronique peut également se faire entre alliés, bien que des accords entre pays soient sensés limiter ou interdire ces pratiques. La France a par exemple été accusée d'espionner le Canada (Follorou et Untersinger 2014a; Follorou et Untersinger 2014b), alors que trois présidents français avaient eux-mêmes été espionnés par les États-Unis pendant des années (Guiton et al. 2015).

Cet espionnage à grande envergure par les différents États est sans précédent. Il est malgré tout difficile d'en mesurer la taille exacte tant le nombre de cibles est élevé et tant les méthodes d'intrusion sont efficaces, bien que parfois assez rudimentaires. Le fait que l'information soit principalement rendue publique par le biais de lanceurs d'alertes ou d'organisations comme *Wikileaks* limite grandement la possibilité d'évaluer précisément l'état de la surveillance dans le cyberespace. Compte tenu du caractère furtif des techniques et logiciels utilisés, il est également assez difficile de dépister ces réseaux de surveillance à moins qu'ils ne soient mis en évidence par des experts en sécurité informatique.

Ces réseaux de renseignement et d'espionnage sont d'ailleurs fréquemment utilisés en soutien dans des cas de conflits classiques. Il y a en effet eu une utilisation de plus en plus importante des technologies du cyberespace dans les conflits militaires au cours des dernières années.

2.2 Cyberguerre et appui aux conflits classiques

2.2.1 Doctrine de la guerre de l'information et cyberguerre

Peu importe l'époque, l'information a toujours été au centre des guerres puisqu'elle donne des avantages stratégiques afin de mener des opérations et triompher de ses adversaires. Que ce soit dans *l'Art de la guerre* de Sun Tzu (Zi Sun et al. 1987) ou grâce au décodage de la machine *Enigma* par les Anglais pendant la Seconde Guerre mondiale (sur l'importance du « codebreaking » pendant la guerre, voir Kahn 1980), l'information et sa manipulation ont historiquement été des éléments clé dans le succès ou l'échec des activités militaires. Avec la modernisation des armées et l'utilisation d'un grand nombre de technologies présentes dans le cyberespace, cette dynamique s'est accélérée, la guerre de l'information dans cet espace faisant

maintenant partie intégrante des stratégies de différentes armées.

L'exemple de la Chine est probant, puisque la guerre de l'information est un élément de doctrine en elle-même. Ainsi, contrôler l'information, la modifier et la rendre trompeuse pour l'ennemi est une base pour l'armée chinoise (Clarke et Knake 2010, 14). Cette importance du cyberespace pour la Chine a conduit à la recherche d'un commandement unifié visant à intégrer cet espace de guerre aux autres espaces et aux missions et priorités de l'APL en général. Cette dynamique a également été accélérée par la modernisation de l'armée, forçant une prise en compte de l'informatisation et des stratégies de surveillance et de perturbation des réseaux du cyberespace afin de soutenir des guerres conventionnelles. En faisant du cyberespace un espace critique à sa gouvernance, à son développement mais aussi à sa sécurité nationale, la Chine en a *de facto* fait un espace d'action pour l'armée (Clarke et Knake 2010, 35).

> Information warfare, in the context of systems operations theory, is viewed by some PLA authors as one of many combat macro-systems to be integrated under this concept, but one with the ability to influence battlefield perception, information, transmission, and command networks (Clarke et Knake 2010, 17)

Ces capacités dans le cyberespace passent notamment par une guerre de l'information. Il s'agit par exemple de faire remonter aux adversaires de fausses informations, de corrompre ou de détruire leurs réseaux et infrastructures d'informations, etc. (Krekel, Adams et Bakos 2012, 19) Le but de ces stratégies peut aussi bien être le fait d'empêcher des adversaires de prendre des décisions rapidement, que tout simplement de rendre impossible la coordination de leurs actions.

Combinées à une modernisation de l'armée, ces stratégies pourraient devenir particulièrement efficaces. Il reste tout de même d'importants problèmes de contrôle et d'utilisation de ces stratégies, puisque toutes les composantes des armées ne sont pas encore modernisées (Krekel, Adams et Bakos 2012, 22). Les armées faisant usage

de ces technologies peuvent également être menacées par ces mêmes stratégies. Il est donc important de maîtriser parfaitement ces technologies tout en s'assurant de ne pas se rendre vulnérable soi-même. Dans le cas de la Chine, cette vulnérabilité a été évaluée rapidement par l'APL. La protection des réseaux de communication et de conduite des activités militaires et étatiques a ainsi été érigée comme étant d'importance vitale pour le pays (Krekel, Adams et Bakos 2012, 44).

Ainsi, dans l'APL, le puissant Troisième Département est spécialisé dans la collecte d'information. Le Quatrième Département quant à lui aurait la charge des missions d'attaque contre des ennemis ou des cibles :

> The GSD Fourth Department [...] holds an equal bureaucratic rank as the Third Department within the GSD hierarchy, but unlike the Third Department, it is charged with an offensive mission rather than a defensive electronic warfare or purely intelligence collection and analysis function (Krekel, Adams et Bakos 2012, 47)

Le Quatrième Département a par ailleurs pour mission de superviser des organismes et instituts de recherche technologique qui pourraient lui fournir des équipements et des outils afin de mener à bien ses objectifs. Ces partenariats permettent ainsi à l'APL d'utiliser des méthodes de brouillage ou de parasitage des systèmes ennemis afin de les combiner avec des attaques informatiques ou conventionnelles (Krekel, Adams et Bakos 2012, 48). Par ailleurs, le travail de ces deux départements serait effectué avec la collaboration du Ministère de la sécurité publique (MSP). Ce dernier s'occupant notamment du transfert des technologies industrielles et civiles vers l'armée et l'appareil d'État, il aurait un rôle charnière pour l'organisation et la modernisation des armées ainsi que des différents services gouvernementaux.

Ces exemples d'organisations militaires et étatiques travaillant dans le cyberespace montrent l'importance qu'il peut avoir pour la stratégie chinoise. Les ressources allouées à ces stratégies sont également révélatrices de l'accent mis sur l'espionnage

et la guerre de l'information dans le cyberespace.

D'un autre côté, les pays émergents ayant limité leur utilisation des technologies présentes dans le cyberespace auraient un certain avantage stratégique. En limitant la présence des différentes sphères de la vie humaine dans cet espace et en gardant un ensemble d'infrastructures économiques et industrielles plus traditionnelles (comme les centrales au charbon ou les transports en commun reliés par des moyens de communication peu sensibles aux perturbations dans le cyberespace comme les radios ou les lignes téléphoniques classiques), ces pays ont limité leur dépendance et le nombre de vulnérabilités pouvant être exploitées. Certains régimes politiques comme la Chine ou certains pays arabes ont également développé des capacités afin d'isoler totalement les réseaux nationaux du restant du cyberespace en cas de besoin. Cela offre une défense efficace face aux menaces venant de l'extérieur, tout en n'empêchant pas la possibilité de mener des cyberattaques depuis un pays tiers. Il serait difficile de justifier un tel contrôle étatique du cyberespace par les États dans les régimes libéraux, bien que ces stratégies soient mises en avant périodiquement par des militaires ou des hommes politiques peu intéressés par le principe universel de neutralité d'Internet et du cyberespace en général.

De même, la guerre de l'information n'a prouvé qu'une utilité relative dans le cas de guérilla ou de théâtres d'opérations qui ne sont pas situés dans des environnements ayant un haut développement technologique. La combinaison entre renseignement militaire classique et utilisation de moyens technologiques a plutôt donné lieu à des pertes civiles importantes accompagnées de succès militaires discutables (on pensera notamment aux guerres en Irak et en Afghanistan). De nombreux groupes terroristes ou militants n'utilisent plus non plus de technologies numériques afin de communiquer et sont donc relativement à l'abri de ces moyens de projection de la puissance.

Par ailleurs, l'intégration des technologies du cyberespace dans les doctrines militaires de différents acteurs nous mène à nous questionner sur l'utilisation de ces outils dans le cadre de guerre classiques. Nous tâcherons donc de faire un court portrait de cette intégration de la cyberguerre et des théories de la guerre de l'information dans le cadre de conflits militaires classiques entre États.

2.2.2 Cyberattaques et projection de la force dans le cyberespace en appui aux conflits militaires classiques

Un cas intéressant d'utilisation de technologies présentes dans le cyberespace dans un cadre de guerre est le conflit militaire entre la Russie à la Géorgie en 2008. Rappelons que le conflit opposait originellement deux provinces géorgiennes séparatistes, l'Ossétie du sud et l'Abkhazie, au gouvernement central du pays. Ces deux provinces avaient à plusieurs reprises voté pour la séparation et fait des démarches afin d'accéder à l'indépendance. Le gouvernement géorgien, bien qu'il ait fait des concessions, ne pouvait toutefois pas accorder l'indépendance à ces deux provinces, pour des raisons stratégiques et économiques.

La Russie a quant à elle prit part au conflit au prétexte que des citoyens russes (naturalisés en masse après la chute de l'Union soviétique) se trouvaient en grand nombre dans ces deux provinces. Il s'agissait également de bloquer la possible adhésion de la Géorgie à l'OTAN, la Russie ne souhaitant pas cette présence militaire si proche de son territoire.

Les tensions historiques ont finalement atteint un point critique en aout 2008 lorsque les forces armées géorgiennes sont intervenues en Ossétie du sud sous le prétexte d'avoir été ciblées par des bombardements. La Russie a alors également décidé d'intervenir afin de protéger l'Ossétie du sud et l'Abkhazie et étendre sa zone

d'influence. La guerre se terminera une dizaine de jours plus tard avec l'écrasante victoire russe face aux forces armées géorgiennes. Les deux provinces ont été reconnues *de facto* comme indépendantes et sont sous la protection de la Russie depuis.

L'intérêt de cet épisode pour notre étude, outre que de constater les velléités expansionnistes russes, est que ce conflit a été marqué par une utilisation intensive des cyberattaques. Avant même le conflit armé, la Russie a été accusée de mener des opérations de guerre de l'information et de cyberguerre contre la Géorgie (voir par exemple Markoff 2008). Comme dans le cas de l'Estonie en 2007, des sites gouvernementaux, des services publics, banques et autres systèmes informatiques présents dans le cyberespace ont été visés et rendus hors-service pendant de longues périodes.

> Without access to European settlement systems, Georgia's banking operations were paralyzed. Credit card systems went down as well, followed soon after by the mobile phone system (Clarke 2010, 20)

Ces perturbations ont touché un ensemble de services et ont permis une invasion terrestre bien plus efficace par les forces armées russes. C'est notamment ce qui a poussé différents acteurs à attribuer la responsabilité de ces attaques à la Fédération de Russie (Swaine 2008). Cette dernière a bien sur nié avoir orchestré l'opération, pointant la responsabilité vers des pirates nationalistes russes. Si ces attaques étaient particulièrement simples, composées en majorité d'attaques de type déni de service, elles ont toutefois été soigneusement planifiées à l'avance (Hagen 2012, 7).

Outre le piratage de sites Internet gouvernementaux et privés, la Géorgie aurait également été ciblée par des cyberattaques visant à dérober de l'information et à l'utiliser dans le cadre de l'opération militaire contre son territoire :

> these attacks were not only designed to control the flow of information or form the perception of the people, they were also part of information exfiltration activities that tried to steal and accumulate military and political intelligence from Georgian networks as well (Hagen 2012, 6)

Lors du conflit, la Russie aurait utilisé ces cyberattaques afin de créer un climat de peur et de tension en Géorgie, en rendant inaccessibles les sites gouvernementaux et d'information ainsi qu'en parasitant des réseaux nécessaires au fonctionnement de l'armée (Hagen 2012, 7). Une partie du trafic Internet géorgien aurait également été redirigée vers la Russie pendant le conflit (Hagen 2012, 9), rendant vulnérable l'accès de la Géorgie au restant du cyberespace. Ces attaques ont donc servi comme une forme de cyberinfluence auprès des populations locales en les démotivant et en rendant opaque la situation, créant de l'instabilité politique.

De façon générale, ces attaques ont donc été utiles à l'invasion armée par la Russie, tant par la démobilisation qu'elles ont créé dans la population, qu'en rendant partiellement aveugles et muettes les forces armées géorgiennes. Il est intéressant de noter que la plus grande partie des attaques a été menée lors de l'intervention de la Russie, laissant penser que ces attaques ont été préparées afin de servir d'appui aux autres formes de guerre déployées par les différents acteurs (Hagen 2012, 13).

Même si la Russie a été pointée du doigt par différents acteurs, les difficultés d'attribution dans le cyberespace ont compliqué l'identification des réels organisateurs de ces attaques. Certains avancent d'ailleurs que si la Russie a pu être impliquée dans une certaine mesure, la vague de sympathisants pro-russes ayant mené des cyberattaques individuelles aurait elle aussi participé à la perturbation du cyberespace géorgien (Hagen 2012, 14).

En dehors des considérations stratégiques pour la Russie, ce conflit a mis en lumière les utilisations possibles de cyberattaques dans le cadre de conflits militaires

classiques. En paralysant les communications géorgiennes et en perturbant les systèmes informatiques de l'armée, la Russie a pu accentuer sa domination militaire. Il s'agit donc d'un cas intéressant d'utilisation de technologies du cyberespace à des fins de supports aux activités classiques de la guerre.

La simplicité des attaques est également une donnée importante à prendre en compte pour la projection de la force dans le cyberespace par des pays émergents. Puisque cette forme de soutien aux activités de guerre traditionnelles ne demande que peu de ressources, il pourrait s'agit d'une forme de guerre et de perturbation particulièrement importante pour ces pays.

2.2.3 Le cyberpouvoir comme outil de dissuasion et de réplique pour des pays émergents

Les technologies du cyberespace et la cyberinfluence pourraient également être utilisées dans le cadre de stratégies de dissuasion par certains pays émergents.

Par exemple, les tensions entourant les revendications chinoises concernant Taïwan pourraient bien être le théâtre d'affrontements dans le cyberespace. Les États-Unis et d'autres acteurs ne souhaitent pas que la Chine annexe l'île et en fasse un territoire chinois alors que la Chine se fait menaçante depuis des décennies. Ce conflit territorial et diplomatique pourrait mener à une guerre si d'une part la Chine décidait d'accélérer ses politiques d'annexion et que d'autre part les États-Unis décidaient de défendre Taïwan.

Dans ce contexte, le cyberespace pourrait devenir un théâtre d'affrontements entre les puissances concernées. Le recours à des cyberattaques ou à des actes de cyberguerre, couplé à des stratégies de cyberinfluence et de guerre de l'information pourrait être

un élément de défense ou de dissuasion visant à empêcher ou limiter toute attaque militaire adverse. Ces stratégies seraient d'autant plus efficaces si elles étaient combinées avec des attaques classiques (Krekel, Adams et Bakos 2012, 27). Par exemple, en cas d'attaque par la Chine, la défense de Taïwan demanderait aux États-Unis et aux autres alliés de déployer de grandes capacités logistiques en un temps très court. Des cyberattaques contre les forces états-uniennes dans la région et leurs capacités technologiques ou contre les pays hôtes de leurs bases militaires seraient un élément potentiellement clé pour l'action militaire chinoise (Krekel, Adams et Bakos 2012, 28). Cette forme de guerre en soutien aux activités militaires classiques ou déployée de façon dissuasive pourrait ainsi éviter des destructions physiques ou des affrontements menant à une situation de guerre ouverte.

> Chinese commanders may elect to use deep access to critical U.S networks carrying logistics and command and control data to collect highly valuable real time intelligence or to corrupt, the data without destroying the networks or hardware (Krekel, Adams et Bakos 2012, 31)

En cas de conflit, les cyberattaques et menaces dans le cyberespace pourraient également servir d'élément de perturbation psychologique des activités des adversaires. En faisant croire que certains systèmes ont été contaminés ou en les contaminant réellement, la Chine pourrait faire perdre un temps précieux à ses victimes, les forçant à procéder à un nouvel examen de la situation, négligeant ainsi d'autres activités. Ces cyberattaques pourraient viser tant des cibles militaires que des réseaux privés travaillant avec l'armée (approvisionnement, traitement de données, maintenance des matériels militaires, etc.). Les multiples sous-traitants des armées étant autant de cibles et de potentielles vulnérabilités à exploiter pour des pirates (Krekel, Adams et Bakos 2012, 34). Par exemple, en ciblant le système de réapprovisionnement en carburant au sol ou en vol des armées adverses, l'APL pourrait mener des attaques catastrophiques, profitant de la confusion et de la paralysie de ses adversaires (Krekel, Adams et Bakos 2012, 37).

Les réseaux civils pourraient également être visés dans ces conflits. Par exemple, en ciblant les réseaux d'approvisionnement électrique, ou encore le système financier de ses adversaires, la Chine pourrait divertir l'attention de ces acteurs vers des questions de sécurité intérieure ou tout simplement dissuader ces derniers d'intervenir militairement.

> Electric grid outages in densely populated areas of the United States or attacks against networks supporting financial institutions could put significant strain on U.S policymakers to coordinate domestic crisis management, and while simultaneously attempting to deal with impending or actual hostilities in the Taiwan Strait [...] Targeting elements of U.S infrastructure that support financial markets means that sudden disruptions to the clearing and settlement infrastructure (even if only experienced by one participant in a geographically limited area) can quickly cascade into market-wide liquidity dislocations, solvency problems, and severe operational inefficiencies, according to U.S Federal Reserve analysis. (Krekel, Adams et Bakos 2012, 41, 42)

Même si la Chine est encore en retard sur les moyens militaires conventionnels, elle pourrait donc être en mesure de perturber des adversaires plus forts en faisant usage de cyberattaques contre leurs réseaux et infrastructures. Cette capacité qu'a la Chine à menacer les pays développés et leurs réseaux informatiques serait donc un levier important dans les interventions que ces pays pourraient faire en réponse à des actes militaires de la Chine dans la région (Krekel, Adams et Bakos 2012, 39),
Par ailleurs, grâce à son contrôle de l'Internet et des autres réseaux du cyberespace sur son territoire, la Chine serait probablement plus apte à se protéger contre des répliques dans le cyberespace. Le fait que l'armée chinoise ait gardé des éléments d'action militaire non liés au cyberespace est également un autre avantage pour ce pays puisqu'elle est ainsi moins vulnérable aux attaques dans le cyberespace.

Ces capacités de dissuasion et de réplique en cas de conflit pourraient également être utilisées par d'autres acteurs dans le système international. En menant une guerre

asymétrique dans le cyberespace, certains pays émergents pourraient se défendre contre des politiques impérialistes de pays dominants. Il y a également un élément intéressant de dissuasion dans le fait de développer des capacités de cyberpouvoir et de projection de la force dans le cyberespace pour ces acteurs puisque ces moyens peuvent être efficaces tout en étant déployés à moindre coût. L'exemple de l'utilisation que la Chine fait de ces moyens pourrait ainsi se propager à d'autres acteurs souhaitant acquérir des moyens dissuasifs sans devoir investir dans des armées classiques très onéreuses et de toute façon inférieures à la puissance militaire des acteurs dominants.

2.3 Espionnage industriel

Une autre utilisation clé des technologies du cyberespace à des fins de politiques intérieure et internationale est le cas de l'espionnage industriel. En tant que moteurs économiques historiques, la copie et la reproduction de processus industriels ont souvent été au cœur des innovations technologiques ainsi que dans la production des différents pays entrant en concurrence dans l'économie mondiale.

Cette recherche de la compétitivité peut passer par le financement des secteurs de recherche et développement, par la subvention de fleurons industriels nationaux, ou encore par de l'espionnage industriel. En tant que source d'avantages économiques et politiques, les procédés d'innovation sont donc souvent considérés comme devant être protégés et gardés secrets autant que possible. Il s'agit en fait d'une question de sécurité nationale élargie pour bien des États et de sécurité économique pour les entreprises privées.

Puisque de nombreuses organisations font un usage important des technologies de l'information et des télécommunications, il existe un ensemble de risques portant sur

la protection de leur propriété intellectuelle. Compte tenu des différentes vulnérabilités en présence, il n'est pas rare que des entreprises se fassent pirater. Le vol de secrets industriels est devenu une problématique importante pour ces dernières, voulant à la fois profiter des avantages technologiques amenés par le cyberespace et Internet tout en garantissant leur sécurité et leur compétitivité. De plus, dans un mode de production capitaliste avancé où une grande partie de la plus-value est tirée des innovations technologiques, il n'est pas étonnant que des pays désavantagés par la division internationale du travail veuillent accélérer leur développement économique et technologique afin de se démarquer et obtenir une meilleure position dans le système international.

Afin de mesurer l'importance de l'espionnage industriel dans le cyberespace, nous avons choisi deux cas d'école portant sur l'utilisation par la Chine de ces technologies. Il nous semble que ces deux exemples sont particulièrement révélateurs des dynamiques pouvant se jouer dans le cyberespace quant aux problématiques liées à l'espionnage industriel.

> Collectively, recent developments in Chinese computer network operations reflect a nation fully engaged in leveraging all available resources to create a diverse, technically advanced ability to operate in cyberspace. Computer network operations have assumed a strategic significance for the Chinese leadership that moves beyond solely military applications and is being broadly applied to assist with long term strategies for China's national development. (Krekel, Adams et Bakos 2012, 13)

Bien entendu, notre étude comporte un ensemble de limites puisque nous ne nous sommes intéressés ici qu'à la Chine, qui est un pays particulièrement actif dans le cyberespace et agressif dans ses négociations commerciales. Il s'agit malgré tout d'un exemple intéressant de mise à profit d'une main d'œuvre qualifiée et d'utilisation de technologies présentes dans le cyberespace à des fins d'espionnage industriel. Il s'agit également du cas le mieux documenté en matière d'espionnage industriel parmi tous les pays émergents. Si nous reconnaissons donc les limites de nos exemples, ils nous

semblent malgré tout pertinents à notre étude.

Un des cas les plus récents et significatif d'espionnage industriel et militaire mis au jour est celui de « APT1 » (pour *Advanced persistent threat 1*). Depuis 2004, la firme de sécurité *Mandiant* a suivi la présence d'APT1 dans le cyberespace, tentant de répertorier ses actions et de valider l'identité de ses membres. Si au début de l'enquête il n'était pas certain que le gouvernement chinois soit responsable ou soutienne cette cellule, il maintenant clair qu'APT1 est situé en Chine et que le gouvernement est minimalement au courant des activités de cette organisation (Mandiant 2013, 2).

Pour les chercheurs de Mandiant, le groupe serait en fait une division - l'unité 61398 - de l'armée chinoise elle-même. Cette unité, classée secret défense et au fonctionnement opaque, a longtemps été suspectée de mener des opérations de guerre de l'information et d'espionnage industriel dans différents espaces, dont plus particulièrement le cyberespace. Si les capacités précises de cette unité sont inconnues, elles sont estimées par les auteurs du rapport à des centaines, voire des milliers de personnes, ne serait-ce que par la taille et les infrastructures (branchement spéciaux d'Internet, réseau électrique, etc.) du complexe dans lequel elle opérerait.

Depuis 2006, grâce à ses opérations d'espionnage industriel, APT1 aurait compromis au moins 141 compagnies dans 20 secteurs industriels majeurs (Mandiant 2013, 3). Juste en janvier 2011, APT1 avait fait 17 nouvelles victimes dans 10 industries différentes, majoritairement en occident. Ces secteurs industriels sont généralement ceux que la Chine a identifié comme étant stratégiques pour son développement.

Il ne s'agit là que des cas répertoriés d'attaque, la recherche de Mandiant ne se basant que sur des documents publics. Il est en effet ardu de mesurer précisément l'étendue des vols puisque les méthodes utilisées sont souvent difficiles à retracer et que les

délais entre les attaques et les enquêtes sont souvent trop grands. De plus, les victimes cherchent généralement plus à sécuriser un réseau qu'à savoir comment les brèches sont apparues et encore moins à diffuser ce type d'information. Par ailleurs, beaucoup de systèmes de sécurité ne seraient pas aptes à détecter les intrusions et les vols quand ils se produisent.

Les opérations d'APT1 seraient donc particulièrement efficaces puisque difficiles à déceler. En moyenne, APT1 a réussi à maintenir un accès de 356 jours dans les réseaux des victimes, exportant et dérobant des données. Ces attaques se feraient grâce à des méthodes récurrentes, propres au groupe. ATP1 aurait notamment établi un réseau d'ordinateurs et de serveurs de presque 1000 unités dans treize pays différents. La majorité de ces serveurs se trouve toutefois en Chine (709/937) et plus précisément à Shanghai (698/709) sur quatre réseaux principaux (Mandiant 2013, 39).

Toutes les connexions passant par ces serveurs ou presque venaient de Chine et avaient comme langue le chinois : « Of the 832 IP adresses, 817 (98,2%) were Chinese and belong predominantly to four large net blocks in Shanghai wich we will refer to as ATP1's *home* network. » (Mandiant 2013, 40). D'autres preuves, comme le type de claviers utilisés ou la langue système des ordinateurs se connectant sur ces serveurs, prouvent clairement que ces connexions proviennent de Chine continentale (Mandiant 2013, 40).

Notons qu'il est plutôt rare que des pirates dans des organisations secrètes ou sous-terraines ne prennent que si peu de précautions quant aux possibilités d'être retracés. Cela laisse clairement penser que le fait d'être identifiés n'est pas un problème pour ces pirates, ou, comme le souligne le rapport de *Mandiant*, que ce groupe a réussi sans faire aucune erreur à se faire passer pour des chinois de Shanghai. Si techniquement, cette seconde hypothèse est possible, elle serait toutefois très

complexe à réaliser tant le nombre d'opérations lancées est grand et ne représenterait qu'un intérêt limité pour tout État.

Afin de faire fonctionner les réseaux d'APT1 et de les exploiter à pleine capacité, les chercheurs estiment « de façon conservatrice » que le groupe nécessite l'intervention humaine de plusieurs centaines de personnes, avec différents types de spécialistes allant des pirates informatiques aux linguistes ou aux chercheurs dans divers domaines industriels.

> Given the volume, duration and type of attack activity we have observed, APT1 operators would need to be directly supported by linguists, open source researchers, malware authors, industry experts who translate task requests from requestors to the operators, and people who transmit stolen information to the requestors. (Mandiant 2013, 5)

APT1 bénéficierait donc d'importants moyens. Les personnels engagés dans cette unité recevraient notamment des formations intensives d'anglais et seraient recrutés en fonction de compétences académiques axées sur l'informatique (Mandiant 2013, 11). D'autres personnels formés dans divers domaines seraient également présents afin de mettre en valeur l'information acquise et la redistribuer correctement au sein de l'appareil militaire chinois ainsi que dans l'industrie et la recherche nationale.

Par sa taille, APT1 représente un réseau d'envergure dont les activités ne pourraient pas passer inaperçues dans un pays comme la Chine où le cyberespace est très surveillé et contrôlé. Les infrastructures déployées par APT1 ainsi que ses victimes pointent également vers l'implication de l'appareil d'État chinois dans le support ou la mise en place de la cellule.

De plus, toutes les industries ciblées (technologies de l'information, de l'aérospatiale, des administrations publiques, des télécommunications et satellites, de la recherche

scientifique, de l'énergie, des transports et de l'industrie en général) représentent des priorités économiques et de développement pour la Chine. L'espionnage à grande échelle de ces secteurs permettrait ainsi au pays de bénéficier de meilleurs rapports de force lors de négociations commerciales, mais aussi de développer sa propre industrie de façon plus rapide.

Si l'unité 61398 aurait eu comme première mission de cibler les pays nord-américains afin d'extraire des données sur leur situation politique, économique ou militaire (Mandiant 2013, 9), elle aurait par la suite ciblé des dizaines de victimes simultanément dans différents pays et différentes branches industrielles. Les données volées seraient de toutes les natures possibles et pourraient être utilisées dans un large éventail de situations :

> Once the group establishes access to a victim's network, they continue to access it periodically over several months or years to steal large volumes of valuable intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails and contact lists from victim organizations' leadership. (Mandiant 2013, 20)

Au niveau opérationnel, les techniques employées par APT1 seraient relativement rudimentaires, se basant notamment sur de l'hameçonnage (Mandiant 2013, 28). Plutôt que de développer des logiciels espions extrêmement complexes (comme *Stuxnet* ou *Flame*), les Chinois auraient plutôt ciblé les vulnérabilités liées aux actions des êtres humains dans le cyberespace. Afin de mieux leurrer les victimes de ses opérations, APT1 aurait par exemple utilisé un grand nombre de noms de domaines ressemblant à des sites Internet légitimes (près de 2551 au cours des six années de surveillances de *Mandiant*).

Une des façons de pénétrer dans les systèmes visés reposait donc sur le vol d'identités et l'incitation à cliquer sur des liens infectés qui vont ensuite installer des logiciels

pirates sur les ordinateurs visés. Ces logiciels permettent de contrôler un ensemble de paramètres et de mener un certain nombre d'actions sur les ordinateurs et serveurs infectés. Les pirates ont par exemple récupéré des mots de passe et autres informations permettant d'acquérir plus de privilèges d'accès aux réseaux et aux systèmes des victimes. Une fois un système contrôlé depuis l'intérieur, il devient difficile de détecter les intrusions puisque celles-ci usent des identifiants et des commandes dites légitimes qui ne sont pas associées à des attaques mais à une utilisation normale par des utilisateurs autorisés. Le cycle de vie du piratage finit généralement par la création d'une archive contenant tous les documents volés. Cette archive est par la suite téléchargée par un des serveurs de contrôle des logiciels pirates.

Bien qu'il s'agisse de techniques assez simples, les logiciels pirates employés sont généralement inédits et probablement directement développés par APT1, ce qui rend leur détection plus difficile. Près de 42 familles différentes de logiciels pirates auraient été identifiées jusqu'à présent, visant tous les types de systèmes informatiques (de l'ordinateur Windows ou Mac en passant par les tablettes et les cellulaires intelligents, Mandiant 2013, 31), multipliant ainsi les façons d'accéder aux informations recherchées. Ces programmes auraient évolué avec le temps et les besoins, ce qui laisse penser que des développeurs spécialisés travailleraient pour APT1 de façon continue sur chacune des branches de *malware* identifiées (Mandiant 2013, 32).

Si ces opérations sont techniquement assez rudimentaires, il n'en reste pas moins que les pirates chinois ont réussi au fil des années à s'infiltrer dans des centaines de systèmes informatiques étatiques ou privés, dérobant de précieuses informations. Les ressources humaines bien formées et en bonne quantité au sein d'APT1 auraient par ailleurs permit au groupe de faire redescendre les informations et secrets industriels au sein des entreprises nationales et des groupes de recherche en

lien avec l'APL. Ces méthodes rejoignent notre hypothèse de recherche sur la question de l'utilisation du cyberespace par des pays émergents ayant axé leur développement sur une main d'œuvre formée et une massification de l'éducation. En utilisant des moyens de projection de la force peu couteux et de cyberespionnage, mais surtout en ayant une main d'œuvre disponible et qualifiée, la Chine a pu acquérir de l'information pertinente à son développement et à la négociation d'accords commerciaux ou politiques avec d'autres acteurs. Ces stratégies ont donc pu renforcer sa puissance et sa force dans le système international, tant au plan politique qu'économique.

Bien que le rapport de Mandiant porte essentiellement sur le groupe le plus prolifique, APT1, les chercheurs estiment qu'il existe au moins vingt APT opérant en Chine, avec des opérations de taille variable, toutes en lien avec des questions d'espionnage industriel ou d'opérations de cyberespionnage ou encore de préparation à la cyberguerre (on soupçonne d'ailleurs le rôle de la Chine dans une cellule nommée « APT-30 » ayant été très active en Asie de l'Est, voir FireEye Labs / FireEye Threat Intelligence 2015).

Un autre rapport important paru récemment sur l'espionnage industriel et militaire mené par la Chine a été publié par la firme de sécurité *Crowdstrike*. Il faut noter que ce rapport a été publié lors d'une période de tension entre États-Unis et Chine concernant les activités dans le cyberespace et l'espionnage industriel en général (Ackerman et Kaiman 2014). Il s'agissait alors de mettre en lumière l'implication d'une autre unité de l'APL dans les opérations chinoises d'espionnage économique et politique dans le cyberespace. Après le rapport de la firme *Mandiant*, cette étude porte quant à elle sur l'Unité 61486 du 12^{e} bureau du 3^{e} département général de l'APL, identifié sous le nom « *Putter panda* ».
La mission principale de cette unité, œuvrant depuis 2007, serait de pirater des compagnies afin de voler des secrets industriels dans un ensemble de secteurs

manufacturiers et technologiques. *Putter Panda* s'est spécialisé dans des opérations d'espionnage ciblant les gouvernements, le complexe militaro-industriel ainsi que les secteurs de la recherche et la technologie en général. Parmi ces cibles, sont spécifiquement visées la défense américaine ainsi que les industries aérospatiales européennes et américaines (Crowdstrike Global Intelligence Team 2014, 1). Mentionnons qu'en 2013, les revenus de la filière du satellite dans l'aérospatiale s'élevaient à 189.2 milliards de dollar américains, en faisant ainsi une cible particulièrement intéressante pour l'espionnage industriel. Dans une industrie aussi lucrative mais aussi extrêmement couteuse en termes de recherche et développement, l'espionnage industriel peut devenir essentiel aux potentiels concurrents.

Au niveau opérationnel, comme pour l'unité 61398, la majorité des attaques était également orientée vers les failles que les humains peuvent représenter dans le cyberespace. Plutôt que de développer des logiciels complexes, *Putter Panda* a visé avant tout des logiciels populaires connus pour leurs problèmes de sécurité (on pourra également penser que la Chine a acheté et exploité des *Zero day exploit*). Ces attaques et infiltrations remonteraient au moins à 2007, année où l'on peut retrouver des traces du groupe dans la compilation des logiciels utilisés pour mener des attaques. *Putter panda* serait également associé à d'autres groupes menant des opérations d'espionnage et partageant ses infrastructures comme « *Comment panda* » ou « *vixen panda* ».

De plus, comme dans le cas de l'unité 61398, des noms de domaines enregistrés afin de mener des activités d'espionnage ont mené directement à l'unité 61486 de l'APL. Les noms de domaines utilisés étaient souvent représentatifs des secteurs d'intérêt de *Putter panda* (aérospatial, secteur des télécommunications, etc.) (Crowdstrike Global Intelligence Team 2014, 10) et étaient parfois enregistrés par des opérateurs de l'APL sous leurs vrais noms.

Cette possibilité d'identifier des opérateurs de l'APL a d'ailleurs permis de mettre en

lumière l'importance du recrutement de l'armée dans les universités et dans les groupes de hackers amateurs. L'exemple de Chen Ping, membre de l'APL spécialisé dans les domaines informatiques et dans l'aérospatial, est intéressant. Lors de sa scolarité supérieure, il aurait notamment fait partie d'un groupe de pirates s'étant illustrés dans le domaine universitaire, la « 711 network security team » (Crowdstrike Global Intelligence Team 2014, 16), qui aurait attiré l'attention de l'APL. L'armée chinoise surveille en effet le réseau universitaire qu'il considère comme étant un vivier de recrutement intéressant pour ses activités (Crowdstrike Global Intelligence Team 2014, 16).

Les universitaires recrutés par l'armée, comme Chen Ping, seraient ainsi directement intégrés aux unités de l'APL œuvrant dans le cyberespace. Les photos que Chen Ping a publié après son passage à la SJTU semblent également corroborer l'idée qu'il travaille maintenant dans un immeuble ayant des mesures de sécurité spéciales, destinées à limiter et à couvrir les possibilités d'espionnage. De grandes antennes satellites semblent également prouver que l'espace de travail n'est pas un simple immeuble. Par ailleurs, lorsque comparées avec des informations officielles données par l'APL, il semble que les locaux et positions GPS rendues disponibles par Chen Ping sur Internet soient les mêmes que l'Unité 61486 de l'APL, spécialisée dans l'interception de communications satellitaires et de l'espace (Crowdstrike Global Intelligence Team 2014, 23).

Comme dans le cas de l'unité 61398, il y a donc des liens clairs entre Putter Panda, des opérateurs de l'APL comme Chen Ping et l'unité 61486. Le cas de cette unité permet également de constater l'important rôle du recrutement universitaire pour l'APL. Le fait d'avoir axé son développement sur une main d'œuvre formée et qualifiée est alors un avantage significatif pour la Chine qui peut recruter de façon massive afin de mener ses opérations dans le cyberespace. De plus, comme dans le cas de l'unité 61398, *Putter Panda* semble également être responsable du traitement

et de la transmission des données recueillies vers les entreprises nationales et programmes de l'armée pouvant en bénéficier. Ainsi, que ce soit en dérobant des secrets industriels, des informations sur les procédés employés par différentes entreprises ou organisations étatiques, la Chine a probablement été en mesure d'accélérer son développement technologique dans un certain nombre d'industries. Ces opérations ont également pu servir à acquérir du renseignement pouvant être utilisé dans le cadre militaire (acquisition de données, infiltration dans les réseaux de commande des satellites, etc.).

Il ne fait que peu de doutes que d'autres pays émergents aient cherché – et potentiellement réussi – à développer des capacités d'espionnage industriel dans le cyberespace. Tant par les coûts faibles associés à la mise en place de ces stratégies que par les avantages qu'elles peuvent rapporter au niveau du développement industriel, l'espionnage industriel dans le cyberespace pourrait devenir une composante importante des politiques économiques des pays émergents. Ces pays ont déjà tous les éléments nécessaires à la poursuite de telles stratégies, il ne leur reste ainsi qu'à aller de l'avant.

3. Conclusion

> Human capital is an even more crucial resource in the cyber environment. (Clarke et Knake 2010, 270)

Afin de conclure, il est nécessaire de rappeler brièvement l'importance des politiques de massification de l'éducation ainsi que d'enseignement technologique pour certains pays émergents ou en voie de réindustrialisation. Ces stratégies sont notamment pertinentes pour les BRICS et ont permis à cet ensemble de se développer rapidement dans la dernière décennie. Si la massification de l'éducation était au début un impératif économique mis en avant par des organisations comme le Fonds monétaire

international ou la Banque mondiale, afin de dynamiser la croissance et les capacités de développement industriel, ces politiques ont également permis l'émergence d'une population formée et compétente dans l'utilisation des technologies de l'information et des télécommunications. Comme nous l'avons mentionné, ces politiques éducatives ont parfois donné lieu à des soutiens étatiques et militaires à la recherche universitaire ainsi qu'à la recherche effectuée par des entreprises étatiques. Tous les pays émergents n'ont toutefois pas les mêmes capacités financières ou de recherche et développement. Il faut donc se souvenir que les exemples étudiés sont plus des cas d'école démontrant un potentiel d'utilisation des technologies du cyberespace grâce des politiques éducatives audacieuses, qu'un standard répandu parmi les pays émergents.

Ces dynamiques conjointes à la modernisation des armées et à l'utilisation de plus en plus importante des technologies présentes dans le cyberespace dans une grande variété d'activités renforcent également l'importance de l'éducation supérieure et de la disponibilité d'une main d'œuvre qualifiée pour répondre aux besoins nouveaux des différents acteurs en présence. Les systèmes d'éducation ayant encore un certain potentiel avant d'atteindre une saturation de leurs capacités et une population importante étant disponible pour recevoir ces formations devrait permettre d'accentuer encore plus la disponibilité de la main d'œuvre dans ce cadre.

Par ailleurs, si la guerre a toujours été présentée comme centrale aux théories des relations internationales et comme étant une composante intégrante du système international, dans le cadre de sa transposition dans le cyberespace, elle prend une dimension nouvelle. Venant reconfigurer les rapports entre acteurs (États, groupes politiques, terroristes, civils, entreprises, etc.), la cyberguerre à grande échelle pourrait donner plus de capacités d'influence et d'action aux pays émergents. Les cyberattaques et la cyberguerre peuvent également être utilisées comme un moyen d'appui aux attaques militaires conventionnelles, comme le cas de la Géorgie nous l'a

montré. Avec la guerre de l'information, il s'agit d'un élément de doctrine non négligeable pour nombre de pays voulant gagner en puissance dans le système international. En menant une efficace guerre de l'information, les armées peuvent déstabiliser et perturber les commandements adverses et acquérir de précieux avantages dans leurs opérations. Il est aussi clair que les technologies du cyberespace peuvent être utilisées à des fins défensives

La question de la cyberinfluence est également un sujet à ne pas négliger. Cette forme d'influence peut être utilisée dans le système international afin de réagir à des situations sans nécessairement passer par des conflits armés. Comme le cas de l'attaque contre l'Estonie le montre, les cyberattaques peuvent perturber de façon efficace des États ou des organisations sans nécessairement justifier de réponses militaires classiques en représailles. Par ailleurs, les difficultés d'attribution des cyberattaques peuvent rendre ce genre d'actions intéressantes pour des acteurs souhaitant projeter une certaine forme d'influence sans s'exposer entièrement. La diplomatie s'en voit donc quelque peu bousculée et d'une certaine façon, enrichie dans la gamme de moyens qu'elle peut employer (Kramer, Starr et Wentz 2009, 314).

Enfin, la question de l'espionnage industriel, qui était déjà un enjeu de sécurité élargie, a également évolué de façon considérable avec la généralisation de l'utilisation des technologies de l'information et des télécommunications ainsi que la mise en réseau d'un grand nombre d'activités humaines. L'espionnage industriel pose notamment des problèmes de compétitivité des différents acteurs en présence ainsi que de sécurité nationale à certains égards, en rendant accessibles à d'autres acteurs des données qui devraient être protégées. Comme nous l'avons vu, certains pays font déjà une utilisation intensive de ces pratiques d'espionnage afin de bénéficier d'avantages dans leur développement. En mettant en réseau des unités d'espionnage industriel et des entreprises étatiques ou encore des centres de recherche, ces pays peuvent ainsi bénéficier du piratage des secrets industriels d'autres acteurs.

Ces stratégies de développement couplées à des politiques de massification de la formation supérieure sont des avantages importants dans l'accroissement de la compétitivité dans un monde où la division internationale du travail est avant tout fixée par les capacités de chaque pays et par les intérêts des pays occidentaux. À notre avis, les politiques de massification de l'éducation ainsi que de formation des populations aux technologies présentes dans le cyberespace sont la pierre angulaire d'une utilisation fructueuse du cyberespace, tant les outils sous leurs aspects techniques et financiers sont relativement faciles d'accès. Cela pourrait notamment mener à l'*emporwent* de certains pays comme la Chine, pouvant entrer en compétition avec les États-Unis ou d'autres puissances.

> Cyberpower contributes to the growing strength of many actors in global politics; it is a significant reason why a number of previously impoverished countries are becoming wealthier. As many countries acquire greater economic strength, owing partly to cyberpower, they will acquire greater diplomatic and political influence, allowing them to pursue more assertive strategic agendas in their regions and beyond (Clarke et Knake 2010, 316)

Afin de conclure, il est à noter que certains pays émergents font déjà une utilisation intéressante et étendue de certaines technologies présentes dans le cyberespace. Que ce soit à des fins de diplomatie, de guerre ou de soutien aux guerres classiques, ou encore pour mener des activités de cyberespionnage, ces pays font une utilisation du cyberespace qui leur est stratégique et avantageuse.

Le fait que les coûts d'engagement soient faibles et que les outils utilisés soient simples nous semble également être un point important pour comprendre les possibilités que ces technologies offrent à des pays émergents. En étant « une arme largement accessible aux plus démunis », la cyberguerre et les cyberattaques pourraient être un outil de choix pour des pays ne pouvant investir dans de grandes armées ou même rivaliser avec des puissances dominantes. Il y a donc un réel potentiel en « dormance » dans l'utilisation de ces outils.

CHAPITRE V

L'UTILISATION PAR DES ACTEURS NON DOMINANTS DE TECHNOLOGIES DANS LE CYBERESPACE PRÉSENTE-T-ELLE VRAIMENT UN RISQUE DE RENVERSEMENT DU SYSTÈME INTERNATIONAL ?

Afin de vérifier la validité de notre hypothèse de recherche, il est nécessaire de revenir sur les grandes lignes présentées dans notre recherche. En premier lieu, il faut resituer la place du cyberespace dans l'ensemble des activités humaines, mais aussi dans le cadre du système international. S'agit-il vraiment d'un espace révolutionnaire comme certains auteurs l'avancent ? Si tel est le cas, comment se fait-il qu'il n'y ait pas eu pour le moment de cyberguerres ou d'attaques majeures, autres que des formes d'espionnage industriel et militaire ?

Ces questions nous pousserons également à aborder d'autres sujets connexes n'ayant pas nécessairement fait l'objet d'une présentation exhaustive, mais méritant tout de même une certaine attention pour l'élaboration d'une analyse cohérente et satisfaisante des enjeux liés au cyberespace. Il s'agira également de donner au lecteur un ensemble de pistes de réflexion qui pourraient être poursuivies dans d'autres études. Pour ce faire, nous nous intéresserons notamment aux questions de dépendance nord-sud dans le capitalisme contemporain ainsi qu'aux tensions entre développement économique et politiques étrangères.

Enfin, nous tâcherons de conclure sur la validité théorique de notre hypothèse de recherche.

1. Un espace révolutionnaire?

1.1 Un nouvel espace des activités humaines

Comme nous l'avons vu aux chapitres II et III, le cyberespace est un nouvel espace des activités humaines. Son omniprésence et la dépendance rapide qui s'est créé en lien avec l'utilisation des technologies le structurant ont profondément modifié le fonctionnement des sociétés modernes. Que ce soit dans les sphères sociales, économiques, politiques ou diplomatiques, le passage à l'ère numérique a généré un ensemble de nouvelles pratiques et de nouveaux référents culturels et politiques.

Un ensemble d'activités est désormais connecté dans le cyberespace et s'appuie sur les technologies présentes en son sein pour contrôler d'autres systèmes, capter et acheminer de l'information, mener à bien des opérations commerciales, etc. La technologie est partout chez les civils : du téléphone intelligent permettant de prendre ses courriels, de se retrouver à l'aide de cartes reliées à Internet, de communiquer d'un bout à l'autre de la planète sans délais; aux fournisseurs de contenus en ligne comme YouTube, Facebook et autres, le cyberespace a révolutionné en peu de temps la façon dont nous communiquons, interagissons et organisons nos vies.

La généralisation de l'utilisation de technologies du cyberespace dans les activités humaines a aussi entrainé une grande dépendance vis-à-vis de ces outils. Ce lien est au cœur des vulnérabilités et menaces qui pèsent dans le cyberespace. Le fait que la majorité des activités humaines soient maintenant exclusivement gérées de façon électronique crée nécessairement une dépendance forte aux infrastructures et réseaux dans le cyberespace. Comme nous l'avons avancé, ces technologies sont notamment marquées par un grand nombre de vulnérabilités. Qu'elles soient logicielles ou physiques, ces dernières peuvent grandement menacer un ensemble d'activités humaines et avoir des conséquences en cascade en cas de défaillances. Les réseaux

étant tous reliés entre eux, en cas d'attaque contre l'un d'eux, d'autres pourraient également être affectés. Quant aux infrastructures physiques elles-mêmes, elles sont fragiles et font souvent l'objet de dégradations involontaires, les rendant parfois inaccessibles pendant de nombreuses semaines, avec toutes les conséquences qui s'en suivent.

Le cyberespace a également permis à des entreprises privées de gagner rapidement de l'influence. Que ce soit Google, Microsoft, Apple, Huawei ou Facebook, les compagnies des secteurs de l'informatique, des technologies de l'information et des télécommunications ont rapidement gagné en taille et en puissance. Cette influence n'est pas que commerciale, elle est aussi sociale, technique et politique. Derrière une apparence de sociétés innovatrices et à l'écoute, ces entreprises ont un pouvoir important et sont à même de faire changer au besoin des politiques publiques. L'édiction de normes techniques ou de modes technologiques est en elle-même une forme de pouvoir social et transformateur pour la société. La technologie est en effet porteuse de valeurs sociales et politiques inextricables de la forme qu'elle prend. En produisant et en imposant de façon habile de nouvelles technologies, ces entreprises privées peuvent ainsi modifier en partie les paradigmes par lesquels nous interprétons et expérimentons le monde qui nous entoure.

Rajoutons enfin que le cyberespace est marqué par une grande accessibilité, ayant fait son succès. Il est en effet peu onéreux de rejoindre le réseau des réseaux et d'y mener des opérations, quelle qu'en soit la nature. Cette facilité d'accès vient ici accentuer le fait qu'avec la bonne information, il est possible d'utiliser les technologies du cyberespace de façon peu onéreuse tout en étant efficace. Cette dimension d'aplatissement des moyens requis pour la mise en place de capacités opérationnelles dans cet espace est importante pour comprendre comment le cyberespace peut s'inscrire comme un espace révolutionnaire pour le système international.

Dans ce cadre, l'image même du cyberespace est rapidement devenue une construction sociale dont l'importance est centrale pour beaucoup d'acteurs. Cet espace et les technologies en son sein ont ainsi été élevés au titre d'objet de sécurisation par une variété d'intervenants. Les attaques et les problèmes techniques dans cet espace ont également marqué l'imaginaire et sont l'objet de beaucoup de fictions et d'œuvres cinématographiques, capitalisant sur une forme de chaos social et technique généralisé en cas d'attaque ou de disfonctionnement majeur.

1.2 Cyberespace et système international

Le fait que le cyberespace soit à la fois poreux, accessible à un grand nombre d'acteurs et marqué par de grandes vulnérabilités crée ce que Chamayou appelle une « crise d'intelligibilité ». Dans cet espace, tout devient plus diffus et difficile à saisir. Les attaques ne sont plus vraiment clairement identifiables, les lignes de front en cas de conflit sont très mouvantes et les différents acteurs en présence sont multiples à s'exprimer sur les questions de sécurisation. Il n'y a pour ainsi dire, plus de monopole de la gestion du système international par les États.

Certains auteurs affirment ainsi que le cyberespace est un espace révolutionnaire pour la guerre et le système international. La dématérialisation des conflits, avancée considérable dans la façon de mener la guerre, couplée à une grande facilité d'accès aux technologies présentes dans le cyberespace, pourrait ainsi venir bousculer la façon dont on perçoit les affrontements dans le système international.

Le cyberespace a également changé la façon dont les États projettent leur force dans le système international. Que ce soit par la modernisation des armées et l'utilisation de nouvelles technologies de communication, de repérage, etc., les technologies de l'information et des télécommunications ont amené beaucoup de changements.

Ces capacités ont également été rendues accessibles à d'autres acteurs, pour la première fois à un tel niveau dans l'histoire. Par l'utilisation de réseaux d'ordinateurs infectés et de logiciels de piratage, des acteurs non étatiques peuvent eux aussi projeter de la force de façon efficace dans le système international. Que ce soient des entreprises privées, des groupes terroristes ou des communautés politiques, ces acteurs peuvent utiliser leur cyberinfluence et d'autres formes de cyberpouvoir pour faire avancer leurs politiques et intérêts.

> Nonstate actors will seek to make cyberspace a medium where guerrilla campaigns, orchestrated dispersal, and surreptitious disruption make large land, sea, and air forces fighting decisive battles irrelevant (Kramer, Starr et Wentz 2009, 268)

Par diverses stratégies dans le cyberespace, ces acteurs pourraient viser des fins politiques, mais aussi de guerre ou de déstabilisation. Que ce soient des entreprises privées menant des opérations d'espionnage industriel, des groupes politiques cherchant à gagner de l'influence dans la sphère publique ou encore des groupes terroristes voulant recruter et diffuser de la propagande, ou bien des criminels souhaitant étendre leurs sphères d'activité, la massification de l'utilisation de technologies liées au cyberespace a créé de nouvelles opportunités pour un grand nombre d'acteurs.

Autre point important, l'apparition des technologies du cyberespace a mené à une reconfiguration des zones de conflits. Dans cet espace, il n'y a que peu ou pas de bataille linéaire, de lignes de front et d'affrontements face à face. Le tout se fait dans un espace mouvant et pouvant être reconfiguré à la volée afin d'en modifier les limites et les routes. L'aspect logiciel du cyberespace permet par exemple de créer de nouveaux chemins d'information ou de couper des routes déjà existantes. C'est la doctrine contemporaine de la guerre elle-même qui est remise en cause dans cet espace.

Cette difficulté de conception des conflits est également à lier avec le fait qu'il est extrêmement ardu d'attribuer correctement les attaques et autres actions dans le cyberespace, puisqu'il est facile de s'y dissimuler et que les lignes de fronts y sont plus floues. Il y a ici un changement de paradigme important dans la façon dont les acteurs projettent la force dans le système international. Le sabotage anonyme ou encore l'espionnage à grande envergure sans être détecté ni laisser de traces pourraient être des moyens de guerre efficaces pour éviter le conflit frontal.

Cette reconfiguration du conflit dématérialisé vient également changer la nature de la violence dans le système international. Comme le souligne Chamayou, « cette forme d'expérience présente une seconde caractéristique d'importance : le fait d'exercer la violence de guerre depuis une zone de paix » (Chamayou 2013, 169) et change donc la façon dont on peut percevoir le conflit.

Dans ce cadre, c'est notamment l'interprétation intersubjective des différents acteurs qui vient cristalliser le conflit ou la menace. Le *speech act* pour réussir à créer un objet référent devient d'autant plus important. En effet, en l'absence de conflit formé physiquement, le discours de la menace ou de l'attaque devient central pour acquérir l'approbation des autres acteurs. La légitimité de la réponse éventuelle vient donc tirer sa source dans la construction intersubjective de la menace et de la gravité de la situation. La capacité à exercer de la cyberinfluence joue alors grandement dans la façon dont la menace est perçue et reconnue par les autres acteurs. Plus un acteur a des capacités de cyberinfluence, plus la création d'un objet de sécurisation sera aisée et rapide, suscitant l'approbation des acteurs référents et la mise en place d'une réponse à l'agression ou à la menace énoncée. Il s'agit en quelque sorte d'une nouvelle forme de capital symbolique détenu non seulement par des États, mais aussi par des sociétés privées spécialisées en sécurité ou responsables de la gestion des réseaux. Cette forme d'influence nouvelle donne du pouvoir à des acteurs non

étatiques, pouvant déclarer l'existence ou l'absence d'une menace. Il s'agit d'ailleurs d'un marché lucratif pour certains de ces acteurs, puisqu'en maintenant la peur des attaques, ces derniers peuvent vendre des solutions de protection.

Les règles d'engagement dans le cyberespace créent également des problèmes d'interprétation et d'application du droit international, notamment des questions relatives au droit de la guerre (voir à cet effet Barat-Ginies 2014). Le droit international n'a notamment pas été prévu pour une dématérialisation des conflits et leur apparition dans une sphère où les questions de souveraineté sont plus floues, où les acteurs sont multiples et où les difficultés d'attribution sont importantes. Dans le cyberespace, il n'y a par exemple plus nécessairement besoin d'un acte d'agression clair pour créer le conflit (la menace ou sa construction intersubjective suffit parfois, voir à cet effet Nieto Gómez 2014), de même que la notion de combattant est presque obsolète puisque de nombreux acteurs non étatiques y exercent leurs capacités d'action et de cyberinfluence.

Ce flou juridique est assez visible dans les règles d'engagement d'organisation de défense comme l'OTAN. Cette organisation, comme d'autres, a décidé d'appliquer dans le cyberespace le droit international déjà existant, malgré les difficultés que cela pose. D'autres organisations comme l'Union européenne ou l'ONU n'ont pas jugé bon de développer un droit du cyberespace ou des éléments de politiques internationales pouvant aider les États à interagir dans ce cadre (pour la comparaison des modèles OTAN-UE, voir Joubert et Samaan 2014). Tout au plus, certains États ont édicté du droit local et régional (dans le cas de l'UE), sans nécessairement se doter des moyens d'appliquer ces textes.

Cette carence du droit international est à lier avec celle de la gouvernance. Marqué par un hégémon partiel, le cyberespace n'a pour le moment pas de structures de gestion qui réponde efficacement à toutes les problématiques que nous venons de

nommer. Les tensions sont d'ailleurs fortes concernant la gouvernance de cet espace, certains groupes de pays voulant avoir leur mot à dire face aux États-Unis.

Cette vision du cyberespace comme étant révolutionnaire pour le système international n'est toutefois pas partagée par tous. Certains avancent que le cyberespace ne fait finalement qu'aider à renforcer des façons de faire la guerre déjà existantes et ne constitue donc pas un changement révolutionnaire. Malgré tout, il nous semble clair que le cyberespace offre des opportunités dépassant largement le seul cadre de l'appui à des opérations militaires classiques. Cette façon de concevoir le cyberespace est d'ailleurs probablement un manque de compréhension des dynamiques de cet espace, puisqu'elle ne prend pas en compte les acteurs non étatiques et les activités que ces derniers peuvent y déployer. Cette vision ne considère pas non plus la capacité d'influence et de guerre que certains États, qui ne sont pas dominant actuellement, pourraient acquérir par la formation d'une main d'œuvre qualifiée agissant dans le cyberespace.

1.3 Un potentiel de guerre totale à ne pas négliger

> In all the wars America has fought, no nation has ever done this kind of damage to our cities. A sophisticated cyber war attack by one of several nation-states could do that today, in fifteen minutes, without a single soldier ever appearing in this country. (Clarke et Knake 2010, 68)

Avec la reconfiguration des zones de conflit dans le cyberespace vient également la modification de la temporalité de la guerre. Dans cet espace, la menace est en fait toujours présente, en sommeil. En effet, dans le cadre de la cyberguerre ou des cyberattaques, la planification des attaques et l'identification de failles dans les systèmes informatiques de potentielles cibles revêt un caractère stratégique fondamental. Qu'il s'agisse des services de renseignements ou des militaires, ces

organisations cherchent fréquemment à s'infiltrer dans des infrastructures sensibles d'éventuels adversaires afin de maintenir des accès à ces systèmes et s'y procurer de l'information à long terme. Il peut également s'agir de rendre ces systèmes hors service lors d'une attaque (Krekel, Adams et Bakos 2012, 96).

Dans notre étude, nous avons par exemple mentionné les cas de piratages d'infrastructures essentielles par la Chine (Clarke 2010, 59). Au fil des années, il est devenu évident que l'armée chinoise utilise les vulnérabilités d'Internet et le piratage informatique en temps de paix afin de procéder à des missions de renseignement et d'espionnage (Krekel, Adams et Bakos 2012, 25). La Chine, comme d'autres États (les États-Unis en premier lieu), aurait donc des programmes d'infiltration dans des infrastructures d'autres pays, même en temps de paix (il a par exemple été révélé en 2014 que des pirates chinois avaient compromis des sattelites météo américains, voir Samenow et Rein 2014). Ces logiciels espions pourraient être activés en cas de conflit, et seraient indétectables entretemps. Cela donne dans les faits des avantages non négligeables aux différents acteurs utilisant ces stratégies.

Si des mesures ont par exemple été prises aux États-Unis (comme l'implantation du réseau *Einstein* qui vise à surveiller le trafic des organismes gouvernementaux et veiller à détecter des anomalies), il reste que de nombreux autres acteurs (États ou non) manquent de protection et de préparation face à ces menaces. Ces vulnérabilités issues d'une grande utilisation des réseaux dans le cyberespace, sont rendues plus dangereuses à cause d'un manque de protection et de coordination des pouvoirs publics avec le secteur privé, notamment.

Le risque est donc important et représente une menace perpétuelle pour les États qui n'ont pour le moment que trop peu fait pour assurer la sécurité de ces infrastructures critiques (que ce soit par l'absence de régulation du secteur privé, par ignorance ou par négligence).

D'autres risques existent également dans les processus industriels de fabrication des produits manufacturés dans des pays tiers. La modification intentionnelle de produits réseaux ou servant à la communication dans le cyberespace a notamment poussé des pays comme le Canada ou les États-Unis à bannir du matériel produit par certaines entreprises chinoises ayant des liens avec l'APL. S'il n'existe pas de preuves formelles que l'APL ait pu intercepter des produits lors de leur production afin d'y intégrer des logiciels pirates, il n'y a toutefois aucun moyen de vérifier l'intégrité de ces composants. Ce risque est d'autant plus crédible que les États-Unis mènent eux-mêmes ce genre d'opérations dans des cas particuliers (voir par exemple Greenwald 2014b; Spiegel 2013; Krekel, Adams et Bakos 2012, 11).

La dispersion importante des marchés d'approvisionnements en composants comme les semi-conducteurs ou les cartes à puces fait qu'il serait possible pour un État ou des conglomérats criminels d'exploiter les vulnérabilités de ces composants contrefaits. Ces technologies, utilisées dans tous les équipements électroniques, se retrouvent en effet dans la majorité des outils utilisés par les États et armées.

> Deliberate modification of semiconductors upstream of final product assembly and delivery could provide an adversary with capabilities to gain covert access and monitoring of sensitive systems, to degrade a system's mission effectiveness, or to insert false information or instructions that could cause premature failure or complete remote control or destruction of the targeted system. The modifications need not to be complex. One of the simplest modifications would be the degradation of the interconnectors that distribute signals and provide power and ground to the various ICs, which will lead to premature failure under load. More complex attacks could introduce entirely new logic through the addition of extra transistors and circuitry. (Krekel, Adams et Bakos 2012, 88)

Cet ensemble de risques et de stratégies déployées en amont des conflits crée une reconfiguration des vulnérabilités des différents acteurs et donc de la façon dont la guerre pourrait être menée. En implantant en temps de paix des logiciels espions

pouvant être utilisés lors des conflits, les États procèdent à la préparation des cyberguerres avant même de se trouver en conflit. La cyberguerre peut donc être partout et déclenchée à n'importe quelle occasion.

Ces stratégies de préparation des conflits sont notamment possibles à cause de la grande pénétration du cyberespace dans nos activités quotidiennes. Puisque « de la dématérialisation des flux financiers au fonctionnement en réseau des feux de signalisation d'une grande métropole, tout est régi par les technologies de l'information et de la communication » (Arpagian 2009a, 70), il existe un grand nombre de vulnérabilités dans les sociétés modernes. La porosité du cyberespace, couplée à des systèmes généralement mal protégés, fait que tout devient une cible potentielle et un risque pour la sécurité dans les pays développés.

Cela est également vrai pour « les entreprises qui gèrent des équipements d'importance vitale » qui utiliseraient des solutions à bas prix, mettant en risque des infrastructures et des systèmes stratégiques (Arpagian 2009a, 70). Pour des raisons économiques et de convenance, les entreprises privées ainsi que les États ont tendance à utiliser des logiciels grands marchés afin de sécuriser des infrastructures sensibles pour le fonctionnement des sociétés humaines. Qu'il s'agisse des réseaux d'électricité ou des oléoducs, ou encore des barrages, la majorité de ces infrastructures est gérée et protégée par des systèmes largement disponibles sur le marché, dont les vulnérabilités ne cessent d'être exploitées. Les implications sont donc grandes tant nos sociétés sont connectées et reposent sur la technologie. La dérégulation et la privatisation des infrastructures essentielles a également été pointée du doigt à répétition comme étant une source de vulnérabilités, puisque les entreprises privées cherchent généralement le profit à court terme plutôt que la stabilité et la sécurité à long terme.

Alignment of executive and owner interests is essential to any free-market

> solution to the infrastructure protection problem. But this alignment is difficult to achieve when income and cost are separated in time and the magnitude of cost in uncertain. This is a case where cost may be imposed a long way in the future and where its amount (and even incidence) is wildly uncertain. In such circumstances, it is extremely tempting for executives to focus on present-day income and neglect the highly uncertain future costs of infrastructure attack (Kramer, Starr et Wentz 2009, 139)

Les failles sont également partout dans notre quotidien le plus immédiat, du photocopieur au cellulaire (une faille de sécurité révélée en 2014 pourrait par exemple permettre à quiconque d'intercepter des appels téléphoniques de façon très simple, voir Timberg 2014b) que nous utilisons en passant par le système de gestion des métros. Tout simplement car, lors de la construction et de la production, personne n'aurait pu penser que de telles attaques pourraient arriver (« they didn't think about people hacking them and turning their systems into weapons » Clarke et Knake 2010, 73). La grande utilisation des technologies du cyberespace dans les activités humaines crée donc un niveau de synergie et d'interdépendance entre sphères étatiques, économiques, civiles et militaires qui a rarement été observé dans l'histoire moderne. Cette connectivité n'est pas sans poser de problèmes puisque parfois les moyens technologiques sont défaillants ou propices à être corrompus, mettant en danger les opérations utilisant ces moyens.

Si la guerre totale existe depuis des siècles, elle nécessitait toutefois d'envahir physiquement les territoires visés et n'était que rarement profitable aux attaquants, qui en subissaient également les contre-couts (problèmes d'approvisionnements, de survie, de contrôle du territoire, etc.). Le cyberespace, en permettant l'attaque à distance, vient modifier cette donne. Il est maintenant possible d'attaquer sans jamais violer la souveraineté physique d'un acteur. Il est également possible de procéder à des attaques massives, pas seulement contre les États ou autres acteurs, mais contre l'intégralité des sociétés visées, du fait de la porosité du cyberespace et de l'interconnexion entre les différentes activités s'y déroulant (Arpagian 2009a, 73).

Ainsi, la guerre à distance peut être totale et viser non seulement les États, mais aussi la société civile, l'économie, les infrastructures essentielles, les entreprises privées, les marchés financiers, les systèmes de transport (ferroviaire, aviation), les médias et systèmes de communication, les hôpitaux, etc. Cette guerre à distance peut avoir différents objectifs, qu'ils soient liés à la déstabilisation d'un acteur, ou encore liés à des enjeux économiques, de défense ou de politique étrangère. Il pourrait donc potentiellement s'agir un jour d'une « arme ultime » pouvant être utilisée à distance (pour remettre en perspective cette question, voir Liff 2012).

Ces attaques auraient d'autant plus de conséquences importantes et tangibles si elles étaient menées dans un contexte plus large d'attaques terroristes ou de guerre. Qu'il s'agisse de conséquences physiques (interruption des services courants et de la vie matérielle), de conséquences pour l'environnement (réseau électrique, d'hydrocarbures, etc.), de conséquences économiques liées au ralentissement ou à la neutralisation de secteurs d'activités, de conséquences politiques liées aux crises liées aux autres conséquences ou à l'incapacité à gérer ces attaques, de conséquences liées à l'ensemble de ces potentialités, la capacité de perturbation et de destruction est massive et peut se décliner à l'échelle de l'ensemble de la société.

Imaginons seulement qu'un acteur mal intentionné décide de couper les réseaux de fibre optique à plusieurs emplacements stratégiques, le potentiel de perturbation serait particulièrement important pour de grands ensembles géographiques et entrainerait probablement une riposte collective de plusieurs acteurs (voir à cet effet l'article sur la « cybergéographie » de Robine et Salamatian 2014) Ce type d'attaques ne demanderait pourtant que peu de ressources, restant à la portée de tout acteur moindrement organisé et étant capable d'envoyer des individus dans plusieurs zones géographiques à la fois. N'importe quel État, entreprise privée de bonne taille ou groupe politique ou terroriste pourrait procéder de la sorte. Si l'on considère la

dépendance aux technologies du cyberespace, il est possible d'affirmer que ces problématiques ne seraient que les premières conséquences négatives liées aux attaques de ce type. Un ensemble d'autres problèmes se poserait du fait de l'absence de systèmes alternatifs pouvant prendre le relais.

Le fait que les échanges dans le cyberespace se fassent à la vitesse de la lumière est également un des enjeux à considérer. Dans le cadre d'une cyberguerre, il y a tout intérêt pour les différents acteurs à attaquer en premier, de peur de se voir priver de toute capacité de riposte. Contrairement aux conflits traditionnels, les attaques dans le cyberespace peuvent avoir des effets instantanés sur les différents systèmes. Il n'y a que peu de délais (quelques millisecondes) entre le lancement de l'attaque et le moment où elle touche sa cible, forçant les acteurs à prévoir le plus possible à l'avance leurs moyens de dissuasion et de défense. Cette rapidité des échanges pourrait également pousser des acteurs à attaquer directement de façon massive tout adversaire afin de limiter ses capacités de réplique. Il y aurait alors une onde de choc se propageant à la totalité des activités dans le cyberespace.

Dans ce contexte, une guerre dans le cyberespace pourrait bien déborder dans l'espace plus classique du système international (voir notamment Libicki 2014). Comme le mentionnait en 2011, la Stratégie internationale pour le cyberespace des États-Unis, une attaque dans le cyberespace pourrait faire l'objet d'une riposte classique :

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means — diplomatic, informational, military, and economic — as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad

> international support whenever possible. (The Executive Office of the President - The White House 2011)

Par l'étendue des sphères touchées en cas de cyberguerre ou d'attaques massives, tant étatiques, civiles, économiques que militaires, ces attaques auraient alors une apparence de guerre totale. Les risques de destruction étant élevés et relativement faciles à mettre en œuvre, il y a donc ici un fort potentiel pour un grand nombre d'acteurs pouvant vouloir déstabiliser des acteurs, États, systèmes internationaux régionaux ou globaux.

1.4 Les États réussissent-ils à assurer leur sécurité?

> Les grands mythes d'invulnérabilité sont presque tous les récits d'un échec [...] La leçon est non seulement que l'invulnérabilité ne saurait être totale, mais encore que toute tentative d'invulnérabilisation engendre en contrepartie sa vulnérabilité correspondante. (Chamayou 2013, 109, 110).

Dans un espace où les attaques se font à distance, sans la confrontation physique habituelle, il est nécessaire de se questionner sur la capacité des États à assurer leur sécurité. Dans cet espace, il n'existe pas vraiment de séparation entre réseaux étatiques, militaires et civils, toutes ces sphères fonctionnant grâce aux mêmes technologies et mêmes infrastructures. Il en ressort que pour la première fois dans l'histoire, les États peuvent être les victimes les plus directes de ces formes de conflit, contrairement à d'autres formes d'affrontements ou de guerre.

Pour pouvoir évaluer l'atteinte de l'objectif qu'est la sécurité, il faut avant tout se poser la question : quel est le type de sécurité en jeu? Pour évaluer cette question dans le cyberespace, il est nécessaire de prendre en compte un ensemble de variables rentrant dans la sécurité élargie. On pensera notamment questions de sécurité économique, au secteur des communications, aux approvisionnements électriques,

aux infrastructures essentielles mais aussi à un ensemble d'activités civiles.

Pour Bockel, les menaces contre les États prennent deux formes : celles portant sur « les services essentiels au fonctionnement du pays ou à sa défense, tributaires de systèmes d'information qui pourraient être visés par des attaques tendant à les paralyser » (Bockel 2012, 11) et celles contre la « protection des informations sensibles », tant politiques, militaires, qu'industrielles. Cette définition est quelque peu limitée et incite à présenter d'autres éléments. Par exemple, il est clair que le fait que des civils perdent des jours de travail ou d'activité économique à cause de vulnérabilités dans le cyberespace est un problème pour les États et les entreprises.

De plus, autant les effectifs insuffisants attribués aux questions liées au cyberespace que les politiques publiques défaillantes concernant les infrastructures essentielles ou la protection des réseaux étatiques nous laissent penser que malgré les efforts investis, il n'existe pas de sécurité réelle. Il y a donc une forme de '*speech act*' non suivie de mesures effectives pour assurer l'accomplissement des objectifs visés.

Compte tenu de la facilité d'accès aux opérations dans le cyberespace, il serait important d'être alerte. En ce sens, le rééquilibre des forces internationales pourrait se faire rapidement si les États ne se décident pas à se doter de meilleures politiques de sécurité élargie :

> When an American President sends U.S. forces to bomb a rogue state's nuclear weapons factory or terrorist camp, that nation may not be able to respond against our impressive conventional military forces. And yet, for a small investment in a cyber war capability, it may respond by destroying the international financial system, in which it has very little stake (Clarke et Knake 2010, 259)

Il nous semble ainsi que les stratégies mises en avant par les États sont généralement insuffisantes ou mal articulées. Ces derniers misent parfois plus sur une surveillance

de masse des réseaux que sur une protection des infrastructures et une sécurisation afin de limiter les vulnérabilités. De même, cibler le grand ensemble du cyberespace plutôt que des industries clés relève d'un autre choix qui n'est pas forcément bien avisé. En ciblant tout le monde et personne à la fois, ces stratégies ne font finalement que tenter d'attraper des bribes d'information, sans réellement contraindre des acteurs clés à sécuriser des infrastructures essentielles, par exemple. Le récent piratage de Sony laisse d'ailleurs entendre que malgré l'énorme appareil de surveillance mis en place par les États-Unis, celui-ci est totalement inefficace pour attribuer correctement la source des attaques (Taia Global 2014). Cela n'a malgré tout pas empêché la France d'adopter une loi (jugée liberticide par beaucoup) sur la surveillance massive des réseaux (Tual 2015; Valls), malgré les réticences marquées tant par son Conseil d'État (Conseil d'État 2014) que par le Conseil de l'Europe (Omtzigt 2015; Harding 2015) face aux violations de la vie privée que cette surveillance peut entrainer. Les États-Unis, cibles de nombreuses critiques pour sa surveillance du cyberespace, ont également renforcé leurs outils législatifs et juridiques dans cet espace au début 2015 (Greenberg 2015a).

Par les différentes autres vulnérabilités existant dans la société civile et pouvant mener à des violations de la souveraineté des États ou à des actes d'agression, il nous semble possible d'affirmer que la sécurité en tant que concept polymorphe est loin d'être atteinte dans le cyberespace.

2. Pourquoi n'y a-t-il pas encore eu de cyberguerre ou d'utilisation des outils présents dans le cyberespace par des pays du sud ?

S'il existe, comme nous l'avançons, un risque de guerre totale lié aux projections de la force dans le cyberespace, il est alors nécessaire de se questionner pour savoir pourquoi un tel conflit n'a pas déjà eu lieu. Bien que plusieurs conflits récents aient

été marqués par l'utilisation des technologies présentes dans le cyberespace, que ce soit dans le cadre de conflits sur des questions de politique régionale (Estonie 2007) ou encore en appui à des opérations classiques (Géorgie 2008), il n'y a eu aucun cas de cyberguerre majeure jusqu'à présent.

Quelques éléments peuvent expliquer cette absence de réelle cyberguerre à grande échelle. Premièrement, si le cyberespace offre des opportunités stratégiques intéressantes et peut offrir de nouvelles capacités de projection de la force à des acteurs non-dominants, il reste que la dissuasion classique joue encore un rôle important dans les relations internationales. En cas de cyberattaque massive, les victimes pourraient toujours répliquer par la projection d'une force militaire, voire par l'utilisation potentielle de la force nucléaire dans le cas des États-Unis (Department of Defense, Defense science board 2013).

De plus, une perturbation massive des activités dans le cyberespace dans le but de déstabiliser le système international ou les sociétés occidentales, voire le capitalisme mondialisé, ne serait pas pour le moment profitable aux attaquants. Il existe par exemple encore de forts liens de dépendance économique, politique, financière, etc. entre nord et sud. Les pays du sud, qui auraient le plus grand intérêt à déstabiliser le système international, n'ont pas non plus une capacité d'organisation suffisante pour mener de façon conjointe des cyberattaques massives.

Enfin, d'autres acteurs n'ont pas nécessairement intérêt à voir s'effondrer le système tel qu'il existe actuellement. Soit parce qu'ils profitent largement de son fonctionnement, soit parce qu'ils visent plutôt la réforme du système plutôt que son remplacement par un autre modèle.

2.1 La question de la dissuasion

Dans le cyberespace la question de la dissuasion joue un rôle important dans la prévention des conflits entre acteurs. Comme les autres domaines, le cyberespace est marqué par un système complexe d'interactions et de menaces, conditionnant la conduite de la politique internationale par les différents acteurs.
Dans toutes nos recherches un élément récurent est identifiable : toute stratégie de dissuasion dans le cyberespace doit se baser sur les autres espaces de la guerre et des activités humaines. La dissuasion dans le seul cyberespace aurait en fait une efficacité assez limitée. Cela serait notamment vrai en cas d'attaque rendant non opérationnels les réseaux de défense dans le cyberespace ou encore dans des cas de cyberattaques menées par des acteurs non étatiques ou des pays ne faisant pas une grande utilisation des technologies présentes dans cet espace.

Pour les différents acteurs, il est important d'adapter ces théories de la dissuasion face aux menaces en présence (« the United States will need a strategy of 'tailored' cyber deterrence that treats each category of potential adversary, type of attack, and type of U.S. response on its own merits » (Kramer, Starr et Wentz 2009, 310)). Par exemple, une entreprise ne répondra pas de la même façon à une cyberattaque qu'un État ou qu'une organisation internationale. Différentes formes de dissuasion et de ripostes existent donc. Certains acteurs ne possédant pas de forces armées pourraient préférer dénoncer les attaques dans la sphère publique afin de susciter une réponse d'autres acteurs (étatiques par exemple, surtout si les cibles sont stratégiques), garder secrètes ces attaques (de peur d'être ciblé à nouveau ou de perdre de la crédibilité), blâmer d'autres acteurs concurrents afin de leur faire perdre du soutien dans le système international, etc. Dans ces cas, la dissuasion ou la menace passe largement plus par l'énonciation d'un discours dans la sphère publique que par le spectre de la menace armée.

Par ailleurs, compte tenu des spécificités du cyberespace, la dissuasion fonctionnerait nécessairement dans un cadre plus large que les relations internationales et les actions

conventionnelles. Face à des acteurs qui ne sont plus nécessairement des États-nations mais plutôt des groupes terroristes ou des groupes d'activistes qui sont prêts à prendre plus de risque tout en n'étant pas nécessairement touchés par les ripostes classiques, les différentes stratégies doivent être adaptées. L'intensité et la forme des attaques doivent également être prises en compte dans cet espace. Violer une frontière dans le cyberespace est par exemple nettement plus commun que dans le monde physique où un tel acte pourrait générer d'importantes tensions diplomatiques (Kramer, Starr et Wentz 2009, 329).

De plus, pour des acteurs dominants, il n'est pas nécessairement intéressant de déclencher une guerre dans le cyberespace puisqu'une riposte économique, diplomatique ou militaire classique pourrait avoir des effets dissuasifs ou punitifs bien plus efficaces et durables.

Même si la dissuasion dans le cyberespace est importante, il reste qu'elle est parfois difficile à appliquer. Différent obstacles peuvent empêcher l'adoption ou l'application de politiques de dissuasion efficaces. Par exemple, l'absence de moyens efficaces pour évaluer la puissance dans le cyberespace crée une double dynamique : elle décourage certains acteurs de mener des cyberattaques afin de ne pas gaspiller de ressources contre des défenses perçues comme efficaces ; et elle peut au contraire inciter des attaquants à passer à l'acte puisqu'ils ne pensent pas raisonnablement s'exposer à une riposte considérable.

Un autre des obstacles se présentant à l'application de stratégies de dissuasion est la grande difficulté d'attribution des attaques. Le fait que le cyberespace favorise un anonymat relatif rend difficile pour les États et autres acteurs d'identifier les auteurs des attaques et d'y riposter de façon légitime. Il est donc malaisé d'appliquer des théories de la dissuasion classiques puisqu'il est difficile de cibler précisément l'origine d'une attaque, faute de preuves tangibles dans la majorité des cas (Kramer,

Starr et Wentz 2009, 273). Dans ces cas, c'est essentiellement le discours qui va justifier ou non la riposte et la réaction de la cible des attaques. En faisant entrer en jeu des concepts philosophiques ou des analyses intersubjectives, les acteurs peuvent formuler un discours pour justifier des représailles.

La dissuasion repose donc grandement dans la projection sur les autres acteurs de la représentation de sa propre force et du discours de sécurisation. Il a par exemple été clairement énoncé par les États-Unis que toute attaque massive dans le cyberespace pourrait entrainer le déclenchement automatique de réseaux de contre-attaque, sans même une intervention humaine (Zetter 2014a). Toute attaque massive contre ce pays serait également considérée comme un acte de guerre classique. Ces *speech act* participent à l'articulation d'un discours de la dissuasion, qu'ils soient réalistes ou non, puisqu'ils font partie des éléments que chaque acteur se doit de considérer avant de procéder à une attaque. Les différentes menaces et discours peuvent donc servir comme outil de dissuasion dans le système international (pour un aperçu complet de la question des menaces dans la cyberstratégie, voir Douzet 2014).

Les ripostes les plus efficaces seraient peut-être des ripostes ne passant ni par la sphère militaire ni par l'utilisation de moyens de projection de la force dans le cyberespace. D'autres moyens de riposte comme les sanctions économiques, l'isolement diplomatique ou la perte de statut dans le système international pourraient être aussi, voire plus, efficaces que les moyens de dissuasion armés (Kramer, Starr et Wentz 2009, 329).

Enfin, notons que si la question de l'attribution des attaques est une problématique importante, un certain nombre d'acteurs risquent toutefois de revendiquer publiquement leurs attaques ou d'avancer des menaces. Notamment dans le but de faire avancer leurs intérêts dans le système international. Il faut donc nuancer cet obstacle à l'application de stratégies de dissuasion.

2.2 Dépendance nord-sud, développement économique et politique étrangère dans le cyberespace

Un autre élément jouant un rôle important dans l'absence de cyberguerres menées par des acteurs non dominants est la domination du nord grâce au capitalisme mondialisé. Par l'imposition de ce mode de production et la division internationale du travail, se sont créés des liens de dépendance entre acteurs. Il s'agit notamment du cas des relations nord-sud, qui nous intéressent particulièrement.

Promoteur de la division internationale du travail, l'Occident, qui domine le capitalisme mondial depuis au moins deux-cents ans, a été en mesure d'imposer des types d'économies et d'industries aux pays du sud (par le colonialisme notamment). De façon classique, les pays du sud ont des industries à faible intensité technologique et servent avant tout d'« armée de réserve » aux industries occidentales. On y délègue des tâches ne requérant que peu d'expertise et ne générant pas une valeur ajoutée importante, alors que l'occident conserve les étapes à haute intensité technologique et à grande rentabilité (conception, recherche, mise en marché, etc.). Dans ce cadre, et même si des pays du sud ont misé sur des politiques de transfert technologique à long terme, l'occident garde le contrôle sur la production et sur les différentes sphères de l'activité économique. Il est d'ailleurs notable que seuls quelques pays du sud sont à même d'imposer de telles politiques de transfert technologique, la majorité semblant figée dans des rôles subalternes.

Si cette division du travail et de la production crée aussi des liens de dépendance pour le nord, dans la mesure où la production est délocalisée et repose sur la collaboration

des pays du sud, il demeure quand même que ce sont ces derniers qui sont les perdants en cas d'arrêt de la production imposé par les pays du nord (pertes d'emplois, de revenus, d'expertise, de capitaux étrangers, etc.). De plus, même si les pays du sud représentent des marchés importants pour les entreprises privées et le complexe militaro-industriel financé par les États, les pays du nord pourraient subsister et se maintenir sans ces nouvelles zones d'activité économique.

Il est donc clair que les pays du sud ont des liens de dépendance face aux Occidentaux. Ne serait-ce qu'en vertu des différents accords internationaux, ces pays s'exposent à d'importantes pénalités en cas de rupture du commerce international ou d'attaques contre le nord. Ainsi, les menaces d'isolement économique au niveau international, de sanctions financières, d'exclusion de traités commerciaux, etc. créent une dépendance doublement forte dans le capitalisme mondial. Il nous semble donc que cet impérialisme économique du nord et la menace de représailles économiques doivent jouer pour beaucoup dans l'équation de la cyberguerre et de son absence jusqu'à présent.

Cette dépendance est également liée au système financier international. Dans un monde où ce sont majoritairement les monnaies occidentales qui servent pour le commerce international (et de réserve) et la projection d'une forme de pouvoir économique, il serait périlleux pour des pays du sud de s'attaquer à ceux qui contrôlent ces devises. D'une part, la dévaluation du dollar ou de l'euro pourrait entrainer un effondrement des économies en question, d'une autre part la majorité des réserves monétaires planétaires se font dans ces monnaies. Il n'y a donc que peu d'intérêt à faire s'effondrer le cours de ces devises, tant et aussi longtemps qu'une autre devise n'est pas en position de force. Si le yuan chinois tend à prendre en importance, il reste sous le contrôle total de l'État et est maintenu artificiellement à un niveau favorable à l'économie nationale. Il n'y a donc pour le moment aucune devise venant d'un pays du sud capable de rivaliser avec le dollar américain. Tout

effondrement de cette devise aurait alors un impact important sur les pays du sud.

Notons également que les bourses mondiales les plus importantes sont encore situées dans des pays occidentaux. La capitalisation des entreprises du sud passe d'ailleurs généralement par ces bourses. Il y a donc ici aussi un lien de domination et de dépendance économique entre le nord et le sud. En cas d'effondrement de ces bourses, les pays du sud verraient eux aussi leurs fleurons industriels gravement menacés et handicapés par les circonstances.

Il faut toutefois souligner les efforts des BRICS dans l'établissement d'institutions financières et de coopération dans le développement. Ces pays ont par exemple lancé en juillet 2015 la Nouvelle banque de développement (Golubkova 2015; Agence France-Presse 2015b), visant à favoriser la coopération entre pays du sud. Il s'agit également de concurrencer des institutions comme la banque mondiale et le FMI qui sont perçus comme étant avant tout des instruments de contrôle et de puissance de l'hégémon américain. Cette banque devant être opérationnelle dès la fin de l'année 2015 pourrait ainsi venir bousculer la façon dont le système financier international fonctionne entre pays du nord et pays du sud.

De plus, rappelons que par sa structure, le cyberespace est également à risque pour les pays du sud en cas de cyberguerre. Puisque les fibres optiques sont les mêmes pour tout le trafic à travers le monde et permettent à des ensembles géographiques aussi grands que des continents de communiquer entre eux, toute attaque contre ces infrastructures aurait des répercussions importantes sur les pays du sud. En l'absence de stratégie de ces pays visant à se doter de réseaux alternatifs (notons toutefois l'initiative du Brésil de se doter de réseaux de fibre optique leur appartenant, voir Robertson 2014b), il est difficile d'envisager des cyberattaques massives contre les infrastructures de l'Internet, partagées à l'échelle mondiale.

Si le cyberespace peut servir d'espace d'*empowerment* pour les pays du sud, cette théorie reste à nuancer. Dans un mode de production où la domination nord-sud est au cœur de la division internationale du travail et des activités économiques mondialisées, il semble clair que les pays du sud ont pour le moment plus à perdre qu'à gagner en menant des opérations de cyberguerre contre l'occident.

Par ailleurs, comme nous le verrons plus tard, il semble clair que l'espionnage industriel et l'exploitation du cyberespace à des fins commerciales sont pour le moment plus rentables que la mise en place de capacités offensives contre l'Occident. Il y a en effet beaucoup plus à tirer dans l'espionnage à grande envergure de sociétés occidentales fortes d'un savoir industriel et technique pouvant être récupéré afin de développer des industries locales que de chercher à détruire ces entreprises.

2.3 La désorganisation actuelle des pays du sud contrairement à la période des « non alignés »

En plus de la dissuasion, un autre point fondamental pour expliquer la non-utilisation des moyens de cyberguerre par un ensemble de pays du sud contre l'occident est leur désorganisation politique sur le cyberespace. Cette désorganisation est notamment liée à la domination américaine dans le cyberespace; aux politiques étrangères occidentales lors du XXe siècle ainsi qu'aux différences dans les types de régimes politiques, économiques et culturels.

Comme nous l'avons vu précédemment, la gouvernance du cyberespace a longtemps été marquée par le contrôle quasi-total des États-Unis. Le contrôle technique et technologique exercé sur le cyberespace a notamment eu pour effet de décourager la participation d'autres acteurs, tout en mettant les États-Unis en position dominante dans cet espace. Le contrôle des normes techniques et technologiques par les États-

Unis en tant que principale source d'innovation a également joué un rôle important dans la possibilité pour d'autres acteurs de s'organiser et de contester cette domination. Cette dynamique est toutefois lentement en train de changer avec l'arrivée de concurrents, chinois notamment (comme Huawei), à même d'établir de nouveaux standards technologiques et de fournir des équipements de bonne qualité et à bas prix à travers le monde.

Une autre raison expliquant la désorganisation des pays du sud face à la domination occidentale se trouve dans les politiques que les pays du nord ont menées tout au long du XXe siècle et en ce début de siècle. Si le XXe siècle est couramment appelé le siècle des idéologies, il faut rappeler que la concurrence entre blocs de l'Ouest et de l'Est est aussi passée par une forme renouvelée d'impérialisme militaire, économique et culturel. Les pays du sud en ont souvent été les premières victimes. Par exemple, les États-Unis se sont distingués comme l'État ayant le plus misé sur cette forme de pouvoir pour maintenir une domination dans ses zones d'influence et limiter la montée en puissance d'autres acteurs. Que ce soit en renversant des régimes élus (Syrie 1949; Iran 1953; Guatemala 1954; République dominicaine 1961; Brésil 1964; République démocratique du Congo 1965; Chili 1973; Argentine 1976; Afghanistan 1979-1989; Turquie 1980), en finançant des guérillas d'extrême droite (Colombie 1964 à maintenant; « Contras » au Nicaragua 1981-1990 ; Salvador 1979-1992) ou encore en soutenant logistiquement et par le biais de la propagande des révoltes organisées par des élites économiques ou sociales (Pologne 1980-1989; Iran 2005 à maintenant), les États-Unis ont une politique étrangère très interventionniste. D'autres pays, comme l'Union soviétique (Tchécoslovaquie 1968; Afghanistan 1979-1989), et d'autres puissances coloniales (membres de l'OTAN, Belgique, France, etc.) se sont illustrées par ces mêmes politiques impérialistes.

Cette hégémonie bipolaire a notamment donné lieu à des rapprochements entre certains pays du sud ne voulant se soumettre à aucun des deux blocs. C'est de cette

façon qu'est né le Mouvement des non-alignés au début des années 1960. Il s'agissait de défendre l'indépendance et la souveraineté de chacun des États membres sans se ranger derrière un des deux hégémons en présence. Dans la déclaration de la Havane en 1979, le Mouvement des non-alignés se positionnait également contre l'impérialisme, le colonialisme, toutes formes de racisme, d'expansionnisme et d'hégémonie. La déclaration de la Havane mettait aussi en avant la recherche d'un système international plus juste ainsi qu'un nouvel ordre économique dans lequel les pays émergents ne seraient pas soumis à l'impérialisme des deux blocs rivaux (Non-Aligned Movement 1979).

Malgré l'importance des principes adoptés par les non-alignés, cette alliance n'a finalement eu que peu de poids face aux hégémon présents dans le système international. Certaines collaborations ont eu lieu dans des cas de conflits (par exemple lors de l'intervention de Cuba en République Démocratique du Congo dans les années 1960), sans nécessairement fondamentalement changer la façon dont le système international fonctionne. L'absence volontaire de liens militaires ou d'engagements armés en cas d'attaque contre un des membres de cet ensemble a également fragilisé les capacités d'organisation et de projection de la force de cet ensemble.

Les solidarités économiques se sont depuis relâchées au profit d'une recherche de l'intérêt individuel. La concurrence internationale s'est en fait accentuée avec la mondialisation du capitalisme et la division internationale du travail telle qu'elle existe depuis la fin des années 1980. Chaque État rentre donc en concurrence avec les autres et doit faire preuve d'initiative afin d'obtenir une part de la production et des ressources qu'elle peut amener.

Dans ce cadre, le mouvement des non-alignés, bien qu'il existe encore et regroupe la plus que la moitié de la population planétaire, semble avoir perdu de son intérêt pour

différents États. Les dynamiques internationales ayant évolué depuis la fin des politiques formelles de colonialisme, en plus de la perception d'un ralentissement de l'impérialisme occidental au profit d'acteurs montants (BRICS, Asie de l'Est), le mouvement des non-alignés a peiné à maintenir un discours actualisé et revendicateur dans le système international. On voit plutôt des alliances se faire sur des sujets précis (militaire, technologie, économie, etc.) entre États ayant des positions communes ou des intérêts semblables. C'est notamment le cas des BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud) qui sont tous des pays nouvellement industrialisés (réindustrialisé dans le cas de la Russie) ayant des économies dynamiques marquées par un fort taux de croissance, ainsi qu'une influence régionale et mondiale considérable.

Les BRICS sont également les principaux concurrents des États-Unis dans la gouvernance contestée du cyberespace. Comme nous l'avons vu précédemment, ce groupe de pays a commencé à revendiquer une plus grande place dans la gestion du cyberespace et de l'Internet. Ce sont également les BRICS qui ont pris les moyens les plus audacieux pour tenter de contourner ou renverser l'hégémon partiel américain. A l'exemple du Brésil, certains membres des BRICS ont par exemple commencé à poser des nouveaux câbles sous-marins afin de ne pas faire passer leur trafic par des infrastructures américaines, susceptibles d'être surveillées.

Ce sont aussi les BRICS qui ont fait part de la façon la plus virulente de leur opposition à la surveillance généralisée du trafic dans le cyberespace, notamment par les États-Unis et d'autres pays appartenant au groupe des *Five eyes* (Grande-Bretagne, États-Unis, Australie, Canada et Nouvelle-Zélande). Cette opposition à la surveillance tire ses racines de considérations politiques (secret des communications diplomatiques et gouvernementales), économiques (le Canada a par exemple espionné le Brésil afin de voler des secrets industriels et avantager des compagnies canadiennes, voir Lukacs et Groves 2013), philosophiques (refus de l'espionnage à

grande échelle des populations) ou encore de facteurs liés aux politique étrangères et nationales, comme le fait de vouloir influencer le système international (ou national) sans être surveillé par un hégémon.

Si les BRICS semblent pour le moment motivés par la volonté de réclamer prudemment une part croissante de la gestion du cyberespace face aux États-Unis, ces puissances pourraient utiliser le cyberespace de façon plus agressive. Les BRICS possèdent en effet toutes des stratégies de projection de la force dans le cyberespace et montrent un intérêt marqué pour les technologies qui y sont présentes. Malgré cette potentielle force commune, les BRICS n'ont pas encore trouvé de terrain d'entente sur l'utilisation du cyberespace et quelle forme sa gouvernance devrait prendre. Comme nous l'avons vu, le sous-groupe IBSA (Inde, Brésil, Afrique du Sud) est en porte à faux avec la Russie et la Chine sur la question de la gouvernance et de l'encadrement des activités sur Internet. Alors que l'IBSA désire une gouvernance plus ouverte et plus démocratique, la Russie voudrait voir un encadrement formel du droit international dans le cyberespace, tout en étant très opportuniste dans ses choix politiques entourant la question. Quant à la Chine, elle défend une vision nationale du contrôle des activités dans le cyberespace, marquée par ses impératifs de politique intérieure (gestion d'Internet, censure, contrôle du trafic, etc.).

Ces divergences philosophiques et politiques concernant le cyberespace montrent que les BRICS ne sont pas capables pour le moment de renverser l'hégémon américain. Il s'agit plutôt d'une stratégie assez lente d'expansion et de contestation.

Que ce soit le cas des non-alignés ou des BRICS, il semble clair que tant qu'il n'existera pas un front commun de pays et d'organisations visant à revendiquer une plus grande collégialité dans la gestion du cyberespace, les États-Unis et ses alliés ne seront pas réellement menacés. Cette absence de structure collective et revendicatrice est d'ailleurs un gage de sa sécurité. Mentionnons également que d'autres

organisations comme l'Union Européenne n'ont pas grand intérêt à bousculer le fonctionnement actuel du cyberespace puisqu'ils en tirent de nombreux avantages, préférant donc collaborer avec les États-Unis que de les confronter.

Soulignons enfin que les pays du sud n'ont pas nécessairement un intérêt politique suffisamment fort pour renverser la structure du cyberespace et tenter de bousculer en profondeur le système international. En effet, une question importante à se poser dans le cadre de l'utilisation des moyens d'attaques dans le cyberespace est celle de l'émancipation des puissances en voie de développement. Les études critiques de la sécurité nous fournissent ici un cadre d'analyse intéressant. À savoir, que la guerre n'est pas nécessairement un moyen d'émancipation, pas plus que le développement économique. Les pays émergents seraient-ils plus prompts à s'émanciper si l'occident était victime de son développement technologique? Y aurait-il un monde meilleur pour les pays du sud si l'occident, encore majoritairement impérialiste, tombait et que le développement international ralentissait?

Si l'on considère que le développement économique tel qu'il est prôné actuellement est bénéfique aux pays du sud à long terme (ce qui est loin d'être une certitude), renverser le système international ne serait pas nécessairement profitable à ces pays. En effet, les pays du sud bénéficient tout de même (maigrement) en partie du capitalisme mondial et ne sont pas en mesure dans l'immédiat de produire des technologies à haute intensité de capital et de valeur ajoutée. Sur le long terme cette donne pourrait changer puisque les BRICS et d'autres pays du sud développent des capacités de production de biens à haute valeur ajoutée. Ces pays pourraient alors avoir intérêt à bousculer le système international, quitte à être eux-mêmes victimes de cyberguerres.

2.4 Autres acteurs dans le cyberespace

Le cyberespace n'étant pas investi exclusivement par les États, on peut se demander pourquoi d'autres acteurs n'ont pas encore mené de réelles attaques massives. Nous nous pencherons sur les cas des groupes terroristes et des organisations politiques afin de comprendre pourquoi les États et entreprises privées sont relativement en sécurité.

2.4.1 Groupes terroristes

L'avènement des guerres irrégulières (guérilla, combats urbains, absence d'armée, combattants civils, etc.) a mené à de nombreuses évolutions dans la façon dont sont perçus les conflits et le droit de la guerre (voir notamment l'excellent ouvrage « Nouvelles guerres et théorie de la guerre juste » de Flükiger 2011). Avec la massification des technologies du cyberespace dans les sociétés occidentales, il est raisonnable de se questionner sur la pertinence de mener des actes de cyberterrorisme.

Kramer et al. définissent le cyberterrorisme comme étant le pendant des actes de terrorismes classiques, mais dans le cyberespace. Pour être qualifiée comme cyberterrorisme, une attaque devrait avoir des effets similaires aux attentats classiques (destruction, mort, contamination des eaux par exemple).

> a computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, planes crashes, water contamination, or major economic loss would be examples... *Attack that disrupt nonessential services or that are mainly a costly nuisance would not be cyber terrorism.* (Kramer, Starr et Wentz 2009, 438)

D'une part ces attaques seraient assez peu onéreuses à mener, d'autre part elles

seraient intéressantes puisqu'elle n'exposerait que peu les attaquants à une riposte physique. En conduisant des attaques massives à distance, les groupes terroristes pourraient infliger des dégâts importants à leurs cibles, qu'il s'agisse d'États ou non. Ces attaques massives offriraient l'avantage d'être difficiles à arrêter et à contrer, tout en se faisant en sécurité pour les assaillants puisqu'il est complexe de réussir à identifier correctement les sources de cyberattaques dans le cyberespace.

Dans la mesure où il est assez simple de projeter de la force dans le cyberespace, que ce soit par le biais de cyberattaques, ou d'attaques contre les infrastructures physiques (câbles sous-marins, *data center*, relais de fibre optique, etc.), il est étonnant de ne pas avoir observé d'attaques de grande envergure de la part de groupes terroristes. Il y a malgré tout peu de risques que les groupes terroristes se tournent vers des *hackers* ou des groupes criminels. Premièrement parce que ce sont des groupes différents, dont les motivations divergent et que cela représenterait un risque d'infiltration et de sabotage pour les groupes terroristes. Mais aussi car ces deux catégories d'acteurs ont besoin des infrastructures existantes afin de continuer leurs activités.

Sur cette question, de nombreux auteurs s'accordent pour avancer que les groupes terroristes n'ont pas d'intérêt à mener des cyberattaques d'envergure contre des États. D'une part, ces groupes bénéficient bien plus d'une utilisation criminelle (levée de fonds, crime organisé, etc.) et médiatique (cyberinfluence, propagande, etc.) des technologies du cyberespace. D'autre part, en cas d'attaques massives, il serait probable que l'État ciblé accuse un autre État d'apporter le soutien au groupe terroriste. Cela mettrait non seulement en péril la sécurité de l'État allié aux groupes terroristes, mais aussi celle des groupes eux-mêmes en cas de réponse militaire classique.

Il nous semble également important de nuancer la portée symbolique des actes de cyberterrorisme. Par son caractère en grande partie dématérialisé, ces formes de

terrorisme ne frapperaient probablement pas autant l'imaginaire qu'une attaque terroriste classique. À moins qu'une cyberattaque massive ne vienne perturber un ensemble de réseaux et de services en même temps, créant un chaos organisationnel, il est moins frappant de subir des cyberattaques que de faire exploser une bombe ou de rentrer dans un lieu public et se mettre à tirer au hasard parmi les personnes présentes. En ce sens, les cyberattaques n'auraient en quelque sorte pas l'attrait des attaques terroristes pour les groupes qui les mènent : frapper l'imaginaire, instiller un climat de peur et tenter d'influencer par le fait même les décisions politiques des différents acteurs. Ainsi, même en cas d'attaque dommageable à l'économie ou aux services de l'État, le cyberterrorisme n'aurait probablement pas la même puissance symbolique que les attentats classiques (Kramer, Starr et Wentz 2009, 448).

Les groupes terroristes ont donc jusqu'à présent utilisé Internet et le cyberespace majoritairement pour faire de la propagande (de façon parfois très efficace, comme dans le cas de Daech. Voir par exemple Farwell 2014) ou s'organiser et non pour cibler des armées ou des infrastructures essentielles. Il y a également une utilisation intensive du cyberespace à des fins criminelles pour financer les activités de ces groupes dans certains cas (groupes de narcotrafiquants en Colombie, par exemple).

S'il y a eu quelques exemples de piratages de drones, cela reste toutefois assez mineur en termes d'importance stratégique et militaire. D'autres cas ont rapportés de piratages de sites Internet gouvernementaux ou politiques et médiatiques (Farhi et Tsukayama 2013) dans le cadre de l'exercice plus large du cyberpouvoir dans le système international (pensons par exemple à la « Syrian Electronic Army », voir Kristanadjaja 2014). Ces piratages isolés n'ont pas mené à l'utilisation de moyens technologiques contre les armées les utilisant, ni plus à de véritables attaques terroristes sur des réseaux d'infrastructures essentielles ou contre des armées (voir à cet effet Kempf 2014).

Ainsi, il nous semble que les groupes terroristes ont pour le moment plus à gagner en investissant le cyberespace à des fins criminelles ou de propagande. Cela ne veut pas dire que cette situation va perdurer indéfiniment, mais dans un avenir proche, il serait étonnant que cela change.

2.4.2 Les groupes politiques sortent rarement du spectre libéral et sont une force négligeable pour le moment

De même que pour les groupes terroristes, les groupes d'activistes politiques ne semblent pas faire une utilisation intéressante des moyens liés au cyberespace en termes de capacité offensive. Certes, le cyberespace aide ces groupes à s'organiser et à diffuser leurs messages, mais ils utilisent rarement des cyberattaques pour faire avancer leurs idées ou faire pression sur d'autres acteurs.

Dans les quelques cas où nous avons pu voir des utilisations dommageables (comme les différentes attaques menées par le groupe *Anonymous*), ces groupes n'avaient finalement pas de visées anticapitalistes ou visant à remettre en question le système international, limitant la portée de leurs critiques et de leurs actions à un cadre philosophiquement libéral acceptant généralement l'ordre international.

En fait, ces attaques sont généralement menées en réaction à des événements sociaux ou politiques suscitant la colère ou l'indignation des membres de ces groupes. Il y a en filigrane l'idée de rétablir une justice, déficiente dans son application par les instances étatiques, d'exposer des vérités et ainsi de suite. Certaines attaques ont un fondement politique, comme dans le cas d'attaques contre des États ou des partis

politiques racistes, xénophobes, etc. Cela ne représente toutefois pas fondamentalement une menace pour qui que ce soit d'autre que dans les cas spontanés et limités à des critères de justice libérale et de réformisme politique.

Ces cyberattaques restent d'ailleurs peu sophistiquées et limitées à l'utilisation plutôt mécanique de logiciels rendant la chose extrêmement simple d'accès. Il y a en quelque sorte une volonté de se réapproprier un pouvoir de manifestation délaissé par les civils dans la sphère physique de nos sociétés. En bloquant l'accès à un site Internet, à des services gouvernementaux, à des sites d'entreprises privées, etc. les membres de ces collectifs exercent une forme de pouvoir qui pourrait s'apparenter à piquet de grève dans d'autres contextes.

À notre avis, il s'agit donc plus de manifestations de l'utilisation d'une forme de pouvoir politique actualisée grâce aux technologies présentes dans le cyberespace que d'une vraie menace systémique et globale. Le fait que ces collectifs ne soient que rarement anticapitalistes, par exemple, peut nous indiquer qu'il manque à ces groupes un ensemble de réflexions politiques et économiques nécessaires à l'élaboration de visées révolutionnaires. Si ces groupes politiques, qu'ils soient nationalistes ou ayant d'autres motivations politiques peuvent avoir des impacts importants et peuvent causer des dégâts ou divulguer des documents secrets, la menace de changements réels qu'ils représentent est quasiment nulle pour le moment. Le cas de la cybercriminalité, que nous aborderons par la suite, est par contre bien plus inquiétant et menaçant.

CONCLUSION

Au fil de la présente recherche nous avons pu étudier les politiques de massification de l'éducation de certains pays du sud. Ces politiques originellement mises en avant afin de dynamiser le développement économique ont apporté avec elles d'importants avantages dans la capacité à utiliser des technologies de l'information et des télécommunications à différentes fins.

Après avoir étudié des cas d'utilisation par des pays du sud de technologies du cyberespace dans le système international, il semble clair que ces capacités représentent un avantage dans la projection de la force et la conduite de différents types d'activités dans le cyberespace. Que ce soit à des fins diplomatiques, militaires ou économiques, les pays du sud ayant adopté des stratégies de massification de l'éducation ont donc développé des avantages humains dans le cyberespace qui pourraient leur permettre à terme de concurrencer les pays du nord.

La grande vulnérabilité des pays occidentaux pourrait d'ailleurs devenir un levier intéressant pour les puissances émergentes. Que ce soit par les BRICS ou d'autres puissances, l'utilisation de technologies de cyberguerre ou d'espionnage industriel pourrait reconfigurer de façon profonde le système international. En l'absence de stratégies de cyberdéfense convaincantes, les pays du nord restent vulnérables et exposés aux cyberattaques pouvant les viser. Cela est également vrai pour les entreprises privées qui ne sont que trop peu conscientes des risques liés à l'espionnage industriel dans le cyberespace.

Malgré tous ces facteurs, il nous semble tout de même que le renversement du système international n'est pas proche. La dissuasion et les liens de dépendance nord-

sud sont encore trop prégnants pour permettre aux pays du sud d'aller de l'avant. L'absence de front commun unifié visant le renversement de l'hégémon partiel américain et de ses alliés est également une condition ne favorisant pas l'utilisation des moyens de la cyberguerre contre ces derniers.

Il est donc possible de souligner que si ces risques et possibilités existent et pourraient devenir réalité dans un avenir plus ou moins éloigné, les conditions ne sont pour le moment pas remplies pour assister à un renversement du système international. Comme nous allons le voir, cela ne veut toutefois pas dire que d'autres menaces plus immédiates ne subsistent pas dans le cyberespace.

1. Cybercrime et espionnage industriel : la plus grande menace?

Dans la mesure où les pays émergents et les groupes terroristes ne semblent pas avoir d'intérêt immédiat à renverser le système international, il nous semble qu'il est nécessaire de réévaluer les menaces les plus importantes existant dans le cyberespace (excluant les incidents logiciels ou physiques).

Par son envergure, nous pensons que l'espionnage industriel est la plus grande menace dans le cyberespace (sur la question des impacts des cyberattaques et de l'espionnage dans le cyberespace, voir Watkins 2014). Du fait de la digitalisation de plus en plus massive des activités humaines, les entreprises privées ont largement investi cet espace. Ces dernières étant avant tout poussées par la recherche du profit à court terme, il est fréquent de constater que la sécurité informatique n'est pas une priorité. Ces choix déficients concernant la sécurité les exposent à un double risque : la possibilité pour des concurrents de mener des opérations d'espionnage industriel, et l'opportunité pour des groupes criminels de mener des actions de cybercriminalité contre ces entreprises.

Comme nous l'avons vu avec les cas chinois de *APT-1* et de *Putter Panda*, l'espionnage industriel dans le cyberespace peut se révéler être une stratégie de guerre économique fort lucrative pour des États ou d'éventuelles entreprises concurrentes. Par l'acquisition de technologies secrètes ou d'informations sur les entreprises visées, des acteurs sont en mesure d'accélérer leur développement technologique et industriel. L'espionnage industriel peut également viser les stratégies commerciales mises en place par les différents acteurs afin de mieux les concurrencer ou de les parasiter. Ces stratégies sont extrêmement simples à mettre en place et ne présentent que peu de risques (« Spying used to be a dangerous business for the spies. Today it is done remotely » (Clarke et Knake 2010, 234)).

L'espionnage industriel serait tellement développé qu'il s'agirait littéralement d'une stratégie de développement et de guerre économique pour certains acteurs comme la Chine (sur la guerre économique dans le cyberespace, voir D'Elia 2014 ainsi que ; Lambert 2014). En misant sur le piratage d'entreprises privées, d'universités, de centres de recherche, de réseaux étatiques, etc. ces acteurs pourraient extraire de l'information afin de la mettre en valeur et l'utiliser dans les processus locaux de production et d'innovation. Pour des acteurs ayant déjà une base industrielle solide, ainsi que des ressources humaines formées et en bon nombre, ces stratégies peuvent devenir intéressantes en complément à la recherche fondamentale menée localement.

L'autre menace représentant un des plus grands risques dans le cyberespace est la cybercriminalité. Comme nous l'avons vu, la cybercriminalité est une sphère du crime organisé en pleine expansion. Les coûts associés à ce type de criminalité sont déjà astronomiques et semblent être sur une pente ascendante (en 2014, on estimait les coûts à environ quatre cent quarante-cinq milliards de dollars américains, voir Nakashima et Peterson 2014; Center for Strategic and International Studies 2014; Anderson et al. 2013).

Au Canada, il s'agit par exemple d'une des menaces considérées comme étant majeure pour la sécurité des activités se déroulant dans le cyberespace. Les corps policiers sont d'ailleurs déjà dépassés par la situation et réclament plus de soutien technique et logistique de la part des différents paliers de gouvernement. Un rapport paru en 2013 soulignait notamment ces problématiques et mettait en lumière les dynamiques liées au cybercrime au Canada (nous avons eu copie et autorisation écrite d'utiliser ce rapport, voir Deloitte 2008).

Le cybercrime présente un autre problème important : il vise tout le monde. Civils, entreprises, États ou tout autre type d'acteur, tout le monde peut être touché par le cybercrime. Que ce soit par la propagation de logiciels rendant les systèmes informatiques inutilisables ou sérieusement perturbés, l'utilisation de virus forçant le versement d'une rançon pour accéder à ses données (voir par exemple InfoSec Institute 2013 sur le cas des « ransomware »), ou le vol d'identité sur Internet, le cybercrime peut toucher toutes les sphères d'activités présentes dans le cyberspace. S'il est difficile de mesurer son impact financier (autrement que dans les cas de vol d'identité, de fraude et autres crimes de ce type), ces attaques ont de plus en plus de répercussions sur les activités économiques et sociales. Que ce soit en nombre de jours non-travaillés pour des raisons techniques, ou encore en montants remboursés pour compenser les victimes de vol d'identité et autre, le cybercrime coûte cher et représente une menace importante pour les secteurs économiques dans le cyberespace (Organisation for Economic Co-operation and Development 2009).

Les groupes criminels se sont ainsi emparés des technologies présentes dans le cyberespace afin d'étendre leurs activités. Pensons notamment aux différents types de trafic présents dans les couches les plus reculées d'Internet (ce que l'on appelle communément le *dark web*) : drogue, animaux, êtres humains, pédophilie, etc. L'utilisation des technologies liées au cyberespace représente pour ces groupes des

ouvertures vers de nouveaux marchés très lucratifs en plus d'être sécuritaires. La dématérialisation et la capacité à se cacher ou à brouiller les pistes sont en effet un avantage non négligeable comparativement à la 'vie réelle' des activités classiques.

La cybercriminalité a également généré un marché en pleine expansion de services liés aux cyberattaques et autres infiltrations. Ce marché noir génère d'importants revenus pour des pirates se mettant à disposition d'autres acteurs afin de mener des opérations de toutes natures dans le cyberespace. Il s'agit d'un enjeu de sécurité pour les différents acteurs en présence, mais aussi d'un enjeu économique pour les États qui ne prélèvent pas de taxes sur ces marchés tout en subissant d'éventuelles attaques dans un espace où ils ne peuvent pas faire appliquer leurs pouvoirs et leurs lois.

2. L'industrie de la sécurité

Rappelons enfin que la présence d'autant de vulnérabilités dans le cyberespace n'a pas seulement profité aux pays du sud ou aux cybercriminels, mais également à des entreprises privées puisque le marché très lucratif de la sécurité informatique est en pleine expansion (voir notamment PricewaterhouseCooper 2014, 5).

Afin de mieux saisir les dynamiques en présence, il est important de se poser la question de qui crée le discours sur la sécurité dans le cyberespace. Autant les États peuvent créer une partie de ce discours en orientant leurs politiques publiques ou en identifiant des zones d'activité à protéger, tant pour leur propre fonctionnement que pour celui de la société civile, autant les entreprises privées dans le secteur de la sécurité ont une tendance lourde à véhiculer un discours mettant en avant des besoins de protection des réseaux et infrastructures. La publication incessante de nombreux rapports de recherche assez concis mais souvent alarmistes sur la sécurité dans le cyberespace nous semble être une des façons assez efficaces par laquelle ces groupes

génèrent du discours public et favorisent l'émergence de nouveaux pans d'industrie. Si ces rapports sont souvent intéressants (nous les avons utilisés à de nombreuses reprises) et s'appuient sur de bonnes recherches factuelles, il reste toutefois que ces entreprises proposent en général des services payants comme réponse, plutôt que de chercher à diffuser largement de meilleures solutions de sécurité et de protection du public ou des entreprises. La création de ce marché de la peur des attaques est en elle-même une opération d'influence (et de cyberinfluence) à des fins commerciales. Pour Arpagian, « c'est aussi de ce sentiment d'inquiétude que naît la grande profitabilité de leur industrie » (Arpagian 2009a, 168).

Avec un marché devant dépasser cent-cinquante milliards de dollars américains d'ici 2020 (Cybersecurity ventures 2015), l'enjeu est gigantesque. Il n'est donc pas étonnant que ces intérêts monétaires encouragent certains acteurs à créer un discours visant la sécurisation et les mettant en position d'offrir des services très lucratifs pour eux. Il s'agit donc d'un enjeu économique de protection des réseaux existants mais aussi de création de nouveaux marchés. L'instrumentalisation de la question de la sécurité, qui touche tout le monde dans le cyberespace, est une bonne façon pour ces entreprises privées de vendre leurs produits et de garder captive une grande base de clients.

La création du discours de la menace est donc importante pour un ensemble d'acteurs puisqu'elle est aussi gage d'un financement étatique généreux pour étudier les questions de sécurité dans le cyberespace. La recherche dans ce secteur est grandement subventionnée par les armées (les armées américaine et chinoise au premier chef) ainsi que par les diverses agences de renseignement. Aux États-Unis, les organismes étatiques principaux en matière de recherche se partagent ainsi plusieurs milliards de dollars par année, afin d'établir de nouvelles technologies militaires ou civiles. Ce financement étatique est souvent associé à une participation du secteur privé : « là où l'intégration dans l'appareil économique prend toute sa

mesure, c'est quand on constate qu'une large part de cette manne redescend vers des entités privées, sous la forme de subventions ou de contrats » (Arpagian 2009a, 142). Près de 60% des recherches du ministère de la défense seraient transférés au secteur privé et près de 75% pour ceux de la NASA. La CIA aurait d'ailleurs son propre fond d'investissement visant à dynamiser et financer la recherche avec le secteur privé (le fond *In-Q-Tel*). Le gouvernement américain est même allé jusqu'à financer des technologies sensées garantir l'anonymat sur Internet (comme dans le cas du réseau Tor, qui est souvent présenté comme un réseau garantissant l'anonymat sur Internet, Levine 2014)

En Chine, l'important soutien de l'Armée populaire de libération (APL) à l'industrie et aux milieux de la recherche a été exposé et explique en partie ses capacités de cyberinfluence. En se positionnant comme un acteur de pointe dans le cyberespace, ce pays gagne en influence et en cyberpouvoir. Le Canada n'est pas en reste, puisqu'une étude de l'Institut de recherche et d'informations socio-économiques (IRIS) soulignait que les investissements du gouvernement fédéral en sécurité avaient explosé depuis la fin des années 1990, et ce malgré la rigueur budgétaire (voir Hebert et Hurteau 2014).

Si les États sont souvent de généreux argentiers de la recherche sur le cyberespace, ils sont aussi de bons clients des entreprises de cybersécurité. Que ce soit pour se protéger, surveiller les populations ou attaquer d'autres acteurs, les États ont largement investi dans l'achat de logiciels commerciaux afin de mener ces activités. Le logiciel pirate *Careto,* par exemple, a défrayé la chronique en 2014 (voir par exemple Breton 2014), sept ans après sa création. Ce logiciel très sophistiqué aurait été utilisé dans le secret par des États et des entreprises privées de grande taille pour espionner et dérober de l'information à d'autres acteurs (Kaspersky Labs 2014). Plus récemment, la firme de piratage informatique *Hacking Team* a été exposée à de virulentes critiques après s'être faite piratée (Greenberg 2015c). Parmi les documents

publiés (disponibles en ligne sur le site de Wikileaks, Wikileaks 2015), se trouvaient des informations quant au recours aux services de la firme par des pays à différentes fins (surveillance d'opposants politiques, surveillance de groupes terroristes, piratage de systèmes informatiques, etc.). Le Mexique était par exemple le premier acheteur dans le monde avec près de sept millions de dollars investis dans les services de la firme (Hernandez et Gorbea 2015). D'autres clients prestigieux ont également eu recours à ces services, parmi lesquels des organisations gouvernementales comme la *Drug Enforcement Agency (DEA)* aux États-Unis (Franceschi-Bicchierai 2015a). Rappelons également que les États paient de plus en plus de chercheurs et de pirates afin de déceler des failles de sécurité dans des logiciels et dans leurs systèmes. Que ce soit pour se protéger ou pour disposer de failles *zero day exploits* (une faille du logiciel « Adobe Flash » a par exemple été utilisée pendant plusieurs années par le groupe Hacking Team, voir Warren 2015), les États sont donc dans une posture de plus en plus préventive, tant en termes offensifs que défensifs.

Certains États ont même décidé de dépasser la seule acquisition de technologies vendues par des firmes de sécurité pour plutôt espionner ces mêmes entreprises. Les États-Unis et le Royaume-Uni ont par exemple espionné des fabricants d'antivirus afin de dérober des secrets industriels et s'assurer de la non-détection de leurs propres logiciels pirates (Fishman et Marquis-Boire 2015). Israël est également soupçonné d'avoir piraté une compagnie d'antivirus afin de se doter d'avantages stratégiques dans la création de logiciels pirates (Zetter 2015b).

Les États se sont aussi avérés être de bons promoteurs pour les entreprises de sécurité à travers le monde. Les groupes occidentaux n'ont en effet « guère de scrupules à intervenir sur le marché chinois » (Arpagian 2009a, 197), voyant là un univers d'opportunités commerciales (sur cette question, voir l'article du Washington Post suite aux révélations de Wiki Leaks sur la question : Asokan et Tate 2011). Les États-Unis auraient également aidé des compagnies américaines à vendre des logiciels de

sécurité à travers le monde (voir par exemple Gellman 2014). Quand les États n'ont pas activement fait la promotion de ces logiciels, ils sont pour la plupart du temps restés impassibles devant la vente de logiciels menaçant les libertés civiles et individuelles dans d'autres pays (comme Bahrain, voir Toor et Brandom 2015). Le Canada et l'Allemagne se sont ainsi distingués par la fabrication et la vente de logiciels de surveillance et de censure auprès de régimes autoritaires (voir respectivement Buzzetti 2011, pour le Canada; et Wagner et Guarnieri 2014, pour l'Allemagne). Ces ventes ont fourni des outils aux différents régimes liberticides afin de pouvoir mieux contrôler Internet et d'autres technologies du cyberespace (en 2012, il était par exemple possible pour 61 pays de couper Internet au besoin. McMillan 2012).

L'industrie de la sécurité est donc en pleine expansion et largement soutenue par les États. Cette création d'un discours portant sur la menace dans le cyberespace génère donc des revenus importants et mérite d'être prise en compte lorsque l'on évalue les vulnérabilités et les menaces dans cet espace.

3. Le cyberespace a déjà tout changé et va continuer de tout changer

> Like Cortés burning his ships after arriving in the New World, U.S. companies and government agencies built a new world in wich there were only computer-based systems. When the computers fail, employees stand around doing nothing or go home. [...] Computer networks are essential for companies or government agencies to operate. 'Essential' is a word chosen with care, because it conveys the fact that we are dependent upon computer systems. Without them, nothing works. If they get erroneous date, systems may work, but they will do the wrong things. (Clarke et Knake 2010, 97)

Le cyberespace a déjà tout changé dans nos vies. De la façon dont nous communiquons ou interagissons avec notre environnement, les technologies de

l'information et des télécommunications à la base du cyberespace sont partout. Le cyberespace serait ainsi devenu le système nerveux des pays développés (Department of Homeland Security 2003). Cette tendance devrait s'accentuer encore avec la progression des objets connectés (*Internet of things*) et celle de la mise en réseau de plus en plus de systèmes structurant nos vies.

Les technologies du cyberespace ont également déjà commencé à changer les règles d'engagement dans le système international. Par la possibilité donnée à des acteurs non étatiques de projeter de la force de façon efficace, facilement et à moindre coût, les technologies dans le cyberespace ont suscité un ensemble de nouvelles dynamiques. Que ce soit dans les règles d'engagement lors de conflits, dans la façon d'exercer un pouvoir d'influence ou encore dans les questions relatives au droit international, les dynamiques d'action et de confrontation dans le cyberespace ont soulevé de nombreux enjeux nouveaux (un article intéressant a été écrit à ce sujet par Choucri et Goldsmith 2012). Compte tenu de la pénétration de plus en plus importante des technologies du cyberespace dans différentes sphères d'activités et auprès d'un ensemble d'acteurs, il parait difficile de concevoir un ralentissement de cette dynamique.

S'agit-il donc d'une évolution ou d'une révolution ('Revolution in military affairs') dans la manière de mener la guerre et de concevoir la sécurité (en évoquant par exemple des 'guerres postmodernes' où il y aurait « préservation par substitution » (Chamayou 2013, 257) des combattants par des moyens technologiques)? Puisqu'il y aurait potentiellement une nouvelle façon de faire la guerre, liée à la transition entre des armées de conscription et des armées de métier (notamment à cause de la réception difficile du public face aux morts), plus petites, mais plus axées sur la technologie, il faut se poser la question de l'impact de l'apparition du cyberespace et de l'utilisation de capacités offensives en son sein par des acteurs non dominants. L'aspect de plus en plus dématérialisé des conflits et l'absence de combats directs

dans certains cas sont des données importantes des modifications à la façon de mener la guerre au XXIe siècle. Comme pour le drone, dans certains cas le cyberespace « présente tous les traits d'une *tactique – ou plus précisément, d'un élément de technologie – en train de se substituer à une stratégie* » (Chamayou 2013, 99) sans réelle doctrine sous-tendant à son utilisation. En « exerçant la violence de guerre depuis une zone de paix » (Chamayou 2013, 169), l'utilisation technologies dans le cyberespace, comme les drones, est une manière de remettre en question la pratique de la guerre et de son encadrement. Mais encore plus important est le fait que les cyberattaques ou la cyberguerre pourraient avoir des conséquences graves, allant jusqu'à la guerre totale, tout en requérant un investissement minimal en capital humain et militaire.

Cette « Révolution technétronique » (Brzezinski 1982), mêlant technologie et électronique dans une « société aux éléments extraordinairement enlacés » ne semble pas proche de s'arrêter ou de ralentir. Le train technologique avance en effet à plein régime depuis le début du XXIe siècle. Comme Richard Wyn Jones, nous considérons que la technologie a une logique qui lui est inhérente, changeant les rapports sociaux et politiques (sur cette question, voir par exemple « Authoritarian and Democratic Technics ». Mumford 1964) et en bonne partie la façon de mener la guerre.

Afin de comprendre comment cette reconfiguration se produit dans le cas du cyberespace, comme pour d'autres technologies existantes, il faut souligner que contrairement à l'idée relativement linéaire que l'on peut se faire du progrès technique (déjà critiquée par Walter Benjamin au début du XXe siècle, voir Löwy 2003a), l'utilisation des nouvelles technologies de l'information et des télécommunications pourrait être un facteur important de déstabilisation des sociétés occidentales et modernes, et pas seulement un gage de progrès social et humain. La dépendance au réseau est, par exemple, une des premières conséquences du transfert

d'un certain nombre d'activités humaines dans le cyberespace (cette dynamique a poussé certains auteurs à se questionner sur le sujet, voir par exemple Santos 2010). En cas de cyberguerre (ou d'événements naturels comme des tempêtes solaires majeures ayant un potentiel de destruction civilisationnel important, voir National Aeronautics and Space Administration 2014), il serait difficile de voir comment ces sociétés pourraient subsister sans les technologies de l'information et des télécommunications, et du cyberespace en général.

Il est possible de faire une critique du progrès technique tant la technologie ne semble pas garante d'un progrès social et civilisationnel. Cette forme de progrès technique est d'ailleurs souvent celle de puissances capitalistes profitant de ces nouvelles formes de guerre, notamment en créant un marché à haute intensité capitalistique ainsi qu'une demande visant à sécuriser des objets référents. Que ce soit chez Walter Benjamin (Löwy 2003b) ou chez d'autres auteurs, cette critique du progrès technique est récurrente à chaque grand cycle d'innovation (pour plus de matière sur ce point, on pourra se référer à l'excellent ouvrage de Feenberg « Pour une théorie critique de la technique ». Feenberg 2014). Dans le cas du cyberespace, il semble toutefois que cette critique de la technologie et de la technique ait pris une nouvelle dimension. En se demandant si ces technologies ne nous rendent pas plus captifs que libres (voir l'ouvrage de Sillard (2011) par exemple) ou encore si le cyberespace n'est pas en train de nous mener à terme à une « guerre civile numérique » (Jorion 2011), différents auteurs ont tenté de théoriser les enjeux liés au cyberespace et aux activités humaines qu'il touche. D'autres auteurs ont quant à eux tenté de sonner l'alarme sur les dérives que l'utilisation de technologies dans le cyberespace peut générer (Greenwald 2014a; Harding 2014).

De plus, le cyberespace apporte également des questions liées au droit international et à son application, notamment en termes de Droit international humanitaire (DIH). En redéfinissant les zones de front et de conflit, le cyberespace met à risque des

populations et des infrastructures civiles qui étaient relativement protégées dans les types de conflits plus classiques (à l'exception des guerres civiles et des guerres mondiales).

> Comment voir des combattants au moyen d'une arme qui annule le combat ? Ceci est une contradiction profonde. En privant les militaires des critères manifestes permettant de *constater de facto* la différence entre combattants et non-combattants, c'est l'applicabilité même du principe de distinction que cette arme met en péril. (Chamayou 2013, 204).

Enfin, en robotisant la guerre, en la rendant automatique et non soumise aux aléas humains, les technologies présentes dans le cyberespace risquent de déshumaniser les conflits et de faire perdre une zone d'appréciation nécessaire pour l'application du droit international, notamment dans le cas de la protection des civils (Chamayou 2013, 303). Il y a donc un recul certain dans la façon de concevoir le droit de la guerre et le droit international humanitaire, censé protéger les populations civiles. Recul qui ne peut rien augurer de bon pour le futur de nos sociétés et l'utilisation qui peut être faite de ces technologies.

Le peu d'entrain que nous avons à réfléchir à ces considérations au sein des sociétés occidentales est un problème fondamental. Dans la mesure où le développement technologique et ses significations sociales et culturelles ont été « capturés » par des entreprises privées, le débat sur le progrès technique et son acceptation ne se fait que trop peu. L'enthousiasme irréfléchi de tous les acteurs économiques et politiques utilisant le cyberespace est également un frein à la réflexion portant sur ces questions ainsi qu'à une meilleure compréhension des problématiques générées par ces technologies.

Certains avancent même que, comme pour le cas du développement industriel et de l'écologie, le développement technologique et la massification du cyberespace pourraient nous mener vers un gouffre civilisationnel en cas d'attaque majeure.

Comme pour l'écologie, la réflexion critique et le débat de société nécessaire font les frais de la recherche du profit et du développement économique, érigés comme des valeurs transcendant toute autre question sociale ou philosophique. Le danger est pourtant présent, mais articulé comme une source de profits et non de débats sociétaux.

Nous pouvons donc raisonnablement nous questionner sur le progrès technique et sa signification pour nos sociétés. Le cyberespace n'en étant que l'itération la plus récente, il est clair que ces questions ne vont que s'accentuer à mesure du développement de nouvelles technologies desquelles dépendront toujours plus d'activités humaines.

Ainsi, à notre avis, la facilité d'accès à des moyens de projection de la force dans le cyberespace, couplée à des politiques éducatives audacieuses visant à former un grand nombre d'individus compétents dans ces domaines devrait donner un avantage à des pays comme la Chine, la Russie et d'autres pays émergents comme l'Iran (qui a augmenté ses dépenses dans le cyberespace de près de 1200% dans les trois dernières années, et est considérée par certains comme une puissance montante dans le domaine, voir Small Media 2015; Cylance 2014). Que ce soit dans la conduite des activités dans le cyberespace ou dans l'exercice de la cyberinfluence, ces deux formes de pouvoir pourraient à terme déstabiliser le système international. Il s'agit d'ailleurs d'une préoccupation pour de nombreuses institutions, dont le Forum économique mondial qui l'a intégré dans sa liste de risques majeurs à surveiller (Howell 2013).

Que ce soit en attaquant l'hégémon américain ou en insufflant de profonds changements dans la division internationale du travail, la projection de la force dans le cyberespace par ces pays pourrait bien avoir des effets importants sur le système international et les relations internationales en général. S'il n'y a pas eu de

cyberguerre jusqu'à présent, le risque est bel et bien réel. Sans prôner le retour à la machine à écrire comme certaines unités militaires allemandes le font (Phillip 2014), il est nécessaire de mettre en place des stratégies de défense dès maintenant. Il est également nécessaire de se doter de technologies non-informatiques pouvant prendre le relais en cas de pannes ou d'attaques.

N'oublions pas que la sécurité informatique a comme premier postulat que cette sécurité est de toute façon impossible à atteindre.

BIBLIOGRAPHIE

MONOGRAPHIES

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore et Stefan Savage. 2013. « Measuring the Cost of Cybercrime. » Dans *The Economics of Information Security and Privacy*, sous la dir. de Rainer Böhme, p. 265-300. Springer Berlin Heidelberg. En ligne. <http://link.springer.com/chapter/10.1007/978-3-642-39498-0_12>. Consulté le 1 février 2015.

Aron, Raymond. 1984. *Paix et guerre entre les nations*. 8e éd., avec une présentation inédite de l'auteur. Coll. « Collection « Liberté de l'esprit » ». Paris : Calmann-Lévy.

Arpagian, Nicolas. 2009. *La cyberguerre: la guerre numérique a commencé*. Paris : Vuibert.

Battistella, Dario. 2003. *Théories des relations internationales*. Coll. « Références inédites ». Paris : Presses de la fondation nationale des sciences politiques.

Brzezinski, Zbigniew. 1982. *Between two ages: America's role in the technetronic era*. Westport, Conn : Greenwood Press.

Buzan, Barry, Ole Wæver et Jaap de Wilde. 1998. *Security: a new framework for analysis*. Boulder, Colo : Lynne Rienner Pub.

Chamayou, Grégoire. 2013. *Théorie du drone*. Paris : La Fabrique.

Clarke, Richard A. et Robert K. Knake. 2010. *Cyber war: the next threat to national security and what to do about it*. 1st ed. New York : Ecco.

Department of Homeland Security. 2003. *The national strategy to secure cyberspace*. Washington, D.C. : Department of Homeland Security. En ligne. <http://purl.access.gpo.gov/GPO/LPS28730>. Consulté le 11 juillet 2015.

Feenberg, Andrew. 2014. *Pour une théorie critique de la technique*. Montréal, Qc : Lux Éditeur.

Flükiger, Jean-Marc. 2011. *Nouvelle guerres et théorie de la guerre juste.* Infolio.

Gilpin, Robert. 1981. *War and change in world politics.* Cambridge ; New York : Cambridge University Press.

Greenwald, Glenn. 2014. *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state.* First Edition. New York, NY : Metropolitan Books/Henry Holt.

Harding, Luke. 2014. *The Snowden files: the inside story of the world's most wanted man.* London; London : Faber et Faber ; Guardian Books.

Hayhoe, Ruth, Jun Li, Jing Lin et Qiang Zha. 2011. *Portraits of 21st century Chinese universities : in the move to mass higher education.* Hong Kong : Comparative Education Research Centre, University of Hong Kong : Springer.

Jorion, Paul. 2011. *La guerre civile numérique.* Coll. « Conversations pour demain ». Paris : Textuel.

Jung, Jisun et Gerard A. Postiglione. 2015. « From Massification Towards the Post-massification of Higher Education in Hong Kong. » Dans *Mass Higher Education Development in East Asia,* sous la dir. de Jung Cheol Shin, Gerard A. Postiglione, et Futao Huang, p. 119-136. Coll. « Knowledge Studies in Higher Education 2 ». Springer International Publishing. En ligne. <http://link.springer.com/chapter/10.1007/978-3-319-12673-9_7>. Consulté le 17 juin 2015.

Kerschischnig, Georg. 2012. *Cyberthreats and international law.* The Hague : Eleven International Publishing.

Klein, Lawrence R. et Marshall I. Pomer. 2001. *The New Russia: Transition Gone Awry.* Stanford University Press.

Klimburg, Alexander et NATO Cooperative Cyber Defence Centre of Excellence. 2012. *National cyber security framework manual.* [Talinn, Estonia] : NATO Cooperative Cyber Defense Center of Excellence. En ligne. <http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf>. Consulté le 3 juin 2015.

Kopetz, Hermann. 2011. *Real-time systems. Design Principles for Distributed Embedded Applications.* New York : Springer.

Kramer, Franklin D., Stuart H. Starr et Larry K. Wentz. 2009. *Cyberpower and national security.* 1st ed. Washington, D.C : National Defense University Press : Potomac Books.

Krause, Keith et Michael C Williams. 1997. *Critical security studies: concepts and cases*. London : UCL Press.

Lillian Ablon, Martin C. Libicki et Andrea A. Golay. 2014. *Markets for cybercrime tools and stolen data: hackers' bazaar*. Santa Monica, CA : RAND Corporation.

MacKenzie, Donald et Judy Wajcman. 1999. *The social shaping of technology*. Sous la dir. de. Donald MacKenzie et Judy Wajcman. Buckingham, UK : Open University Press. En ligne. <http://mcgraw-hill.co.uk/openup/>. Consulté le 3 juin 2015.

Macleod, Alex et Dan O'Meara. 2007. *Théories des relations internationales : contestations et résistances*. [Montréal] : CEPES : Athéna éditions : Université Concordia.

Miyahara, Shizuko. 2015. « Regional Quality Assurance System for Higher Education in Southeast Asia. » Dans *Quality Assurance in LIS Education*, sous la dir. de Makiko Miwa et Shizuko Miyahara, p. 25-38. Springer New York. En ligne. <http://link.springer.com/chapter/10.1007/978-1-4614-6495-2_2>. Consulté le 17 juin 2015.

Mok, Ka-Ho. 2012. *Education reform and education policy in East Asia*. London : Routledge.

National Research Council (U.S.). 2007. *Toward a safer and more secure cyberspace*. Washington, DC : National Academies Press.

Nye, Joseph S. 2004. *Soft power: the means to success in world politics*. 1st ed. New York : Public Affairs.

Organisation for Economic Co-operation and Development (dir.). 2009. *Computer viruses and other malicious software: a threat to the Internet economy*. Paris : OECD.

———. 2012. *OECD internet economy outlook 2012*. Paris : OECD. En ligne. <http://public.eblib.com/choice/publicfullrecord.aspx?p=1057623>. Consulté le 2 mars 2015.

——— (dir.). 2013. *The internet economy on the rise: progress since the Seoul Declaration*. Paris : OECD.

Quiggin, Thomas, Ont.) Queen's University (Kingston et Centre for International and Defence Policy. 2012. *« Don't call us » : governments, cyber security, and implications for the private sector*. Kingston, Ont. : Centre for International and Defence Policy, Queen's University.

Ramesh, M. 2004. *Social policy in east and southeast Asia: education, health, housing and income maintenance*. Coll. « Routledge advances in Asia-Pacific studies 7 ». London ; New York, NY : RoutledgeCurzon.

Santos, Fabio Batista dos. 2010. *Cyber War and Cyber-attacks How is our strongest network at risk of becoming our weakest link?* Kindle.

Schmitt, Michael N., et NATO Cooperative Cyber Defence Centre of Excellence (dir.). 2013. *Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge ; New York : Cambridge University Press.

Schwartzman, Simon, Rómulo Pinheiro et Pundy Pillay. 2015. *Higher Education in the BRICS Countries: Investigating the Pact between Higher Education and Society*. Springer.

Sillard, Benoît. 2011. *Maîtres ou esclaves du numérique?: 2049: internet, notre second cerveau*. Paris : Eyrolles.

Vaughan-Williams, Nick. 2010. *Critical security studies: an introduction*. Milton Park, Abingdon, Oxon ; New York, NY : Routledge.

Waltz, Kenneth N. 1979. *Theory of international politics*. Coll. « Addison-Wesley series in political science ». Reading, Mass : Addison-Wesley Pub. Co.

Weber, M. (1998). *L'éthique protestante et l'esprit du capitalisme: suivi de Les sectes protestantes et l'esprit du capitalisme*. Paris : Pocket.

World Bank. 2014. *Enhancing competitiveness in an uncertain world.* Washington, D.C : World Bank. En ligne. <http://elibrary.worldbank.org/content/book/9781464804304>. Consulté le 18 juin 2015.

———. 2015. *World Bank East Asia and Pacific Economic Update, April 2015: Adjusting to a Changing World.* World Bank Publications.

Zi Sun, Samuel B Griffith, Basil Henry Liddell Hart et Françis Wang. 1987. *L'art de la guerre*. [Paris] : Flammarion.

ARTICLES SCIENTIFIQUES

Altbach, Philip G. 2013. « The prospects for the BRICs: The new academic superpowers? » *The global future of higher education and the academic profession: The BRICs and the United States*, p. 1–27.

Barat-Ginies, Oriane. 2014. « Existe-t-il un droit international du cyberespace ? » *Hérodote*, vol. 152-153, no 1, p. 201-220.

Bilge, Leyla et Tudor Dumitras. 2012. « Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World. » Dans *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, p. 833–844. Coll. « CCS '12 ». New York, NY, USA : ACM. En ligne. <http://doi.acm.org/10.1145/2382196.2382284>. Consulté le 28 mai 2015.

Bonaci, Tamara, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno et Howard Jay Chizeck. 2015. « To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots. » *arXiv:1504.04339 [cs]*. En ligne. <http://arxiv.org/abs/1504.04339>. Consulté le 25 avril 2015.

Brenner, Susan W. et Leo L. Clarke. 2010. « Civilians in Cyberwarfare: Conscripts. » *Vand. J. Transnat'l L.*, vol. 43, p. 1011.

Butler, Ally. 2010. « Security and the "Smokeless War": A Critical Look at Security as Speech Act" Theory via Internet Security in China ». *On Politics*, vol. 0, no 0, p. 107-119.

La Chapelle, Bertrand de. 2014. « Souveraineté et juridiction dans le cyberespace. » *Hérodote*, vol. 152-153, no 1, p. 174-184.

Choucri, N. et D. Goldsmith. 2012. « Lost in cyberspace: Harnessing the Internet, international relations, and global security. » *Bulletin of the Atomic Scientists*, vol. 68, no 2, p. 70-77.

Douzet, Frédérick. 2014. « L'art de la guerre revisité. Cyberstratégie et cybermenace chinoises. » *Hérodote*, vol. 152-153, no 1, p. 161-173.

Ebert, Hannes et Tim Maurer. 2014. « Revendications sur le cyberespace et puissances émergentes. » *Hérodote*, vol. 152-153, no 1, p. 276-295.

Elia, Danilo D'. 2014. « La guerre économique à l'ère du cyberespace. » *Hérodote*, vol. 152-153, no 1, p. 240-260.

Farwell, James P. 2014. « The Media Strategy of ISIS. » *Survival*, vol. 56, no 6, p. 49-55.

Gerber, Theodore P. et Michael Hout. 1998. « More Shock than Therapy: Market Transition, Employment, and Income in Russia, 1991-1995. » *American Journal of Sociology*, vol. 104, no 1, p. 1-50.

Gong, Fang et Jun Li. 2010. « Seeking excellence in the move to a mass system: Institutional responses of key Chinese comprehensive universities. » *Frontiers of Education in China*, vol. 5, no 4, p. 477-506.

GUMPORT, PATRICIA J., MARIA IANNOZZI, SUSAN SHAMAN et ROBERT ZEMSKY. 1997. « Trends in United States Higher Education from Massification to Post Massification. » En ligne. <http://web.stanford.edu/group/ncpi/documents/pdfs/1-04_massification.pdf>. Consulté le 5 juillet 2015.

Joubert, Vincent et Jean-Loup Samaan. 2014. « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE. » *Hérodote*, vol. 152-153, no 1, p. 261-275.

Kahn, David. 1980. « Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes and Their Effects. » *The Historical Journal*, vol. 23, no 3, p. 617-639.

Kempf, Olivier. 2014. « Le cyberterrorisme : un discours plus qu'une réalité. » *Hérodote*, vol. 152-153, no 1, p. 82-97.

Lambert, Nicholas A. 2014. « The Strategy of Economic Warfare: A Historical Case Study and Possible Analogy to Contemporary Cyber Warfare. » *Cyber Analogies*. En ligne. <http://calhoun.nps.edu/public/bitstream/handle/10945/40037/NPS-DA-14-001.pdf#page=89>. Consulté le 18 février 2015.

Libicki, Martin C. 2014. « De Tallinn à Las Vegas, une cyberattaque d'importance justifie-t-elle une réponse cinétique? » *Hérodote*, vol. 152-153, no 1, p. 221-239.

Liff, Adam P. 2012. « Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. » *Journal of Strategic Studies*, vol. 35, no 3, p. 401-428.

Limonier, Kevin. 2014. « La Russie dans le cyberespace : représentations et enjeux. » *Hérodote*, vol. 152-153, no 1, p. 140-160.

Löwy, Michael. 2003. « Progrès et catastrophe. La conception de l'histoire de Walter Benjamin. » *HISTOREIN*, vol. 4, p. 7.

Macleod, Alex. 2004. « Les études de sécurité : du constructivisme dominant au constructivisme critique. » *Cultures & Conflits*, no 54, p. 13-51.

Mumford, Lewis. 1964. « Authoritarian and Democratic Technics. » *Technology and Culture*, vol. 5, no 1, p. 1-8.

National Aeronautics and Space Administration. 2014. « Near Miss: The Solar Superstorm of July 2012. » En ligne. <http://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm/>. Consulté le 23 juillet 2014.

Nieto Gómez, Rodrigo. 2014. « Cybergéopolitique : de l'utilité des cybermenaces. » *Hérodote*, vol. 152-153, no 1, p. 98-122.

O'Keeffe, Derek T., Spyridoula Maraka, Ananda Basu, Patrick Keith-Hynes et Yogish C. Kudva. 2015. « Cybersecurity in Artificial Pancreas Experiments. » *Diabetes Technology & Therapeutics*. En ligne. <http://online.liebertpub.com/doi/full/10.1089/dia.2014.0328>. Consulté le 17 mai 2015.

Post, David. 1996. « The Massification of Education in Hong Kong: Effects on the Equality of Opportunity, 1981-1991. » *Sociological Perspectives*, vol. 39, no 1, p. 155-174.

Robine, Jérémy et Kavé Salamatian. 2014. « Peut-on penser une cybergéographie ? » *Hérodote*, vol. 152-153, no 1, p. 123-139.

Schneier, B. 2011. « Lockheed Martin hack linked to RSA's SecurID breach. » *Schneier on Security, 30th May,${$Online Resource$}$ Available at: http://www. schneier. com/blog/archives/2011/05/lockheed_martin. html [Accessed 04/12/12].*

Sheng-jun, YUAN. 2011. « Educational Policies and Economic Growth in BRICS: Comparative Perspectives. » *Journal of US-China Public Administration*, vol. 8, no 2, p. 188–197.

Stone Fish, Isaac et Keith Johnson. 2015. « China's New Airstrip in the South China Sea Is Almost Completed. » *Foreign Policy*. En ligne. <http://foreignpolicy.com/2015/04/16/chinas-new-airstrip-in-the-south-china-sea-is-almost-completed/>. Consulté le 5 juillet 2015.

Teichler, Ulrich. 1998. « Massification: A challenge for institutions of higher education. » *Tertiary Education and Management*, vol. 4, no 1, p. 17-27.

Wæver, Ole. 2011. « Politics, security, theory. » *Security Dialogue*, vol. 42, no 4-5, p. 465-480.

Wan, Calvin. 2011. « Reforming higher education in Hong Kong towards post-massification: the first decade and challenges ahead. » *Journal of Higher Education Policy & Management*, vol. 33, no 2, p. 115-129.

Xiong, Jie. 2011. « Understanding higher vocational education in China: Vocationalism vs confucianism. » *Frontiers of Education in China*, vol. 6, no 4, p. 495-520.

RAPPORTS ET DOCUMENTS DE RÉFÉRENCE

Alperovitch, Dmitri. 2011. *Revealed: Operation Shady RAT.* McAfee. En ligne. <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>.

Bockel, Jean-Marie. 2012. *La cyberdéfense : un enjeu mondial, une priorité nationale.* Paris : Commission des affaires étrangères, de la défense et des forces armées du Sénat. En ligne. <http://www.senat.fr/rap/r11-681/r11-6811.pdf>. Consulté le 30 janvier 2013.

Cabinet Office, United-Kingdom Government. 2011. *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world.* London.

Center for Strategic and International Studies. 2014. *Net Losses: Estimating the Global Cost of Cybercrime.* Washington, D.C : Center for Strategic and International Studies. En ligne. <http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf>. Consulté le 2 janvier 2015.

China Scholarship Council. 2009. « Top 10 destinations of students from China studying abroad. » En ligne. <http://www.iie.org/Services/Project-Atlas/China/Chinas-Students-Overseas>. Consulté le 5 juillet 2015.

Conseil d'État. 2014. *Le numérique et les droits fondamentaux.* Coll. « Etudes et documents, Conseil d'Etat ». Paris : Conseil d'État. En ligne. <http://www.conseil-etat.fr/fr/communiques-de-presse/etude-annuelle-2014-le-numerique-et-les-droits-fondamentaux.html>. Consulté le 8 septembre 2014.

Crowdstrike Global Intelligence Team. 2014. *CrowdStrike Intelligence Report - Putter Panda.* Irvine, California, USA : CrowdStrike. En ligne. <http://resources.crowdstrike.com/putterpanda/>. Consulté le 18 août 2014.

Crowell, Richard M. 2010. *War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare.*

Cylance. 2014. *Operation cleaver.* En ligne. <http://www.cylance.com/operation-cleaver/>. Consulté le 13 février 2015.

Deichmann, Uew et Deepak Mishra. 2014. *World Development Report 2016: Internet for Development - Concept note.* World Bank. En ligne. <http://www.worldbank.org/content/dam/Worldbank/Publications/WDR/WDR%202016/WDR2016_Concept_Note.pdf>. Consulté le 23 mai 2015.

Deloitte. 2008. *A report on cybercrime in Canada*. Canadian Association of Police Boards.

Department of Defense, Defense science board. 2013. « Resilient Military Systems and the Advanced Cyber Threat. » Department of Defense. En ligne. <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>. Consulté le 11 juillet 2015.

Directorate for science, technology and industry et Commitee for information, computer and communcations policy. 2008. *THE DEVELOPMENT OF POLICIES FOR THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURES (CII) A COMPARATIVE ANALYSIS IN SEVEN OECD COUNTRIES: AUSTRALIA, CANADA, KOREA, JAPAN, THE NETHERLANDS, THE UNITED KINGDOM AND THE UNITED STATES.* OCDE. En ligne. <http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=DSTI/ICCP/REG(2007)20/FINAL&docLanguage=En>. Consulté le 15 août 2013.

FireEye Labs / FireEye Threat Intelligence. 2015. *APT30 AND THE MECHANICS OF A LONG-RUNNING CYBER ESPIONAGE OPERATION.* En ligne. <https://www.fireeye.com/company/press-releases/2015/04/fireeye-reveals-details-of-decade-long-cyber-espionage-campaign.html>. Consulté le 12 avril 2015.

Fortify, H.P. 2014. *Internet of Things Research Study*. En ligne. <http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA5-4759ENW>. Consulté le 15 février 2015.

Goncharov, Max. 2012. *Russian Underground 101*. Trend Micro.

———. 2014. *Russian Underground Revisited*. Coll. « Cybercriminal Underground Economy Series ». Trend Micro.

Gouvernement du Canada [Sécurité publique Canada]. 2010. *Stratégie de cybersécurité du Canada renforcer le Canada et accroître sa prospérité*. [Ottawa, Ont.] : Gouvernement du Canada [Sécurité publique Canada] = Govt. of Canada [Public Safety Canada]. En ligne. <http://site.ebrary.com/id/10425698>. Consulté le 30 janvier 2013.

Government of the Russian Federation. 2000. « MFA of Russia | 09/09/2000 | INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION. » En ligne. <http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument>. Consulté le 3 juin 2015.

———. 2011. « Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space. » En ligne. <https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf>. Consulté le 3 juin 2015.

———. 2013. « Basic principles for State Policy of the Russian Federation in the field of Internation Information Security to 2020. » En ligne. <https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf>. Consulté le 3 juin 2015.

Gropello, Emanuela Di, Shahid Yusuf et Prateek Tandon. 2012. *Putting Higher Education to Work: Skills and Research for Growth in East Asia*. World Bank Publications, col. World Bank East Asia and Pacific Regional Report. En ligne. <http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/EASTASIAPACIFICEXT/0,,contentMDK:22535968~pagePK:146736~piPK:226340~theSitePK:226301,00.html>.

Hagen, Andreas. 2012. *The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict*. The Armed Forces Communications and Electronics Association. En ligne. <http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf>. Consulté le 29 juin 2015.

Hebert, Guillaume et Philippe Hurteau. 2014. *Les coûts de l'escalade sécuritaire au Canada*. En ligne. <http://www.iris-recherche.qc.ca/publications/depenses-securitaires>. Consulté le 4 février 2014.

High representative of the European Union for foreign affairs and security policy (dir.). 2013. « Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. » En ligne. <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf>. Consulté le 3 juin 2015.

Howell, Lee. 2013. *Global Risks 2013 Eighth Edition*. Genève, Suisse : World Economic Forum. En ligne. <http://reports.weforum.org/global-risks-2013/>. Consulté le 9 janvier 2013.

HP Fortify. 2015. *How safe are home security systems?* En ligne. <http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-7342ENW&cc=us&lc=en>. Consulté le 15 mars 2015.

Intel Security. 2014a. *McAfee Labs Threats Report, August 2014*. Santa Clara, CA : Intel Security. En ligne. <http://www.mcafee.com/ca/resources/reports/rp-quarterly-threat-q2-2014.pdf>. Consulté le 2 janvier 2015.

———. 2014b. *McAfee Labs Threats Report, November 2014*. Santa Clara, CA : Intel Security. En ligne. <http://www.mcafee.com/ca/resources/reports/rp-quarterly-threat-q3-2014.pdf>. Consulté le 2 janvier 2015.

Kaspersky Labs. 2014. *Unveiling « Careto » - The Masked APT*.

Kaspersky Labs' Global Research & Analysis Team. 2015a. *Equation : The Death Star of Malware Galaxy*. Kaspersky Labs' Global Research & Analysis Team. En ligne. <http://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/>. Consulté le 16 février 2015.

———. 2015b. *EQUATION GROUP: QUESTIONS AND ANSWERS*. Kaspersky Labs' Global Research & Analysis Team. En ligne. <http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Equation_group_questions_and_answers.pdf>. Consulté le 16 février 2015.

Krekel, Bryan, Patton Adams et George Bakos. 2012. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Washington, D.C : U.S.-China Economic and Security Review Commission.

Mandiant. 2013. *APT1 : Exposing One of China's Cyber Espionage Units*.

Matis, Michael S. 2012. *The Protection of Undersea Cables: A Global Security Threat*. DTIC Document. En ligne. <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA561426>. Consulté le 26 mai 2015.

McAfee Labs. 2015. *Threats Predictions*. Santa Clara, CA : Intel Security. En ligne. <http://www.mcafee.com/ca/resources/misc/infographic-threats-predictions-2015.pdf>. Consulté le 2 janvier 2015.

McNabb, John. 2010. « Cyberterrorism & the Security of the National Drinking Water Infrastructure. » 31 juillet 2010). En ligne. <https://www.defcon.org/images/defcon-18/dc-18-presentations/McNabb/DEFCON-18-McNabb-Cyberterrorism-Drinking-Water.pdf>.

Ministry of Communications & IT. 2013. *National Cyber Security Policy -2013*. New Delhi : Government of India. En ligne. <http://deity.gov.in/sites/upload_files/dit/files/National_cyber_security_policy-2013(1).pdf>. Consulté le 1 juin 2015.

Myrli, Sverre. 2009. *NATO PA - 173 DSCFC 09 F bis - L'OTAN et la cyberdéfense*. Coll. « Rapports de commission ». Bruxelles : Organisation du traité de l'Atlantique nord. En ligne. <http://www.nato-pa.int/default.asp?CAT2=1765&CAT1=16&CAT0=2&COM=1782&MOD=0&SMD=0&SSMD=0&STA=&ID=0&PAR=0&LNG=1>.

National Cybersecurity and communications integration center. 2014. *Incident response activity : Internet accessible control systems at risk*. U.S Department of Homeland Security. En ligne. <https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf>. Consulté le 15 février 2015.

Non-Aligned Movement. 1979. « Documents of the Sixth Conference of Heads of State or Government of Non-Aligned Countries - I. Political Declaration. »

Obama, Barack et The Executive Office of the President - The White House. 2015. « National Security Strategy. » En ligne. <https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf>. Consulté le 3 juin 2015.

Office of the Auditor General of Canada. 2012. *Report of the Auditor General of Canada to the House of Commons : CHAPTER 3 Protecting Canadian Critical Infrastructure Against Cyber Threats*. Ottawa, Canada : Office of the Auditor General of Canada. En ligne. <http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html>. Consulté le 19 août 2013.

Omtzigt, Pieter. 2015. *Mass surveillance*. Strasbourg, France : Conseil de l'Europe. En ligne. <http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2>. Consulté le 31 janvier 2015.

Organisation du traité de l'Atlantique nord. 2011. *Defending the networks The NATO Policy on Cyber Defence*. Bruxelles : Organisation du traité de l'Atlantique nord. En ligne. <http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf>. Consulté le 30 janvier 2013.

———. 2014. « Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. » En ligne. <http://www.nato.int/cps/en/natohq/official_texts_112964.htm>. Consulté le 3 juin 2015.

Organisation for Economic Co-operation and Development. 2008. *The Seoul Declaration for the Future of the Internet Economy*. OECD Digital Economy Papers. En ligne.

<http://www.oecd-ilibrary.org/science-and-technology/the-seoul-declaration-for-the-future-of-the-internet-economy_230445718605>. Consulté le 23 mai 2015.

PricewaterhouseCooper. 2014. *Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015*. En ligne. <http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>. Consulté le 12 février 2015.

Rasmussen, Anders Fogh. 2013. « Secretary General's Annual Report 2012. » Organisation du traité de l'Atlantique nord. En ligne. <http://www.nato.int/cps/en/natohq/opinions_94220.htm>. Consulté le 3 juin 2015.

Robert T. Marsh. 1997. *Critical Foundations, Protecting America's Infrastructures*. Washington, D.C : President's Commission on Critical Infrastructure Protection.

Small Media. 2015. *Iranian Internet Infrastructure and Policy Report: Special Edition, The Rouhani Review (2013-15)*. En ligne. <http://www.smallmedia.org.uk/content/135>. Consulté le 17 avril 2015.

Symantec. 2014. *Regin: Top-tier espionage tool enables stealthy surveillance*. En ligne. <http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance>. Consulté le 24 novembre 2014.

Taia Global. 2014. *Taia Global Linguists Establish Nationality of Sony Hackers as Russian, not Korean | Taia Global, Inc.* En ligne. <https://taia.global/2014/12/taia-global-linguists-establish-nationality-of-sony-hackers-as-russian-not-korean/>. Consulté le 30 décembre 2014.

The Executive Office of the President - The White House (dir.). 2011. « International strategy for cyberspace. » En ligne. <https://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf>.

United Nations et International Telecommunication Union. 2003. « Geneva Declaration of Principles. » En ligne. <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161%7C1160>.

United States Air Force. 2011. *Cyberspace Operations - Air Force Doctrine Document (AFDD) 3-12*. Doctrine Document. Maxwell, Alabama, United States of America. En ligne. <http://www.e-publishing.af.mil/?txtSearchWord=AFDD+3-12&btnG.x=0&btnG.y=0&client=AFPW_EPubs&proxystylesheet=AFPW_EPubs&i

e=UTF-8&oe=UTF-8&output=xml_no_dtd&site=AFPW_EPubs>. Consulté le 8 janvier 2013.

United States Government Accountability Office. 2011. *CRITICAL INFRASTRUCTURE PROTECTION Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use.* United States Government Accountability Office. En ligne. <http://www.gao.gov/products/GAO-12-92>. Consulté le 8 janvier 2013.

U.N Secretary-general. 2012. *Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels: Report of the Secretary-General.* New York, NY, USA : United Nations. En ligne. <http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1164>. Consulté le 3 juin 2015.

Verizon Enterprise Solutions. 2015. *Verizon 2015 Data Breach Investigations Report.* En ligne. <http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/>. Consulté le 17 avril 2015.

Watkins, Bryan. 2014. *The Impact of Cyber Attacks on the Private Sector.* Association for International Affairs. En ligne. <http://www.amo.cz/editor/image/produkty1_soubory/the-impact-of-cyber-attacks-on-the-private-sector---briefing-paper.pdf>. Consulté le 3 juin 2015.

Working Group on Internet Governance (WGIG). 2005. *Report of the Working Group on Internet Governance.* United Nations. En ligne. <http://www.wgig.org/docs/WGIGREPORT.pdf>. Consulté le 5 septembre 2014.

LOIS, TRAITÉS ET AUTRES ACTES JURIDIQUES

Council of Europe. . « Convention on Cybercrime. » En ligne. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. Consulté le 1 juin 2015.

European Commission. . *Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union.* En ligne. <ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and>. Consulté le 1 juin 2015.

———. . « EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive. » En ligne. <ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>. Consulté le 1 juin 2015.

International Committee of the Red Cross (ICRC). . « Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I). » En ligne. <https://www.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/D9E6B6264D7723C3C12563CD002D6CE4/FULLTEXT/AP-I-EN.pdf>. Consulté le 29 mai 2015.

Organisation du traité de l'Atlantique nord. . « Traité de l'Atlantique Nord. » En ligne. <http://www.nato.int/cps/fr/natolive/official_texts_17120.htm>. Consulté le 3 juin 2015.

Valls, Manuel. . *PROJET DE LOI relatif au renseignement.* En ligne. <http://www.assemblee-nationale.fr/14/projets/pl2669.asp>. Consulté le 3 juin 2015.

ARTICLES DE JOURNAUX, ARTICLES TECHNIQUES ET PUBLICATIONS SPÉCIALISÉES (NON-SCIENTIFIQUES)

Ackerman, Spencer et Jonathan Kaiman. 2014. « Chinese military officials charged with stealing US data as tensions escalate. » *the Guardian*. En ligne. <http://www.theguardian.com/technology/2014/may/19/us-chinese-military-officials-cyber-espionage>. Consulté le 28 juin 2014.

Agence France-Presse. 2015a. « Presque toutes les voitures connectées sont vulnérables. » *Le Devoir*. En ligne. <http://www.ledevoir.com/societe/science-et-technologie/431342/presque-toutes-les-voitures-connectees-sont-vulnerables>. Consulté le 10 février 2015.

———. 2015b. « Brics: la Nouvelle Banque de Développement opérationnelle fin 2015 - Libération. » En ligne. <http://www.liberation.fr/economie/2015/06/26/brics-la-nouvelle-banque-de-developpement-operationnelle-fin-2015_1337828>. Consulté le 1 juillet 2015.

Aron, Jacob. 2015. « The internet is running out of room – but we can save it. » *New Scientist*. En ligne. <http://www.newscientist.com/article/dn27536-the-internet-is-running-out-of-room--but-we-can-save-it.html>. Consulté le 17 mai 2015.

Arthur, Charles. 2013. « Undersea internet cables off Egypt disrupted as navy arrests three. » *the Guardian*. En ligne. <http://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests>. Consulté le 26 mai 2015.

Asokan, Sari Horwitz, Shyamantha et Julie Tate. 2011. « Trade in surveillance technology raises worries. » *The Washington Post*, 22 novembre 2011. En ligne. <http://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO_story.html?hpid=z2>. Consulté le 11 juin 2015.

Associated Press. 2013. « Les marchands d'armes se tournent vers la cybersécurité | Internet. » *La Presse*. En ligne. <http://techno.lapresse.ca/nouvelles/internet/201302/18/01-4622650-les-marchands-darmes-se-tournent-vers-la-cybersecurite.php>. Consulté le 18 février 2013.

Atmani, Mehdi. 2011. « Voler une voiture en passant par le réseau de téléphonie mobile, c'est possible - LeMonde.fr. » *Le Monde*, 15 août 2011. En ligne.

<http://www.lemonde.fr/technologies/article/2011/08/15/voler-une-voiture-en-passant-par-le-reseau-de-telephonie-mobile-c-est-possible_1559864_651865.html>.

Ball, James. 2015. « GCHQ captured emails of journalists from top international media. » *the Guardian*. En ligne. <http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post>. Consulté le 31 janvier 2015.

van Beijnum, Iljitsch. 2010. « Understanding the Internet's insecure routing infrastructure. » *Ars Technica*. En ligne. <http://arstechnica.com/tech-policy/news/2010/11/understanding-the-internets-insecure-routing-infrastructure.ars>. Consulté le 28 mai 2015.

Bohlen, Celestine. 1992. « Yeltsin Deputy Calls Reforms "Economic Genocide". » *The New York Times*, 9 février 1992, sect. World. En ligne. <http://www.nytimes.com/1992/02/09/world/yeltsin-deputy-calls-reforms-economic-genocide.html>. Consulté le 24 juin 2015.

Bowcott, Owen. 2014. « UK intelligence agencies spying on lawyers in sensitive security cases. » *the Guardian*. En ligne. <http://www.theguardian.com/world/2014/nov/06/intelligence-agencies-lawyer-client-abdel-hakim-belhaj-mi5-mi6-gchq>. Consulté le 31 janvier 2015.

Braga, Matthew. 2015. « How Canadian Spies Infiltrated the Internet's Core to Watch What You Do Online. » *Motherboard*. En ligne. <http://motherboard.vice.com/read/how-canadian-spies-infiltrated-the-internets-core-to-watch-what-you-do-online>. Consulté le 12 février 2015.

Brandom, Russell. 2014. « South Korean nuclear plant finds malware connected to control systems. » *The Verge*. En ligne. <http://www.theverge.com/2014/12/30/7467809/south-korean-nuclear-plant-finds-malware-connected-to-control-systems>. Consulté le 13 février 2015.

Breton, Johann. 2014. « Careto, un spyware de pointe pour gouvernements et grandes entreprises. » En ligne. <http://www.lesnumeriques.com/careto-spyware-pointe-pour-gouvernements-grandes-entreprises-n33189.html>. Consulté le 18 février 2014.

Buzzetti, Hélène. 2011. « Censurer internet avec de la technologie canadienne | le devoir. » *Le Devoir*, 12 juillet 2011. En ligne. <http://www.ledevoir.com/politique/canada/327223/censurer-internet-avec-de-la-technologie-canadienne>. Consulté le 18 février 2015.

Carrington, Damian. 2014. « "Climategate" had only fleeting effect on global warming scepticism ». *the Guardian*. En ligne. <http://www.theguardian.com/environment/2014/may/20/climategate-longterm-level-climate-change-scepticism>. Consulté le 25 juin 2015.

CBC News. 2015. « New York Stock Exchange reopens after glitch halts trading. » *CBC News*. En ligne. <http://www.cbc.ca/1.3143031>. Consulté le 9 juillet 2015.

Chowdhry, Amit. 2014. « Google Invests In $300 Million Underwater Internet Cable System To Japan. » *Forbes*. En ligne. <http://www.forbes.com/sites/amitchowdhry/2014/08/12/google-invests-in-300-million-underwater-internet-cable-system-to-japan/>. Consulté le 26 mai 2015.

Clarke, Elizabeth. 2013. « The Underground Hacking Economy is Alive and Well. » *Dell SecureWorks Security and Compliance Blog*. En ligne. <http://www.secureworks.com/resources/blog/the-underground-hacking-economy-is-alive-and-well/>. Consulté le 28 mai 2015.

Col, Pierre. 2011. « Une pelleteuse coupe le site web du ministère de la Défense... et beaucoup d'autres ! » *ZDNet France*. En ligne. <http://www.zdnet.fr/actualites/une-pelleteuse-coupe-le-site-web-du-ministere-de-la-defense-et-beaucoup-d-autres-39760750.htm>. Consulté le 26 mai 2015.

Cooper, Rob. 2012. « Ship's anchor accidentally slices internet cable cutting off access in six African countries. » *Mail Online*. En ligne. <http://www.dailymail.co.uk/news/article-2108868/Ships-anchor-accidentally-slices-internet-cable-cutting-access-African-countries.html>. Consulté le 29 mai 2015.

Cowie, Jim. 2013. « The New Threat: Targeted Internet Traffic Misdirection. » *Dyn Research*. En ligne. <http://research.dyn.com/2013/11/mitm-internet-hijacking/>. Consulté le 26 juin 2015.

Cuthbertson, Richard. 2015. « Eastlink sues Newfoundland fishing vessel for subsea cable break. » En ligne. <http://www.cbc.ca/1.2987832>. Consulté le 26 mai 2015.

Cybersecurity ventures. 2015. « The Cybersecurity Market Report covers the business of cybersecurity, including market sizing and industry forecasts, spending, notable M&A and IPO activity, and more. » *Cybersecurity Ventures*. En ligne. <http://cybersecurityventures.com/cybersecurity-market-report/>. Consulté le 24 mai 2015.

Dilanian, Ken et Ted Bridis. 2015. « Officials: Second hack exposed military and intel data. » *The Big Story*. En ligne.

<http://bigstory.ap.org/article/d842d757851b4a59aca2aecf2f31995a/union-says-all-federal-workers-fell-victim-hackers>. Consulté le 26 juin 2015.

European Internet Exchange Association. 2015. « List of 102 known North America IXPs. » *List of IXPs in North America - Euro IX.* En ligne. <https://www.euro-ix.net/north-america>. Consulté le 26 mai 2015.

Farhi, Paul et Hayley Tsukayama. 2013. « Syrian Electronic Army hacks Washington Post Web site. » *The Washington Post,* 15 août 2013. En ligne. <http://www.washingtonpost.com/lifestyle/style/syrian-group-hacks-washington-post-web-site/2013/08/15/4e60d952-05bd-11e3-88d6-d5795fab4637_story.html>. Consulté le 1 février 2015.

Finkle, Jim. 2014. « Hacker says to show passenger jets at risk of cyber attack. » *Reuters,* 4 août 2014. En ligne. <http://www.reuters.com/article/2014/08/04/us-cybersecurity-hackers-airplanes-idUSKBN0G40WQ20140804>. Consulté le 4 août 2014.

Fishman, Andrew et Morgan Marquis-Boire. 2015. « Popular Security Software Came Under Relentless NSA and GCHQ Attacks. » *The Intercept.* En ligne. <https://firstlook.org/theintercept/2015/06/22/nsa-gchq-targeted-kaspersky/>. Consulté le 8 juillet 2015.

Flitter, Emily. 2015. « FBI says Sony hackers "got sloppy," posted from North Korea servers ». *Reuters,* 7 janvier 2015. En ligne. <http://www.reuters.com/article/2015/01/07/us-northkorea-cyberattack-usa-fbi-idUSKBN0KG1V220150107>. Consulté le 7 janvier 2015.

Follorou, Jacques et Martin Untersinger. 2014a. « La France suspectée de cyberespionnage. » *Le Monde.fr.* En ligne. <http://www.lemonde.fr/international/article/2014/03/21/la-france-suspectee-de-cyberattaque_4387232_3210.html>. Consulté le 21 mars 2014.

———. 2014b. « Quand les Canadiens partent en chasse de « Babar ». » *Le Monde.fr.* En ligne. </international/article/2014/03/21/quand-les-canadiens-partent-en-chasse-de-babar_4387233_3210.html>. Consulté le 26 juin 2015.

Franceschi-Bicchierai, Lorenzo. 2015a. « The DEA Has Been Secretly Buying Hacking Tools From an Italian Company. » *Motherboard.* En ligne. <http://motherboard.vice.com/read/the-dea-has-been-secretly-buying-hacking-tools-from-an-italian-company>. Consulté le 8 juillet 2015.

———. 2015b. « The Massive Hack on US Personnel Agency is Worse Than Everyone Thought. » *Motherboard.* En ligne. <http://motherboard.vice.com/read/the-massive-

hack-on-us-personnel-agency-is-worse-than-everyone-thought>. Consulté le 22 juin 2015.

Fung, Brian. 2014. « Online attack cripples U.S. court system. » *Washington Post*. En ligne. <http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/24/online-attack-cripples-u-s-court-system/>. Consulté le 25 janvier 2014.

Gallagher, Ryan. 2015. « New Zealand Spies on Neighbors in Secret "Five Eyes" Global Surveillance ». *The Intercept*. En ligne. <https://firstlook.org/theintercept/2015/03/04/new-zealand-gcsb-surveillance-waihopai-xkeyscore/>. Consulté le 4 mars 2015.

Gallagher, Ryan et Glenn Greenwald. 2015. « Canada Casts Global Surveillance Dragnet Over File Downloads. » *The Intercept*. En ligne. <https://firstlook.org/theintercept/2015/01/28/canada-cse-levitation-mass-surveillance/>. Consulté le 22 avril 2015.

Gardels, Nathan et Mike McConnell. 2009. « Mike McConnell: An American Spymaster on Cyberwar. » *The Huffington Post*. En ligne. <http://www.huffingtonpost.com/nathan-gardels/mike-mcconnell-an-america_b_227944.html>. Consulté le 3 juin 2015.

Gellman, Barton. 2014. « U.S. firm helped the spyware industry build a potent digital weapon for sale overseas. » *The Washington Post*, 15 août 2014. En ligne. <http://www.washingtonpost.com/world/national-security/spyware-tools-allow-buyers-to-slip-malicious-code-into-youtube-videos-microsoft-pages/2014/08/15/31c5696c-249c-11e4-8593-da634b334390_story.html?tid=sm_fb>. Consulté le 21 août 2014.

Gibbs, Samuel. 2013. « FBI adds five new hackers to cyber most wanted list. » *the Guardian*. En ligne. <http://www.theguardian.com/technology/2013/nov/06/fbi-hackers-cyber-most-wanted>. Consulté le 1 février 2015.

———. 2014. « Google reinforces undersea cables after shark bites. » *the Guardian*. En ligne. <http://www.theguardian.com/technology/2014/aug/14/google-undersea-fibre-optic-cables-shark-attacks>. Consulté le 26 mai 2015.

Gilbert, Angela. 2014. « Data centre outage cost $1.6M in equipment, lost productivity. » En ligne. <http://www.cbc.ca/1.2840346>. Consulté le 26 mai 2015.

Golubkova, Katya. 2015. « New BRICS bank to look at local, international borrowing - president. » *Reuters India*. En ligne.

<http://in.reuters.com/article/2015/07/09/emerging-brics-bank-idINKCN0PJ1FH20150709>. Consulté le 11 juillet 2015.

Greenberg, Andy. 2012. « Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits. » *Forbes*. En ligne. <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>. Consulté le 28 mai 2015.

———. 2014a. « Why the Security of USB Is Fundamentally Broken | Threat Level. » *WIRED*. En ligne. <http://www.wired.com/2014/07/usb-security/?mbid=social_twitter>. Consulté le 31 juillet 2014.

———. 2014b. « Watch This Wireless Hack Pop a Car's Locks in Minutes | Threat Level. » *WIRED*. En ligne. <http://www.wired.com/2014/08/wireless-car-hack/?mbid=social_fb>. Consulté le 15 août 2014.

———. 2014c. « Watch a Hacker Fry a Hair Dryer With Her Radio | Threat Level. » *WIRED*. En ligne. <http://www.wired.com/2014/08/this-hackers-radio-can-fry-your-hair-dryer/>. Consulté le 15 août 2014.

———. 2015a. « House Passes Cybersecurity Bill Despite Privacy Protests. » *WIRED*. En ligne. <http://www.wired.com/2015/04/house-passes-cybersecurity-bill-despite-privacy-protests/>. Consulté le 23 avril 2015.

———. 2015b. « This Radio Bug Can Steal Laptop Crypto Keys, Fits Inside a Pita. » *WIRED*. En ligne. <http://www.wired.com/2015/06/radio-bug-can-steal-laptop-crypto-keys-fits-inside-pita/>. Consulté le 7 juillet 2015.

———. 2015c. « Hacking Team Breach Shows a Global Spying Firm Run Amok. » *WIRED*. En ligne. <http://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/>. Consulté le 9 juillet 2015.

Greenwald, Glenn. 2014. « Glenn Greenwald: how the NSA tampers with US-made internet routers. » *the Guardian*. En ligne. <http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden>. Consulté le 29 juin 2015.

Griffin, Andrew. 2015. « Someone 'accidentally' sent the UK's nuclear weapons data through Ukraine. » *The Independent*. En ligne. <http://www.independent.co.uk/life-style/gadgets-and-tech/news/uks-nuclear-weapons-data-and-other-sensitive-internet-traffic-accidentally-sent-through-ukraine-10107168.html>. Consulté le 26 juin 2015.

Guiton, Amaelle, Alexandre Léchenet, Jean-Marc Manach et Julian Assange. 2015. « WikiLeaks - Chirac, Sarkozy et Hollande : trois présidents sur écoute - Libération. » En ligne. <http://www.liberation.fr/monde/2015/06/23/chirac-sarkozy-et-hollande-trois-presidents-sur-ecoute_1335767>. Consulté le 26 juin 2015.

Halsey, Ashley III. 2015. « Automation problem led to ground stop for United Airlines. » *The Washington Post*, 8 juillet 2015. En ligne. <http://www.washingtonpost.com/local/trafficandcommuting/faa-says-all-united-airlines-flights-grounded-because-of-automation-problem/2015/07/08/360f8364-2571-11e5-aae2-6c4f59b050aa_story.html>. Consulté le 9 juillet 2015.

Hamburger, Tom et Matea Gold. 2014. « Google, once disdainful of lobbying, now a master of Washington influence. » *The Washington Post*, 12 avril 2014. En ligne. <http://www.washingtonpost.com/politics/how-google-is-transforming-power-and-politicsgoogle-once-disdainful-of-lobbying-now-a-master-of-washington-influence/2014/04/12/51648b92-b4d3-11e3-8cb6-284052554d74_story.html>. Consulté le 3 juin 2015.

Hammouche, Sid Ahmed. 2012. « Cyberattaque contre l'une des plus importantes compagnies pétrolières | Rue89. » En ligne. <http://www.rue89.com/2012/08/24/cyberattaque-contre-lune-des-plus-importantes-compagnies-petrolieres-234811>.

Harding, Luke. 2015. « Mass surveillance is fundamental threat to human rights, says European report. » *the Guardian*. En ligne. <http://www.theguardian.com/world/2015/jan/26/mass-surveillance-threat-human-rights-council-europe>. Consulté le 31 janvier 2015.

Hernandez, Daniel et Gabriela Gorbea. 2015. « Mexico Is Hacking Team's Biggest Paying Client — By Far. » *VICE News*. En ligne. <https://news.vice.com/article/mexico-is-hacking-teams-biggest-paying-client-by-far>. Consulté le 8 juillet 2015.

Hickman, Leo. 2012. « Climategate detective: "I"m deeply disappointed' we didn't catch hacker | Leo Hickman ». *the Guardian*. En ligne. <http://www.theguardian.com/environment/blog/2012/jul/20/climategate-detective-disappointed-catch-hacker>. Consulté le 25 juin 2015.

Holmes, Oliver. 2012. « Global hacking network declares Internet war on Syria. » *Reuters*, 30 novembre 2012. En ligne. <http://www.reuters.com/article/2012/11/30/us-syria-crisis-internet-idUSBRE8AT0PN20121130>. Consulté le 2 janvier 2015.

ICI.Radio-Canada.ca, Zone Nouvelles-. 2014. « Les sites web de la Cour suprême et de la police d'Ottawa inaccessibles | ICI. » *Radio-Canada.ca*. En ligne. <http://ici.radio-

canada.ca/nouvelles/societe/2014/11/22/004-attaque-site-web-ville-ottawa-police-cour-supreme-hors-ligne.shtml>. Consulté le 23 novembre 2014.

InfoSec Institute. 2013. « Cybercrime as a Service. » *InfoSec Institute*. En ligne. <http://resources.infosecinstitute.com/cybercrime-as-a-service/>. Consulté le 28 mai 2015.

———. 2015. « Cybercrime and the Underground Market. » *InfoSec Institute*. En ligne. <http://resources.infosecinstitute.com/cybercrime-and-the-underground-market/>. Consulté le 28 mai 2015.

Isikoff, Michael. 2013. « Chinese hacked Obama, McCain campaigns, took internal documents, officials say. » *NBC News*. En ligne. <http://investigations.nbcnews.com/_news/2013/06/06/18807056-chinese-hacked-obama-mccain-campaigns-took-internal-documents-officials-say>. Consulté le 9 juillet 2015.

Kastrenakes, Jacob. 2014. « London airspace restricted after computer failure. » *The Verge*. En ligne. <http://www.theverge.com/2014/12/12/7382429/london-airspace-restricted-after-nats-computer-failure>. Consulté le 12 décembre 2014.

Kirsch, Julian, Christian Grothoff, Monika Ermert, Jacob Appelbaum, Laura Poitras et Henrike Moltke. 2014. « GCHQ/NSA: Le programme HACIENDA. » *c't magazin*. En ligne. <http://www.heise.de/ct/artikel/GCHQ-NSA-Le-programme-HACIENDA-2293122.html>. Consulté le 26 août 2014.

Knapton, Sarah. 2014. « Driverless cars could be hacked by terrorists, warn transport experts », 21 novembre 2014, sect. News. En ligne. <http://www.telegraph.co.uk/news/science/11243376/Driverless-cars-could-be-hacked-by-terrorists-warn-transport-experts.html>. Consulté le 24 mai 2015.

Knibbs, Kate. 2015. « State Dept. Stops Issuing New Overseas Passports, Possibly Due to Hack. » *Gizmodo*. En ligne. <http://gizmodo.com/state-dept-stops-issuing-new-overseas-passports-may-r-1710997907?utm_campaign=socialflow_gizmodo_facebook&utm_source=gizmodo_facebook&utm_medium=socialflow>. Consulté le 26 juin 2015.

Kopan, Tal. 2014. « FBI briefed on alternate Sony hack theory. » *POLITICO*. En ligne. <http://www.politico.com/story/2014/12/fbi-briefed-on-alternate-sony-hack-theory-113866.html>. Consulté le 30 décembre 2014.

Kristanadjaja, Gurvan. 2014. « J'ai discuté avec la Syrian Electronic Army, les jeunes hackers pro-Assad. » *Rue89*. En ligne. <http://rue89.nouvelobs.com/2014/07/07/jai-

discute-syrian-electronic-army-les-jeunes-hackers-pro-assad-253479>. Consulté le 19 août 2014.

Kushner, David. 2014. « An Inside Look at Anonymous, the Radical Hacking Collective. » *The New Yorker*. En ligne. <http://www.newyorker.com/magazine/2014/09/08/masked-avengers>. Consulté le 1 février 2015.

Lardinois, Frederic. 2015. « Microsoft Invests In 3 Undersea Cable Projects To Improve Its Data Center Connectivity. » *TechCrunch*. En ligne. <http://social.techcrunch.com/2015/05/11/microsoft-invests-in-3-undersea-cable-projects-to-improve-its-data-center-connectivity/>. Consulté le 26 mai 2015.

Lasalle, Laurent. 2015. « Anonymous revendique une cyberattaque contre le SPVM. » *Branchez-vous*. En ligne. <http://branchez-vous.com/2015/04/11/anonymous-revendique-cyberattaque-le-spvm/>. Consulté le 24 mai 2015.

Lauer, Stéphane. 2014. « Des banques américaines ont été la cible de pirates informatiques. » *Le Monde.fr*. En ligne. <http://www.lemonde.fr/economie/article/2014/08/29/des-banques-americaines-ont-ete-la-cible-de-pirates-informatiques_4478829_3234.html>. Consulté le 30 août 2014.

Lee, Micah. 2015. « Secret "BADASS" Intelligence Program Spied on Smartphones ». *The Intercept*. En ligne. <https://firstlook.org/theintercept/2015/01/26/secret-badass-spy-program/>. Consulté le 2 février 2015.

Le Monde. 2011. « Anonymous prétend avoir piraté des bases de données de l'OTAN - LeMonde.fr. » En ligne. <http://www.lemonde.fr/technologies/article/2011/07/21/anonymous-pretend-avoir-pirate-des-bases-de-donnees-de-l-otan_1551416_651865.html>. Consulté le 21 juillet 2011.

———. 2014. « La NSA aurait piraté cinq opérateurs télécom allemands. » *Le Monde.fr*. En ligne. <http://www.lemonde.fr/pixels/article/2014/09/13/la-nsa-et-le-gchq-auraient-pirate-cinq-operateurs-telecom-allemands_4487181_4408996.html>. Consulté le 6 octobre 2014.

Levine, Yasha. 2014. « Almost everyone involved in developing Tor was (or is) funded by the US government. » *PandoDaily*. En ligne. <http://pando.com/2014/07/16/tor-spooks/>. Consulté le 5 août 2014.

Lewis, Peter H. 1987. « Phone company finds sharks cutting in. » *The New York Times*, 11 juin 1987, sect. U.S. En ligne. <http://www.nytimes.com/1987/06/11/us/phone-company-finds-sharks-cutting-in.html>. Consulté le 26 mai 2015.

Löwy, Michael. 2003. « "Avertisseur d'incendie": la critique de la technologie chez Walter Benjamin ». En ligne. <http://multitudes.samizdat.net/spip.php?page=imprimer&id_article=733>. Consulté le 25 février 2014.

Lukacs, Martin et Tim Groves. 2013. « Canadian spies met with energy firms, documents reveal. » *the Guardian*. En ligne. <http://www.theguardian.com/environment/2013/oct/09/canadian-spies-met-energy-firms-documents>. Consulté le 10 juin 2015.

MacAskill, Ewen. 2015. « British army creates team of Facebook warriors. » *the Guardian*. En ligne. <http://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade>. Consulté le 1 février 2015.

MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies et James Ball. 2013. « GCHQ taps fibre-optic cables for secret access to world's communications. » *the Guardian*. En ligne. <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>. Consulté le 31 janvier 2015.

Mackinnon, Rebecca. 2012. « The United Nations and the Internet: It's Complicated. » *Foreign Policy*. En ligne. <http://foreignpolicy.com/2012/08/08/the-united-nations-and-the-internet-its-complicated/>. Consulté le 22 avril 2015.

Madory, Doug. 2014. « Chinese Routing Errors Redirect Russian Traffic. » *Dyn Research*. En ligne. <http://research.dyn.com/2014/11/chinese-routing-errors-redirect-russian-traffic/>. Consulté le 26 juin 2015.

Markoff, John. 2008. « Before the Gunfire, Cyberattacks. » *The New York Times*, 13 août 2008, sect. Technology. En ligne. <http://www.nytimes.com/2008/08/13/technology/13cyber.html>. Consulté le 29 juin 2015.

———. 2010. « Cars' Computer Systems Called at Risk to Hackers. » *The New York Times*, 14 mai 2010. En ligne. <http://www.nytimes.com/2010/05/14/science/14hack.html>. Consulté le 24 mai 2015.

McLaughlin, Jenna. 2015. « IPT Flip-Flops on Unlawful GCHQ Surveillance of Amnesty International. » *The Intercept*. En ligne.

<https://firstlook.org/theintercept/2015/07/01/major-reversal-british-tribunal-confirms-surveillance-amnesty-international-violated-rights/>. Consulté le 7 juillet 2015.

McMillan, Robert. 2012. « The 61 Countries a Mad Despot Could Instantly Unplug From the Internet. » *WIRED*. En ligne. <http://www.wired.com/2012/12/internet_plug/>. Consulté le 11 juin 2015.

———. 2014a. « Why Gadgets in the Internet of Things Must Be Programmed to Die | Enterprise. » *WIRED*. En ligne. <http://www.wired.com/2014/05/iot-death/?mbid=social_fb>. Consulté le 25 mai 2014.

———. 2014b. « The Internet Has Grown Too Big for Its Aging Infrastructure | Enterprise. » *WIRED*. En ligne. <http://www.wired.com/2014/08/router_problem/?mbid=social_fb>. Consulté le 15 août 2014.

———. 2014c. « The Internet Is Broken, and Shellshock Is Just the Start of Our Woes. » *WIRED*. En ligne. <http://www.wired.com/2014/09/shellshocked-bash/>. Consulté le 1 octobre 2014.

Mitchell, Scott. 2015. « Authorities at Odds Over Secret Australian Police Operation that Bugged Officers and Journalists. » *VICE News*. En ligne. <https://news.vice.com/article/authorities-at-odds-over-secret-australian-police-operation-that-bugged-officers-and-journalists>. Consulté le 8 février 2015.

Moore, Solomon. 2012. « Ship Accidents Sever Data Cables Off East Africa. » *Wall Street Journal*, 28 février 2012, sect. World News. En ligne. <http://www.wsj.com/articles/SB10001424052970203833004577249434081658686>. Consulté le 26 mai 2015.

Nakashima, Ellen. 2012. « Iran blamed for cyberattacks on U.S. banks and companies. » *The Washington Post*, 21 septembre 2012. En ligne. <http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html>. Consulté le 13 février 2015.

———. 2015. « With a series of major hacks, China builds a database on Americans. » *The Washington Post*, 5 juin 2015. En ligne. <http://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html?tid=sm_fb>. Consulté le 23 juin 2015.

Nakashima, Ellen et Andrea Peterson. 2014. « Report: Cybercrime and espionage costs $445 billion annually. » *The Washington Post*, 8 juin 2014. En ligne. <http://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html>. Consulté le 1 février 2015.

National Telecommunications & Information Administration. 2014. « NTIA Announces Intent to Transition Key Internet Domain Name Functions. » En ligne. <http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>. Consulté le 14 mars 2014.

Olavsrud, Thor. 2015. « Security Experts React to President's Cybersecurity Proposals. » *CIO*. En ligne. <http://www.cio.com/article/2867992/security0/security-experts-react-to-presidents-cybersecurity-proposals.html>. Consulté le 3 juin 2015.

Ollstein, Alice. 2014. « Google's Political Spending Topped All Other U.S. Companies This Year. » *ThinkProgress*. En ligne. <http://thinkprogress.org/election/2014/11/14/3591983/google-political-spending-report/>. Consulté le 3 juin 2015.

Orazio, Dante D'. 2014a. « North Korea proposes a "joint investigation" with US to prove its innocence in Sony hack ». *The Verge*. En ligne. <http://www.theverge.com/2014/12/20/7426793/north-korea-proposes-joint-investigation-with-us-into-sony-hack>. Consulté le 20 décembre 2014.

———. 2014b. « North Korea blames US for internet outage, calls Obama a reckless "monkey". » *The Verge*. En ligne. <http://www.theverge.com/2014/12/27/7454241/north-korea-blames-us-for-internet-outage>. Consulté le 27 décembre 2014.

Osborne, Charlie. 2015. « Hackers prompt flight cancellation at Polish airport. » *ZDNet*. En ligne. <http://www.zdnet.com/article/hackers-prompt-flight-cancellation-at-polish-airport/>. Consulté le 22 juin 2015.

Phillip, Abby. 2014. « Germany considers the ultimate antidote to high-tech espionage: The humble typewriter. » *The Washington Post*, 15 juillet 2014. En ligne. <http://www.washingtonpost.com/blogs/worldviews/wp/2014/07/15/germany-considers-the-ultimate-antidote-to-high-tech-espionage-the-humble-typewriter/?Post+generic=%3Ftid%3Dsm_twitter_washingtonpost>. Consulté le 16 juillet 2014.

de Pierrebourg, Fabrice. 2013. « Nouvelle cyberattaque contre le SPVM. » *La Presse*, février 2013. En ligne.

<http://www.lapresse.ca/actualites/regional/montreal/201302/18/01-4623001-nouvelle-cyberattaque-contre-le-spvm.php>. Consulté le 19 février 2013.

Renaud, Daniel. 2012. « Piratage informatique - 11 000 policiers touchés par une attaque. » En ligne. <http://tvanouvelles.ca/lcn/infos/regional/montreal/archives/2012/06/20120614-045745.html>. Consulté le 24 mai 2015.

Riley, Michael. 2014. « How Russian Hackers Stole the Nasdaq. » *BloombergView*. En ligne. <http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq>. Consulté le 24 mai 2015.

Robertson, Adi. 2014a. « Politicians respond to Sony hack, call for cybersecurity bill. » *The Verge*. En ligne. <http://www.theverge.com/2014/12/18/7415291/politicians-respond-to-the-sony-hack-mccain-calls-for-cybersecurity-bill>. Consulté le 19 décembre 2014.

Robertson, Anna EdgertonJordan. 2014b. « Brazil-to-Portugal Cable Shapes Up as Anti-NSA Case Study. » *Bloomberg.com*. En ligne. <http://www.bloomberg.com/news/articles/2014-10-30/brazil-to-portugal-cable-shapes-up-as-anti-nsa-case-study>. Consulté le 13 février 2015.

Robertson, Jordan et Michael Riley. 2014. « Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era. » *Bloomberg*. En ligne. <http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html>. Consulté le 5 janvier 2015.

Saksena, Amit R. 2014. « India Scrambles on Cyber Security. » *The Diplomat*. En ligne. <http://thediplomat.com/2014/06/india-scrambles-on-cyber-security/>. Consulté le 3 juin 2015.

Samenow, Mary Pat Flaherty, Jason et Lisa Rein. 2014. « Chinese hack U.S. Weather systems, satellite network. » *The Washington Post*, 12 novembre 2014. En ligne. <http://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html?tid=sm_fb>. Consulté le 12 novembre 2014.

Sanger, David E. et Thom Shanker. 2014. « N.S.A. Devises Radio Pathway Into Computers. » *The New York Times*, 14 janvier 2014. En ligne. <http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html>. Consulté le 1 février 2015.

Sang-hun, Choe. 2014. « North Korea Denies Hacking Sony but Calls Attack a 'Righteous Deed'. » *The New York Times*, 7 décembre 2014. En ligne. <http://www.nytimes.com/2014/12/08/business/north-korea-denies-hacking-sony-but-calls-attack-a-righteous-deed.html>. Consulté le 7 décembre 2014.

Sayer, Peter. 2013. « Data center outage takes French state financial system offline for four days. » *Computerworld.* En ligne. <http://www.computerworld.com/article/2498154/enterprise-resource-planning/data-center-outage-takes-french-state-financial-system-offline-for-four.html>. Consulté le 26 mai 2015.

Scahill, Jeremy et Josh Begley. 2015. « iSpy: The CIA Campaign to Steal Apple's Secrets. » *The Intercept.* En ligne. <https://firstlook.org/theintercept/2015/03/10/ispy-cia-campaign-steal-apples-secrets/>. Consulté le 10 mars 2015.

Scher, Bill. 2009. « Climategate is a flop, not Copenhagen. » *the Guardian.* En ligne. <http://www.theguardian.com/environment/2009/dec/11/climategate-copenhagen>. Consulté le 25 juin 2015.

Schneier, Bruce. 2014. « The Internet of Things Is Wildly Insecure — And Often Unpatchable | Wired Opinion | Wired.com. » *Wired Opinion.* En ligne. <http://www.wired.com/opinion/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/>. Consulté le 29 janvier 2014.

Shalal, Andrea et Matt Spetalnick. 2015. « Data hacked from U.S. government dates back to 1985: U.S. official. » *Reuters*, 6 juin 2015. En ligne. <http://www.reuters.com/article/2015/06/06/us-cybersecurity-usa-idUSKBN0OL1V320150606>. Consulté le 22 juin 2015.

Siddique, Haroon. 2015. « North Korea responds with fury to US sanctions over Sony hack. » *The Guardian*, 4 janvier 2015, sect. World news. En ligne. <http://www.theguardian.com/world/2015/jan/04/north-korea-fury-us-sanctions-sony>. Consulté le 4 janvier 2015.

Sottek, T.C. 2015. « New Snowden documents show that the NSA and its allies are laughing at the rest of the world. » *The Verge.* En ligne. <http://www.theverge.com/2015/1/17/7629721/nsa-is-pwning-everyone-and-having-a-chuckle-about-it>. Consulté le 18 janvier 2015.

Spencer, Ben. 2015. « Is the internet on the brink of collapse? » *Mail Online*. En ligne. <http://www.dailymail.co.uk/sciencetech/article-3064915/The-Internet-reach-limit-just-eight-years-warn-engineers.html>. Consulté le 26 mai 2015.

Spiegel. 2013. « Inside TAO: Documents Reveal Top NSA Hacking Unit. » *Spiegel Online*, 29 décembre 2013, sect. International. En ligne. <http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html>. Consulté le 29 juin 2015.

Sternstein, Aliya. 2015a. « Is Obama's $14 Billion Cybersecurity Request Enough? » *Defense One*. En ligne. <http://www.defenseone.com/technology/2015/02/obamas-14-billion-cybersecurity-request-enough/104421/>. Consulté le 3 juin 2015.

———. 2015b. « US Cyber Command Has Just Half the Staff It Needs. » *Defense One*. En ligne. <http://www.defenseone.com/threats/2015/02/us-cyber-command-has-just-half-staff-it-needs/104847/>. Consulté le 3 juin 2015.

Swaine, Jon. 2008. « Georgia: Russia "conducting cyber war". » *The Telegraph*, 11 août 2008, sect. World. En ligne. <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html>. Consulté le 29 juin 2015.

Symantec Security Response. 2014. « Turla: Spying tool targets governments and diplomats. » *Symantec Security Response*. En ligne. <http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats>. Consulté le 18 février 2015.

Teisceira-Lessard, Philippe. 2012. « Anonymous attaque le gouvernement du Québec | Philippe Teisceira-Lessard | Politique québécoise. » *La Presse*, 19 mai 2012. En ligne. <http://www.lapresse.ca/actualites/quebec-canada/politique-quebecoise/201205/19/01-4526911-anonymous-attaque-le-gouvernement-du-quebec.php?utm_categorieinterne=trafficdrivers&utm_contenuinterne=cyberpresse_BO2_quebec_canada_178_accueil_POS3>.

TeleGeography. 2015. « Submarine Cable Map. » *Submarine Cable Map*. En ligne. <http://www.submarinecablemap.com/>. Consulté le 26 mai 2015.

The Moscow Times. 2015. « Number of Foreign Students in Russia Climbed 14% in 2014 | News. » *The Moscow Times*. En ligne. <http://www.themoscowtimes.com/news/article/number-of-foreign-students-in-russia-climbed-14-in-2014/516234.html>. Consulté le 5 juillet 2015.

Thornhill, Ted et Reuters. 2015. « China navy warns U.S. spy plane in disputed South China Sea - CNN. » *Daily Mail*. En ligne. <http://www.dailymail.co.uk/news/article-3090728/China-navy-warns-U-S-spy-plane-disputed-South-China-Sea-CNN.html>. Consulté le 5 juillet 2015.

Timberg, Craig. 2014a. « U.S. to relinquish remaining control over the Internet. » *The Washington Post*, 14 mars 2014. En ligne. <http://www.washingtonpost.com/business/technology/us-to-relinquish-remaining-control-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.html>. Consulté le 1 juin 2015.

———. 2014b. « German researchers discover a flaw that could let anyone listen to your cell calls. » *The Washington Post*, 18 décembre 2014. En ligne. <http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/?tid=sm_fb>. Consulté le 19 décembre 2014.

Times Higher Education. 2015. « BRICS & Emerging Economies Rankings 2015. » *Times Higher Education*. En ligne. <https://www.timeshighereducation.co.uk/world-university-rankings/2015/brics-and-emerging-economies>. Consulté le 5 juillet 2015.

Titcomb, James. 2015. « Bloomberg outage causes financial havoc as UK forced to delay £3bn debt sale », 17 avril 2015, sect. Finance. En ligne. <http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/11544186/Finance-world-in-the-dark-as-Bloomberg-terminals-go-offline.html>. Consulté le 26 mai 2015.

Toor, Amar et Russell Brandom. 2015. « NSA-grade spyware is up for sale, and the world's worst dictatorships are buying. » *The Verge*. En ligne. <http://www.theverge.com/2015/1/21/7861645/finfisher-spyware-let-bahrain-government-hack-political-activist>. Consulté le 25 janvier 2015.

Tual, Morgane. 2015. « Les députés approuvent un système de surveillance du trafic sur Internet. » *Le Monde.fr*, 16 avril 2015. En ligne. </pixels/article/2015/04/16/les-deputes-approuvent-un-systeme-de-surveillance-du-trafic-sur-internet_4616652_4408996.html>. Consulté le 3 juin 2015.

UNESCO Institute for Statistics. 2012. « Global Flow of Tertiary-Level Students. » En ligne. <http://www.uis.unesco.org/Education/Pages/international-student-flow-viz.aspx>. Consulté le 5 juillet 2015.

Violet Blue. 2015. « Hackonomics: Street prices for black market bugs. » *ZDNet*. En ligne. <http://www.zdnet.com/article/hackonomics-street-prices-for-black-market-bugs/>. Consulté le 28 mai 2015.

Wagner, Ben et Claudio Guarnieri. 2014. « EXCLUSIVE: German Companies Are Selling Unlicensed Surveillance Technologies to Human Rights Violators – and Making Millions », 5 septembre 2014. En ligne.

<http://globalvoicesonline.org/2014/09/05/exclusive-german-companies-are-selling-unlicensed-surveillance-technologies-to-human-rights-violators-and-making-millions/>.

Ware, Willis H. 1979. « Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security - RAND Report R-609-1 | RAND. » En ligne. <http://www.rand.org/pubs/reports/R609-1/index2.html>. Consulté le 15 octobre 2013.

Warren, Tom. 2015. « Major Adobe Flash security flaw discovered in Hacking Team leak. » *The Verge*. En ligne. <http://www.theverge.com/2015/7/8/8911077/adobe-flash-hacking-team-vulnerability>. Consulté le 8 juillet 2015.

Waterman, Shaun. 2013. « NSA chief's admission of misleading numbers adds to Obama administration blunders. » *The Washingtion Times*. En ligne. <http://www.washingtontimes.com/news/2013/oct/2/nsa-chief-figures-foiled-terror-plots-misleading/>. Consulté le 3 juin 2015.

White, Bobby. 2007. « Its Creators Call Internet Outdated, Offer Remedies. » *Wall Street Journal*, 3 octobre 2007, sect. News. En ligne. <http://www.wsj.com/articles/SB119128309597345795>. Consulté le 28 mai 2015.

Whitney, Lance. 2013. « Anonymous hacks North Korea's Twitter and Flickr accounts. » *CNET*. En ligne. <http://www.cnet.com/news/anonymous-hacks-north-koreas-twitter-and-flickr-accounts/>. Consulté le 1 février 2015.

Wikileaks. 2015. « Wikileaks - Hacking Team. » *Wikileaks - Hacking Team*. En ligne. <https://wikileaks.org/hackingteam/emails/>. Consulté le 10 juillet 2015.

Williams, Christopher. 2012. « Internet IPv4 address system hits its limit », 14 septembre 2012, sect. Technology. En ligne. <http://www.telegraph.co.uk/technology/internet/9543870/Internet-IPv4-address-system-hits-its-limit.html>. Consulté le 26 mai 2015.

Woodall, Jessica. 2013. « Australia's vulnerable submarine cables. » *Australian Strategic Policy Institute*. En ligne. <http://www.aspistrategist.org.au/australias-vulnerable-submarine-cables/>. Consulté le 26 mai 2015.

World Health Organization. 2015. « WHO | Pharmaceutical Industry. » *WHO*. En ligne. <http://www.who.int/trade/glossary/story073/en/>. Consulté le 24 mai 2015.

Wueest, Candid. 2014. « Underground black market: Thriving trade in stolen data, malware, and attack services. » *Symantec Security Response*. En ligne.

<http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>. Consulté le 28 mai 2015.

Zarate, Juan C. et Thomas M. Sanderson. 2014. « In Iraq and Syria, ISIS Militants Are Flush With Funds. » *The New York Times*, 28 juin 2014. En ligne. <http://www.nytimes.com/2014/06/29/opinion/sunday/in-iraq-and-syria-isis-militants-are-flush-with-funds.html>. Consulté le 1 février 2015.

Zetter, Kim. 2013. « Prison Computer "Glitch" Blamed for Opening Cell Doors in Maximum-Security Wing ». *WIRED*. En ligne. <http://www.wired.com/2013/08/computer-prison-door-mishap/>. Consulté le 24 mai 2015.

———. 2014a. « Meet MonsterMind, the NSA Bot That Could Wage Cyberwar Autonomously | Threat Level. » *WIRED*. En ligne. <http://www.wired.com/2014/08/nsa-monstermind-cyberwarfare/>. Consulté le 15 août 2014.

———. 2014b. « Russian "Sandworm" Hack Has Been Spying on Foreign Governments for Years ». *WIRED*. En ligne. <http://www.wired.com/2014/10/russian-sandworm-hack-isight/>. Consulté le 14 octobre 2014.

———. 2014c. « An Unprecedented Look at Stuxnet, the World's First Digital Weapon. » *WIRED*. En ligne. <http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>. Consulté le 13 février 2015.

———. 2015a. « Feds Say That Banned Researcher Commandeered a Plane. » *WIRED*. En ligne. <http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/>. Consulté le 17 mai 2015.

———. 2015b. « Attackers Stole Certificate From Foxconn to Hack Kaspersky With Duqu 2.0. » *WIRED*. En ligne. <http://www.wired.com/2015/06/foxconn-hack-kaspersky-duqu-2/>. Consulté le 23 juin 2015.