ECOLE NATIONALE SUPERIEURE DES SCIENCES POLITIQUES

Département des Etudes Militaires et Stratégiques

CYBER-MENACES ET SÉCURITISATION DU CYBERESPACE

(ÉTUDE DU MODELE AMERICAIN)

Mémoire présenté en vue de l'obtention du diplôme de master en sciences politiques
Option : Études Stratégiques et Internationales

Réalisé par :
SAIBI Zineddine

Supervisé par :
LADJANI Ghania

JURY

Dr. FERSHOULI Fatma-Zohra ……..……. Présidente.
LADJANI Ghania ……. Rapporteur.
BELFERD Lotfi ……. Membre.

Année Universitaire : 2014 – 2015
5ème Promotion

« Qu'une victoire soit obtenue avant que la situation ne se soit cristallisée, voilà ce que le commun ne comprend pas. C'est pourquoi l'auteur de la prise n'est pas revêtu de quelque réputation de sagacité. Avant que la lame de son glaive ne soit recouverte de sang, État ennemi s'est déjà soumis. Si vous subjuguez votre ennemi sans livrer combat, ne vous estimez pas homme de valeur. »

Sun Tzu, *l'art de la guerre*

"Cyber Warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood."

U.S. department of defense

À mon père *in memoriam*
À ma mère pour son soutien indéfectible
À mes frères et ma sœur
À mes professeurs, mes camarades et mes ami(e)s

RESUME

L'utilisation à grande échelle des systèmes informatiques a rendu l'échange d'informations facile et rapide. Cependant, cela a contribué à l'apparition de nouvelles menaces relatives à ces nouvelles technologies qui fragilisent les infrastructures critiques et les patrimoines informationnels des États. Les processus de sécuritisation du cyberespace, c'est à dire la présentation de celui-ci comme une source de menaces existentielle pour un objet référent et y remédier, se sont déclenchés partout dans le monde pour essayer de se protéger des cyber-menaces.

Ces menaces sont le résultat de phénomènes très variables : des défis entre individus, volonté de nuire ou encore des situations géopolitiques. En effet, les États ont trouvés dans le cyberespace un nouveau terrain d'affrontement, nous pouvons le considérer comme une nouvelle grammaire des conflits ou une adjonction à la guerre conventionnelle à laquelle une révolution dans les affaires militaires viendrait s'installer et changerait partiellement la manière de penser le conflit armé.

Si le cyberespace change le conflit, il peut aussi devenir une zone d'opération des armées en temps de paix. Les États ciblent les systèmes informatiques des adversaires pour les saboter et recueillir des informations en parfait anonymat. Chose qui représente une menace pour les autres États. Les cibles qui peuvent être mises en danger sont variables : infrastructures critiques, systèmes d'armes, patrimoine informationnel, etc.

La prise de conscience de l'émergence des cyber-menaces est accompagnée par des politiques de cyber-sécurité. En 2013, les États-Unis d'Amérique ont identifié le cyberespace comme la source de menaces la plus sérieuse à sa sécurité nationale. Ils ont mis en place des institutions militaires, comme le cyber command, pour sécuriser les réseaux de la défense. L'accent est aussi mis sur l'augmentation des cyber-capacités militaires pour obtenir un effet de dissuasion sur l'adversaire, manière de se protéger en l'absence de solutions véritables au problème des cyber-menaces.

Mots clés : sécuritisation ; cyber-menaces ; cyberespace ; États-Unis.

ABSTRACT

The widespread use of computer systems has made easy and quick to exchange informations. However, this has contributed to the rise of new threats related to these new technologies that undermine critical infrastructure and information assets of States. The securitization of cyberspace process, i.e. presenting it as a source of existential threats to a referent object and remedy, shall be triggered over the world to try to protect themselves from cyber threats.

These threats are the result of variable phenomena: challenges between individual's desire to harm or geopolitical situations. Indeed, States have found in cyberspace a new battleground, we can consider it as a new grammar of conflicts or addition to conventional war in which a revolution in military affairs would settle down and partially change the thinking of armed conflict.

If cyberspace is changing the conflict, it can also become an area of operation of the armies in peacetime. States target the adversaries' computer systems for sabotage and gather information in perfect anonymity. This represents a threat to other States. Targets may be endangered are multiple: critical infrastructure, weapons systems, information assets, etc.

The awareness of the rise of cyber-threats is accompanied by cyber-security policies. In 2013, the United States has identified cyberspace as the source of the most serious threats to its national security. They have established military institutions, such as cyber command, to secure networks of defense. Emphasis is also placed on increasing military cyber capabilities to achieve a deterrent effect on the opponent. A way to protect themselves from persistent cyber threats in the absence of real solutions to the problem.

Key words: securitization; cyber threats; cyberspace; United States.

SOMMAIRE

LISTE DES FIGURES

ABREVIATIONS

API	l'Automate Programmable Industriel
DDoS	Destributed Denial of Service
EC	École de Copenhague
ECES	École de Copenhague des Études de Sécurité
ES	Études de Sécurité
NTIC	Nouvelles Technologies de l'Information et de la Communication
SCI	Système de Contrôle Industriel
STDA	Système de Traitement de Données Automatisé
TIC	Technologies de l'information et de la Communication
WWW	World Wide Web
USCYBERCOM	United States Cyber Command
ARCYBER	United States Army Cyber Command
MARFORCYBER	Marine Forces Cyber Command
FLTCYBERCOM	Fleet Cyber Command
AFCYBER	Air Forces Cyber
NSA	National Security Agency
JTF-CND	Joint Task Force-Global Network Operations

INTRODUCTION

L'ère de l'information est le qualificatif le plus usité pour nommer notre époque. En effet, les Nouvelles Technologies de l'Information et de la Communication (NTIC) ont eu une incidence décisive sur les valeurs sociales et les mécanismes d'interactions entre différentes entités, nous parlons d'un ordre numérique (*digital order*) ou l'information dématérialisée peut circuler plusieurs milliers de kilomètres en moins d'une seconde à un coût extrêmement bas. L'information est partout, elle est plus stratégique qu'elle ne l'a jamais été, Cependant, si elle est importante, sa sauvegarde l'est aussi. Aujourd'hui, les systèmes informatiques dans lesquels nous stockons les informations numériques s'utilisent aussi pour gérer des infrastructures critiques comme des aéroports, des systèmes de distribution d'eau et d'électricité, des centrales nucléaires, etc. Si l'utilisation de l'informatique facilite la gestion de ces infrastructures et la manipulation des informations numériques, ces systèmes se trouvent aussi vulnérables à des dysfonctionnements et des attaques ciblées. Cela pose donc des problèmes de sécurité quand l'on sait que les individus, entreprises et États emploient, à des proportions variables, ce genre de technologies. Une menace qui exposerait ces systèmes informatiques serait aussi une menace pour l'utilisateur, et cela peut se révéler extrêmement dangereux au niveau d'un État.

De nouveaux concepts sont apparus dans le domaine des Relations Internationales pour rendre compte de ce problème : cyber-sécurité, cyber-attaque, cyber-défense, cyber-guerre, etc. des concepts au préfixe *cyber* qui pointent vers des réalités passées, présentes ou futures. Des questionnements apparaissent : sommes-nous dans une guerre de l'information ? Dans une cyber-guerre ? Tout le monde cherche à acquérir des informations sur tout le monde, les armées et leurs services de renseignements dépensent des milliards de dollars chaque années pour sécuriser leurs systèmes d'informations et se renseigner sur ceux des autres et de leur contenus, voire même les saboter pour des intérêts stratégiques.

Pour une nouvelle question, la cyber-sécurité semble assez classique dans ses mécanismes si nous la pensons dans le cadre des Relations Internationales. Le cyberespace n'est qu'un nouveau domaine de rivalité, à côté de la terre, la mer, l'air et la stratosphère. C'est un sujet de géopolitique, la rivalité de pouvoir et d'influence dans le cyberespace est actuelle et pour cela même, les États se préparent, organisent leur défense, préparent la riposte, donc perçoivent le cyberespace comme une source de menace à laquelle il est impératif de répondre.

En effet, les questions cyber-sécuritaires se posent donc au niveau de l'État en des termes géopolitiques et se soumettent aux différentes représentations que l'on s'y fait : la conquête offensive des intérêts nationaux par les uns provoque chez les autres des réactions défensives visant à s'en protéger. Une cyber-stratégie initiée par un acteur des relations internationales provoquerait une cyber-défense chez l'acteur cible, quand toutes ces entreprises se généralisent et deviennent structurelles on aura affaire a une cyber-géopolitique ou des affrontements se déroulent dans l'espace virtuel qu'est le cyberespace. La nécessité de se protéger devient essentielle devant des menaces existentielles pesant sur l'État dont la source est le cyberespace. La théorie de la sécuritisation apparait comme une manière d'analyser l'*émergence et le développement* des cyber-menaces nées de situations géopolitiques et la réaction des acteurs concernés pour s'en protéger.

Problématique

Nous pouvons résumer la problématique en une question de recherche, on partira de la question de départ très générale : **comment les États réagissent-t-ils à l'émergence et au développement des cyber-menaces ?** Pour la reformuler de manière plus précise : **comment les États réagissent-ils aux menaces militaires venant du cyberespace**. Ou encore, si l'on prend en compte notre étude de cas et en élargissant le types de menaces : **comment les États-Unis d'Amérique se protègent-ils des cyber-menaces dont la source sont des rivalités géopolitiques ?** Les cyber-menaces ne seraient plus exclusivement militaires mais comprendront des éléments qui rajoutent à la vulnérabilité des États en temps de guerre ou de conflit. Des concepts comme cyber-guerre, cyber-conflit, cyber-espionnage, pourraient être mobilisés.

Des questions subsidiaires peuvent être rajoutées pour éclairer et compléter cette question de recherche :

- Comment le cyberespace peut-il être une source de menaces ?
- Comment l'utilisation géopolitique du cyberespace peut-elle être l'origine de (cyber-) menaces existentielles pour l'État ?
- Quelles sont les cyber-stratégies de sécurité et de défense adoptées par les États-Unis pour se protéger des cyber-menaces ?

Hypothèses de la Recherche

L'hypothèse principale est la suivante :

La réaction des États face aux menaces venant du cyberespace se fait par l'organisation des forces armées pour l'absorption des attaques informatiques et l'augmentation des capacités militaires cybernétiques pour des buts de (cyber-) dissuasion

Les hypothèses secondaires sont les suivantes :

- Les attaques informatiques exploitent les failles logicielles qui représentent des menaces pour les informations contenues dans, et les machines gérées par, le cyberespace.
- la militarisation du cyberespace pour des objectifs stratégiques et géopolitiques représente une plus grande menace pour l'État.
- La cyber-stratégie américaine vise à augmenter ses capacités militaires dans le cyberespace pour garder sa supériorité en termes de puissance et assurer sa sécurité.

Buts de la recherche

Le but de la recherche que nous entreprenons est **la prise de connaissance** de la réalité des cyber-menaces qui existent et leurs dangerosité pour ainsi **comprendre** ses répercussion sur la (cyber-) sécurité nationale des pays en général et des États-Unis en particulier et arriver à **expliquer** la manière dont des gouvernements entreprennent des stratégies dans le cyberespace (cyber-stratégies) pour réaliser leurs intérêts nationaux d'un côté, et les réactions des éventuelles cibles à ce genre de menaces. Ceci en gardant une approche systémique de la question en-là considérant comme un problème de sécurité résultante de situations géopolitiques.

Eu égard aux objectifs susmentionnés, nous allons procéder comme suite : le premier chapitre va être consacré à la présentation du cadre théorique et conceptuel de ce travail. En outre, nous allons essayer de comprendre, puis critiquer, la théorie de la sécuritisation et analyser le concept de cyberespace pour arriver à identifier les menaces dont il est la source.

Au cours du second chapitre, nous allons essayer de comprendre les cyber-menaces résultant de situations géopolitiques en abordant des phénomènes comme la cyber-conflictualité, la cyber-guerre, le cyber-terrorisme et autres concepts consacrés à définir le cyberespace en des termes sécuritaires. Puis nous progresseront vers l'étude du modèle américain de réaction aux cyber-menaces géopolitiques en abordant sa réaction au niveau des institutions et de sa stratégie de puissance dans le cyberespace.

Notre conclusion va prendre en compte tous ce qui a été abordé dans l'étude pour tirer des leçons sur plusieurs niveaux : ceux du cyberespace comme source de menaces, la géopolitique comme cause d'une catégorie de cyber-menaces et la réaction des États-Unis à cela.

Méthodes utilisées

L'analyse de contenu : pour analyser les différents rapports des agences internationales et gouvernementales concernant la cyber-sécurité

L'Étude de cas : cette recherche prend comme modèle d'analyse les États-Unis d'Amérique pour étudier les dynamiques de réaction aux cyber-menaces dans ce pays.

Approches et Théories

Nous utiliserons une **approche géopolitique et réaliste** en considérant les rivalités de pouvoir et d'influence comme une caractéristique essentielle des relations internationales. Les États concourent pour garantir leur survie, donc leur sécurité, qui représente le plus haut intérêt qui soit pour l'État. Pour cela, ils ont recours à l'augmentation de leur puissance, définie en termes militaires et économiques.

La Théorie de la Sécuritisation nous servira à analyser la réaction des États quant au développement des cyber-menaces et la transformation du cyberespace en un environnement menaçant les sécurités nationales en général et la sécurité nationale des États-Unis d'Amérique en particulier.

Revue de littérature

Les études sur les cyber-menaces ne sont pas très répandues mais nous remarquons un intérêt naissant, dans les milieux académiques, des études traitant des cyber-menaces et de la cyber-insécurité dans les relations internationales. L'ouvrage de Nazli Choucri intitulé *Cyberpolitics in International Relations* en est un exemple qui traite du cyberespace comme domaine des relations internationales en désignant les différents niveaux d'analyse de la cyber-sécurité en s'inspirant des images d'analyse que Kenneth Waltz a formulé dans ses ouvrages clés.

La sécuritisation est une théorie de l'Ecole de Copenhague (EC), un article parlant de la vision de cette école fut rédigé par Lene Hansen sous le titre *Digital Disaster, Cyber Security and the Copenhagen School* ou il a utilisé les différents concepts et théories de l'EC, comme la sécuritisation (ou l'hypersécuritisation dans ce cas) et les secteurs de la sécurité, pour étudier la cyber-sécurité. Myriam Dunn Cavelty a aussi traité de la sécuritisation du cyberespace à travers plusieurs de ses publications comme l'ouvrage publié sous le titre *Cyber-security and Threat Politics : US efforts to secure the information age* ; l'un de ses articles intitulé *Cyber-security* ou encore : *From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse* et d'autres encore.

CHAPITRE PREMIER: CADRE THÉORIQUE ET ANALYSE DES CONCEPTS

Ce chapitre vise à comprendre la théorie de la sécuritisation que l'on utilise pour analyser le cyberespace en le considérant comme une source d'insécurité pour l'État. Ce concept de cyberespace devrait aussi être compris et défini pour délimiter les frontières de cette recherche, et enfin arriver à répondre à la question des origines des vulnérabilités du cyberespace et ses conséquences. Les conséquences de ces vulnérabilités se matérialisent dans le concept de cyber-menace, nous allons analyser le cyberespace comme source de menace et dresser un portrait de ces cyber-menaces et leur dangerosité pour les systèmes d'informations.

Les menaces ne sont qu'une question de perceptions, ou de construction sociale, c'est à cela que postule la théorie de la sécuritisation dans sa compréhension de l'émergence des menaces. Les cyber-menaces ne seraient qu'une question de représentation germée dans l'esprit d'une élite qui essaie de convaincre une audience, par l'intermédiaire d'un discours, qu'elle représente un danger pour elle (l'audience) ou pour le cadre socio-politique dans lequel elle vit. L'analyse serait centrée sur ce discours politique visant à convaincre d'une menace imminente. Celle-ci représente une vision de la sécuritisation que nous allons explorer et critiquer pour construire notre propre grille d'analyse des menaces cybernétiques. Ce chapitre commencera donc par cette analyse de la théorie de la sécuritisation et du concept de cyberespace. Puis essaiera de comprendre pourquoi ce dernier représente une source de menace.

SECTION 1. LA SECURITISATION DU CYBERESPACE : THEORIES ET CONCEPTS

L'expression *sécuritisation du cyberespace* est utilisée dans les milieux académiques pour analyser le cyberespace comme source de menaces utilisant la théorie de la sécuritisation issue de l'Ecole de Copenhague (EC) pour analyser les différents discours politiques visant à pointer du doigt les danger du cyberespace pour différents objets référents. Nous comprendrons ici ces deux concepts de sécuritisation et de cyberespace pour fournir à notre étude un cadre conceptuel précis que l'on va utiliser pour analyser les cyber-menaces à la sécurité nationale et les différentes questions stratégiques relatives au cyberespace.

Paragraphe 1. INTRODUCTION A LA THEORIE DE LA SECURITISATION

La Sécuritisation est une théorie qui se veut l'un des résultats des débats sur la redéfinition du concept de sécurité depuis les années 80s. Nous allons mettre cette théorie dans ce cadre en définissant la sécurité et ses différentes approches puis nous progresserons vers la compréhension de la théorie de la sécuritisation.

I. Le concept de sécurité : du traditionalisme aux nouvelles approches

La sécurité est sans conteste le sujet prédominant dans les études internationales depuis la fin de la seconde guerre mondiale. Un champ académique fut érigé : les études stratégiques ou les études de sécurité. La pluralité des théories des relations internationales et leurs visions parfois très divergentes, influencent grandement la façon de penser les études de sécurité et surtout, la définition du concept central de ce champ d'étude : la sécurité.

L'étymologie de la sécurité est très opposée à l'idée que l'on en se fait aujourd'hui. En effet, le mot "sécurité" vient de la combinaison de deux mots

grecs : sine (sans) et cura (soin), les deux mots mis ensemble donnent à la sécurité le sens d'absence de soin[1], alors que son sens contemporain va dans la direction opposée pour signifier l'absence de menace ou le sentiment de quiétude résultant d'une situation stable ou l'on n'est pas exposé au danger.

1) Le débat pour la (re)définition de la sécurité

La sécurité est un concept essentiellement controversé,[2] sa substance est largement débattue, particulièrement après l'apparition des approches visant à le redéfinir pour l'élargir et l'approfondir. L'élargir à d'autres secteurs autres que militaire, et l'approfondir pour comprendre des objets référents autres que l'Etat. Ainsi, un débat s'est installé entre les traditionnalistes et les "*widners-deepners*".

Plusieurs points sont au centre de ce débat, parmi lesquels, **L'épistémologie** qui pose le problème sur le moyen d'acquérir le savoir et comment on devrait étudier la sécurité,[3] deux principales épistémologies s'affrontent, l'approche objective et l'approche subjective qui prennent corps respectivement dans le positiviste et le post-positivisme.[4] Ces conceptions objective et subjective de la sécurité sont très tôt soulignées par Arnold Wolfers à travers sa définition très reprise de la sécurité :

> *« Au sens objectif, la sécurité mesure l'absence de menaces sur des valeurs acquises, au sens subjectif, elle mesure l'absence de peur que ces valeurs soient attaquées »*[5]

Malgré son ancienneté, cette définition ne reste pas moins pertinente en dépit des fragmentations survenues dans la théorie des relations internationales bien après sa formulation, cette définition souligne la dimension objective de la

---

[1] Thierry Balzacq, "Qu'est-ce que la Sécurité Nationale ?", *Revue internationale et stratégique*, N 52 (2003/4), p.35.

[2] L'expression : "concept essentiellement controversé" (de Walter Bryce Gallie) renvoie à la difficulté intrinsèque à avoir un consensus sur le sens d'un concept, en l'occurrence, la sécurité. Voir : Steve Smith, the contested concept of security.

[3] Barry Buzan and Lene Hansen, *evolution of international security studies* (UK: Cambridge University Press, 2009), p.32

[4] Ibid., p.p.32-33.

[5] Arnold Wolfers, *Discord and Collaboration: Essays on International Politics* (USA: The John Hopkins Press, 1962) p.150.

sécurité ou les menaces sont concrètement présentes ou pas, et une dimension subjectif qui renvoie au sentiment d'être menacé ou pas.

L'objet référent : La question ontologique de l'objet référent est centrale dans la pensée sécuritaire contemporaine. Les théories s'interrogent sur l'entité que l'on doit sécuriser, l'Etat, l'individu, le groupe ethnique, l'environnement, la planète ?

Les secteurs de la sécurité entre les approches traditionnalistes qui postulent sur l'importance du secteur militaire et les nouvelles approches élargissant le concept de sécurité à d'autres secteurs tel que l'économie, l'environnement, l'identité, etc.

2) Le paradigme réaliste et la sécurité nationale

La sécurité nationale fut le concept dominant dans les études stratégiques réalistes pendant la guerre froide.[1] Le réalisme postule que le système international est anarchique,[2] de là découle le conflit comme inhérent à la nature de ce système où les Etats, acteurs principaux des relations internationales, usent de moyens coercitifs pour réaliser leurs intérêts et continuer d'exister.

Le réalisme considère donc que l'Etat est l'objet référent de la sécurité, les menaces à la sécurité nationale viennent essentiellement de l'extérieur, par d'autres Etats et par voie militaire. La sécurité nationale est presque devenue le synonyme de la sécurité militaire[3]. L'étude réaliste se fait à travers des épistémologies positiviste et rationaliste.[4]

Les Etudes Sécuritaires des premiers temps étaient excessivement centrées sur la dimension militaire de la sécurité nationale en raison des relations que les principaux chercheurs entretiennent avec le département de la défense,[5] ceux-là et leurs héritiers intellectuels refusèrent la révision profonde du concept de sécurité engagée dans les années 1980s. Les idées fondamentales de cette vision

[1] Barry Buzan and Lene Hansen, op. cit., p.21.

[2] L'anarchie est l'absence d'une autorité supranationale qui contrôlerait les Etats.

[3] Ibid., p.12.

[4] Ibid., p.21.

[5] Les théoriciens réalistes sont majoritairement des citoyens américains.

sont relatées par Joseph Nye et Sean Lynn-Jones qui, pour eux, les sujets dont s'occupent les Études de Sécurité Internationale (*international security studies*) ne doivent pas s'éloigner des problèmes politiques centraux portant sur les perceptions des menaces et leur gestion par des Etats souverains. Ils citent quelques sujets fondamentaux de ce domaine d'études : les causes des guerres, les dynamiques de conflits, la nature et la perception des menaces, les efforts pour améliorer ou résoudre des conflits causés par ce genre de menaces, les problématique relatives au nucléaire, à la dissuasion, etc.(1)

Stephen Walt reprend cette vision en définissant le domaine de la sécurité comme « *l'étude de la menace, de l'emploi et du contrôle de la force militaire* ». Pour lui, ce domaine correspond au phénomène de la guerre(2). Cependant, il reconnait la présence de menaces non militaires à la sécurité nationale comme la pauvreté, le sida, les risques environnementaux, la récession économique… Mais pense que l'élargissement du concept de sécurité à considérer de tels phénomènes comme appartenant au domaine académique des études sécuritaires rendrait celui-ci intellectuellement incohérent.(3)

3) L'élargissement du concept de sécurité

Les approches visant à élargir le concept de sécurité sont nées de la prise de conscience de la dégradation de l'environnement qui menace la planète et le bien-être des individus(4) et de la critique du réalisme dominant. Pour elles, l'approche militaire Etato-centrée du réalisme explicite l'idée que les menaces à la sécurité nationale sont externes alors que, si l'on observe l'état des conflits présents depuis 1945, on s'apercevrait que ce sont des conflits internes aux Etats (comme les guerre civiles) surtout dans les pays moins développés. Cette vision du réalisme généralise cette idée à cause du caractère ethnocentrique de cette théorie, c'est donc une théorie applicable aux grandes puissances et la sphère

(1) Joseph S. Nye Jr and Sean M. Lynn-Jones, "International Security Studies: A Report of a Conference on the State of the Field", *international security Vol. 2: the transition to the post-cold war security agenda*, edited by Barry Buzan and Lene Hansen (SAGE Publications, 2007), p.85.

(2) Stephen M. Walt, "the renaissance of security studies", in *international security: The Transition to the Post-Cold War Security Agenda*, ed. Barry Buzan and Lene Hansen, vol. 2 (London: SAGE publications, 2007), p.215.

(3) Ibid.

(4) Keith Krause and Michel C. Williams, "Broadening the Agenda of Security Studies : Politics and Methods", *Mershon International Studies Review*, Vol. 40, N. 2 (oct., 1996),

occidentale et non au reste du monde. Mohammed Ayoob, théoricien réaliste, s'est aperçu de cela et fondit un "réalisme subalterne"[1] qui prendrait en compte des visions non occidentales du monde et compris de la sécurité. Pour cela, il introduit les sources de menaces intérieures à la sécurité nationale.

L'élargissement de la réflexion théorique des études sécuritaires était essentiel à cause du nouvel environnement auquel les États sont confrontés à partir des années 1980s.[2] On retiendra ici l'apport théorique de l'école de Copenhague et ses plus importants contributeurs : Barry Buzan et Ole Wæver qui, à travers leurs écrits, ont contribué significativement à l'élargissement du concept de sécurité par la "sectorialisation" de celui-ci. En effet, Barry Buzan a initié cette idée en 1983 dans son livre : *People, States and Fear : The National Security Problem in International Relations* en proposant l'intégration de quatre secteurs non militaires au concept de sécurité pour élargir le programme de recherche des traditionnelles Etudes Stratégiques centrées sur le secteur militaire. Cette vision fut revue dans une réédition de ce même ouvrage en 1991 puis par la publication en 1998 de ce qui allait devenir l'un des livres référence des études de sécurité : *Security, a Framework for Analysis* coécrit avec Ole Waever et Jaap de Wilde.

Dorénavant, Le domaine de la sécurité comprendrait cinq secteurs : le secteur militaire, politique, économique, sociétal et environnemental. L'idée de secteur fait référence à un type d'interaction donné. Si l'on parle de secteur militaire on se référerait aux rapports de forces entre des Etats ; si l'on traite du secteur politique on parlerait de relations entre autorité, situation du gouvernement et sa reconnaissance ; le secteur économique concernerait le commerce, la production et les finances ; le secteur sociétal, les relations entre les identités collectives ; le secteur environnemental indiquerait les relations entre l'activité humaine et la biosphère.[3]

---

[1] Voir: Mohammed Ayoob, "Inequality and Theorizing in International Relations: The Case for Subaltern Realism", *International Studies Review*, Vol. 4, No. 3. (Autumn, 2002), pp. 27-48.

[2] Steve Smith, "The Essentially Contested Concept of Security", in *critical security studies and world politics*, ed. Ken Booth (Boulder, Colorado: Lynne Rienner Publisher), p.28.

[3] Barry Buzan et al., *Security: A Framework for Analysis* (USA: Lynne Rienner Publisher, 1998), p.7.

4) L'approfondissement du concept de sécurité

L'école de Copenhague a aussi contribuée, par sa sectorialisation du concept de sécurité, à l'approfondissement du concept de sécurité pour l'inclusion d'acteurs non étatiques comme objets référents. Cela s'est fait après la reconsidération de la vision formulée en 1983 et 1991 par Barry Buzan et expliciter la reformulation ontologique de la sécurité.

Ainsi, dans bien des secteurs, l'Etat n'est plus au centre de la réflexion sur la sécurité. Suivant le secteur étudié, un objet référent s'impose comme une unité à protéger. Dans les années 1990s, l'Europe était en plaine mutations sécuritaires quand Buzan et Waever se sont appliqués à développer le concept de sécurité sociétale dans un contexte où l'Europe se souciait des problèmes d'immigration. L'Etat n'est plus l'objet référent mais l'identité collective d'une société[(1)] menacée par de multiples évènements comme l'immigration, l'influence culturelle d'un voisin, etc.[(2)]

D'autres approches approfondissant le concept de sécurité ont vu le jour et se sont répandues dans les études non-traditionnelles de la sécurité comme l'école critique (*critical security studies*) qui prend l'individu comme l'unité à sécuriser, ou encore d'autres approches plus flexibles comme celle initiée par Buzan et développée par les autres chercheurs de l'école de Copenhague et en particulier Ole Wæver : la sécuritisation (*securitization*). Au point où l'on parle des Études de Sécuritisation (*Securitization studies*) pour se référer à la construction discursive des menaces à un objet référent donné.

II. Construction des menaces et fondements théoriques de la sécuritisation

La théorie de la sécuritisation s'inscrit dans cette initiative de développement du concept de sécurité. C'est une théorie initiée par les chercheurs de l'EC avec des principes inspirés de la théorie sociale constructiviste. Notons que les chercheurs de l'école de Copenhague sont considérés comme appartenant à une école plus large qui est le constructivisme dont une partie de celui-ci appartenant à la théorie critique. Nous allons

(1) Barry Buzan et al., op. cit., p. 120.

(2) Ibid., p.121.

examiner les fondements théoriques de la sécuritisation pour bien comprendre son apport qualitatif a l'analyse sécuritaire, cela se fera en rendant compte de l'importance de ces deux écoles de pensées que sont l'école de Copenhague et la théorie sociale constructiviste dans l'analyse des relations internationales et des problématiques liées à la sécurité en nous arrêtant sur leurs apports respectifs a ces champs académiques.

1) Introduction à l'école de Copenhague des études sécuritaires

L'école de Copenhague s'est développée autours de chercheurs travaillant au *Conflict and Peace Research Institute* (COPRI)[1] a Copenhague, Danemark. Elle regroupe un certain nombre de chercheurs et théoriciens travaillant sur des problématiques sécuritaires non-traditionnelles. Le nom d'« Ecole de Copenhague » leur ait été donné par Bill McSweeney dans l'un de ses articles critiques en 1996.[2] Ses chercheurs les plus connus, comme Barry Buzan et Ole Wæver, ont eu la plus grande influence sur le renouveau des programmes de recherches des Etudes Sécuritaires à la fin de la guerre froide, ou du moins l'élargissement de ces programmes dans les Etudes Stratégiques.

L'EC est considérée par beaucoup comme une partie de la théorie constructiviste,[3] principalement à cause de la théorie de la sécuritisation qui est en effet une théorie employant une logique singulièrement constructiviste. Mais la pluralité des origines intellectuelles de ses théoriciens rend difficile l'affiliation théorique de cette école, si ce n'est, en faire référence en tant qu'Ecole de Copenhague. Pour Ole Wæver, les concepts centraux de l'école de Copenhague sont : « secteurs », « sécuritisation » et « complexes de sécurité régionale »[4]. La publication des travaux en relation avec ces sujets furent dans un cadre historique et théorique particulier, celui de la fin de la guerre froide et

[1] Créé en 1985 sous le nom de « *Center for Peace and Conflict Research* ».

[2] Voir : Bill McSweeney, "Identity and Security: Buzan and the Copenhagen School", in *Review of International Studies,* Vol. 22, No. 1 (January, 1996), p.p. 81-93

[3] Voir Matt McDonald, "constructivism", in Security Studies: an Introduction, ed. Paul D. Williams (New York: Routledge, 2008) ; Shahin Malik. "Constructing Security", in *International Security Studies: Theory and Practice*. Eds. Peter Hough et al. (New York: Routledge, 2015).

[4] Matt McDonald, "constructivism", in *Security Studies: an Introduction*, ed. Paul D. Williams (New York: Routledge, 2008), p. 68.

l'apparition des approches post-positivistes et la remise en cause des définitions et conceptions traditionnelles de la sécurité.

Les travaux les plus aboutis de l'Ecole de Copenhague sont ceux développant le concept de sécurité sociétale, ainsi que la théorie de la sécuritisation qui se veut une nouvelle approche pour penser la sécurité.

2) Le Social Constructivisme dans les Relations Internationales

On peut retrouver les prémisses théoriques de l'école constructiviste des relations internationales en philosophie et en sciences sociale : Pour l'italien Giambattista Vico, le monde historique est différent du monde naturel, les Etats et le système international sont des constructions humaines et pour cela, s'ils le veulent, les États peuvent refonder le système ou le changer. Pour Emmanuel Kant, le savoir sociologique ne peut être objectif parce qu'il ne peut être séparé de la conscience humaine. On retrouve la même idée dans les écrits de Max Weber chez qui, pour appréhender les interactions humaines, les hommes assignent un sens aux interactions entre individus, on ne peut donc pas décrire les phénomènes sociaux de la même façon que l'on décrit les phénomènes physiques. La réalité est socialement construite, les relations humaines et les relations internationales consistent en des idées et des croyances et non seulement en l'aspect matériel de la vie.[1]

Le monde social n'est pas une donnée existante *per se*, il n'existe pas indépendamment des pensées et des idées des gens qui en font partie, il n'est pas une réalité externe qui peut être découverte par des recherches scientifiques et expliquée par des théories scientifiques comme c'est le cas avec les réalités physiques. Il n'y a pas de lois naturelles du social, de l'économique ou du politique, on ne peut pas les étudier objectivement au sens positiviste du terme.[2]

Les premiers écrits constructivistes en Relations Internationales remontent aux années 1980s, ils furent rassemblés sous une même bannière sous le livre de Nicholas Onuf publié en 1989 sous le titre *world of Our Making* ou il

[1] Robert Jackson and George Sørensen, *Introduction to International Relations: Theories and Approaches.* Fifth edition (Oxford, Oxford University Press, 2013), p. 211.

[2] Ibid., p. 212.

les l'a nommés comme tel.[1] Le constructivisme fut développé dans les années 1990s, plusieurs écrits majeurs furent publiés en forme d'articles scientifiques ou d'ouvrages dont les travaux d'Alexander Wendt qui restent les plus influents en la matière, d'abord en 1992 son article intitulé *Anarchy is What States Make of It,* puis l'ouvrage référence du constructivisme qui fut publié par lui sous le titre *Social Theory of International Politics* en 1999.

Le constructivisme comme théorie des Relations Internationale prend conscience des phénomènes négligés par les précédentes théories, il essaye de pousser sa réflexion au-delà des apparences matérielles et immédiates[2] pour arriver à considérer le monde comme socialement constitué à travers des interactions intersubjectives.[3] Il reconnait la centralité des facteurs idéationnels (comme les normes, les identités ou les idées en général) dans les relations internationale.[4] Richard Price et Christian Reus-Smith décrivent les constructivistes comme suite :

> *« Épistémologiquement, [ils] remettent en cause les approches positivistes de la connaissance, et critiquent les tentatives de formuler des énoncés objectifs et empiriquement vérifiables sur le monde naturel et social. Méthodologiquement, ils rejettent l'hégémonie d'une seule méthode scientifique, et plaident en faveur d'une pluralité de méthodes, de même qu'ils privilégient les stratégies interprétatives. Ontologiquement, ils défient les conceptions rationalistes de la nature et des actions humaines, soulignant tout au contraire la construction sociale des identités des acteurs, ainsi que l'importance de l'identité dans la constitution des intérêts et des actions. Et normativement ils condamnent la théorisation axiologiquement neutre dont ils nient jusqu'à la possibilité même, tant ils en appellent au développement de*

[1] Matt McDonald, op. cit., p. 60.

[2] Gérard Dussouy, *Traité de relations internationales. Tom II : les théories de l'interétatique,* (Paris : l'Harmattan, 2008) p.224.

[3] Un phénomène est intersubjectif quand il a du sens pour les gens qui l'ont fait et le comprennent parce qu'il est de leur construction. Ils partagent la compréhension d'un phénomène.

[4] Matt McDonald, op. cit., p.p. 59-60

théories explicitement désireuses de dévoiler et de dissoudre les structures de domination »[1]

Le programme de recherche constructiviste remédie a une carence théorique du réalisme, celle du changement. Le réalisme considère les choses comme existantes *a priori*, le constructivisme les considère comme socialement construites :

« Alors que le réalisme et le libéralisme tendent à se concentrer sur les facteurs matériels tels que la puissance et le commerce, les […] constructivistes soulignent l'impact des idées. Au lieu de prendre l'État pour une donnée et de supposer qu'il cherche tout simplement à survivre, les constructivistes considèrent les intérêts et les identités comme des produits extrêmement malléables de processus historiques spécifiques. Ils accordent une grande attention au(x) discours prédominant(s) au sein des sociétés parce que le discours reflète et façonne les croyances et les intérêts, et établit les normes du comportement accepté. Par conséquent, le constructivisme est attiré par les sources du changement»[2]

Selon les constructivistes, la réalité est loin d'être objective comme le prétendent les rationalistes positivistes (les réalistes et les libéraux), elle est socialement construite. À travers un *processus d'interaction* des *agents,* une réalité sociale, culturelle et politique se crée, cette réalité n'est pas indépendante des sens que les hommes peuvent donner aux choses. Dans ce sens, les relations internationales sont socialement construites à travers les processus d'interaction des *agents* (qui, dans ce cas, sont les Etats). De ces interactions peut résulter un changement de *structure.*[3] Wendt introduit la notion sociologique de *structuration* dans son analyse, pour lui, contrairement à ce que dit Kenneth Waltz, il n'y a pas de logique d'anarchie, ce sont les agents (dans ce cas, les Etats)

---

[1] Richard Price and Christian Reus-Smith, "Dangerous Liaisons? Critical International Theory and Constructivism, in E*uropean Journal of International Relations*, vol. 4, N. 3 (September 1998), p. 261. Cite dans et traduit par : Dario Battistella, *Théories des Relations Internationales*, (Paris : Presses de Sciences Po, 2012), p.p. 329-330.

[2] Stephen Walt. "International Relations: one world, many theories", in *Foreign Policy*, No. 110, (spring, 1998), p.p. 41-42. Cited in and translated by: Dario Battistella. Op. cit., p.p. 32-33.

[3] Selon Nicolas Onuf, la structure et les agents se co-construisent. La structure conditionne, certes, le comportement des agents, mais ceux-ci peuvent la modifier et la changer.

qui façonnent la structure (dans ce cas, l'anarchie) par leurs agissements, et cette dernière conditionne les actions et les intérêts des agents. L'anarchie productrice de conflictualité n'est pas une réalité externe mais une culture parmi d'autres[1] construite par des interactions intersubjectives au sein du système international,[2] elle n'est donc pas immuable, elle est *ce que les Etats en font.*[3]

3) La construction sociale des menaces

Cette idée selon laquelle la réalité est socialement construite peut être appliquée aux Etudes de Sécurité pour étudier les menaces comme des constructions sociales. La désignation des menaces ne serait plus objective ou subjective mais intersubjective. Privilégiant les facteurs sociaux, culturels et historiques qui encouragent la formation d'une certaine forme de sens donné aux différents acteurs et à leurs intentions,[4] le constructivisme percevrait le domaine de la sécurité dans les relations internationales à partir de l'identité et des normes. Wendt donne un exemple pour justifier cela en disant que 500 bombes nucléaires Britanniques sont moins menaçantes pour les Etats-Unis que 5 bombes nucléaires Nord-Coréennes. Parce que les Britanniques sont des amis et les Nord-Coréens ne le sont pas. Ce ne sont pas les réalités numériques de la puissance nucléaire qui importe mais la manière dont les acteurs se pensent les uns les autres.[5] Les éléments matérialistes sont certes à prendre en compte dans une analyse mais sont subsidiaires aux éléments intellectuels formés d'idées et de croyances qui leurs donnent leurs sens, les organise et les guident.

La même réflexion peut être appliquée au comportement des Etats-Unis dans leur traitement de l'Irak : pourquoi la possibilité que l'Irak développe des armes nucléaires, entre 2002 et 2003, eut elle été estimée plus menaçante que les

---

[1] A.Wendt distingue trois cultures d'anarchie, la première qui dominait le monde pré-Wesphalien qui est la culture hobbesienne (tout le monde est l'ennemi de tout le monde), puis est apparue la culture lockienne (reconnaissance du droit à l'existence des autres Etats, l'inimitié se transforme en rivalité et les guerres sont limitées) après le traité de Westphalie. Enfin, la culture kantienne (les Etats acceptent de coopérer entre eux, ils sont amis et construisent des communautés de sécurité comme l'Union Européen) est apparue après la seconde guerre mondiale.

[2] Matt McDonald, op. cit., p.p. 66.

[3] Voir Alexander Wendt, "Anarchy is What States Make of It: the social construction of power politics", *International Organization,* Vol. 46 N. 2 (1992), 391-425

[4] Matt McDonald. Op. cit., p. 61.

[5] Robert Jackson and George Sørensen. Op. cit., p. 212.

arsenaux nucléaires des autres pays nucléaires ? L'analyse constructiviste prendrait en compte une série de facteurs sociaux, historiques et culturels qui auraient aidé à façonner le sens qu'un acteur pourrait donner aux intentions d'un tiers. Dans cet exemple, le facteur historique est déterminant : l'expérience de conflit avec l'Irak aurait aidé à construire une *représentation* d'un régime politique Irakien dangereux pour la sécurité nationale amaéricaine.[1]

III. La construction discursive des menaces

La théorie de la sécuritisation est sans doute la plus importante contribution de l'École de Copenhague aux Études de Sécurité. Cette théorie fut introduite par Ole Wæver dans un article paru en 1995 sous le titre "*Securitization and Desecuritization*" puis développée par Barry Buzan, Ole Wæver et Jaap de Wilde en 1998 dans leur ouvrage intitulé *Security : A New Framwork for Analysis.* Wæver a défini la sécuritisation comme la construction discursive de la menace.

S'inscrivant dans un contexte géopolitique et intellectuel particulier,[2] Le but de Buzan et Wæver était d'étudier la manière avec laquelle une affaire vient à être perçue comme suffisamment grave pour que l'on cherche à lui allouer les ressources suffisantes et limiter son impact[3]. Ole Wæver s'interroge sur « *ce qui fait réellement de quelque chose un problème de sécurité* »,[4] il répond en disant que l'on considère « *quelque chose comme un problème de sécurité quand une élite le déclare comme tel* ».[5]

C'est par cela qu'Ole Wæver vient à définir la sécurité comme une résultante d'un acte de langage et la sécuritisation comme un processus linguistique qui conduit une question particulière à être perçue comme une menace existentielle. Cela représente une nouvelle manière de problématiser la

[1] Matt McDonald, ibid.

[2] Contexte géopolitique qui se caractérise par la fin de la guerre froide, le contexte intellectuel fait références aux nouvelles approches visant à redéfinir le concept de sécurité. L'École de Copenhague était au centre de ce débat pour élargir le programme de recherche des traditionnelles Études Stratégiques.

[3] Matt McDonald. op. cit., p. 69.

[4] Ole Wæver. 'Securitization and Desecuritization", in *International Security: Widening Security*, vol. 3. Eds. Barry Buzan and Lene Hansen (SAGE Publications, 2007), p. 72.

[5] Ibid., p. 73.

sécurité en la pensant comme un acte de langage, cela permet aussi de dépasser le débat sur l'objectivité et la subjectivité dans la désignation des menaces en pensant la sécurité comme intersubjectivement déterminée et discursivement construite.[1]

1) L'acte de langage

Au tout début, l'acte de langage était le synonyme de ce que l'on qualifie aujourd'hui de sécuritisation, on utilisait le concept d'acte de langage pour désigner la sécuritisation mais cela a vite fait de changer. Dans le livre publié en 1998, les actes de langage sont défini comme des « mouvements de sécuritisation » (*securitization moves*), à partir de là, une question est sécuritisée seulement si l'*audience* l'accepte comme une question de sécurité.[2]

Le concept d'*acte de langage* est emprunté de la théorie du langage de John L. Austin. Il renvoi a une déclaration qui, elle-même, représente un acte : en disant je te promets, quelqu'un fait une action, celle de promettre. L'énonciation elle-même est une action. Quand elle est déclarée, quelque chose est fait.[3] La déclaration est, selon Austin, fait plus que décrire une réalité, elle réalise des actions spécifiques, elle est *performative.*[4]

Dans le contexte de la sécurité, « En disant "sécurité" le représentant d'un État déclare un état d'urgence, réclamant ainsi le droit d'user de tous les moyens nécessaires pour arrêter le développement d'une menace ».[5] A travers des discours, argumentaires et de la persuasion, une communauté politique vient à considérer une question particulière comme étant une menace existentielle.

2) De la politisation a la sécuritisation

L'École de Copenhague oppose la sécurité a la conception de politisation (*politization*) ou à la « politique habituelle » (*normal politics*) qui se réfère aux règles de la loi et du débat public (surtout répandu dans les États

[1] Barry Buzan et al. op. cit., p. 31.

[2] Matt McDonald, op. cit., p. 69.

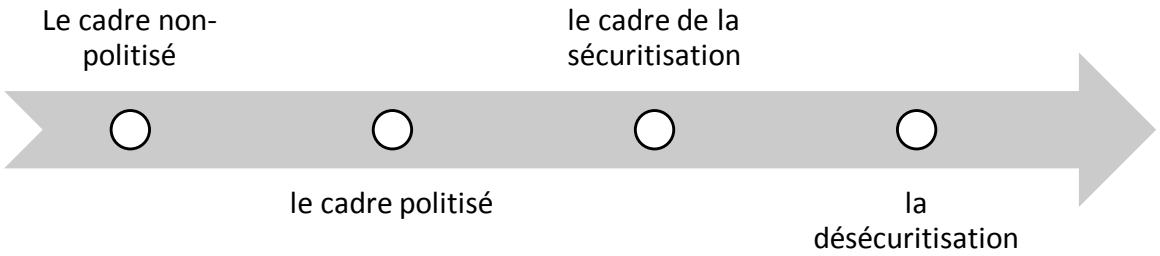
[3] Ole Waever, op. cit., p. 73.

[4] Thierry Balzacq. Securitization Theory: How security problems emerge and dissolve. (New York: Routledge, 2001), p. xiv.

[5] Ibid. ; Barry Buzan and Lene Hansen. *op.cit.,* p.p.33-34.

démocratiques),[1] et pense les différentes questions comme appartement à trois cadres possibles et évoluant d'un cadre à l'autre : le cadre non-politisé ; le cadre politisé et le cadre de la sécuritisation (sans inclure le cadre de la désécuritisation que l'on ne traitera pas dans cette recherche).

Figure 1. Schéma représentant l'évolution d'une question de sécurité dans divers cadres selon la théorie de la sécuritisation



Le cadre non-politisé représente le cadre dans lequel des questions ne sont pas sujet à discussion dans le débat public et ne fait pas objet de décision de la part du gouvernement.

Le cadre politisé est le cadre dans lequel une question fait objet de débat public et fait partie de la politique publique. Elle requiert une allocation de ressources pour la traiter et des décisions gouvernementales.

Une question sécuritisée est une question qui dépasse le cadre politique habituel, elle peut être perçue comme une politisation extrême. C'est quand une question est présentée comme une menace existentielle requérant des mesures d'urgence. Présentée comme telle, le traitement de la menace justifie l'emploi de moyens qui peuvent sortir du cadre conventionnel de la politique.[2]

On pourrait s'interroger sur les questions qui peuvent être sécuritisée, celles qui peuvent être considérées comme des menaces existentielles. La réponse est la suivante : tout peut être sécuritisé, cela dépend de l'acteur sécuritisant et du contexte. Mais on doit insister sur le fait qu'une question est sécuritisée non pas parce qu'elle représente une menace existentielle a un objet référent mais parce qu'elle est *présentée* comme telle. le caractère menaçant n'est donc pas inhérent

[1] Matt McDonald. Op. cit., p.p. 69-70.

[2] Barry Buzan et al. op. cit., p.p. 23-24.

à son statut,[1] c'est parce que les acteurs politiques l'ont décidé, et que l'audience l'a accepté ainsi qu'une question particulière est sécuritisée.[2] La question de la dangerosité de la menace ou de sa réalité ne se pose pas.[3] Selon Wæver, « quelque chose est un problème de sécurité quand une élite le déclare comme tel ».

Suivant l'acteur sécuritisant et le contexte de la sécuritisation (ou de la politisation), une question peut finir dans n'importe quel cadre cité ci-haut. Des États peuvent politiser la religion (Iran, arabie Saoudite) et d'autres non (France, États-Unis). Certains peuvent sécuritiser la culture (Iran, ex-URSS) et d'autres non (le Royaume Uni, Pays-Bas).[4]

Une question est sécuritisée seulement si l'audience l'accepte comme une question de sécurité. Cette même acceptation est conditionnée par l'existence de « *conditions facilitatrices* » (*facilitating conditions*) incluant la forme de l'acte de langage, la position de l'acteur qui sécuritise (*securitizing actor*) et les conditions historiquement associées à la menace.[5]

3) Les éléments clé de la sécuritisation

Plusieurs éléments cités (et d'autres pas encore) méritent une attention particulière pour bien comprendre la sécuritisation, nous allons donc définir quelques concepts utilisés par la théorie de la sécuritisation :

Le mouvement sécuritisant (*securitizing move*) est une déclaration publique de la part d'un acteur annonçant qu'une certaine question ou un acteur représente une menace à la sécurité d'un objet référent.

Les conditions facilitatrices (*facilitating conditions*) représentent tout ce qui peut être fait dans le but de permettre à un mouvement sécuritisant d'être accepté par l'audience visée. Cela inclut la forme de l'acte de langage, le statut de l'énonciateur et l'histoire associé à la menace.[6]

---

[1] Barry Buzan and Lene Hansen, op. cit., p. 34.

[2] Barry Buzan et al. Op. cit., p. 31

[3] Ibid., p. 29.

[4] Barry Buzan et al. op. cit., p. 24.

[5] Matt McDonald, op. cit., p. 69.

[6] Matt McDonald. Op. cit., p. 70.

L'acteur sécuritisant (***securitizing actor***) est celui qui sécuritise une question en la déclarant comme menaçante a un objet référent,[1] c'est lui qui déplace une question de la sphère politique conventionnelle vers le sillage de la sécuritisation.

L'audience est le récepteur de l'acte de langage, la réussite de la sécuritisation est conditionnée par l'acceptation de celle-ci qu'une question représente une menace pour des valeurs partagées.[2]

4) Critique de la théorie de la sécuritisation et construction du modèle d'analyse

Beaucoup de questions restent sans réponse : comment sait-on qu'une question est sécuritisée avec succès ? Quelle audience doit être convaincue de la légitimité du mouvement sécuritisant ? Est-ce que les autres formes de représentations, autre que l'acte de langage (comme les images), peuvent être perçu comme un mouvement sécuritisant ? Si les acteurs sécuritisateurs sont souvent des élites gouvernementales, ne font-ils pas que sécuritiser les questions qui garantissent des intérêts de classe ?[3] Beaucoup de questions auxquelles la théorie de la sécuritisation ne répond pas, mais nous enregistrons des volontés de les corriger, au cours de cette dernière décennie en essayant de remédier à certaines manquement relativs à la théorisation de l'audience

Thierry Balzacq donne une définition assez simple de ce qu'est la sécuritisation, pour lui, c'est la théorie qui examine « *comment les questions de sécurité émergent, se développent et se dissolvent* ».[4] L'approche de la sécuritisation que l'on va utiliser est proche de cette vision, nous examinerons comment les États réagissent à l'émergence et le développement des menaces, en l'occurrence, les cyber-menaces. Nous n'essaierons pas de développer une analyse des discours traitant des cyber-menaces et de la dangerosité du cyberespace, mais nous postulerons qu'un *securitization move* est toujours accompagné par une stratégie d'action. C'est-à-dire que présenter quelque chose comme une menace ne veut pas dire que c'est un securitization move, encore

[1] Barry Buzan et al. Op. cit., p. 36

[2] Barry Buzan et al. Op. cit., p. 31.

[3] Ole Wæver. Op. cit., p. 75.

[4] Thierry Balzacq. *Securitization Theory*, p. xiv.

faut-il que cette présentation soit accompagnée par des propositions sur la manière de traiter le problème de sécurité.

Paragraphe 2. RESEAU, INTERNET ET ESPACE CYBERNETIQUE : ANALYSE CONCEPTUELLE DU CYBERESPACE

Le cyberespace est un mot qui fut utilisé pour la première fois par William Gipson en 1982 dans un roman. Ce concept vient de la science-fiction et est définie par Gipson comme la création de la connexion d'ordinateurs dans un monde rempli d'êtres à intelligences artificielles.(1) Aujourd'hui, ce concept est lié aux nouvelles technologies de la communication et de l'information (NTIC) et à internet, ce qui en fait un outil de communication et d'information, ou un espace où des informations peuvent être échangées et ou l'on peut communiquer en temps réel et à coût extrêmement bas. Cela fait du cyberespace un concept complexe lié à internet, aux réseaux et aux systèmes d'informations.

I. Du Réseau Informatique à Internet

Le réseau informatique est l'élément central d'internet, c'est une unité plurielle qui constitue, avec l'interconnexion de ses substances, le réseau mondial qu'est internet.

1) Le réseau informatique

Un réseau informatique consiste en deux ordinateurs ou plus interconnecté via un dispositif matériel et logiciel leur permettant de communiquer et partager des fichiers ou toutes sortes d'informations numériques.(2)

On distingue cinq types de réseaux informatiques catégorisé selon la distance maximale séparant les points les plus éloignés du réseau :

(1) *Encyclopaedia Britannica online*, s.v. "Cyberspace: communication", http://www.britannica.com/EBchecked/topic/147819/cyberspace (accessed in 23, april 2015).

(2) Werner Feibel, "Network", *in Encyclopedia of networking,* second edition (Network Press ,1996), p. 659.

1) PAN (Personal Area Network) qui est un réseau personnel dont la distance n'est que de quelques mètres ;

2) LAN (Local Area Network) qui un réseau local habituellement utilisé par des entreprises pour le transport de leurs informations numériques.

3) MAN (Metropolitan Area Network) : un réseau métropolitain est capable d'interconnecter plusieurs réseaux locaux de différentes entreprises ou particuliers. Il permet une communication a haut débit.

4) RAN (Regional Area Network) : le réseau régional peut couvrir une large surface géographique allant jusqu'à 50 kilomètres pour la couverture sans fil.

5) WAN (Wide Area Network) est un réseau étendu destiné a transporter des données numériques sur des distances à l'échelle d'un pays voir un continent ou plusieurs.[1]

Le réseau renforce la puissance à disposition de l'utilisateur en augmentant les capacités des ordinateurs et les potentialités des utilisateurs. Le réseautage permet de faire une multitude de choses comme :

- distribuer une même connexion internet a toutes les unités composant le réseau ;
- augmenter la capacité de stockage ;
- centraliser la gestion de la sécurité et l'accès aux ressources. [2]

2) Internet et WEB

On peut non seulement interconnecter plusieurs ordinateurs mais aussi plusieurs groupes d'ordinateurs, en d'autres termes, on peut avoir plusieurs réseaux interconnectés pour former un réseau de plus grande ampleur. C'est ce qu'internet représente, un réseau géant se composant d'un nombre de réseaux sans cesse augmenté, ces réseaux sont de différentes tailles et peuvent être publics

[1] Guy Pujolle, *Les Réseaux.* (Paris: Editions Eyrolles, 2007), p.p. 14-15.

[2] *Microsoft encyclopedia of networking.* 2nd ed. Mitch Tulloch and Ingrid Tulloch (Washington: Microsoft Press, 2002), s.vv. "Internet". P. 835.

ou privés.[1] L'expression réseau des réseaux est fréquemment citée en définition d'internet, elle est donc le plus grand réseau du monde constituant une mine d'information extraordinaire et un moyen de communication rapide avec un cout très bas.

Parmi les applications qu'internet utilise : Le *World Wide Web* (WWW) communément abrégé *web*,[2] souvent confondu avec internet, le web est l'application gérant les liens hypertextes, elle est donc l'une des applications les plus importante d'internet, un navigateur internet peut être perçu comme un lecteur de liens hypertexte, il communique avec le serveur via un protocole de transfert, généralement le HTTP (Hypertext Transfer Protocol).

3) L'Utilisation d'internet aujourd'hui

Le nombre d'utilisateurs d'internet est passé de 14 millions en 1993 à presque 3 milliards en 2014. (Voir : annexe I sur l'évolution du nombre d'utilisateurs d'internet) Ces utilisateurs se répartissent inégalement à travers le monde, les éléments régissant cette répartition sont le niveau de développement technologique et économique des populations (voir la figure 1).

Figure 2. Répartition géographique des utilisateurs d'internet

Source : Internet Lives Stats, "internet users"
http://www.internetlivestats.com/internet-users/ (accessed April 24, 2015)

(1) *Encyclopedia of Networking*. 2nd ed. Werner Feibel. P.469.

(2) *Encyclopedia of networking*, s.v. 'WWW (World Wide Web)', 1094.

II. Définition du cyberespace

L'idée selon laquelle les concepts de cyberespace et d'internet ne font référence qu'a un seul et même phénomène n'est pas complétement vraie, certes internet constitue la plus grande partie du cyberespace mais ce dernier ne s'arrête pas à la seule internet mais est plus large. Il est donc nécessaire de définir l'objet référent de la sécuritisation : le cyberespace, qui est la conjonction de *cyber* et *espace*

1) Le Suffixe « cyber » et son Etymologie

À Pléthore de mots nous collons le préfixe « cyber », notre titre se compose de deux concepts qui ont ce même préfixe : cyber-menaces et cyberespace. Cyber vient de Cybernétique qui dérive du mot grec ancien *kubernêtikê* signifiant l'art de la conduite, faisant référence au timonier.(1) Le mot fut utilisé sous plusieurs sens depuis le 19e siècle mais refait son apparition dans les années 40s du siècle dernier à la rencontre de mathématiciens, de physiciens et de physiologistes.(2) Parmi eux, le mathématicien Norbert Wiener dont le livre publié en 1948 sous le titre *cybernetics* est considéré comme l'ouvrage créateur de la cybernétique comme science.(3) Wiener définit donc la cybernétique comme « *le champ entier de la théorie de la commande et de la communication, tant dans la machine que dans l'animal* ».(4)

La cybernétique est donc connue comme la science des machines a information,(5) dès lors, elle s'est développée en mathématiques et en informatique(6) surtout depuis les années 1990s ou son diminutif « cyber » vient s'ajouter en préfix à des mots de longue date pour leur donner un habillage plus

(1) Encyclopaedia Britannica Online, s.v. "Cybernetics", http://www.britannica.com/EBchecked/topic/147802/cybernetics (accessed in April 17, 2015).

(2) Raymond Ruyer, *La Cybernétique et l'origine de l'information* (France : Flamarion, 1954), p. 5.

(3) Encyclopaedia Britannica Online, ibid.

(4) Louis Couffignal, *La Cybernétique,* 3ème éd. (Paris : Presses Universitaires de France, 1968), P. 5

(5) Raymond Ruyer, ibid., p. 5.

(6) Encyclopaedia Britannica Online, ibid.

technologique et moderne[1] et a acquis la signification de « à travers l'utilisation des ordinateurs »[2] ou « vaguement lié à l'informatique »[3]

2) Définition de l'espace

Le dictionnaire Larousse donne plusieurs définitions du mot espace : « *Étendue, surface ou volume dont on a besoin autour de soi* » ; « *portion de l'étendue occupée par quelque chose ou distance entre deux choses, deux points* » ; « *Étendue, surface, région ; domaine localisé dans lequel s'exercent certaines activités* ».[4]

Le Robert le définit comme « [une] *étendue qui ne fait pas obstacle au mouvement* » ou encore un « *milieu géographique* ».[5]

En contemplant ces définitions, des idées ressortent à propos du sens du mot « espace » : l'espace est une Étendue, une surface, une région, un domaine localisé, un milieu. La distance entre deux points représente un espace, un environnement avec une structure et des éléments. Nous devons concevoir l'espace comme une étendue géographique se composant d'éléments divers.

En informatique, on utilise le mot *espace* pour qualifier le poids d'un fichier ou la taille d'un dispositif de stockage (disque dur, clé USB, CD…). L'espace en informatique se mesure par l'unité *Octet*, on trouvera donc des fichiers et dispositifs de stockage dont l'espace (le poids ou la taille) est de plusieurs mégaoctets (Mo)[6], gigaoctets (Go)[7], téraoctets (To)[8]… .

---

[1] Nicolas Arpajian, *La Cyberguerre : la guerre numérique a commencé* (Paris : Magniar-Vuibert, 2009), p. 23

[2] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US efforts to secure the information age* (Routledge, 2008), p. 16.

[3] Daniel Ventre, *Cyberguerre et guerre de l'information : stratégies, règles, enjeux* (Pais : Lavoisier, 2010), p. 32.

[4] *Larousse*, s.v. « espace », http://www.larousse.fr/dictionnaires/francais/espace/31013 (consulté le 15 avril 2015)

[5] *Le Robert : Dictionnaire Français*, s.v. « espace ».

[6] 1 Mo = 1024 Kilooctets (Ko) ; 1 Ko = 1024 octets.

[7] 1 Go = 1024 Mo.

[8] 1 To = 1024 Go.

3) L'espace cybernétique

Si l'espace est un environnement géographique, et que la cybernétique est relative à l'utilisation de l'informatique et des ordinateurs, l'espace cybernétique, ou cyberespace, est l'environnement virtuel informationnel obtenu par la mise en tension et l'utilisation d'un dispositif de stockage, d'un ordinateur ou toutes sortes de Systèmes de Traitement Automatisés de Données[1] (STAD).

La compréhension du concept de cyberespace peut être amélioré à travers l'examen critique d'autres définitions, ainsi, Olivier Kempf le définie comme « *l'espace constitué des systèmes informatiques de toute sorte connectés en réseau et permettant la communication technique et sociale d'informations par des utilisateurs individuels ou collectifs* »[2] cette définition induit que le cyberespace est le produit d'une connexion entre plusieurs systèmes informatiques. Nous pensons que l'existence d'un cyberespace n'est pas conditionnée par une telle connexion, aussi, un seul système informatique peut être considéré comme abritant un cyberespace dès lors que l'on le met sous tension. La communication d'informations incluses dans cette définition n'est que l'une des nombreuses utilisations du cyberespace et ne constitue pas un élément pivot de sa définition, Le cyberespace pourrait ne pas permettre la communication si le dispositif utilisé n'est pas connecté à d'autres dispositifs pour échanger des informations, comme un ordinateur non connecté à internet ou n'appartenant pas à un réseau.

Le cyberespace sera considéré ici comme un environnement informationnel virtuel dans lequel nous stockons et nous échangeons, modifiant et traitant des données numériques, cela peut être internet, un réseau public ou privé ou tout simplement un ordinateur.

4) Le Cyberespace par rapport aux espaces traditionnels

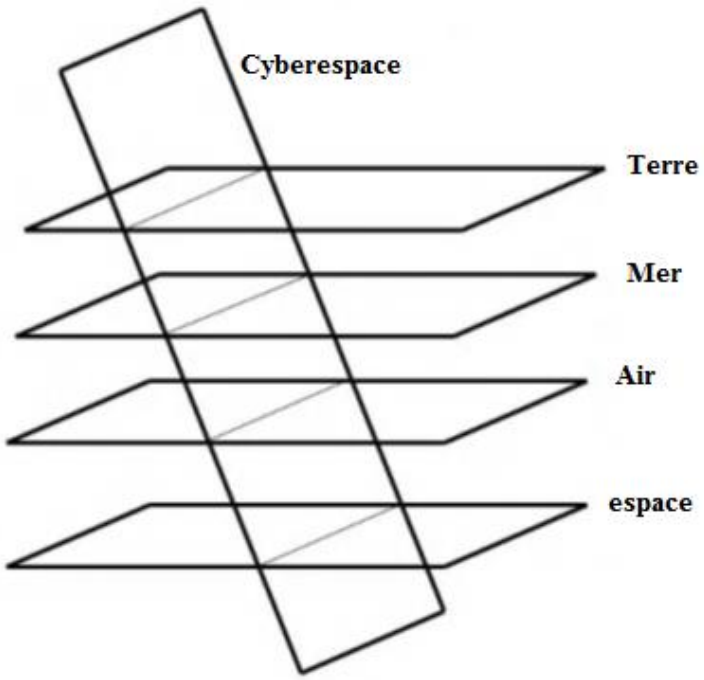
L'une des caractéristiques du cyberespace par rapport aux espaces traditionnels (la terre, la mer, l'air et l'espace) est sa *transversalité.* En effet, le cyberespace n'est pas un environnement indépendant mais le résultat de la connexion de plusieurs Systèmes de Traitement de Données Automatisé (STAD), les infrastructures de ces systèmes se trouvent dans l'un des espaces

[1] Nous considérons un STAD comme tout équipement utilisé pour l'acquisition, le stockage, traitement, transfert, réception, affichage, modification et suppression de données numériques.

[2] Olivier Kempf, *Introduction à la Cyberstratégie* (Paris : Economica, 2012), p. 14

traditionnels, mises sous tension, elles donnent corps à l'espace virtuel qu'est le cyberespace. Les infrastructures du cyberespace sont donc présentes dans le monde réel, et sa dimension virtuelle s'entrecoupe avec les autres espaces, il est donc transversal aux autres espaces.

Figure 3. le cyberespace, une dimension traversant les dimensions traditionnelles.



Source : Daniel Ventre, *Cyber Conflict : competing national perspectives* (Great Britain : ISTE Ltd, 2012) p.301.

Après avoir pris connaissance de la théorie de la sécuritisation et analysé le concept de cyberespace, nous comprendrons que la sécuritisation du cyberespace renvoie dans cette l'étude à l'évolution du cyberespace comme source de menace et d'insécurité, et les différentes réactions que les États adoptent dans le but de s'extraire aux cyber-menaces. Cela requière l'étude des cyber-menaces et leurs caractéristiques, ainsi que les vulnérabilités de l'État par rapport à cette problématique, puis mettre en exergue la réaction de ces États face à ces menaces et les mécanismes mis en place pour s'en défendre.

SECTION 2. CYBER-MENACES ET INSECURITE DU CYBERESPACE

A travers notre analyse conceptuelle du cyberespace, nous pouvons désormais nous essayer à la définition des cyber-menaces pour mieux comprendre de quoi nous parlons. Commençons par dire, qu'ici, le préfix *cyber* fait référence au cyberespace. Quand nous parlons de menaces (cyber-menaces), de sécurité (cyber-sécurité) ou de défense (cyber-défense) nous faisons référence aux menaces, sécurité et défense relatives au cyberespace.

Si la définition du mot *menace* comprend dans sa substance l'idée de nuisance, la cyber-menace est l'exposition du cyberespace, de son contenu informationnel et son intégrité physique, a un danger potentiel qui toucherait à sa bien portance et sa sécurité. Un site, un réseau ou une ordinateur comportant des informations sensibles et qui n'est pas sécurisé est exposé au danger des cyber-menaces qui viseraient à nuire à son contenu ou à l'intégrité de la machine qui abrite ce contenu.

Une cyber-attaque est une offensive utilisant du matériel informatique visant à nuire au contenu d'un système d'information ou aux infrastructures qu'il administre. Cette section visera à comprendre ce que sont les cyber-menaces et les attaques informatiques en dressant un portrait des différentes cyber-menaces et en compartimentant la cyber-insécurité en plusieurs niveaux d'analyse.

Paragraphe 1. VULNERABILITES DU CYBERESPACE ET ATTAQUES INFORMATIQUES

Enumérer les types de cyber-menaces existants requière la compréhension de la cyber-sécurité, cette dernière est l'état d'un système d'information assurant la confidentialité, l'intégrité et la disponibilité des informations qu'il contient. La *confidentialité* assure que seuls les individus autorisés auront le droit de consulter les informations en question, la consultation de ces informations par un tiers représente un échec du système de sécurité mis en place pour protéger ces

données. La consultation de documents par une personne non autorisée est donc une cyber-menace.[1]

L'*intégrité* des informations fait référence à la modification des données, seuls les utilisateurs autorisés doivent avoir la permission de modifier ou supprimer les données protégées. Enfin, la *disponibilité* du système et de ses données doivent être assurée en tout temps, ou du moins, quand l'utilisateur en a besoin.[2] Une politique cyber-sécuritaire vise donc à assurer la confidentialité des données stockées, leur intégrité et leur disponibilité. Tous ce qui pourrait toucher à ces trois principes représente une cyber-menace.

I. La vulnérabilité inhérente au cyberespace

Les acteurs du cyberespace guettent différentes vulnérabilités inhérentes au cyberespace et aux systèmes informatiques pour acquérir des informations, les manipuler ou les saboter, elles ou le système qui l'est contient et les gèrent. Plusieurs raisons font que le cyberespace est vulnérable, les failles logicielles pour les programmes informatiques, les failles des réseaux ainsi que la variable humaine et ses erreurs qui n'est pas moins dangereuse que les autres failles techniques.

1) Les failles logicielles

Les programmes informatiques sont tels que, pour une raison ou une autre, ils connaissent des failles qui rendent les attaques informatiques possibles. Des failles logicielles sont découvertes par milliers chaque année, et les correctifs proposés par les concepteurs (sous formes de mises a jour) [3] ne sont pas toujours appliquées par les utilisateurs, ce qui accroit la vulnérabilité des utilisateur mal informés.

Même les utilisateurs bien informés sont victimes de ces vulnérabilités à cause de l'exploitation de failles dites *Zero day*, c'est à dire celles qui ne sont

[1] Gregory White, Arthur Conklin, Dwayne Williams, Roger Davis and Chuck Cothren, *CompTia Security+ : exam guide, 2nd ed.* (CompTia, 2009), p. 7.

[2] Ibid., p. 8.

[3] Éric Filiol, *Les Virus Informatiques : théorie, pratique et application*, deuxième édition (France : Springer, 2009), p. 113.

découvertes que par l'attaquant et sont inconnues du développeur du produit et ne dispose donc pas de correctif.

L'origine des failles logicielles sont multiples, elle peuvent être le résultat de dysfonctionnements du programme exploitable par l'attaquant, absence de logiciel anti-virus qui protège le système d'exploitation lors de la navigation susr internet ou lors de l'introduction d'un dispositif amovible dans la machine, le manque de connaissance du développeur du produit qui fait qu'il n'a pas sécurisé sans programme ou bien tout simplement un oubli, etc.

2) Les failles des sites web et des réseaux

Le fait que les réseaux soient bien pensés dès les débuts d'internet n'empêche pas que des problèmes exploitables par un acteur malveillant soient toujours présents, surtout avec l'arrivée supports sans fil comme le Wi-Fi qui pose de nouveaux problèmes de sécurité.

Il arrive aussi que le développeur ait commis des erreurs dans son code ou qu'il n'y ait pas sécurisé son programme à cause du manque de connaissance en langages de programmation ou d'un oubli.

La faiblesse de certains mots de passes y est aussi pour beaucoup, dans certains cas, il suffirait de connaitre la personne pour deviner son mot de passe. Le choix d'un mot de passe devrait être plus pensé pour atteindre un niveau de complexité tel qu'il ne pourrait pas être deviné ou cassé par le *brute force.*

3) L'utilisateur comme source de vulnérabilité

L'utilisateur peut être une source de vulnérabilité pour les systèmes informatiques. En effet, plusieurs techniques (ou stratégies) de piratage informatique prennent en compte cette dimension humaine. Certains classent cela dans la case de l'ingénierie sociale,[1] cela renvoi à l'exploitation des mauvaises habitudes ou inclinations de l'utilisateur ou encore la mise en place d'une manipulation psychologique.[2] Par exemple, l'introduction d'une clé USB infecté dans un système sécurisé infecterait le système et pourrait le mettre hors d'usage, suivant le type d'infection dont il a fait l'objet. C'est ce qui s'est probablement passé dans la centrale nucléaire iranienne qui fut infecté par le ver

[1] « *social ingineering* » en anglais.

[2] Ibid., 113.

Stuxnet qui se propageait sur internet alors que les systèmes informatiques de cette centrale n'en étaient pas connectés. Il est possible qu'un employé de la centrale ait introduit un disque amovible (comme une clé USB) infecté dans l'un des ordinateurs, ce qui a fait propager le ver dans le système et à exécuter ce pourquoi il a été conçu.

Les systèmes informatiques sont donc toujours sujet à l'erreur humaine, un périmètre de sécurité bien conçu peut être mis en échec par un individu introduisant une clé USB infectée, cela donne à réfléchir sur les protocoles de sécurité que l'on devrait mettre en œuvre en entreprise ou dans les infrastructures critiques pour solutionner cette faille subsistant même dans les systèmes les plus sécurisés.

II. Les différents types d'attaques informatiques

1) Les infections informatiques

Les infections informatiques sont les attaques les plus fréquentes sur les systèmes informatiques,[1] ce sont des logiciels malveillants s'installant dans les systèmes informatiques dans des buts, soit de renseignement, ou bien de sabotage. Nous pouvons aussi la définir comme suite :

> « *Programme simple ou autoreproducteur à caractère offensif, s'installant dans un système d'information, à l'insu du ou des utilisateurs, en vue de porter atteinte à la confidentialité, l'intégrité ou la disponibilité de ce système, ou susceptible d'incriminer à tort son possesseur ou l'utilisateur dans la réalisation d'un ou d'un délit* »[2]

Cette définition nous donne une autre information rarement connue du grand public, des pirates infectent des cibles afin d'utiliser les systèmes infectés dans un autre but qui pourrait être criminel. Le but derrière tout cela est d'attaquer des cibles ou commettre des crimes ou des délits sans que l'on puisse remonter vers l'instigateur de cette attaque, à sa place, on remonterait à l'ordinateur infecté et l'on accusera son utilisateur.[3]

---

[1] T.J. Samuelle, *CompTia Security+ Certification* (McGraw Hill, 2009), p. 5.

[2] Éric Filiol, op. cit., p. 111.

[3] Ibid., 112.

Les programmes malicieux sont assez divers, ils peuvent être des virus, des vers, chevaux de Troie, portes dérobées, des bombes logiques, etc. les virus et les vers présentent aujourd'hui cette capacité d'autoreproduction et d'infection par réseau.[1] Ils peuvent infecter un ordinateur puis s'envoyer par e-mail ou dans le réseau pour infecter d'autres utilisateurs assurant ainsi sa survie.

Les portes dérobées sonnent à l'agresseur extérieur accès à l'ordinateur victime par le réseau, un logiciel espion peut aussi infecter un ordinateur pour collecter des informations à l'insu de l'utilisateur,[2] c'est informations peuvent être des identifiants d'un compte mail ceux d'une carte bancaire ou d'autres informations secrètes ou privées.

Les risques encourues suite à une infection informatique sont donc très sérieux, le système peut être mis hors service, les informations qu'il contient peuvent être consultées par un tiers, et peuvent être modifiées ou supprimées, l'ordinateur peut aussi être utilisé comme zombie dans les attaques DDoS sans que l'on puisse remonter à l'instigateur de l'attaque en question.

2) Les Attaques directes

Les attaques directes regroupent toutes les techniques utilisées directement par une personne ou un groupe de personnes dans le but de s'introduire dans un système, que ce soit un ordinateur, un site internet ou un compte de messagerie électronique, exploitant les vulnérabilités logicielles de ces systèmes.

L'une des techniques d'attaques les plus performantes pour faire échouer un réseau est l'attaque de déni de service distribuée (Distributed Denial of Service), abrégée DDoS. Sa forme simple, DoS, consiste à ne pas répondre lors d'une demande de connexion auprès d'un serveur, ce dernier reste en attente et bloque pendant un certain temps une partie de ses ressources pour cette nouvelle connexion. Le but est d'envoyer suffisamment de demandes pour que le serveur soit submergé et se voit dans l'incapacité d'y répondre et finira par cracher.[3]

---

[1] Mar Borrelli, ed., *Marlware and Computer Security Insidents : Handing Guides* (New York: Nova Science Publishers, 2013), p. 9.

[2] Lorent Bloch et Christohe Wolfhugel, *Sécurité Informatique : principes et métode à l'usage des DSI, RSSI et administrateurs*, 2e ed. (Paris, Eyrolles, 2009), p. 60.

[3] Joëlle Musset, *Sécurité Informatique : Apprendre l'attaque pour mieux se défendre* (France : Editions ENI, 2009), p. 160.

Une attaque DDoS est plus complexe qu'une attaque DoS puisque l'attaque se fait à partir de plusieurs machines au lieu d'une seule.[1] Les instigateurs d'une telle attaque peuvent, soit appeler d'autres utilisateurs pour attaquer le système cible en envoyant des requêtes constantes au serveur, ou bien construire un réseau de zombies (ordinateurs contrôlés à distance suite à une infection).[2]

Il y a beaucoup d'autres techniques d'attaques. Comme celles exploitant les portes dérobées pour avoir accès à un système (via un logiciel vulnérable),[3] les injections SQL pour accéder a des pages web sécurisées, le Cross-site en mettant un programme JavaScript sur une page web vulnérable et qui s'exécutera lorsqu'un utilisateur y accède, etc.

III. Cibles des cyber-menaces

Faire une liste des cibles possible des cyber-menaces est un exercice ardu, d'abord parce qu'elles sont très diverses, mais aussi, elle dépend de quel point de vu nous nous plaçons. La menace pour un individu n'est pas la même que pour l'entreprise, et la menace pour l'entreprise n'est pas la même que pour l'État. Nous allons donc essayer de faire une liste de cibles potentielles ou d'entités qui peuvent percevoir les actions d'autres acteurs comme pouvant constituer une menace.

1) La liberté menacée

La liberté d'internet est un principe auquel beaucoup d'internautes engagés tiennent au point de refuser la gouvernance d'internet, sa surveillance ou la censure de certaines informations[4], c'est le cas de de John Perry Barlow désormais célèbre pour avoir rédigé la déclaration d'indépendance du

[1] Ibid., 161.

[2] Gregory White et *al.*, op. cit., p. 397.

[3] Une porte dérobée est une ouverture codée dans un programme laissé par son développeur pour y entrer. Si le code est découvert alors tous les systèmes utilisant ce programme seront vulnérables à une attaque. Voir : ibid., p 398.

[4] On parle de la neutralité d'internet (*net neutrality*) dans le traitement égal et sans discrimination des informations en tous genres trouvées sur internet.

cyberespace en 1996[1] ou il exprime son refus de quelque forme d'autorité que ce soir sur le cyberespace (utilisé comme synonyme d'internet).

Cette peur de la mise en tutelle du réseau mondial est justifiée, en effet, beaucoup de gouvernements contrôlent leur populations en interceptant leurs communications et en épluchant leurs e-mails, se faisant aider par des entreprises telle Amesys[2], société française, qui aurait fourni à la Libye le matériel nécessaire pour intercepter les communications et les activités en ligne de la population[3] en plein troubles sociaux en 2011[4]. Si la vente de ce genre de technologies est permise par la loi, nous devons nous interroger sur les implications éthiques de leur utilisation. La garantie de la sécurité nationale ne se soumet certes pas à la même morale que peuvent avoir les personnes, mais elle pose des problèmes de libertés individuelles dès lors que ces techniques servent les intérêts d'une élite.[5]

Pour cette raison, de nouveaux acteurs sont apparus pour alerter la population des pratiques de certains gouvernements. Ces acteurs sont appelés « donneurs d'alertes » comme Edward Snowden et Julian Assange. Nous trouvons aussi des groupes d'activistes (appelés hacktivistes) tel que le groupe de hacker Anonymous.

2) La cybercriminalité ou la menace à l'individu

Un crime est un acte puni par la loi, pouvant apporter des troubles à la société ou une partie de la société. Il pourrait avoir comme cible les individus (meurtre, viole), la propriété (incendie, vol), le gouvernement (trahison), et la

---

[1] John P. Barlow, « Déclaration d'indépendance du cyberespace », http://editions-hache.com/essais/barlow/barlow2.html.

[2] L'entreprise Amesys est poursuivie devant la justice française par la Fédération Internationale des Droits de l'Homme pour complicité de torture. Voir : « Amesys », Les Ennemis d'Internet : Rapport spécial surveillance, http://surveillance.rsf.org/amesys/ (accédé le 28 avril, 2015)

[3] D'autres entreprises auraient fourni du matériel de surveillance a la Libye comme la société chinoise ZTE Corp. et la société sud-africaine VASTech SA Pty Ltd pour intercepter les appels internationaux émis ou reçus sur le territoire libyen.

[4] Paul Sonne And Margaret Coker, "Firms Aided Libyan Spies: First Look Inside Security Unit Shows How Citizens Were Tracked", *The Wall Street Journal*, August 30, 2011, http://www.wsj.com/articles/SB10001424053111904199404576538721260166388.

[5] Pour plus d'informations sur la technologie EAGLE vendue par Amesys, voir son manuel publié par Wikileaks : http://www.wikileaks.org/spyfiles/files/0/99_AMESYS-EAGLE-GLINT-Operator_Manual.pdf

moralité (obscénité).[1] Un cyber-crime n'est qu'un comme on en connaît beaucoup mais qui est commis à l'aide de technologie informatique ou plus généralement les TIC. Le cyberespace est devenu un endroit où l'on commet des crimes conventionnels avec de nouveaux moyens.[2]

Les cyber-crimes sont multiples, ils peuvent aller de la création de virus et leur diffusion au piratage de comptes bancaires et de cartes de crédits, en passant par la fraude et l'extorsion de fonds ou encore le visionnage/diffusion/stockage de photos ou de vidéos pédopornographiques.

3) L'entreprise et la cyber-criminalité

Ces cyber-crimes peuvent aussi prendre comme cible des entités collectives, si l'individu peut être atteint, les entreprises aussi de piratage informatique et d'intelligence économique usant de moyens de communication dans la collecte d'informations ou bien de chantage. Domino's Pizza et Sony pictures sont des exemples d'entreprises piratées. La première fut victime de chantage après avoir essuyée des attaques informatiques visant ses bases de données. Les pirates ont pris les données privées de près de 600 000 clients et on exigés une rançon de 30 000 euros sous peine de les rendre publics.[3] Des demandes de rançons sont souvent demandées après le piratage de sites des grandes sociétés, c'est notamment le cas de a banque Dexia ou de l'entreprise Numericable.[4]

Ainsi, une entreprise peut se faire pirater son site, ses bases de données et perdre des informations précieuses relatives à son activité commerciale ou à ses clients, ces attaques peuvent être initiées par des individus isolés ou bien par d'autres entreprises dans une logique d'intelligence économique.

4) L'État comme cible des cyber-menaces

L'État est cible d'attaques informatiques diverses, que ce soit sur ses informations secrètes, sur ses infrastructures critiques, ou sur ses entreprises clés.

---

[1] Susan W. Brenner, *Cybercrime : Criminal Threats from Cyberspace* (USA : Praeger, 2010), p. 9.

[2] Ibid., p. 10.

[3] Ludwig Gallet, Piratage informatique : danger sur la réputation de l'entreprise, *L'Express* l'Entreprise, 19 juin, 2014, http://lentreprise.lexpress.fr/marketing-vente/promotion-communication/piratage-informatique-danger-sur-la-reputation-de-l-entreprise_1552590.html.

[4] Ibid.

Elle peut donc être victime de vol d'informations comme l'ont été les États-Unis lorsqu'on leur a volé des informations relatives au développement de l'avion F-35.[1]

Les nouvelles attaques contre les entreprises ont pris une autre tournure avec l'arrivée de logiciels malveillants s'attaquant à la sécurité des Systèmes de Contrôle Industriels (SCI),[2] cela s'insère dans le cadre des relations internationales ou les États concourent pour des intérêts stratégiques ou des infrastructures critiques peuvent constituer une cible des attaques informatiques étant donnée l'intégration d'un module informatique dans celle-ci assurant sa gestion et son soutien. Nous traiterons plus en profondeur ces questions dans le chapitre suivant.

La cyber-insécurité prise au niveau de l'état permet non seulement d'étudier des sujets comme la cyber-guerre ou la guerre de l'information comme des questions stratégiques, mais aussi prendre la cyber-insécurité comme un système ou les niveaux sub-étatiques se confondent avec le niveau étatique, en d'autres termes, avoir une approche globale de la cyber-insécurité comprenant les cyber-menaces venant des individus, de l'intelligence économique et d'autres États.

Nous pouvons dès maintenant construire un modèle d'analyse des cyber-menaces en déterminant les acteurs influents et les cibles des attaques potentielles. Ainsi, le premier palier d'analyse serait de l'ordre du criminel, ou les menaces seraient l'atteinte à des systèmes d'informations particuliers ou publics. On cible dans ce cas les systèmes appartenant à des entreprises pour demander des rançons ou pour voler des données. Les attaques sont aussi dirigées vers des individus et leurs systèmes ou leurs coordonnées bancaires sont volées et où leurs identités sont constamment menacées. Un autre niveau d'analyse serait la stabilité économique et sociale d'une société. Les menaces seraient aussi criminelles, les acteurs seraient des entreprises, dans un niveau plus haut, l'État serait la source de menaces pour l'entreprise, les agences de renseignement chercheraient à obtenir des informations utiles pour les entreprises de leurs pays, Nous parlons d'intelligence économique, ou plutôt de cyber-espionnage

[1] Siobhan Gorman, August Cole And Yochi Dreazen, Computer Spies Breach Fighter-Jet Project, *The Wall Street Journal*, april 21, 2009, http://www.wsj.com/articles/SB124027491029837401.

[2] "Internet Security Threat Report", *Symantec*, Volume 20 (April 2015), p. 63.

économique. L'État chercherait aussi des informations d'ordre militaires ou travaillerait au sabotage de certains systèmes d'informations de l'adversaire, en temps de paix ou en temps de guerre.

Ces niveaux et ces menaces ainsi que les acteurs que l'on a cités peuvent se confondre, par exemple, quand la cybercriminalité se propage, les entreprises seront moins enclines à investir dans le pays, l'intérêt de l'État serait donc menacé. Ou quand l'on perçoit les choses à partir de l'État, les donneurs d'alertes peuvent menacer l'intérêt de l'État en diffusant des informations classifiées…

Paragraphe 2. LES COUCHES DU CYBERESPACE ET LEURS RISQUES SPECIFIQUES

La vulnérabilité du cyberespace est la vulnérabilité des ordinateurs et des systèmes d'informations, cette vulnérabilité est intrinsèque à ces machines et les logiciels qui les gèrent. Tout est vulnérable dans le cyberespace, en commençant par les informations qu'il contient, ses infrastructures, les machines pour lesquelles il est conçu (et dont la gestion est informatisée), les programmes qui régissent ces machines et même ses utilisateurs.

I. Les Couches Du Cyberespace

Le cyberespace ne devrait pas être considéré comme un bloc homogène. Certains experts des problématiques liées à la cyber-sécurité ont entrepris de définir le cyberespace en partant du principe que celui-ci se déploie sur plusieurs couches. S'inspirant des travaux d'Edward Waltz sur la guerre de l'information,[1] Daniel Ventre définie trois couches du cyberespace : la première est matérielle ; la seconde est logicielle, et la dernière est cognitive.[2] Olivier Kempf parle de

[1] Voir : Edward Waltz, *Information Warfare: principles and operations* (Norwood, Artech House, 1998).

[2] Daniel Ventre, *Cyber Conflict: competing national perspectives* (Great Britain: ISTE Ltd, 2012), p. 302.

couches matérielle, logique et sémantique ou informationnelle.[1] Martin Libicki y rajoute une couche pragmatique[2] que l'on ne traitera pas ici.

1) La couche matérielle (ou physique)

La couche physique représente l'ensemble des infrastructures et équipements tangibles nécessaires à l'obtention de la couche logique après leur mise sous tension et l'interconnexion. Les ordinateurs, satellites, câbles, fréquences radio, routeurs et les serveurs font partie de cette couche physique. C'est cette couche qui rend le cyberespace géographiquement enraciné.[3]

2) La couche logique ou logicielle

La couche logicielle est l'environnement virtuel construit par la programmation de logiciels gérant le matériel informatique, il contient les instructions pour l'ordinateur ou la machine pour exécuter différents protocoles ou programmes qui sont utilisés par les machines pour permettre une interaction avec une autre machine. Elle se compose des différents programmes, applications, protocoles, algorithmes, relais et nœuds.[4] C'est généralement à cette couche que l'on donne le dénominatif de cyberespace.

3) La couche cognitive, sémantique ou informationnelle

La couche cognitive consiste en les informations présentes dans les dispositifs de stockages et des réseaux et qui sont traités par les éléments logiciels de la couche logique, et l'interaction de ces informations avec l'utilisateur et ses perceptions. Ces informations sont donc manipulées, transférées ou supprimées au moyen de programmes informatiques présents dans ce que l'on a appelé la couche logique par intervention d'un utilisateur.

II. Les Menaces Spécifiques à Chaque Couche

Les menaces qui existent pour chaque couche sont pensées à partir des attaques qu'elles pourraient subir, une attaque probable d'un acteur est une

---

[1] Olivier Kempf, op. cit., p.p. 10-14.

[2] Martin C. Libicki, *Conquest in Cyberspace: national security and information warfare* (Cambridge: The RAND Corporation, 2007), P. 237.

[3] Olivier Kempf, op. cit., p. 11.

[4] Un nœud est n'importe quel appareil avec une adresse IP.

menace pour un autre acteur qui doit penser sa défense. Des attaques peuvent cibler n'importe quelle de ces couches en temps de paix ou en temps de guerre et pour cela, il conviendrait d'examiner les risques liés à ces attaques au niveau de chaque couche.

1) Les menaces pour la couche matérielle

Les attaques sur la couche matérielle sont des attaques physiques sur ces composants touchant l'intégrité des machines ou des moyens de connexion, mais aussi les infrastructures gérées par des outils informatiques.

Au cours d'une guerre, l'une des missions des forces armées est d'attaquer les centres et les canaux de communication de l'adversaire comme les câbles, la mission de ce dernier est d'organiser sa défense de façon à protéger ces centres critiques.

L'autre menace potentielle et le rompt de la connexion entre les différents composant dont le cyberespace fait le lien, cela peut être le résultat du découpage des câbles servant à la connexion, une attaque par impulsions électromagnétiques ou encore le sabotage ou le bombardement d'infrastructures de communication[1] en cas de conflit armé.

2) Les menaces à la couche logique

La couche logique est la plus exposée des trois couches, c'est dans cette couche que les failles de sécurité les plus importantes sont présentes. Les attaques informatiques sur cette cible dépendent des failles présentes dans le système d'exploitation, le logiciel ou le site internet visé. Une attaque au niveau de la couche logique pourrait provoquer des dommages sur la couche physique, nous avons vu des programmes malicieux mettre hors service des ordinateurs et même les centrifugeuses d'une centrale nucléaire.[2]

Le résultat d'attaques informatiques dépendent des cibles visées, elles peuvent être des sites, des comptes e-mail, des bases de données sécurisées, etc. un site peut être attaqué dans le but de le mettre hors service ou seulement le

[1] Daniel Ventre, Cyber-conflict, p. 304.

[2] La centrale nucléaire en question appartient à l'Iran, ses systèmes informatiques furent infectés par un ver : Stuxnet, qui a provoqué l'explosion d'un grand nombre de centrifugeuses.

défaçer,[1] une base de données peut être piraté dans le but de voler des informations, de les modifier ou les supprimer. Des entités organisées comme les États ne peuvent se permettre la perte ou la diffusion d'informations classifiées, cela représenterait une menace sérieuse à la sécurité nationale et à la crédibilité des institutions publiques.

3) Les menaces à la couche cognitive

Une attaque sur cette couche viserait des informations dans le but de les voler, les modifier ou les supprimer après avoir trouvé une faille dans le dispositif logique du système. C'est cette couche qui est le plus concernée par la guerre de l'information et est liée à l'utilisateur qui peut être manipulé dans le but d'introduire l'attaquant, ou le programme malicieux confectionné par celui-ci, dans le système protégé.

Une attaque de la couche cognitive consiste en une attaque informatique ayant pour but la manipulation d'acteurs spécifiques. Elle concerne la manipulation d'informations et les opérations psychologiques.[2] Elle peut être abordée sur deux niveaux : le premier niveau est celui de l'individu, un acteur malveillant peut acquérir des informations sensibles à propos d'une personne et lui soutirer de l'argent sous peine de les diffuser. Le second niveau est celui de l'État : un pirate ou un groupe de pirates activistes (hacktivistes) peuvent attaquer une base de données gouvernementale dont les informations sont classifiées, ces informations sont volées et divulguées au grand public, ou encore la diffusion d'informations pour des buts de propagande.

Ces trois couches doivent être perçues comme étant complémentaires, assurer la sécurité du cyberespace passe par une réflexion et des réactions au niveau de chaque couche. L'ensemble de ces couches forme le cyberespace.

Comme nous avons pu le voir, plusieurs acteurs et entités peuvent être cible de cyber-attaques, ces dernières sont des menaces constantes qui peuvent avoir une nuisance sur le plan de la société dans le sens où elles touchent à

[1] Le défaçage ou le défacement est la modification du contenu d'un site web sans autorisation préalable de l'administrateur. C'est le piratage d'un site et le changement de son aspect informationnel ou esthétique.

[2] Ibid.

l'intégrité des personnes et leur confort, elle peut avoir une nuisance sur l'économie quand elles ciblent les entreprises et entrave leurs activités commerciales. Comme elle peut être source de menaces pour l'État, ses institutions et ses infrastructures vitale et leur existence.

Les dangers résultants de l'utilisation du cyberespace dans diverses activités représentent donc une menace existentielle pour l'État, c'est-à-dire qu'elle est capable de causer suffisamment de dommages, pour les institutions militaires et les infrastructures critiques du pays, pour que le gouvernement perde le contrôle de son territoire ou une partie de celui-ci. C'est cette représentation qui est sécuritisée, le cyberespace est perçu comme une menace existentielle pour la sécurité des États, traiter des *cyber-menaces et la sécuritisation du cyberespace* reviendrait à étudier la vision d'un acteur particulier (dans notre cas, l'État) envers le cyberespace comme source de menaces à sa sécurité et analyser la réaction de cet acteur pour garantir son existence voir d'exploiter cette source de menace dans un projet plus ambitieux.

La sécuritisation du cyberespace comme nous l'étudierons se concentrera donc sur ce niveau étatique en ayant une approche stratégique de l'insécurité informatique et des cyber-menaces. L'État est vulnérable quand on vise son économie et ses infrastructures critiques ou encore chercher à percer ses informations stratégiques, les acteurs principaux seront les États-nations, leur buts sont géopolitiques, et l'objet référent de la sécurité est l'État ainsi que ses infrastructures critiques et ses systèmes d'informations situés dans des emplacements stratégiques. La géopolitique et les cyber-menaces seront le sujet du chapitre suivant.

CHAPITRE DEUXIÈME: LA GÉOPOLITIQUE ET LA SÉCURITÉ À L'AGE DE L'INFORMATION

La communication est un véritable facteur de puissance. Les empires passés se sont concentrés sur la communication pour construire leurs réseaux d'influence. Pour l'empire romain, c'était les routes terrestres qui ont contribué à assurer la suprématie romaine dans le pourtours méditerranéen et au-delà. Pour l'Empire britannique, les routes maritimes constituaient un vecteur de projection de puissance aux XVIIIe et XIXe siècles,[1] même le cœur du monde (*Heartland*) [2] est devenu la plus importante région du monde après que les russes aient construit des voies ferrées, rendant facile la communication entre les quatre coins d'un large territoire et rendant possible une éventuelle émergence de puissance pour défier la puissance britannique une fois de plus.[3] Aujourd'hui, les réseaux numériques assurent cette communication, pourrait-on paraphraser H.J. Mackinder en disant que celui qui contrôle les réseaux numériques contrôlerait le monde ? Une chose est sûre, c'est que le cyberespace est aujourd'hui exploité pour des buts géopolitiques, le recueil d'informations, opérations de sabotage de différentes infrastructures, etc.

Ce que l'on a pu apprendre dans le précédent chapitre sera réutilisé ici mais de façon différente. Les infections informatiques ne sont plus des virus ou des vers mais des cyber-armes, les portes dérobées ne sont plus utilisées pour espionner ses amis mais pour recueillir des renseignements stratégiques, on parle de cyber-espionnage. Les attaques directes sur des systèmes d'informations ne visent plus à faire échouer l'ordinateur d'un particulier par gout d'aventure, mais sont des cyber-opérations militaires destinées à saboter un système d'information tactique ou des infrastructures critiques d'un rival ou d'un ennemi.

---

[1] Stéphane Dossé, « Géopolitique numérique : Omnibus viis americam pervenitur, tous les chemins mènent en Amérique », dans *Stratégies dans le cyberespace*, sous la direction de Stéphane Dossé et Olivier Kempf, (L'esprit du livre éditions, 2011), p. 50.

[2] L'expression « cœur du monde » est issue de la théorie géopolitique de Halford J. Mackinder, elle représente la région s'étendant de l'Europe de l'est et la Sibérie, passant au nord de l'Iran actuelle et du désert de Gobi. Le cœur du monde fait référence aujourd'hui à l'Asie centrale.

[3] C'est d'ailleurs pour cette raison que Mackinder s'est inquiété de la montée russe. Relier un large territoire donne plus d'organisation et plus de contrôle pour le pouvoir central.

La géopolitique est l'une des sources des cyber-menaces, les États l'ont bien compris et réagissent en conséquence : ils sécuritisent le cyberespace. C'est le sujet de ce chapitre. Nous verrons quel genre de menaces la géopolitique génère-t-elle en utilisant le cyberespace dans une première section. Puis nous traiterons de la manière dont les États-Unis d'Amérique ont pu s'organiser pour construire une stratégie de cyber-sécurité pour se défendre des cyber-menaces géopolitiques.

SECTION 1. LA GEOPOLITIQUE COMME SOURCE DE CYBER-MENACES

Selon Yves Lacoste, la géopolitique « *Désigne […] tout ce qui concerne les rivalités de pouvoirs ou d'influences sur les territoires et populations qui y vivent : rivalités entre des pouvoirs politiques de toutes sortes – et pas seulement entre des Etats, mais aussi entre des mouvements politiques ou des groupes armés plus ou moins clandestins* »[(1)]

La géopolitique concernerait donc la concurrence entre deux acteurs ou plus pour des intérêts qui se mesurent en termes de territoires considéré comme source de puissance. Appliquée au cyberespace, la géopolitique le percevrait comme un nouveau domaine d'affrontement d'intérêts nationaux. Et si l'on ajoutait la variable sécuritaire, ces intérêts nationaux se réfèreraient tantôt à la quête de puissance, tantôt à la garantie de l'existence de l'État, ou en d'autres termes, sa sécurité. Notons que la quête de la puissance et la préservation de la sécurité sont les deux intérêts que la théorie réaliste place au centre de sa réflexion.

La vision développée ici met en relation la géopolitique et la sécurité en postulant que la poursuite des intérêts nationaux par les uns, souvent par des initiatives offensives, est représentée par les autres comme une menace à leur sécurité. Nous pouvons approfondir ce constat tout en étant fidèle aux théories géopolitiques des premiers temps en pensant les initiatives géopolitiques comme une garantie d'existence et donc de sécurité. Pour le fondateur de la géopolitique, Friedrich Ratzel, l'État qui ne vise pas l'expansion territoriale est condamnée à disparaitre. Nous sommes tentés de dire que l'État qui ne cherche pas à réaliser ses intérêts est condamnée à la décrépitude, L'intérêt étant la survie et le développement (en termes de puissance économique et militaire). Les prétentions territoriales et géostratégiques des autres doit être perçues comme des menaces à la sécurité nationale. La réaction des États pour faire face ç cela est la préparation au combat. Gaston Bouthoul reprend la locution latine

[(1)] Yves Lacoste, *Géopolitique : la longue histoire d'aujourd'hui* (Paris, Larousse, 2012), p.8.

Si vis pacem, para bellum (qui veut la paix, qu'il se prépare à la guerre)[1] qui, à notre sens, convient parfaitement à l'approche adoptée dans cette étude.

Le cyberespace est un nouveau domaine dans lequel les États rivalisent, Cette section essaiera de rendre compte de cette rivalité tout en-là considérant comme une question de sécurité. Le cyberespace sera donc considéré à la fois comme un domaine et comme un objet référent de la sécurité non indépendamment de la sécurité nationale de l'État.

Paragraphe 1. LE CONFLIT : CATEGORIE D'ANALYSE GEOPOLITIQUE

La guerre, ou plus généralement le phénomène de la conflictualité, est un sujet géopolitique par excellence. Si nous traitions de conflit dans le cyberespace, nous parlerions de cyber-conflit. Traiter des cyber-conflits, de leur existence contestée et de leurs probables développement ou manifestations nous amènera à découvrir les enjeux liés aux rivalités de pouvoirs et d'influence impliquant le cyberespace et de là, les cyber-menaces liées à ce phénomène. Nous commencerons par examiner la conflictualité dans le cyberespace et avec plus de précision, la cyber-guerre.

I. La conflictualité, d'anciens concepts dans un nouveau monde

Les problématiques liées au cyberespace émergent dans la littérature stratégique au lendemain de la guerre froide, et sont mises en relation avec le débat sur la révolution dans les affaires militaires (RAM), des sujets comme la guerre de l'information sont traités, y compris par le pentagone.[2] En 1993, deux chercheurs de la RAND corporation –John Arquilla et David Ronfeldt, publient l'article intitulé *Cyberwar is Coming !* (la cyber-guerre arrive). Après cela, un débat s'est installé sur la possibilité de la tenue d'une cyber-guerre ou pas. Les chercheurs étudiant ce domaine se disent que la cyber-guerre ne s'est jamais

[1] Voir : Gaston Bouthoul, *traité de polémologie : guerre ou paix ?*

[2] Jean-Lopu Samaan, "Mythes et réalités des cyberguerres", *Politique étrangère*, vol. 73, No. 4 (hiver 2008), p. 829.

tenue par le passé, elle ne se tient pas en ce moment et il y a des chances qu'elle ne se tienne jamais.

On suppose que la guerre est un phénomène aussi vieux que l'homme, une notion ancienne qui est toujours d'actualité dans le cyberespace, d'autres notions s'ajoutent aussi, le terrorisme, l'espionnage, tous des concepts que l'on utilisait bien avant l'arrivée du cyberespace, les terroristes et les agences de renseignement se sont adaptées au monde ou nous vivons, désormais, les menaces classiques refont surface dans un nouvel espace d'affrontement, le cyberespace. C'est cela que nous allons brièvement analyser ici.

1) De la Cyber-guerre

Le sens que l'on donne aux cyber-attaques est contextuel, il dépend des acteurs, de leurs motivations et de leurs cibles. Delà, il pourrait s'agir de cyber-guerre, de cyber-criminalité ou de cyber-terrorisme.[1] Nous devons toujours garder à l'esprit l'utilisation abusive du concept de guerre, il est usité non seulement pour exprimer un affrontement armé entre deux entités étatiques qui en résulte destruction et mort d'hommes, comme ce fut le cas dans la seconde guerre mondiale. Le terme guerre froide est aussi utilisé pour désigner une concurrence entre deux pôles ou les belligérants ne sont pas entrés dans une lutte militaire directe. Le terme *guerre* peut être utilisé de manière métaphorique, pas besoin qu'un affrontement soit létal pour qu'il soit considéré comme une guerre.

Mais gardons la définition stratégique de la guerre : une discordance entre deux entités organisées se considérant comme absolument opposées usant d'armes létales pour arriver à leurs fins. Delà découlerait la définition de la cyber-guerre comme *une discordance entre deux entités, ou plus, qui se considèrent comme absolument opposées, utilisant les systèmes d'informations et leurs composantes comme moyens d'affrontements.* La guerre est le monopole des armées organisées, Carle von Clausewitz en a formulé 3 caractéristiques. Selon lui, la guerre : est une violence physique ; un instrument pour soumettre l'ennemi a sa volonté ; a un objectif politique qui se cache derrière l'acte, et pour cela, l'acte de la guerre doit être attribué à une certaine entité instigatrice. Or, si la cyber-guerre n'était qu'une guerre sur réseaux, elle ne serait que virtuelle et la

[1] Sanjay Goel and Yuan Hong, "Cyber War Games: strategic jostling among traditional adversaries", in *Cyber Warfare: building he scientific foundation*, ed. Sushil Jajodia, Paulo shakarian, V.S. Subrahmanian, Vipin Swarum and Cliff Wang, p.p. 1-14 (New York: Springer, 2015), p. 3.

violence physique serait absente, sauf si une attaque virtuelle peut produire des effets physiques.

La cyber-guerre serait donc une guerre en réseaux, les cyber-guerriers seraient des pirates informatiques formés pour porter atteinte à des systèmes informatiques sophistiqués, ou pour coder un logiciel malveillant suffisamment complexe pour qu'ils opèrent sans intervention du concepteur après son « largage » dans le cyberespace.

S'il est vrai que des hackers sont présents dans les armées ou dans les services de renseignements, cet affrontement direct entre deux armées cybernétiques n'a jamais eu lieu, des cyber-attaques s'opèrent chaque jour dans des armées ou des entreprises mais de façon unilatérale et sans déclaration de guerre préalable. La nature du cyberespace qui assure l'anonymat à celui qui le veut est une variable non négligeable pour penser philosophiquement la cyber-guerre. La question de *est-ce qu'une cyber-attaque représente un acte de guerre*, la réponse est difficile, si oui, la chine et les États-Unis seraient en guerre en voyant la quantité d'attaques informatiques initiées par chacune des deux nations, or, il n'en est rien, même s'ils sont dans un *cyber-conflit intense.*[1]

L'existence contestée de la cyber-guerre et la pertinence même de ce concept fait débat dans les milieux académiques. Certains postulent sur l'arrivée d'une cyber-guerre et d'autres ne croient pas à la possibilité qu'une cyber-guerre eut lieu. Dans son article *Cyber War Will Not Take Place* (la cyber-guerre n'aura pas lieu), Thomas Rid défend la thèse selon laquelle les critères de la guerre formulées par Clausewitz, que l'on a cité ci-haut, ne s'appliquent pas aux cyber-attaques. La guerre est violente, violence que le cyberespace est incapable de reproduire[2] de par sa nature virtuelle. Il est donc peu probable, selon Thomas Rid, qu'une cyber-guerre arrive un jour. Le qualificatif de cyber-guerre que l'on a utilisé pour faire référence aux attaques informatiques russes envers l'Estonie ne serait pas justifié. Précisons néanmoins que cela ne veut pas dire qu'il n'y a pas d'affrontements d'intérêts nationaux dans le cyberespace, les armées prennent conscience de la réalité de ces affrontements et nombre d'entre elles

[1] Mark Clayton, "The new cyber arms race", *The Christian Science Monitor,* March 07, 2011, www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race.

[2] Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies,* Vol. 35, No. 1 (February 2012), p. 7.

ont créée des unités de combats ou des commandements cyber. La cyber-guerre fait aussi son entrée dans les doctrines militaires des nations.

Il serait aussi dommage d'effacer des siècles d'évolution de la pensée stratégique et l'histoire militaire du 20e siècle pour affirmer que l'État est le seul acteur de la guerre moderne et donc de la cyber-guerre. Des acteurs non-étatiques font leur entrée dans l'art de la guerre, et compris, dans la cyber-guerre. Cela est notamment souligné par un rapport de Chatham House qui inclut les acteurs non étatiques dans sa définition de la cyber-guerre qui peut viser des cibles militaires, industrielles et civiles.(1) La cyber-guerre comprendrait donc cet aspect asymétrique que l'on perçoit dans l'attaque de l'Estonie par un groupe de patriotes russes. Et il serait, à notre sens, une erreur de considérer qu'une cyber-attaque n'aurait pas de répercussions physiques sous prétexte que, pour l'instant, il n'y ait pas beaucoup d'expériences relatant de telles conséquences. En effet, si aujourd'hui les exemples d'attaques informatiques causant des dommages matériels ne sont pas légion, l'attaque d'une centrale nucléaire par le ver Stuxnet dont a résulté la destruction de centaines de centrifugeuses, est un exemple qui pourrait prochainement se reproduire et serait potentiellement létales cette fois. Et la peur des autorités américaine d'une éventuelle attaque qui causerait des dommages physiques, justifie largement cette idée selon laquelle les cyber-attaques ne seront plus exclusivement un problème dans un espace virtuel mais s'étendront au monde tangible.

Cette peur n'est peut-être pas innocente, les services de sécurité américains sont connaisseurs en matière de cyber-armes, la peur qu'une attaque engendre des pertes matérielles peut cacher une capacité à produire une même attaque et la peur qu'un rivale ait aussi la possibilité d'en reproduire une. Que ce soit dans une attaque purement informatique ou comme complément à une attaque cinétique. Et si des groupes non étatiques pouvaient initier de telles attaques ?

(1) Paul Cornish, David Livingstone, Dave Clemente et Claire Yorke, "On Cyber Warfare", *Chatham House Report*, November 2010, p. 37.

2) Terrorisme, guerre asymétrique et infrastructures critiques

On remarque l'émergence de groupes de pirates informatique sur internet qui utilisent des techniques de haut niveau,(1) à côté des terroristes utilisateurs d'internet pour des buts essentiellement de propagande et de recrutement. Il est probable qu'un jour, ces organisations utilisent les systèmes d'informations pour des buts de terreur, le coût bas, l'anonymat et l'ouverture d'internet au monde peuvent constituer des éléments encourageant ce phénomène. D'un autre côté, les États deviennent de plus en plus vulnérables au fur et à mesure qu'ils relient leurs infrastructures critiques aux nouvelles technologies, et le sont encore plus quand ils les connectent à internet.(2)

Le cyber-terrorisme peut opérer de deux façons différentes : soit l'attaque physique des infrastructures cyber (la couche matérielle du cyberespace) par des armes réelles. Une autre manière d'accomplir les objectifs tracés sans recourir à l'attaque physique, est l'utilisation de l'attaque informatique pour saboter les systèmes d'informations.(3) En sabotant les systèmes d'informations, on met aussi hors service les éventuelles machines que ces systèmes contrôlent, ces machines sont diverses, elles peuvent même être d'extrême importance comme des satellites.(4)

Les risques présents quand on parle de cyber-terrorisme c'est les risques liés aux infrastructures critiques, pour Daniel Ventre, « *l'infrastructure critique désigne l'ensemble des biens, services, technologies, processus, systèmes, industries, essentiels au fonctionnement de la société et de son économie* »(5) les centrales nucléaires ; les systèmes aériens ; les systèmes de gestion des transports ; les

(1) Joshua E. Keating, "Shots Fired - The Ten Worst Cyberattacks", *Foreign Policy*, http://www.foreignpolicy.com/articles/2012/02/24/shots_fired (accessed May 9, 2015).

(2) Kevin Coleman, "The Increased Threat of Attacks on SCADA Systems", *Defense Tech*, Septmber 26, 2011, http://defensetech.org/2011/09/26/the-increased-threat-of-attacks- on-scada-systems/.

(3) On-Ching Yue, "Cyber Security", *Technology in Society*, Vol. 25 (2003), p. 566.

(4) Jan Kallberg, "Designer satellite Collisions from Covert cyber War", *Strategic Studies Quarterly*, Vol. 6, No. 1 (spring 2012), p.p. 124-137.

(5) Daniel Ventre, *cyberespace et acteurs du cyberconflit* (Paris : Lavoisier, 2011), p. 204.

systèmes de gestion des grands ports de commerce internationaux, sont tous considérés comme des infrastructures critiques.[1]

Ces infrastructures critiques peuvent être considérées comme des cibles potentielles pour les attaques terroristes. On parle de sabotage quand un acteur non étatique, ou un commando, attaque une cible dans le but de la détruire au lieu d'y recueillir des informations. Le cyber-sabotage est une phase qui reflète des dommages dans le cyberespace[2] suite à la mise en œuvre d'une volonté de nuisance. Plusieurs expériences relatent une attaque initiée par un individu ou un groupe d'individus sur des infrastructures critiques, parmi elles, l'attaque d'un pirate chinois sur des systèmes de distribution d'électricité aux États-Unis en 2003 causant des coupures d'électricité à grande échelle.[3]

La cyber-guerre est donc une guerre foncièrement asymétrique, les acteurs non étatiques y jouent un rôle déterminant dans certains cas, nous pensons notamment à l'offensive des cyber-patriotes russes sur l'Estonie et la Géorgie. Les conflits symétriques modernes ont déjà une dimension cyber, mais le cyber-terrorisme est encore jeune, tout comme la cyber-guerre, des académiciens pensent qu'il n'existe pas encore de cyber-terroristes. P. Singer et A. Friedman écrivent dans leur livre qu'il y a plus de 31 000 articles parlant de cyber-terrorisme, mais il n'existe aucun décès provoqué par celui-ci.[4] Le cyber-terrorisme ne serait qu'un concept sans ancrage dans le réel, tout comme la cyber-guerre. Toutes ces réflexions soulèvent un autre débat, celui sur les répercussions de cyber-attaques sur le réel, est ce qu'une attaque informatique doit provoquer un décès pour qu'elle soit terroriste ? Ne faut-il pas changer de paradigme quand on change d'environnement de réflexion ? Des questions qui restent en suspension, mais la réalité fait que des attaques massives sur des infrastructures critiques provoqueraient la terreur chez la population, une simple coupure électrique mènerait les citoyens à penser au pire, et donc à paniquer.

---

[1] Ibid.

[2] Jennifer L. Bayuk, et *al.*, op. cit., p. 150.

[3] Daniel Ventre, *cyberespace et acteurs du cyberconflit,* p. 206.

[4] Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: what everyone needs to know* (New York: Oxford, 2014), p. 96.

II. La Cyber-guerre comme Adjonction à la Guerre Conventionnelle

Des cyber-attaques émergent pendant les conflits internationaux, comme la réponse des hackers Serbes aux attaques de l'OTAN en 1999 en attaquant les sites internet de l'alliance, rendant leurs serveurs hors service pendant plusieurs jours.[1] Cela représente une réponse patriotique utilisant des moyens informatiques contre un agresseur extérieur, mais ces attaques peuvent être initiées par une armée organisée dans une opération militaire. Les cyber-attaques constitueraient dans ce cas un complément à une opération menée au sol ou dans un autre domaine, de la même façon que des bombardiers viendraient en soutien à des troupes au sol. C'est ce que nous allons voir à travers quelques expériences ou les cyber-attaques servaient de soutien aux opérations militaires. Nous prendrons l'exemple de l'attaque israélienne contre la Syrie, les cyber-attaques russes pendant la guerre de Géorgie en 2008, puis nous nous intéresserons à la vulnérabilité des armes conventionnelles aux cyber-attaques.

1) L'opération Orchard : la cyber-attaque comme soutien directe aux frappes cinétiques

L'opération Orchard est un exemple d'opération militaire ou les moyens informatiques soutiennent directement une frappe armée. En 2007, le Mossad aurait découvert que la Syrie abritait un programme nucléaire en infectant l'ordinateur d'un officiel syrien, en visite à Londres, par un cheval de Troie et aurait copié les informations secrètes que celui-ci contenait, parmi lesquels, les informations relatives à ce programme nucléaire lancé avec l'aide de la Corée du Nord.[2]

L'opération militaire a été menée en octobre 2007 par un bombardement sur un bâtiment à Deir-ez-Zor qui fut effectué par des F-15 et des F-16 israélien.[3] Pour que ces avions rentrent dans l'espace aérien syrien sans qu'ils soient

[1] Dan Verton, "Serbs Lunch Cyberattack on NATO", *FCW*, April 04, 1999, http://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx.

[2] Ofer Aderet, "Report: Mossad hacked Syrian computer to uncover nuke site", *Haaretz*, Novembre 02, 2009, http://www.haaretz.com/news/report-mossad-hacked-syrian-computer-to-uncover-nuke-site-1.4935

[3] John Leyden, "Israel suspected of 'hacking' Syrian air defences", *The Register*, 4 October 2007, http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

détectés et aussitôt intercepté par l'aviation syrienne, les services israéliens ont attaqués les radars syriens les rendant momentanément inopérants et incapable de détecter les avions israéliens. Ces radars furent achetés à la Russie, ils sont composés de capteurs reliés à un centre informatique. L'attaque fut initiée à l'intermédiaire de *Suter*, logiciel développé par BAE Systems et intégré dans les avions pour brouiller les radars de la défense aérienne. Ce logiciel peut pénétrer ce genre de systèmes et, entre autres, les rediriger pour indiquer de fausses cibles.(1)

2) Les cyber-opérations dans la guerre de Géorgie en 2008

En Aout 2008, l'armée géorgienne attaque les séparatistes de la province d'Ossétie du sud. La Russie répond militairement à l'attaque. En même temps, des cyber-attaques furent initiées sur des sites géorgiens comme ceux appartenant à des banques, au ministère des affaires étrangères ainsi que le site du parlement.(2)

Les attaques dont la Géorgie eut été prise comme cible étaient soit des défaçages soit des attaques DDoS. Comme le site du président géorgien qui fut cible d'attaques émanant d'un réseau d'ordinateurs zombis contrôlés à distance au cours des journées du 19 et 20 Juillet 2008, quelques semaines plus tard, le 12 août 2008, les sites des principaux médias, ministères et institutions géorgiennes sont encore attaquées. Des pages internet de ces sites sont défacées, publiant des photomontages de responsables géorgiens portant des uniformes nazis. Dans certains cas, les photos sont carrément remplacées par d'autres, comme ce fut le cas pour la photo du président géorgien Mikheil Saakashvili remplacée par celle d'Adolph Hitler. Pour rester audible, le gouvernement géorgien a choisi d'ouvrir des blogs, comme l'aurait fait un citoyen lambda, sur l'opérateur de blogs de Google : *Blogger*.

La Géorgie a accusé le gouvernement russe d'être responsable des cyber-attaques mais celui-ci a nié son implication. L'OTAN n'a pas trouvé d'indices sérieux prouvant l'implication du gouvernement russe dans ces cyber-attaques

(1) Ibid.

(2) Thomas Rid, "Cyberwar and Peace : Hacking Can Reduce Real-World Violence", *Foreign Affairs*, (November/December, 2013), https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace.

mais nous pouvons, toutefois, noter que ces cyber-attaques avaient l'air synchronisées avec l'entrée des chars russes en Ossétie du Sud.[1]

3) Les armes conventionnelles, vulnérables aux cyber-attaques

Les systèmes d'armes conventionnels et les systèmes informatiques des militaires sont tous vulnérables au cyber-attaques. C'est ce que prouve l'infection, en 2009, de systèmes informatiques des militaires de plusieurs pays par le virus *Conficker*.

Parmi les systèmes infectés, on retrouve ceux des avions Rafale français qui sont restés cloués au sol faute d'avoir pu télécharger leurs paramètres de vol.[2] Ce virus a pourtant fait l'objet d'une alerte par Microsoft qui a corrigé la faille exploité, et cela dès l'automne 2008. Cependant, l'armée n'a pas fait de mise à jour et ses systèmes sont restés vulnérables. Le virus n'a pas causé de dommages, mais il aurait pu le faire si volonté malicieuse il y avait, ce qui rend les systèmes d'armes modernes équipés d'informatique, extrêmement vulnérables à des infections informatiques, voir des cyber-attaques directes.

Les attaques directes sont en effet possibles comme nous l'avons déjà vu dans une attaque iranienne contre un drone américain en Afghanistan. C'était en 2011, un drone américain survolait l'espace aérien afghane, les iraniens ont manipulé ses coordinations GPS et lui ont fait croire qu'il est arrivé à destination et qu'il devait atterrir, il a donc atterrit en Iran au lieu de le faire dans une base militaire américaine.[3] Il est aussi arrivé que les systèmes d'exploitation des drones militaires américains soient infectés par des virus informatiques. Ces drones étaient stationnés dans la base de l'*Air Force* au Nevada, le virus avait infecté plusieurs systèmes classifiés et non classifiés dans la base militaire, il est même possible qu'il ait envoyé des informations collectées sur ces systèmes à un ordinateur se trouvant en dehors de la chaine de commandement, et cela par

---

[1] Nicolas Arpagian, *La Cyberguerre : la guerre numérique a commencé* (Paris : Magnar-Vuibert, 2009), p.p. 36-37.

[2] Jean-Dominique Merchet, "Les Armées Attaquées par un Virus Informatique", *Libération : Secret Défense*, 5 Février 2009, http://secretdefense.blogs.liberation.fr/2009/02/05/les-armes-attaq/

[3] Edouard Pflimlin, "Pirater un drone militaire, une menace réelle ?", *Le Monde : blog guerre des robots*, 06 Mai 2015, http://robots.blog.lemonde.fr/2015/05/06/pirater-un-drone-militaire-une-menace-reelle/.

internet.[1] Des critiques vont jusqu'à dire que les drones ont beaucoup de vulnérabilités, ils ne cryptent même pas les vidéos filmées envoyées aux troupes au sol, si bien qu'en 2009, ces vidéos ont été retrouvées dans les ordinateurs d'insurgés irakiens qui se les ont procuré à l'intermédiaire d'un logiciel à 26 dollars.[2]

Aujourd'hui, nous savons que le risque de piratage d'un drone ou d'un avion de combat est réelle, et cela représente une menace même si aucune armée n'a à déplorer de grandes pertes matérielles suite à une cyber-attaque. Mais cela reste une probabilité dans la conduite des guerres futures, nous savons que, désormais, nos armes sont susceptibles d'être piraté en plein combat, ce qui élargie considérablement le champ de réflexion sur la cyber-guerre.

4) L'informatique dans les conflits modernes

En plus des exemples donnés, il y a d'autres faits qui pourraient alimenter la réflexion sur le rôle des systèmes informatiques dans les conflits d'aujourd'hui et dans la conduite de la guerre moderne. L'épisode exceptionnel de la guerre de Géorgie, ou des attaques cinétiques sont accompagnées par des cyber-attaques, pourrait se reproduire. C'est ce qui a failli se produire en 2011 pendant la planification américaine de la guerre en Libye, on a conseillé à la maison blanche de mener des cyber-attaques contre les systèmes de défense aérienne libyens, qui menaçaient les avions de l'alliance atlantique, dans le but de les brouiller voir de les désactiver.[3] L'attaque aurait ciblée les réseaux libyens en charge de la communication militaire dans le but de perturber les transmissions et les radars d'alerte précoce pour que ceux-là n'aient pas la possibilité d'informer les batteries de missiles servant à la défense aérienne. Par peur que cela crée un précédent, l'option ne fut pas retenue.[4]

Cet exemple est une vraie question stratégique, la sécurité informatique des systèmes d'armes est devenue très importante car vulnérable, mais une autre

---

[1] Noah Shachtman, "Computer Virus Hits U.S. Drone Fleet", *Wired*, October 07, 2011, http://www.wired.com/2011/10/virus-hits-drone-fleet.

[2] Ibid.

[3] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya", *The New York Times*, October 17, 2011, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

[4] Ibid.

question moins technique se pose pendant les conflits internationaux ou même les disputes qui est, certes, de moindre importance mais qui devrait être prise en compte dans la sécurité des réseaux nationaux. La question est le cyber-patriotisme, ces groupes ou individus qui apparaissent pendant une dispute ou un conflit et qui attaquent les systèmes informatiques des institutions et sociétés du pays adverse. Le phénomène fut remarqué pendant l'offensive de cyber-patriotes russes envers l'Estonie en 2007 et la Géorgie en 2008, mais aussi quelques années plutôt, quand, en 1999, l'OTAN est intervenue en ex-Yougoslavie, des pirates serves ont attaqués les sites internet et les comptes e-mail de l'alliance les rendant inaccessible pendant plusieurs jours.

Telle est l'importance de la cyber-sécurité dans les conflits d'aujourd'hui, elle est multidimensionnelle, les conflits peuvent se dérouler dans un environnement complètement virtuel et ne pas en sortir, des attaques virtuelles peuvent aussi avoir des conséquences sur le monde réel et compris sur les systèmes d'armes. Ces attaques peuvent être initiées par un États-nation, ou bien par des groupes croyant à une cause et utilisant des systèmes d'informations à des buts offensifs pour la servir. La réflexion stratégique doit prendre en compte ce genre de variables comme faisant partie de la guerre moderne.

Paragraphe 2. LA GEOPOLITIQUE ET SES ARMES DANS LE CYBERESPACE

Dans le contexte de la cyber-conflictualité, le rapport entre l'attaque et la défense penche fortement en faveur de l'agression. Et mettre en œuvre une cyber-attaque est largement plus couteux qu'un attaque conventionnelle par missiles ou par déploiement terrestres. Une autre caractéristique qu'il faudrait souligner est l'anonymat qu'une cyber-arme bien codée fourni à son concepteur, contrairement aux armes conventionnelles.[1]

I. Les Armes dans le Cyberespace et les attaques à grande échelle

Il est intéressant d'examiner la cyber-conflictualité à travers les risques et les dommages liées aux cyber-armes. Celles-ci ne sont que les logiciels

[1] Jarno Limnéll, « Le Cyber Change-t-il l'art de la guerre ? », *Sécurité Globale*, N. 23 (2013), p. 34.

malveillants construits par des groupes organisés, voir Étatiques, dans le but d'espionner ou détruire des cibles à travers leur propagation via des réseaux informatique et internet puis l'infection de systèmes d'informations rivaux ou ennemis. Ces cyber-armes ne ressemblent pas aux virus, chevaux de Troie ou bombes logiques que l'on a défini dans un précédent chapitre, ils sont infiniment plus complexes et plus déstructures. On compare les cyber-armes aux missiles dit *tire-et-oublie* (*fire-and-forget*)[1] qui sont des missiles autonomes après lancements, les cyber-armes ont la même propriété, après lancement sur un réseau, il met du temps pour atteindre sa cible et se déclencher (comme une bombe logique). Nous examinerons des affaires liées a ces mêmes programmes malicieux qui ont été utilisés par des États dans le but d'atteindre des objectifs géopolitiques.

1) L'affaire Farewell et la riposte américaine

L'affaire Farewell s'est passée au début des années 1980 lorsqu'un agent soviétique, Vladimir Vetrov alias *Farewell*, proposait ses services aux agences de renseignements françaises. Il leur livra 4000 documents soviétiques secrets [2] qui furent exploités par les américains en ce temps pour délivrer une frappe à l'URSS.

A l'époque, l'Union Soviétique cherchait à acquérir des technologies informatiques en occident. Apprenant cela à travers les renseignements que Vetrov leur a fourni, la CIA eut placé une bombe logique dans un système de contrôle informatique dont l'URSS s'efforçait de se doter pour en équiper le gazoduc ourengoï-Sourgout-Tcheliabinsk, essentiel pour sa stratégie énergétique envers l'Europe. Des espions soviétiques ont donc volés cette technologie, infectée par un programme malicieux, à une entreprise canadienne. Une fois implanté sur le gazoduc en question se trouvant en Sibérie, le système échappa au contrôle de ses détenteurs provoquant, en juin 1982, la plus grande explosion non nucléaire connue jusqu'à maintenant.[3]

Le logiciel que la CIA a inséré dans le programme contrôlait les turbines, les pompes et les valves qui sont programmée à fonctionner normalement pour

[1] Thomas Rid, *Cyber War Will not Take Place* (New York, Oxford University Press, 2013), p. 36.

[2] « L'affaire Farewell », *France Info*, http://www.franceinfo.fr/emission/le-roman-des-espions/2014-ete/le-roman-des-espions-ete-2014-du-13-08-2014-08-13-2014-06-40 (consulté le 05/05/2014).

[3] Dominique Mongin, « Les Cyberattaques, Armes de Guerre en Temps de Paix », *Esprit*, No. 1 (janvier 2013), p. 34.

un temps déterminé puis de restaurer les options relatives à la vitesse des pompes et des valves et l'accélérer de façon à ce que le matériel ne supporte pas la pression.[1] C'est à ce moment-là que l'explosion se serait passée, malgré le silence des autorités soviétiques à l'époque.

2) Stuxnet, instrument de la géopolitique

Les vulnérabilités des systèmes de contrôles SCADA[2] (et les failles d'autres systèmes) furent exploités pour accomplir des intérêts stratégiques. En effet, la NSA et l'unité 8200 israélienne ont mis en place un ver informatique appelé Stuxnet dans le but d'attaquer les centrales nucléaires Iraniennes. L'opération fut appelée : *Olympic games*. C'est ce qu'a découvert, en 2010, l'entreprise de sécurité informatique biélorusse VirusBlok qui a détecté Stuxnet en examinant un ordinateur iranien qui redémarrait constamment sans raison apparente. L'entreprise lance une alerte pour ce ver d'une taille surprenante (environ 500 Ko) vue sa complexité (15000 lignes de codes et 4000 différentes fonctions)[3], il exploitait quatre failles zero-day alors que les vers habituels n'en exploitaient qu'une seule au maximum.[4] Des experts en sécurité informatique furent mobilisés et ont travaillés sur ce ver pendant trois mois dans les locaux de Symantec.

Stuxnet n'attaquait pas les systèmes SCADA, mais les utilisait pour avoir accès et contrôler les Automates Programmables Industriels (API). Un API est un ordinateur utilisé pour automatiser des processus comme des commandes sur des machines. Les API que Stuxnet attendait pour se déclencher sont ceux contrôlant les centrifugeuses utilisées dans les centrales nucléaires pour l'enrichissement de l'uranium. [5] Une fois les systèmes d'informations iraniens infectés, ceux-ci ne se sont pas aperçus de ce qui arrivait, parce que Stuxnet avait

---

[1] Thomas Rid, "Cyber War Will Not Take Place", p. 10.

[2] *Supervisory Control and Data Acquisition System* ou SCADA est un système de contrôle qui gère le fonctionnement de machines (valves, pompes, générateurs…) indispensables au bon fonctionnement d'installations dites « vitales » : réseaux de distribution de l'eau ou de l'électricité, réseaux de transport… il est donc installé dans les stations hydroélectrique, nucléaire ou dans des systèmes de contrôle aérien. Ce système fut, a plusieurs reprises, objet de cyber-attaques.

[3] Sean Collins and Stephen McCombie, « Stuxnet : the emergence of a new cyber weapon and its implications », *Journal of Policing, Intelligence and Counter Terrorism*, 7:1 (2012), p. 86

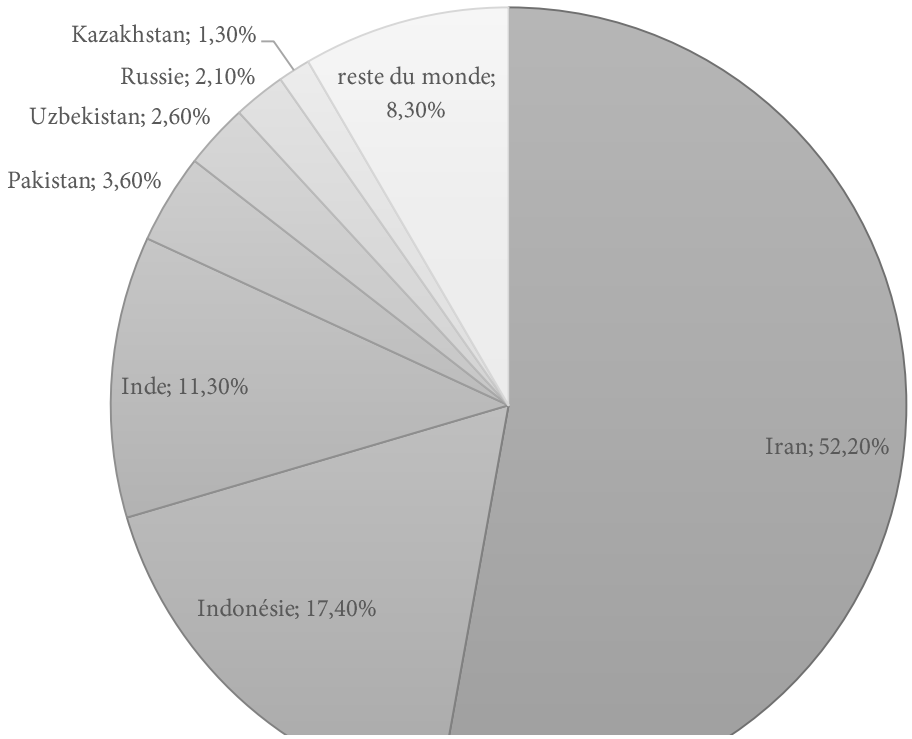
[4] Ibid., p. 85.

[5] Ibid.

deux segments, celui attaquant les centrifugeuses, et celui prenant le contrôle des moniteurs, montrant qu'il n'y a pas de problème particulier à signaler.

Les modes de propagations de Stuxnet sont multiples mais nous ne savons pas encore comment il a pu s'introduire dans les systèmes de la centrale nucléaire Iranienne, certains postulent sur la possibilité qu'il fût introduit par une clé USB infectée ou un dispositif similaire[1] après s'être installé sur des milliers d'ordinateurs de plusieurs pays et dont la majorité se trouvant en Iran (voir la figure 4).

Figure 4. Distribution des infections Stuxnet par pays les plus touchés



Source: Aleksandr Matrosov, Eugene Rodionov, David Harley, Juraj Malcho, Stuxnet Under the Microscope, Revision 1.31 (eset), http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

(1) Ibid.

3) *Flame* et le Cyber-espionnage

Programme de 20 Mo découvert en Mai 2012, Flame est connu pour être le ver informatique le plus complexe jamais construit,[1] et comme Stuxnet, il est visiblement conçu par un État et pour des buts géopolitiques et fait partie de l'opération *Olympic games*. Néanmoins, il est difficile de trouver la cible visée par ses concepteurs mais nous savons tout de même que c'est une cible au moyen orient. Il fait donc suite aux attaques de Stuxnet[2] et est codé par les mêmes concepteurs, mais celui-ci, contrairement à Stuxnet qui vise la destruction d'infrastructures, il vise l'espionnage.

Flame est un ver très complexe, encore plus complexe que Stuxnet, il a une taille de 20 mégabytes et 650 000 lignes de code.[3] Il a la capacité d'enregistrer en audio, prendre des captures d'écran, activer le Bluetooth d'un téléphone portable pour télécharger la liste des numéros de téléphone qu'il contient.[4] Le pays dans lequel il s'est le plus propagé est l'Iran, plus de 189 machines y sont infectés,[5] il serait surement l'État visé mais aucune donnée ne vient pour plus préciser la cible de l'attaque, ceux qui sont infectés sont très variables, individus, compagnie privée, agences gouvernementales, institutions académiques, etc.[6]

4) Shamoon, Destover et DarkSeoul

Shamoon est une cyber-arme d'attaque ciblée qui a la capacité de détruire des fichiers[7] et de rendre inutilisables des systèmes d'informations.[8] Elle fut

---

[1] Oleg Demidov & Maxim Simonenko, "Flame in Cyberspace", *Security Index: A Russian Journal on International Security*, 19:1 (2013), p. 69.

[2] "'End of the world as we know it': Kaspersky warns of cyber-terror apocalypse", *Russia Today*, June 06, 2012, http://rt.com/news/kaspersky-fears-cyber-pandemic-170/.

[3] Kim Zetter, *Countdown to Zero Day : stuxnet and the lunch of the world's first digital weapon* (New York: Crown Publishers, 2014), p. 276.

[4] "'End of the world as we know it': Kaspersky warns of cyber-terror apocalypse". Op. cit.

[5] Kim Zetter, op. cit., p. 277.

[6] Ibid., 278.

[7] The Shamoon Attacks Continue, Symantec Security Response, http://www.symantec.com/connect/blogs/shamoon-attacks-continue. (accessed 07 May, 2015).

[8] "The Shamoon Attacks", Symantec Security Response, http://www.symantec.com/connect/blogs/shamoon-attacks (accessed 07 May, 2015).

découverte par la société israélienne Seculert[1] et après analyse, des experts ont découvert qu'il serait une riposte iranienne.[2] Son mode opératoire consiste à infecter tous les ordinateurs d'un réseau puis les détruit après avoir collecté les noms des fichiers et les avoir envoyé vers un serveur inconnu.[3] En 2012, ce ver a attaqué les systèmes de l'entreprise énergétique Saoudienne Aramco et ceux de l'entreprise Qatari RasGas.[4] Aramco reconnait avoir été infecté par un virus mais affirme que sa production ne sera pas touchée.[5]

Shamoon a refait surface sous le nom Destover en utilisant un certificat Sony que ses concepteurs ont apparemment volé.[6] Un autre ver s'appelant DarkSeoul et ressemblant à Shamoon intégrant une charge destructrice s'était attaqué à des systèmes informatiques en Corée du Nord.

Ce qui est intéressant en analysant ces vers *a priori* différents, est le fait qu'il y ait des similitudes concernant les agissements de leurs concepteurs : la volonté de disparaître une fois le vol commis, une communication peu claire, des forfaits s'appuyant sur un événement « politiquement chargé » suggéré comme étant la cause de l'attaque (dans le cas de Sony, la sortie du film The Interview). Une analyse comparative de ces trois vers par l'entreprise de sécurité informatique Kaspersky conclu que la thèse d'un groupe de pirates sponsorisé

---

[1] "Seculert: 'Shamoon' malware covers its tracks by crippling infected systems after stealing data", Topnews, August 18, 2012, www.topnews.in/seculert-shamoon-malware-covers-its-tracks-crippling-infected-systems-after-stealing-data-2364028 (accessed May 07, 2015).

[2] Ed Blanche, "Cyber Wars", *Middle East Magazine*, issue 438 (December 2012).

[3] Paul Wagenseil, "Shamoon Spyware Searches, then destroys", NBCnew, http://www.nbcnews.com/id/48708157/ns/technology_and_science-security/t/shamoon-spyware-searches-then-destroys/#.VU5V0EiZaSp, (accessed May 07, 2015).

[4] "Sony Pictures malware tied to Seoul, "Shamoon" cyber-attacks", arstechnica, http://arstechnica.com/security/2014/12/sony-pictures-malware-tied-to-seoul-shamoon-cyber-attacks/, (accessed May 07, 2015).

[5] "Saudi Aramco says virus shuts down its computer network", *Reuters*, August 15, 2012, www.reuters.com/article/2012/08/15/us-aramco-virus-idUSBRE87E18S20120815.

[6] "'Destover' malware now digitally signed by Sony certificates", Kaspersky Lab, https://securelist.com/blog/security-policies/68073/destover-malware-now-digitally-signed-by-sony-certificates/ (accessed May 07, 2015).

par un État pourrait paraitre plausible. Ces trois vers seraient conçus par les mêmes pirates.[1]

5) Le patriotisme russe et la cyber-attaque envers l'Estonie

L'Estonie, pays balte membre de l'OTAN et ancienne république soviétique de 1.25 millions d'habitants à forte minorité russophone (29.6%),[2] utilisant les TIC et internet dans divers domaines : les services bancaires, réseaux électriques, les opérations gouvernementales, l'approvisionnement en eau, etc.[3] On en fait référence comme étant un e-État.[4] L'Estonie fut cible de cyber-attaques massives après le déplacement, le 30 avril 2007, d'une statue commémorative de la libération de l'Estonie par les troupes soviétique des mains de l'Allemagne Nazi. Cette statue est perçue par l'ethnie estonienne (majoritaire en Estonie)[5] comme un symbole d'oppression d'une époque passée, la minorité russophone perçoit ce déplacement de la statue du Park Tõnismägi (au centre de la capitale Tallinn) au cimetière militaire de Tallinn comme une marginalisation de leur identité ethnique.[6]

La cyber-attaque s'est opérée par attaque DDoS, les ordinateurs zombies viennent des quatre coins du monde : Egypte, États-Unis, Russie, etc. les attaques se sont étendues du 27 avril au 18 mai 2007,[7] les sites qui sont programmés pour recevoir 1000 visites par jour ont été submergés par 2000 pénétrations par seconde, ce qui leur était fatal. Cette attaque n'a touché que les sites gouvernementaux, bancaires, de partis politiques ou autres, mais aurait pu viser

---

[1] Kurt Baumgartner, "Sony/Destover: mystery North Korean actor's destructive and past network activity : Comparisons with Shamoon and DarkSeaoul", *Securelist*, December 4, 2014, https://securelist.com/blog/research/67985/destover/ (accessed May 07, 2015).

[2] "Estonia", CIA World Factbook, https://www.cia.gov/library/publications/the-world-factbook/geos/en.html, (accessed on May 06, 2015).

[3] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, Vol. 4 (Summer 2011), p. 51.

[4] Häly Laasme, "The Role of Estonia in Developing NATO's Cyber Strategy", *Cicero Fundation Great Debate Paper*, No. 18/08 (December 2012), p. 9.

[5] "Estonia", CIA World Factbook, ibid.

[6] Stephen Herzog, ibid.

[7] Peter W. Singer and Allan Friedman, *op. cit.*, p. 110.

des cibles plus sensibles comme le trafic aérien, l'approvisionnement en eau et en électricité ou encore les systèmes d'armes estoniens. (1)

L'instigateur de l'attaque n'est pas connu, une attaque par DDoS est difficile à tracer, le gouvernement estonien a accusé la Russie d'avoir préparé et exécuté l'attaque,(2) mais les experts techniques de la commission européenne et de l'OTAN n'ont pas pu prouver l'implication du Kremlin.(3) Par la suite, on aurait découvert l'implication d'un groupe de pirates informatiques pro-poutine qui se définissent comme des « patriotes ».(4) L'utilisation de pirates patriotes par un État comme la Russie est pratique puisque le gouvernement n'est pas officiellement une partie de l'attaque et peut donc nier son implication.

II. L'Impact de la Géopolitique sur la Cyber-sécurité Nationale

Comme nous l'avons vu, la géopolitique est source d'insécurité, dans le monde réel ou dans le cyberespace. Nous pouvons récapituler les idées que l'on a pu voir précédemment en quelques points essentiels.

1) Les risques d'escalade, vers un dilemme de (cyber-) sécurité ?

Le dilemme de sécurité est certes une thèse réaliste mais a une forte logique géopolitique : des États *rivalisant* de puissance et, après une course aux armements, rentrent en conflit pour des raisons de domination, de fautes de perception et de sentiment d'insécurité suscité par l'augmentation de la puissance d'un voisin ou d'un joueur géostratégique dans le cas de la course mondiale vers la domination.(5)

La question qui se pose dans ce contexte va dans le sens de la place qu'aura la compétition pour les cyber-armes et la cyber-puissance, dans un contexte plus

(1) Stephen Herzog, op. cit., p. 52.

(2) Aivar Pau, "Statement by the foreign minister Urmas Paet", *Eesti Päevaleht*, Mai 01, 2007, http://epl.delfi.ee/news/eesti/statement-by-the-foreign-minister-urmas-paet?id=51085399.

(3) Stephen Herzog, ibid.

(4) Peter W. Singer et *al*, op. cit., p. 111.

(5) Pour plus d'informations sur la théorie du dilemme de sécurité, voir : Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* vol. 30, No. 2 (January 1978), p.p. 167–174 ; et Robert Jervis. *Perception and Misperception in International Politics* (Princeton: Princeton University Press, 1978), p.p. 58-113.

général de course vers la puissance. La nature du cyberespace encourage plus l'attaque que la défense puisqu'il est plus facile et moins couteux d'attaquer des systèmes d'informations que de détecter et se défendre contre des cyber-attaques. L'attaquant a l'avantage de choisir le temps et la place de l'offensive alors que le défenseur doit être partout en même temps.(1) L'attaque de Stuxnet n'a peut-être pas seulement poussé les nations à augmenter leur niveau de cyber-sécurité mais les a encouragés à investir dans les capacités offensives dans le cyberespace.(2) Cette attaque a peut être ouvert une nouvelle ère de course aux cyber-armements puisque plusieurs nations sont engagées dans le développement de cyber-capacités militaires, on les estime à plus de 120 pays.(3) On assiste donc à ce que l'on pourrait appeler *la militarisation du cyberespace*, et du fait que les armées y sont présentes et que l'offensive est plus avantageuse que la défensive, cela à l'air de mener à une course générale pour les capacités militaires cybernétiques et delà, des cyber-conflits constants, soit dans un contexte de paix (sans déclaration de guerre) ou bien accompagnant des conflits conventionnels, les provoquant ou les approfondissant. C'est donc une prolifération de cyber-armes qui conduit les États qui ne sont pas préparés à se doter à leur tour de cyber-capacités offensives, c'est ce qui engendre une escalade ou un probable dilemme de sécurité comme on le voit dans la course aux armements conventionnel ou nucléaire.

2) Rayonnement culturel et sécurité sociétale

Le rayonnement culturel est, selon Friedrich Ratzel,(4) l'une des sept conditions pour l'expansion des nations. Le principe est d'exporter sa culture vers d'autres contrées pour gagner en influence. D'un point de vu sécuritaire, cela représente une menace d'ordre sociétal.

La sécurité sociétale est un concept développé par les chercheurs de l'École de Copenhague. Il est défini comme étant le développement soutenable des traditions, du langage, de la culture, religion, identité nationale et les coutumes de l'État. Or, le rayonnement culturel de certains acteurs influence grandement

(1) P.W. Singer and A. Friedman, op. cit., p. 154.

(2) Ibid., 157.

(3) Jeffret Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly, 2012), p. 161.

(4) Friedrich Ratzel est considéré comme le fondateur de la géopolitique. Pour lui, l'expansion territoriale est chose normale, voire obligatoire pour la survie de l'État. Un État qui ne suit pas une politique d'expansion est un État condamné à la décadence.

le mode de vie des autres. La généralisation d'internet et de la communication massive permet le rapprochement des personnes justement parce qu'elles se fréquentent constamment, les frontières s'épuisent et laissent place à la communication sans bornes, en cela, le cyberespace est le principal vecteur de propagation de ces cultures vers d'autres contrés dans le monde. Dans l'un de leurs ouvrages, Robert Keohane et Joseph Nye font appel à cette idée en disant que « *la transmission d'idées et d'informations, à travers l'immigration et le cyberespace, peut être culturellement menaçant et désorientant* ».[1]

3) La propagande

Dans la continuité de l'influence d'internet sur les sociétés, Le nouveau canal de propagande qu'est internet représente une menace pour certains gouvernements. On parle parfois de guerre de l'information. Internet est désormais, comme les médias traditionnels, sert à la fabrique du consentement, si bien que les États-Unis forment des blogueurs dans certains pays qui ne sont pas alignés sur sa politique, pour déstabiliser les régimes en place. La *National Endowment for Democracy* financée par le gouvernement américain a contribué à cela en encourageant certaines organisations comme *Otpor* qui forme des blogueurs impliqués dans les révolutions de couleurs en Europe de l'est et dans les « révolutions arabes ».

Cette menace peut être symétrique mais elle peut aussi être asymétrique puisque des organisations terroristes utilisent internet pour diffuser leurs idéologies et recruter de nouveaux militants, une stratégie de cyber-sécurité irait dans le sens de la détection de sites faisant l'apologie du terrorisme et les fermer, ou surveiller ses fréquentations.

4) Les infrastructures critiques et la sécurité nationale

La sécurité des infrastructures critiques est intrinsèquement liée à la sécurité informatique. En cas d'attaque sur une infrastructure critique, c'est une partie de la population qui pourrait paniquer et provoquer une déstabilisation du pays ou un ralentissement de l'économie. C'est donc un problème sérieux auquel il faut faire face. Ce que l'on a appris des attaques informatiques pendant

[1] Robert O. Keohane and Joseph S. Nye, Jr., *Power and interdependence*, 4th ed. (Longman, 2011), p. 231.

les dernières années c'est que les infrastructures critiques devraient gagner en sécurité si elles sont coupées d'internet.

5) Le cyber-espionnage et la sécurité de l'information

Les États sont toujours en quête d'informations stratégiques que ce soit dans le domaine du militaire, de l'économie ou de la politique. Le cyber-espionnage est une menace pour tous les gouvernements et entreprises. Beaucoup de nations ont compris l'avantage que les systèmes d'informations leur confère en matière de renseignement, et ils s'activent pour mettre en place des unités d'espionnage dans le cyberespace ou bien des logiciels servant à recueillir des informations et les envoyer au concepteur du programme.

SECTION 2. SECURITISATION DU CYBERESPACE AUX ÉTATS-UNIS

Nous avons vu comment la géopolitique engendre des menaces pour les États et comment une grande puissance comme les États-Unis conçoit sa sécurité nationale en termes de puissance et de domination. Pour assurer sa survie et sa sécurité (selon la théorie réaliste que l'on a adopté dans cette étude), une grande puissance entreprend d'augmenter sa puissance, cette puissance est perçue en termes militaires et économique.(1)

Le domaine du cyberespace se juxtapose au monde matériel et reprend ses propriétés. La réaction aux menaces existentielles, parmi lesquelles les cyber-menaces, sera d'augmenter les capacités militaires et économiques de la nation. La réaction aux cyber-menaces naissantes de rivalités géopolitiques est donc l'augmentation des cyber-capacités militaires pour faire face aux rivaux des États-Unis et ses ennemis désignés.

Paragraphe 1. GEOPOLITIQUE ET SECURITE NATIONALE DES ETATS-UNIS

Le cyberespace se juxtapose aux domaines réels. La cyber-sécurité des nations ne sont qu'une partie de leur sécurité globale. Et la vision stratégique des nations inclue une dimension cyber. Un rival dans la concurrence mondiale pour la puissance l'est aussi sur le cyberespace puisque tout le monde est engagé dans les mêmes processus d'interactions, et le cyberespace n'est qu'une partie de cet énorme mécanisme de l'histoire qu'est le grand jeu des nations. Devant un environnement stratégique de plus en plus hostile, Les États-Unis pensent leur sécurité à partir de ces principes.

(1) Voir: John Mearsheimer, *The Tragedy of Great Power Politics*.

I. La Vision Américaine de la Sécurité Nationale après le 11 Septembre

Les attentats du 11 septembre marquent un tournant décisif dans la politique étrangère et la stratégie militaire américaine. Cette fois, elle est tournée vers l'extérieur et les moyens qu'elle se donne sont clairement offensifs. Cela se passe dans un environnement stratégique particulier qui apporte son lot d'acteurs nouveaux et façonne une perception des menaces qui s'inscrit dans une continuité historique mais avec des changements sur le plan des réactions et des moyens de réaction. Les États-Unis sont plus offensifs que dans le passé et cela se justifie par le fait qu'elle ait la seule superpuissance existante. Mais cela ne durera pas longtemps puisque de nouveaux acteurs géostratégiques font leur (ré) apparition.

1) Les ennemis des États-Unis

Les ennemis désignés des États-Unis sont les groupes terroristes et les États-voyous (*Rogue states*). Les États voyous sont surtout l'Iran et la Corée du Nord qui sont en dehors de la mondialisation et de l'idéologie dominante promue par les États-Unis et ses alliés depuis la fin de la seconde guerre mondiale.

Pour les groupes terroristes, c'est une préoccupation récente qui a débuté après les attentats du 11 septembre 2001 perpétrée par Al-Qaida. Cette dernière est, dès lors, désignée comme la menace principale à la sécurité nationale des États-Unis et le gouvernement américain a annoncé son entrée en guerre contre « la terreur », menace mal définie que de se battre contre un sentiment. Après le 11 septembre, les États-Unis devient véritablement la première puissance mondiale après dix années d'hésitations. L'aspect offensif de sa doctrine militaire a clairement refait surface pendant cette période.

2) La sécurité américaine ou la vision géostratégique d'une hyperpuissance

Après la chute de l'Union Soviétique, les États-Unis devenaient ce que l'on qualifiait d'hyperpuissance,[1] c'est-à-dire une superpuissance sans rival. La

[1] Le concept d'hyperpuissance est forgé par Hubert Védrine

sécurité d'un tel État se mesure à son statut de grande puissance. Tous ce qui pourrait toucher ou susceptible de réduire de la puissance et de l'influence de cette nation est perçu comme une menace à ses intérêts et à sa sécurité nationale. Cette vision est issue des travaux géopolitiques du siècle dernier. Pour Friedrich Ratzel, pour qu'une nation survive il faut qu'elle gagne en puissance, la puissance est comprise, par les géo-politologues, en terme de territoires géographiques. Cette vision est reprise par la théorie réaliste des relations internationales qui voit dans l'intérêt des nations l'augmentation de leur puissance pour assurer leur survie, cette puissance est cette fois comprise en termes militaire et économique. C'est la vision développée, notamment, dans le livre de John Mearsheimer intitulé *The Tragedy of Great Power Politics*. Telle est la vision géostratégique[1] des États-Unis.

La sécurité nationale des États-Unis intègre cette dimension de puissance et de domination. Les acteurs qui lui disputent cette domination sont perçus comme étant des menaces. Pendant la guerre froide, la puissance qui rivalisait avec les États-Unis était l'ex-Union Soviétique qui lui disputait la prépondérance mondiale. Aujourd'hui, il en existe deux acteurs sérieux qui se veulent des rivaux pour la domination américaine, ces acteurs sont la Russie et la Chine, l'Europe étant un groupe non homogène et allié. Cette vision est explicitée dans les rapports sur la stratégie de sécurité nationale des États-Unis, notamment le rapport de Mai 2010.[2]

II. Les Cyber-capacités des Adversaires Potentiels des USA

Plusieurs nations se sont dotées d'unités militaires spécialisées dans la cyber-guerre et ont intégré la cyber-sécurité dans leurs doctrines militaires. Ces pays sont les traditionnelle puissances européennes et les pays émergents que sont la Russie, la Chine, l'Inde, le Brésil et d'autres encore.

1) Les cyber-capacités de la Chine

Il est de fait notoire que la chine ait entrepris des opérations de cyber-espionnage à grande échelle. On parle d'acteur le plus menaçant du

[1] Nous appelons géostratégie, la géopolitique des grandes puissances. C'est-à-dire la rivalité de pouvoir et d'influence entre les grandes puissances pour la supériorité au niveau mondial.

[2] "National Security Strategy", *Seal of The President of the United States*, May 2010, p. 7. https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

cyberespace.[1] Cependant, le gouvernement chinois a toujours nié les accusations portées contre lui, même après la publication de la stratégie américaine du cyberespace ou l'on considérait la Chine comme la plus grande cyber-menace contre la cyber-sécurité nationale américaine.

La chine aurait initiée plusieurs cyber-attaques visant le sabotage de systèmes d'informations ou l'espionnage sur des gouvernements et des sociétés privés occidentales. L'une des opérations les plus notoires est l'opération *Shadow Network* qui fut rapporté en avril 2010 et qui aurait touché les rapports sur les systèmes de missiles indiens, des lettres du Dalaï Lama et des rapports sur les mouvements des troupes de l'OTAN en Afghanistan.[2] Des entreprises américaines ont aussi dénoncé des attaques perpétrées contre elles en 2010, c'est l'opération *Aurora* qui a visé une trentaine d'entreprises américaine. Ces attaques sont rendues publiques par Google, l'une des victimes de l'opération. Des experts de la sécurité informatique parlent de cyber-attaque la plus sophistiquée envers des cibles non militaires.[3]

Comme beaucoup de nations aujourd'hui, la chine possède des unités de cyber-guerre. Elle en aurait trois types d'unités militaires opérationnelles : des force militaires spécialisées dans le combat sur réseaux qui sont chargées de cyber-défense et de cyber-attaques ; des experts venant d'organisations de la société civile travaillant dans les services de renseignements chinois (ministère de la sécurité de l'État), ils sont autorisés à conduire des opérations militaires dans le cyberespace ; des entités externes comme des organisations ou des pirates individuels ayant la capacité de mobilisation pour une cyber-opération militaire, ils sont sponsorisés par le gouvernement chinois.[4]

Une unité chinoise appelée « l'unité cyber 61398 » est suspectée d'avoir conduit des opérations contre les compagnies, organisations et agences gouvernementales américaines pour recueillir des informations sur des

---

[1] Anthony Capaccio, "China Most Threatening Cyberspace Force, U.S. Panel Says", *BloombergBusiness*, November 6, 2012, http://www.bloomberg.com/news/articles/2012-11-05/china-most-threatening-cyberspace-force-u-s-panel-says.

[2] Daniel Ventre, *cyberespace et acteurs du cyberconflit*, p. 170.

[3] Kim Zetter, "Google Hack Attack was Ultra Sophisticated, New Details Show", *Wired*, January 14, 2010, http://www.wired.com/2010/01/operation-aurora/.

[4] Mohit Kumar, "China Finally Admits it Has Army of Hackers", *The Hacker News*, March 19, 2015, http://thehackernews.com/2015/03/china-cyber-army.html/. (accessed May 18, February 2015).

infrastructures critiques américaines incluant des pipelines, lignes de transmissions, etc.

Même s'il existe beaucoup d'exemples de cyber-attaques chinoises sur les États-Unis, ces attaques ne visent pas le sabotage de systèmes d'informations ou d'infrastructures critiques mais plutôt le recueil de renseignements militaires, technologiques et économiques.

2) Les cyber-capacités de la Russie

De tous les pays, la Russie est sans doute celui qui est le plus actif sur le cyberespace contre ses adversaires : Tchétchénie, Kirghizistan, Estonie, Lituanie, Géorgie,(1) tous ont essuyés des cyber-attaques venant du gouvernement russe ou de ses cyber-patriotes. Traditionnellement, c'est la Chine qui eut été désignée comme la principale menace à la cyber-sécurité des États-Unis, mais en 20015, le Rapport de la Direction du Renseignement National a désigné la Russie comme la cyber-menace la plus sérieuse.(2)

La Russie développe un programme militaire pour le cyberespace. Cela est rendu officiel en 2014 par une annonce du gouvernement russe que ses cyber-unités militaires seront opérationnels d'ici 2017. Ces unités entendent, selon les officiels russes, défendre les forces armées et les infrastructures critiques russes.(3) Cette initiative a fait suite à des attaques dirigées envers la Russie, comme les virus *Red October* et *Rocra* qui ont infecté les systèmes du gouvernement russe et volé des documents secrets en lien avec les files diplomatiques et les organisations gouvernementales et scientifiques.(4)

Les unités de cyber-guerre russes ne sont pas aussi nouvelles que cela, elles remontent aux années 1980 quand la Russie a fait sa Révolution dans les Affaires

(1) Jeffret Carr, op., cit., 161.

(2) "Worldwide Threat Assessment of the US Intelligence Community", James R. Clapper (Washington DC: Direction of National Intelligence, February 24, 2015), p.p. 2-3.

(3) "Russia to Create Cyberwarfare Units by 2017", *Sputnik*, January 1, 2014, http://sputniknews.com/military/20140130/187047301.html.

(4) Kevin Fogarty, "Russian Cyberwar Force Intensifies 'net Arms Race", *Dice*, February 1, 2014, http://insights.dice.com/2014/02/01/russian-cyberwar-force-intensifies-net-arms-race/, (accessed Mary 18, 2015).

Militaires. Depuis, elle cherche des options pour les attaques informatiques comme des bombes logiques, des virus ou toutes sortes de cyber-armes.[1]

III. Les Cyber-menaces Dans la Vision Américaine

L'utilisation à grande échelle des systèmes d'informations donne un avantage sérieux à une nation en matière d'organisation et de communication, néanmoins, à cause des vulnérabilités intrinsèques au cyberespace, cet avantage comporte une source de menace pour la nation. Cette vulnérabilité se ressent sur différents niveaux, les infrastructures critiques de la nation, le secteur privé, ainsi que les institutions publiques et militaires. Si elle est exploitée par un acteur malicieux, ces vulnérabilités peuvent constituer un danger pour la nation. C'est le problème des États-Unis, puissance mondiale en matière technologique, économique et militaire, on parle d'hyperpuissance après la fin de la guerre froide, cet État présente des vulnérabilités sur tous les niveaux, et il en a pris conscience depuis les années 1990.

1) Le cyberespace, la source de menace la plus sérieuse aux États-Unis

En 2013, dans son rapport annuel sur les menaces que la communauté de renseignement fait face, James R. Clapper, Directeur du Renseignement National (*Director of National Intelligence*) classe le cyberespace comme la première source de menaces à la sécurité nationale des États-Unis.[2] Les cyber-menaces sont dès lors considérées comme étant encore plus dangereuses que le terrorisme et la prolifération des armes de destruction massives considérées une année plus tôt comme les menaces les plus sérieuses pour les États-Unis.[3]

---

[1] Jeffrey Carr, op. cit., p. 162.

[2] United States of America, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, March 12, 2013,

[3] United States of America, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, January 31, 2012, p.p. 1-7.

Les cyber-menaces sont passée, en l'espace d'une année, de la troisième place en 2012 à la première place en 2013. Elles gardent cette place dans les rapports de 2014[1] et de 2015.[2]

2) Cyber-espionnage

Les américains font face à la menace d'espionnage dans le cyberespace. L'objectif de l'espionnage dans ce domaine est le même que dans les domaines conventionnels : le vol de secrets militaires, industriels et politiques. Tous les pays pratiquent l'espionnage et le cyber-espionnage à des degrés différents.[3] Selon La commission du congrès américain sur l'économique et la sécurité américano chinoise évalue les pertes causées par le cyber-espionnage et la cyber-criminalité aux États-Unis entre 24 et 120 millions de dollars, ce qui représente entre 0.2% et 0.8% du PIB américain.[4]

La Chine est reconnue comme la menace la plus sérieuse à la sécurité des États-Unis en matière de cyber-espionnage. Ce pays active pour collecter des informations utiles en matière de stratégie et d'industrie. Les États-Unis ont découverts beaucoup de systèmes compromis par des hackers chinois, ces systèmes appartienne, entre autres, au département de la défense. Les informations obtenues sont très sensibles, elle englobe les systèmes d'armes américains comme le F-35, F/A- 18 fighter, le P-8A, l'hélicoptère Black Hawk, le système Aegis de défense anti missile balistique et autres.[5]

---

[1] "Worldwide Threat Assessment of the US Intelligence Community", James R. Clapper (Washington DC: Direction of National Intelligence, January 29, 2014), p. 1.

[2] "Worldwide Threat Assessment of the US Intelligence Community", James R. Clapper (Washington DC: Direction of National Intelligence, February 24, 2015), p. 1.

[3] Daniel Ventre, *cyberespace et acteurs du cyberconflit*, p. 170.

[4] "Report to Congress", U.S.-China Economic and Security Commission, 130th Congress, November 2014, p. 68.

[5] Ibid., 295.

Paragraphe 2. REACTION AMERICAINE AUX CYBER-MENACES EXISTENTIELLES

Dès les années 1990, les États-Unis se voient menacé par des « acteurs occultes » et agressifs. Ces menaces se sont développées dans les années 2000 et se sont faites plus incessantes, [1] le département de la défense devait s'adapter au nouvel environnement par des réformes institutionnelles et des décisions politiques à même de répondre à un environnement stratégique plus hostile ou les agresseurs sont anonymes. L'adaptation s'est faite au niveau institutionnel et doctrinal pour assurer une cyber-sécurité nationale qui dépend fortement des tendances géopolitiques dominantes et les stratégies de puissance des rivaux.

I. Organisation Institutionnelle de la Cyber-Défense

Pour s'adapter au nouvel environnement stratégique, les États-Unis ont développé des institutions pour s'adapter et sécuriser le cyberespace national et ses réseaux sensibles. Parmi ces institutions : le *Cyber Command* qui est au centre de la cyber-stratégie américaine.

1) Les organismes de cyber-défense avant le Cyber Command

Avant le cyber command, les États-Unis disposaient déjà de branches dédiées aux opérations de type cyber-guerre dans ses différentes armées. Parmi les premiers organes militaires chargés de la cyber-défense : Le *Joint Task Force-Global Network Operations* (JTF-CNO) fut créée en décembre 1998 par le département de la défense pour protéger ses systèmes informatiques et ses réseaux contre les attaques.[2]

Les différents commandements des armées se sont dotés d'unités de cyber-guerre. Pour la *Navy*, la 10ème flotte est le commandement qui s'occupe de la cyber-guerre. Désormais il s'appelle : *U.S. Fleet Cyber Command*

---

[1] Chris C. Demchak et François-Bernard Huyghe, « Organiser sa Défense à l'ère du Cyberconflit : le point de vu Étasunien », *Revue Internationale et Stratégique*, No. 87 (2012/3), p. 106.

[2] "Joint Task Force on Computer Network Defense Now Operational" Department of Defense News Release No. 658-98 (Washington DC: Department of Defense), December 30, 1998. http://www.defense.gov/Releases/Release.aspx?ReleaseID=1945.

(FLTCYBERCOM). Dans l'*air force*, on a créé l'*Air Force Cyber Command* ou bien l'unité 24 (*24th USAF*). Et enfin, pour l'armée de terre : l'*Army Cyber Command* (ARCYBER).

2) United States Cyber Command (USCYBERCOM)

Le 23 Juin 2009, le département de la défense américain a décidé de la création d'un commandement militaire pour le cyberespace sous l'égide du commandement stratégique américain (USSTRATCOM) appelé : *United States Cyber Command*, ou le commandement cyber des États-Unis, abrégé : USCYBERCOM.[1] Il a été décidé par les autorités américaines que le commandant en chef de l'USCYBERCOM serait la personne du directeur de la National Security Agency (NSA).[2]

USCYBERCOM est chargé de la défense des réseaux du département de la défense et ses informations numériques, assure et promeut des réseaux de communication et d'information sécurisés ainsi que leur défense contre les éventuelles intrusions, perturbations ou attaques ; il est chargé de la préparation et la conduite des opérations militaires dans le cyberespace et de contrer les cyber-menaces qui représentent un danger pour les réseaux militaires américains afin d'assurer un accès sécurisé au cyberespace et ses ressources.[3] En plus de cela, les autres unités cybernétiques comme l'*army's ninth sign command* ou la *navy's tenth Fleet* sont regroupé au sein du USCYBERCOM.

Il prend en charge plusieurs institutions en rapport avec l'armée dans le cyberespace comme l'Army Forces Cyber Command (ARFORCYBER) ; Air Forces Cyber (AFCYBER) ou 24th USAF ; Fleet Cyber Command (FLTCYBERCOM) ; et la Marine Forces Cyber Command (MARFORCYBER).[4] Le but derrière sa création est la dominance sur tous les terrains d'affrontements,

---

[1] United States of America, The Department of Defense, *U.S. Cyber Command Fact Sheet*, May 25, 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

[2] Sean Gallagher, "White House: NSA and Cyber Command to stay under one boss", *Arstechnica*, December 13, 2013, http://arstechnica.com/tech-policy/2013/12/white-house-nsa-and-cyber-command-to-stay-under-one-boss/.

[3] *U.S. Cyber Command Fact Sheet, ibid.*

[4] Ibid.

le concept utilisé est *full-Spectrum dominance*, ou la supériorité sur tous les types de théâtres.

Le Cyber Command s'est doté d'une armée cybernétique en 2010 : l'*U.S. Army Cyber Command* (ARCYBER). Si l'intention derrière la création, en 1998 du JTF-CNO était purement défensive, la création de l'ARCYBER reflète clairement une volonté offensive et de domination. Cela se comprend aussi à travers la doctrine militaire des États-Unis que nous allons traiter plus tard.

3) Organisation institutionnelle de la cyber-sécurité civile

Plusieurs institutions et organisations furent créées pour se protéger des cyber-menaces aux États-Unis. L'une d'elle : l'*Information Technology Information Sharing and Analysis Center*, fut une initiative de huit entreprises privés américaines qui s'engagent à coopérer entre elles et avec le gouvernement fédéral pour identifier, voire contrer les agressions en ligne.[1]

On s'est aussi occupé des infrastructures critiques en créant le *National Infrastructure Assurance Council* qui conseille le président des États-Unis sur la sécurité des infrastructures critiques.[2]

II. La Cyber-stratégie de sécurité et de défense américaine

Sur le plan doctrinal, plusieurs rapports de la défense et des agences de renseignement américaines travaillent pour construire une réflexion sur le cyberespace comme un domaine où les opérations militaires sont possibles. Cela souligne à la fois la menace d'une attaque militaire sur les systèmes américains, ainsi que la nécessité de développer des cyber-capacités militaires.

1) Les objectifs de la stratégie du département de la défense

En avril 2015, le Département de la Défense américain publie un document ou il présente ses objectifs en matière de stratégie cybernétique, il formule cinq objectifs :

Le premier objectif consiste en la construite et le maintien de capacités et de forces en alerte pour la conduite d'opérations dans le cyberespace, pour cela,

[1] Nicolas Arpajian, *La Cyberguerre*, p. 200.

[2] Ibid.

le gouvernement américain a investi dans le recrutement d'un personnel qualifié, la construite de systèmes de contrôle et de commande et développe les capacités nécessaires pour opérer dans le cyberespace.[1]

Le deuxième objectif consiste à défendre et sécuriser les réseaux informatiques du département de la défense en identifiant les cyber-attaques et les arrêtant.[2]

Le troisième objectif vise à se préparer à la défense de la patrie et de ses intérêts vitaux de cyber-attaques pouvant avoir des conséquences significatives, cela en coopérant avec les autres agences gouvernementales, le secteur privé et les partenaires alliés.[3]

Le quatrième objectif est la construction et le maintien de plusieurs plans et options cyber dans le but de les utiliser pour le contrôle de l'escalade de conflits et façonner les différents niveaux d'un environnement conflictuel.[4]

Le dernier objectif de cette stratégie est la construction et le maintien de forts partenariat et alliances internationales pour dissuader les menaces partagées et pour améliorer la sécurité et la stabilité internationale.[5]

2) Nouveautés de la stratégie de cyber-défense

Ce document est plus explicite que la précédente version publiée en 2011,[6] particulièrement sur les cyber-capacités offensives. Cette fois, les États-Unis formulent leur souhait de construire des forces armées dans le cyberespace dans le but de dissuader leurs adversaires. Ceci, en augmentant le niveau de coopération entre les services de renseignement et le secteur privé pour améliorer les capacités d'attribution des cyber-attaques qui constitue un vrai problème dans le domaine du cyberespace.

---

[1] "The Department of Defense Cyber Strategy" (Washington. D.C: the Department of Defense, 2015), p. 13.

[2] Ibid.

[3] Ibid., p. 14.

[4] Ibid.

[5] Ibid., p. 15.

[6] Voir: "The Department of Defense Cyber Strategy" (Washington. D.C: the Department of Defense, 2011).

La construction de capacités militaires pour la conduite des cyber-opérations est aussi explicite, le département de la défense entend augmenter ses capacités pour pouvoir mener des cyber-opérations dans le but de perturber les réseaux militaires et les infrastructures des adversaires.(1)

Ainsi, nous remarquons plusieurs points à travers ce nouveau rapport, les opérations offensives dans le cyberespace sont officiellement reconnues par le gouvernement américain comme faisant partie de leur puissance militaire. Ces opérations peuvent être conduites non seulement pendant un conflit l'opposant à un adversaire mais aussi au cours de tensions internationales.

3) Le cyber-espionnage américain

La stratégie nationale de renseignement désigne quatre secteurs d'activité de la communauté de renseignement américain : le contre-espionnage, le contre-terrorisme, la lutte contre la prolifération des armes de destruction massive et enfin, la recherche de renseignements en matière de cyber-menaces.(2) Aussi, nous remarquons que les cyber-menaces sont prise au sérieux par les autorités américaines, et particulièrement dans les milieux de renseignement, et adaptent leurs appareilles de renseignement constamment pour répondre à ce qu'ils considèrent comme étant l'intérêt national des États-Unis, cela requiert le recueil de renseignements en tout genre, c'est même considéré par la CIA comme sa préoccupation première.(3)

Plusieurs programmes de renseignements ont vu le jour et ont été dénoncés par nombre de journalistes d'investigation ou des donneurs d'alertes puisqu'ils constituaient une atteinte à la vie privée des citoyens américains. Mais au-delà de cela, ces programmes constituent un avantage stratégique en matière d'informations en tout genre. Parmi ces programmes on trouve ceux révélés par Edward Snowdon(4) comme X-Keyscore, Tempora, Bullrun, Boundless informant ou encore Prism.

---

(1) "The Department of Defense Cyber Strategy", 2015, p. 5.

(2) "The National Intelligence Strategy of the United States of America" (Washington, Director of National Intelligence, 2014), p. 6.

(3) Andy Greenberg, "Cyberespionage Is a Top Priority for CIA's New Directorate", *Wired*, March 9, 2015, http://www.wired.com/2015/03/cias-new-directorate-makes-cyberespionage-top-priority/.

(4) Edward Snowden est un ancien employé de la CIA et de la NSA qui a révélé des informations classifiées des agences de renseignement américain.

Cependant, Si ces programmes sont relativement récents, la surveillance électronique de masse remonte à la fin de la seconde guerre mondiale quand les États-Unis ont signé un accord d'espionnage des communications avec le Royaume-Uni. Visant à l'interception des signaux électromagnétique, cet accord est appelé UKUSA (*United Kingdom – United States of America Agreement*), il est plus tard rejoint par le Canada, l'Australie et la Nouvelle Zélande.(1) Les différentes parties de l'accord sont chargées de recueillir des informations, chacune, sur une partie différente du globe. Cela constitue le plus grand réseau de surveillance du monde.(2) Le Réseau Echelon constitue une partie décisive du système de surveillance globale géré par l'UKUSA, sa tache se résume ne l'interception et le traitement des communications relayées par des satellites de communication commerciale. Des branches de celui-ci s'occupent de l'interception de messages circulant sur internet, à travers des câbles sous-marins, par transmissions radio. Ces gouvernements se servent d'équipements installés dans les ambassades, des satellites en orbite pour mettre sur écoute des signaux sur toute la surface de la terre. L'interception des signaux électroniques servait dans la rivalité contre l'Union Soviétique pendant la guerre froide, après la fin de celle-ci, on prétexta de nouvelles priorités comme le terrorisme, le trafic de drogues et la prolifération des armes, ce qui a permis d'étendre la surveillance aux principales artères de communication du monde.(3)

Programme plus récent : Prism, est, comme Echelon, géré par la NSA. Il a été révélé par Edward Snowden et publié par le *Washington Post* en juin 2013. Actif depuis 2009, ce programme oblige les neuf opérateurs les plus importants en matière de télécommunication comme Microsoft, Yahoo, Google, Facebook, Skype, etc. à ouvrir l'accès de leurs serveurs aux services de renseignements américains,(4) ceux-là auraient donc un accès direct aux mails, documents, photos, vidéos chats, etc. des clients de ces opérateurs, et ce de façon continue.

D'autres programmes d'espionnage électromagnétique et particulièrement les données circulant dans les réseaux informatiques dans le monde, parmi lesquels on trouve XKeyscore qui est aussi géré par la NSA et

(1) Duncan Cambell, *Surveillance Électronique Planétaire* (Paris : Editions Allia, 2001), p.14.

(2) Ibid., p. 8.

(3) Ibid., p. 18.

(4) Éric Cobast, *Que sais-je : les mots qui ont fait 2013* (Paris : Presses Universitaires de France, 2014), p. 36.

aurait la capacité de collecter toutes les données des utilisateurs quand ils envoient leurs e-mails ou visitent des sites, ainsi que leurs métadonnées.[1] Ces programmes d'espionnage auraient la capacité de casser les systèmes de chiffrement de données comme le SSL, le TLS, et reconnaitrait les utilisateurs même s'ils sont derrière un proxy ou un réseau VPN. Un exemple de ce genre de programme est *Bullrun*.[2]

Les services de renseignement américain arrivent aussi à exécuter des opérations d'espionnage dans le cyberespace. Le groupe *Equation* qui a conçu nombre des cyber-armes les plus sophistiquées jamais découverte,[3] serait une unité de la NSA. Ces cyber-armes visent à recueillir des informations dans les systèmes informatiques des cibles qui sont des adversaires des États-Unis mais aussi des alliés.

Une grande partie de la cyber-insécurité des nations est donc causée par les rivalités de pouvoir et d'influence qui fait que des États concourent pour la construction de cyber-capacités militaires dans le but de se protéger et d'être prêt à l'offensive en cas de besoin. Cette culture de l'offensive est susceptible de se développer davantage dans le cyberespace étant donnée la nature de celui-ci qui fait que l'offensive est plus facile et moins couteuse que l'organisation de la cyber-défense qui peut se révéler onéreuse et peu pratique. On pourrait spéculer sur l'efficacité des leçons apprises de l'âge nucléaire en investissant dans une dissuasion cybernétique mais cela pourrait faire tomber le monde dans un dilemme de sécurité qui serait dommageable pour tout le monde.

Les États-Unis ont su s'adapter au nouvel environnement que les technologiques informatiques ont créé. Leur avance technologique remarquée depuis la guerre du golfe n'a cessé de croitre. Cependant, l'utilisation de ces

---

[1] Glenn Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", *The Guardian*, July 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data/

[2] James Ball, Julian Borger and Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security", *The Guardian*, September 6, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security/.

[3] "Equation: The Death Star of Malware Galaxy", *Securelist*, February 16, 2015, https://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/, (accessed May 16, 2015).

technologies et des vulnérabilités qui vont avec font qu'ils sont plus menacés que les autres nations. Les cyber-menaces auxquels ils font face comme le cyber-espionnage que leurs rivaux conduisent envers eux, l'oblige à investir encore plus dans ses cyber-capacités militaires. C'est ce qui les a conduit à la création du CYBERCOM et *ARCYBER* pour se protéger des cyber-menaces, sécuriser les réseaux et les systèmes d'informations de la défense, ainsi que de conduire des opérations offensives dans le cyberespace. Les États-Unis sont désormais des prédateurs plus que des victimes dans le cyberespace.

CONCLUSION

Le cyberespace est une source de menaces à la sécurité des personnes, des groupes -comme les entreprises, et des États. Cette menace est permise par la vulnérabilité inhérente aux systèmes informatiques qui fait que des failles logicielles sont constamment découvertes et les programmes malveillants augmentent de façon exponentielle et ce pour plusieurs raisons, notamment à cause des défis que certains individus se lancent en créant des programmes qui provoqueraient le maximum de dommages possible, et cela est encouragé par l'anonymat que le cyberespace leur confère. Le résultat fait que tous les logiciels sont susceptibles d'être piratés, ce qui donne à l'attaquant une brèche à exploiter dans le système pour y entrer et consulter les informations qui y sont contenues, les modifier ou les supprimer voir même mettre la machine hors d'usage. Si le système d'information se trouve dans une infrastructure critique, l'attaquant pourrait manipuler les données dans le but de saboter entièrement l'infrastructure. C'est cela qui représente une menace. Des informations sensibles de gouvernements ou d'entreprises sont contenues dans des systèmes informatiques et sont exposées aux cyber-attaques, la même chose peut être dite des infrastructures critiques dont les machines peuvent être modifiées et saboter le bon fonctionnement de l'infrastructure.

Aujourd'hui, des systèmes informatiques sont utilisés pour toutes sortes de choses, stockage de données par divers organismes, y compris les plus importants dans un État comme ses infrastructures critiques et son secteur militaire. Les vulnérabilités inhérentes aux systèmes informatiques sont maintenant projetées sur les infrastructures et les secteurs qui utilisent ces systèmes, ce qui fragilise certains secteurs où l'activité doit être protégée de tout regard extérieur et intention nuisible.

Les acteurs principaux des relations internationales se font concurrence pour la puissance et la domination, ils ont trouvés dans le cyberespace un nouveau terrain d'expansion et un domaine qui, si bien utilisé, leur confère un avantage sur les autres. C'est pour cela que les conflits modernes intègrent déjà une dimension cyber, une dispute entre deux nations engendre des attaques informatiques initiées par leurs populations, les cyber-patriotes russe pendant l'attaque des réseaux estoniens en sont un exemple. Des opérations militaires sont aussi accompagnées par des cyber-attaques, c'est ce que l'on a pu constater pendant le conflit russo-géorgien et qu'on ait failli le revivre pendant l'intervention de l'OTAN en Libye.

Ceci se reproduira très certainement à l'avenir, d'autant plus que les systèmes d'armes sont aussi vulnérables étant donné leur intégration de la technologie informatique. La menace qu'un drone ou qu'un avion de combat ait une infection virale sera probablement plus sérieuse à l'avenir. Avec la course aux cyber-armes, celles-ci sont aussi appelée à se propager dans le monde rendant les États encore plus vulnérables, les cyber-attaques n'auraient pas seulement des répercussions sur les couches virtuelle du cyberespace mais aussi sur le réel. Les États sont conscients de cela et réagissent en augmentant leurs cyber-capacités militaires pour faire face aux adversaires de plus en plus nombreux à cause de l'anonymat que ce même cyberespace leur confère.

Le cyberespace se soumet donc aux lois des relations internationales, celles de la puissance et la domination. Des États recrutent tous les jours des pirates informatiques, essaient de trouver de nouvelles failles dans les systèmes des adversaires pour les espionner, voire saboter leurs systèmes et leurs infrastructures critiques. Cela s'inscrit dans des cadres plus généraux, en effet, l'espionnage, les opérations spéciales ou le sabotage existaient avant l'apparition de l'informatique et du cyberespace. Les États ne font que s'adapter à un environnement plus complexe dans lequel le recueil d'informations et le sabotage peuvent être effectués, pour une partie, à travers des systèmes d'informations. Cela s'insère dans ce cadre ou les nations se font concurrence pour la puissance, pour la survie et parfois, pour la proéminence internationale en considérant le cyberespace comme un environnement de rivalité, à côté des environnements plus traditionnels comme la terre, la mer, l'air et la stratosphère. Cette rivalité est accompagnée par des stratégies d'attaque et de défense. C'est ce qu'est la géopolitique, des rivalités de pouvoir et d'influence suscitant des stratégies de conquête pour satisfaire un intérêt national quelconque, et des stratégies de défense pour se protéger de ces conquêtes puisque considérées comme des menaces.

La réaction des États-Unis à ces cyber-menaces s'est faite en trois temps : adaptation institutionnelle ; augmentation des cyber-capacités ; prédation.

En premier lieu, les États-Unis se sont adaptés institutionnellement au nouvel environnement en créant des organismes en charge de la cyber-sécurité et un commandement militaire pour le cyberespace : le Cyber Command. Il est

en charge de la sécurité des réseaux informatiques du département de la défense. Des efforts sont aussi été fournis pour booster la sécurité des infrastructures critiques et le secteur privé, pour cela, le gouvernement américain a eu une approche inclusive en incitant le secteur privés et les infrastructures critiques à coopérer avec les institutions militaires.

Deuxièmement, l'augmentation des cyber-capacités militaires en recrutant et en formant des pirates informatiques de haut niveau qui sont ensuite intégrés dans les différents organismes militaires et de renseignement pour déceler les failles informatiques des adversaires et construire des cyber-armes. La logique étant, pour assurer sa sécurité et sa survie, un État doit investir dans sa puissance et sans cesse l'augmenter.

Troisièmement, les États-Unis sont passés de la sécuritisation du cyberespace qui consiste à mettre en œuvre des politiques pour se protéger des cyber-menaces, à la militarisation de celui-ci en affichant clairement une volonté de dominer militairement tous les espaces, l'expression *full Spectrum domiance* est utilisée dans ce sens. Les virus informatiques sophistiqués sont désormais des cyber-armes que l'on utilise pour attaquer des cibles stratégiques ou les espionner. Le cyberespace est donc passé d'un environnement d'échange d'information et de gestion de machines industrielles à un domaine militaire où les opérations de sabotage et d'espionnage sont perpétrées contre des adversaires ou des ennemis, opérations exécutées en accord avec les intérêts de la nation.

La cyber-stratégie de sécurité et de défense américaine met donc l'accent sur l'augmentation de la puissance comme réponse aux cyber-menaces nées de la géopolitique. Le cyberespace étant difficile à sécuriser, le but est d'être un agresseur au lieu d'une victime. L'augmentation des cyber-capacités militaires est une solution pour obtenir un effet de dissuasion sur les adversaires. Cette réaction s'inspirerait de la stratégie nucléaire de la guerre froide ou l'on a pu éviter une guerre nucléaire. Cependant, toute stratégie de dissuasion repose sur des capacités de représailles en cas d'attaque, alors que pour faire des représailles, encore faut-il identifier l'ennemi dans un tel environnement. Les États-Unis travaillent depuis des années sur l'augmentation des capacités d'identification des initiateurs de cyber-attaques, cela peut être perçu comme un complément à cette cyber-stratégie globale de dissuasion.

BIBLIOGRAPHIE

Ouvrages

1) Arpajian, Nicolas. *La Cyberguerre : la guerre numérique a commencé.* Paris : Magniar-Vuibert, 2009.

2) Balzacq, Thierry. *Securitization Theory: How security problems emerge and dissolve.* New York: Routledge, 2001

3) Battistella, Dario. *Théories des Relations Internationales.* Paris : Presses de Sciences Po, 2012.

4) Bloch, Lorent et Christohe Wolfhugel. *Sécurité Informatique : principes et métode à l'usage des DSI, RSSI et administrateurs.* 2ème édition. Paris, Eyrolles, 2009.

5) Borrelli, Mar, ed. *Marlware and Computer Security Insidents : Handing Guides* (New York: Nova Science Publishers, 2013.

6) Brenner, Susan W. *Cybercrime : Criminal Threats from Cyberspace.* USA : Praeger, 2010.

7) Buzan, Barry and Lene Hansen. *Evolution of international security studies.* UK: Cambridge University Press, 2009.

8) Buzan, Barry. Ole Waever and Jaap De Wilde. *Security: A Framework for Analysis.* USA: Lynne Rienner Publisher, 1998.

9) Carr, Jeffret. *Inside Cyber Warfare: Mapping the Cyber Underworld.* Sebastopol, CA: O'Reilly, 2012.

10) Cavelty, Myriam Dunn. *Cyber-Security and Threat Politics : US efforts to secure the information age.* Routledge, 2008.

11) Cobast, Éric. *Que Sais-Je ? : Les Mots Qui Ont Fait 2013.* Paris : Presses Universitaires de France, 2014.

12) Couffignal, Louis. *La Cybernétique.* 3ème Édition. Paris : Presses Universitaires de France, 1968.

13) Duncan Cambell. Surveillance Électronique Planétaire. Paris : Editions Allia, 2001.

14) Dussouy, Gérard. *Traité de relations internationales. Tom II : les théories de l'interétatique.* Paris : l'Harmattan, 2008.

15) Filiol, Éric. *Les Virus Informatiques : théorie, pratique et application.* deuxième édition. France : Springer, 2009.

16) Jackson, Robert and George Sørensen. *Introduction to International Relations: Theories and Approaches.* 5th Edition. Oxford, Oxford University Press, 2013.

17) Kempf, Olivier. *Introduction à la Cyberstratégie.* Paris : Economica, 2012.

18) Keohane Robert O. and Joseph S. Nye, Jr. *Power and interdependence.* 4th edition. Longman, 2011.

19) Lacoste, Yves, *Géopolitique : la longue histoire d'aujourd'hui* (Paris, Larousse, 2012.

20) Libicki, Martin C. *Conquest in Cyberspace : national security and information warfare.* Cambridge: The RAND Corporation, 2007.

21) Musset, Joëlle. *Sécurité Informatique : Apprendre l'attaque pour mieux se défendre.* France : Editions ENI, 2009.

22) Pujolle, Guy. *Les Réseaux*. 6th édition. Paris : Editions Eyrolles, 2007.

23) Rid, Thomas. *Cyber War Will not Take Place.* New York, Oxford University Press, 2013.

24) Ruyer, Raymond. *La Cybernétique et l'origine de l'information*, France : Flamarion, 1954.

25) Samuelle, T.J. *CompTia Security+ Certification.* 2nd edition. McGraw Hill, 2009.

26) Singer, Peter W. and Allan Friedman. *Cybersecurity and Cyberwar : what everyone needs to know*. New York: Oxford, 2014.

27) Ventre, Daniel, ed. *Cyber Conflict : competing national perspectives.* Great Britain : ISTE Ltd, 2012.

28) Ventre, Daniel. *cyberespace et acteurs du cyberconflit.* Paris : Lavoisier, 2011.

29) Ventre, Daniel. *Cyberguerre et guerre de l'information : stratégies, règles.* enjeux. Pais : Lavoisier, 2010.

30) White, Gregory, Arthur Conklin, Dwayne Williams, Roger Davis and Chuck Cothren. *CompTia Security+ : exam guide, 2nd Edition.* CompTia, 2009.

31) Wolfers, Arnold. *Discord and Collaboration: Essays on International Politics.* USA: The John Hopkins Press, 1962.

32) Zetter, Kim. *Countdown to Zero Day : stuxnet and the lunch of the world's first digital weapon.* New York: Crown Publishers, 2014.

Revues

33) Balzacq, Thierry. "Qu'est-ce que la Sécurité Nationale ?", *Revue internationale et stratégique,* N 52 (2003/4), p.p. 35-.

34) Bayuk, Jennifer L., Jason Healey, Paul Rohmeyer, Marus H. Sachs, Jeffrey Schmidt and Joseph Weiss. *Cyber Security Policy Guidebook.* New Jersey: John Wiley & Sons, 2012.

35) Blanche, Ed. "Cyber Wars". *Middle East Magazine.* issue 438 (December 2012).

36) Collins, Sean, and Stephen McCombie. « Stuxnet : the emergence of a new cyber weapon and its implications ». *Journal of Policing, Intelligence and Counter Terrorism.* 7:1 (2012), p.p. 80-91.

37) Cornish, Paul, David Livingstone, Dave Clemente et Claire Yorke. "On Cyber Warfare". *Chatham House Report.* November 2010.

38) Demchak, Chris C. et François-Bernard Huyghe. « Organiser sa Défense à l'ère du Cyberconflit : le point de vu Étasunien ». *Revue Internationale et Stratégique.* No. 87 (2012/3). p.p. 103-109.

39) Demidov, Oleg & Maxim Simonenko. "Flame in Cyberspace". *Security Index: A Russian Journal on International Security.* 19:1 (2013). p.p. 69-72.

40) Dossé, Stéphane. « Géopolitique numérique : Omnibus viis americam pervenitur, tous les chemins mènent en Amérique ». dans *Stratégies dans le cyberespace.* sous la direction de Stéphane Dossé et Olivier Kempf, p.p. 49-58. L'esprit du livre éditions, 2011.

41) Goel, Sanjay and Yuan Hong. "Cyber War Games: strategic jostling among traditional adversaries". in *Cyber Warfare: building he scientific foundation*. Edited by Sushil Jajodia, Paulo shakarian, V.S. Subrahmanian, Vipin Swarum and Cliff Wang, p.p. 1-14. New York: Springer, 2015.

42) Häly Laasme, "The Role of Estonia in Developing NATO's Cyber Strategy", *Cicero Fundation Great Debate Paper*, No. 18/08 (December 2012).

43) Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses". *Journal of Strategic Security*. Vol. 4 (Summer 2011), p.p. 49-60.

44) Kallberg, Jan. "Designer satellite Collisions from Covert cyber War". *Strategic Studies Quarterly*. Vol. 6, No. 1 (spring 2012). p.p. 124-137.

45) Krause, Keith and Michel C. Williams. "Broadening the Agnda of Security Studies : Politics and Methods". *Mershon International Studies Review*, Vol. 40, N. 2 (oct., 1996), 229-254.

46) Libicki, Martin C. « De Tallinn à Las Vegas, une cyberattaque d'importance justifie-t-elle une réponse cinétique ? ». *Hérodote*. N. 152-153 (2014). p.p. 221-239.

47) Limnéll,Jarno. « Le Cyber Change-t-il l'art de la guerre ? ». *Sécurité Globale*. N. 23 (2013), p.p. 33-41.

48) McDonald, Matt. "Constructivism", in *Security Studies: an Introduction*, ed. Paul D. Williams, New York: Routledge, 2008, p.p. 58-72.

49) Mongin, Dominique. « Les Cyberattaques, Armes de Guerre en Temps de Paix ». *Esprit*. N. 1 (janvier 2013), p.p. 32-49.

50) Nye, Joseph S. Jr and Sean M. Lynn-Jones. "International Security Studies: A Report of a Conference on the State of the Field", *international security Vol. 2: the transition to the post-cold war security agenda*, edited by Barry Buzan and Lene Hansen (SAGE Publications, 2007). Originally published in *International Security*, Vol. 10, N. 4 (1988), p.p. 5-27.

51) Ole Wæver. 'Securitization and Desecuritization", in *International Security: Widening Security*, vol. 3. Edited by Barry Buzan and Lene

Hansen (SAGE Publications, 2007), p.p. 66-98. Originally published in *On Security*, edited by Ronny Lipshutz (New York: Columbia University Press, 1995) p.p. 46-86.

52) On-Ching Yue. "Cyber Security". *Technology in Society*. Vol. 25 (2003). p.p. 565-569.

53) Price, Richard and Christian Reus-Smith. "Dangerous Liaisons? Critical International Theory and Constructivism", in E*uropean Journal of International Relations*, vol. 4, N. 3 (1998), p.p. 259-294

54) Rid, Thomas. "Cyberwar and Peace : Hacking Can Reduce Real-World Violence". *Foreign Affairs.* (November/December 2013). https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace.

55) Rid,Thomas. "Cyber War Will Not Take Place". *Journal of Strategic Studies.* Vol. 35, No. 1 (February 2012), p.p. 5-32.

56) Smith, Steve. "The Essentially Contested Concept of Security", in *critical security studies and world politics*, edited by Ken Booth, Boulder, Colorado: Lynne Rienner Publisher, p.p. 27-62.

57) Walt, Stephen M. "the renaissance of security studies", in *international security Vol. 2: The Transition to the Post-Cold War Security Agenda*, edited by Barry Buzan and Lene Hansen, (SAGE publications, 2007), p.p.214-247. Originally published in International Studies Quarterly, Vol 35, N. 2, 1991, p.p. 211-239.

Journaux

58) "Saudi Aramco says virus shuts down its computer network". *Reuters.* August 15, 2012. www.reuters.com/article/2012/08/15/us-aramco-virus-idUSBRE87E18S20120815.

59) "'End of the world as we know it': Kaspersky warns of cyber-terror apocalypse". *Russia Today.* June 06, 2012. http://rt.com/news/kaspersky-fears-cyber-pandemic-170/.

60) Aderet, Ofer. "Report: Mossad hacked Syrian computer to uncover nuke site". *Haaretz*, Novembre 02, 2009. http://www.haaretz.com/news/report-mossad-hacked-syrian-computer-to-uncover-nuke-site-1.4935.

61) Ball, James, Julian Borger and Glenn Greenwald. “Revealed: how US and UK spy agencies defeat internet privacy and security”. *The Guardian*. September 6, 2013. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security/.

62) Capaccio, Anthony. “China Most Threatening Cyberspace Force, U.S. Panel Says”. *BloombergBusiness*. November 6, 2012. http://www.bloomberg.com/news/articles/2012-11-05/china-most-threatening-cyberspace-force-u-s-panel-says.

63) Gallet, Ludwig. « Piratage informatique : danger sur la réputation de l'entreprise », *L’Express l’Entreprise*. 19 juin, 2014. http://lentreprise.lexpress.fr/marketing-vente/promotion-communication/piratage-informatique-danger-sur-la-reputation-de-l-entreprise_1552590.html.

64) Gorman, Siobhan, August Cole And Yochi Dreazen. “Computer Spies Breach Fighter-Jet Project”. *The Wall Street Journal*. april 21, 2009. http://www.wsj.com/articles/SB124027491029837401.

65) Greenberg, Andy. “Cyberespionage Is a Top Priority for CIA’s New Directorate”. *Wired*. March 9, 2015. http://www.wired.com/2015/03/cias-new-directorate-makes-cyberespionage-top-priority/.

66) Greenwald, Glenn. “XKeyscore: NSA tool collects 'nearly everything a user does on the internet'”. *The Guardian*. July 31, 2013. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data/.

67) Keating, Joshua E. “Shots Fired - The Ten Worst Cyberattacks”. *Foreign Policy*. http://www.foreignpolicy.com/articles/2012/02/24/shots_fired.

68) Leyden,John. "Israel suspected of 'hacking' Syrian air defences". *The Register*. 4 October 2007. http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

69) Merchet, Jean-Dominique. "Les Armées Attaquées par un Virus Informatique". *Libération : Secret Défense*. 5 Février 2009. http://secretdefense.blogs.liberation.fr/2009/02/05/les-armes-attaq/.

70) Pau, Aivar. “Statement by the foreign minister Urmas Paet”. *Eesti Päevaleht.* Mai 01, 2007. http://epl.delfi.ee/news/eesti/statement-by-the-foreign-minister-urmas-paet?id=51085399.

71) Pflimlin, Edouard. “Pirater un drone militaire, une menace réelle ?”. Le *Monde : blog guerre des robots.* 06 Mai 2015. http://robots.blog.lemonde.fr/2015/05/06/pirater-un-drone-militaire-une-menace-reelle/.

72) Schmitt, Eric and Thom Shanker. "U.S. Debated Cyberwarfare in Attack Plan on Libya". *The New York Times.* October 17, 2011. http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

73) Sonne, Paul, and Margaret Coker, “Firms Aided Libyan Spies: First Look Inside Security Unit Shows How Citizens Were Tracked”, *The Wall Street Journal*, August 30, 2011, http://www.wsj.com/articles/SB10001424053111904199404576538721260166388.

74) Verton, Dan. "Serbs Lunch Cyberattack on NATO". *FCW.* April 04, 1999. http://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx.

Rapports

75) “Internet Security Threat Report”. *Symantec.* Volume 20 (April 2015).

76) Matrosov, Aleksandr, Eugene Rodionov, David Harley and Juraj Malcho. “Stuxnet Under the Microscope”. Revision 1.31.eset. http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

Documents Gouvernementaux

77) "The National Intelligence Strategy of the United States of America". Washington, Director of National Intelligence, 2014.

78) “Joint Task Force on Computer Network Defense Now Operational” Department of Defense News Release No. 658-98. Washington DC:

Department of Defense. December 30, 1998. http://www.defense.gov/Releases/Release.aspx?ReleaseID=1945.

79) "National Security Strategy", *Seal of The President of the United States*, May 2010, https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

80) "Report to Congress", U.S.-China Economic and Security Commission, 130th Congress, November 2014.

81) "The Department of Defense Cyber Strategy". Washington D.C: the Department of Defense, 2011.

82) "The Department of Defense Cyber Strategy". Washington D.C: the Department of Defense, 2015.

83) "Worldwide Threat Assessment of the US Intelligence Community". James R. Clapper. Washington DC: Direction of National Intelligence, February 24, 2015.

84) "Worldwide Threat Assessment of the US Intelligence Community". James R. Clapper. Washington DC: Direction of National Intelligence, January 31, 2012.

85) "Worldwide Threat Assessment of the US Intelligence Community". James R. Clapper. Washington DC: Direction of National Intelligence, March 12, 2013.

86) "Worldwide Threat Assessment of the US Intelligence Community". James R. Clapper. Washington DC: Direction of National Intelligence, January 29, 2014.

87) United States of America, The Department of Defense, *U.S. Cyber Command Fact Sheet*, May 25, 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

88) United States of America. The Department of Defense, *The DoD Cyber Strategy*. April 2015.

Dictionnaires et encyclopédies

89) Encyclopaedia Britannica Online, s.vv. “Cybernetics”.

90) Encyclopedia of networking. Second edition. Werner Feibel. Network Press, 1996.

91) Larousse, s.v. « espace », http://www.larousse.fr/dictionnaires/francais/espace/31013 (consulté le 15 avaril 2015)

92) Le Robert : Dictionnaire de Français, ed. Martyn Back et Silke Zimmermann, Paris, 2005.

93) Microsoft encyclopedia of networking. Second edition. Mitch Tulloch and Ingrid Tulloch. Washington: Microsoft Press, 2002.

Sites Internet

94) "Estonia". CIA World Factbook. https://www.cia.gov/library/publications/the-world-factbook/geos/en.html. (accessed May 06, 2015).

95) “'Destover' malware now digitally signed by Sony certificates”. Kaspersky Lab. https://securelist.com/blog/security-policies/68073/destover-malware-now-digitally-signed-by-sony-certificates/. (accessed May 07, 2015).

96) “Equation: The Death Star of Malware Galaxy”. *Securelist.* February 16, 2015. https://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/. (accessed May 16, 2015).

97) “Russia to Create Cyberwarfare Units by 2017”. *Sputnik*, January 1, 2014. http://sputniknews.com/military/20140130/187047301.html.

98) “Seculert: 'Shamoon' malware covers its tracks by crippling infected systems after stealing data”. Topnews. August 18, 2012. www.topnews.in/seculert-shamoon-malware-covers-its-tracks-crippling-infected-systems-after-stealing-data-2364028 (accessed May 07, 2015).

99) "Sony Pictures malware tied to Seoul, "Shamoon" cyber-attacks". Arstechnica. http://arstechnica.com/security/2014/12/sony-pictures-malware-tied-to-seoul-shamoon-cyber-attacks/. (accessed May 07, 2015).

100) "The Shamoon Attacks Continue". Symantec Security Response. http://www.symantec.com/connect/blogs/shamoon-attacks-continue. (accessed 07 May, 2015).

101) "The Shamoon Attacks". Symantec Security Response. http://www.symantec.com/connect/blogs/shamoon-attacks. (accessed May 07, 2015).

102) « Amesys ». Les Ennemis d'Internet : Rapport spécial surveillance. http://surveillance.rsf.org/amesys/ (accédé le 28 avril, 2015).

103) « l'affaire Farewell ». France Info. http://www.franceinfo.fr/emission/le-roman-des-espions/2014-ete/le-roman-des-espions-ete-2014-du-13-08-2014-08-13-2014-06-40 (consulté le 05/05/2014).

104) Barlow, John P. « Déclaration d'indépendance du cyberespace ». http://editions-hache.com/essais/barlow/barlow2.html.

105) Fogarty, Kevin. "Russian Cyberwar Force Intensifies 'net Arms Race". *Dice*. February 1, 2014. http://insights.dice.com/2014/02/01/russian-cyberwar-force-intensifies-net-arms-race/. (accessed Mary 18, 2015).

106) Gallagher, Sean. "White House: NSA and Cyber Command to stay under one boss". *Arstechnica*. December 13, 2013. http://arstechnica.com/tech-policy/2013/12/white-house-nsa-and-cyber-command-to-stay-under-one-boss/.

107) Internet Lives Stats. "Internet Users". http://www.internetlivestats.com/internet-users/ (accessed April 24, 2015)

108) Kevin Coleman, "The Increased Threat of Attacks on SCADA Systems", *Defense Tech*, Septmber 26, 2011, http://defensetech.org/2011/09/26/the-increased-threat-of-attacks- on-scada-systems/.

109) Kumar, Mohit. "China Finally Admits it Has Army of Hackers". *The Hacker News*. March 19, 2015. http://thehackernews.com/2015/03/china-cyber-army.html/. (accessed May 18, February 2015).

110) Kurt Baumgartner, “Sony/Destover: mystery North Korean actor's destructive and past network activity: Comparisons with Shamoon and DarkSeaoul”, *Securelist*, December 4, 2014, https://securelist.com/blog/research/67985/destover/ (accessed May 07, 2015).

111) Mark Clayton. “The new cyber arms race”. *The Christian Science Monitor*. March 07, 2011. www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race.

112) Noah Shachtman, “Computer Virus Hits U.S. Drone Fleet”, *Wired*, October 07, 2011, http://www.wired.com/2011/10/virus-hits-drone-fleet. (accessed May 14, 2015).

113) Paul Wagenseil. “Shamoon Spyware Searches, then destroys”. NBCnew. http://www.nbcnews.com/id/48708157/ns/technology_and_science-security/t/shamoon-spyware-searches-then-destroys/#.VU5V0EiZaSp. (accessed May 07, 2015).

114) Zetter, Kim. “Google Hack Attack was Ultra Sophisticated, New Details Show”. *Wired*. January 14, 2010. http://www.wired.com/2010/01/operation-aurora/. (accessed May 18, 2015).

ANNEXES

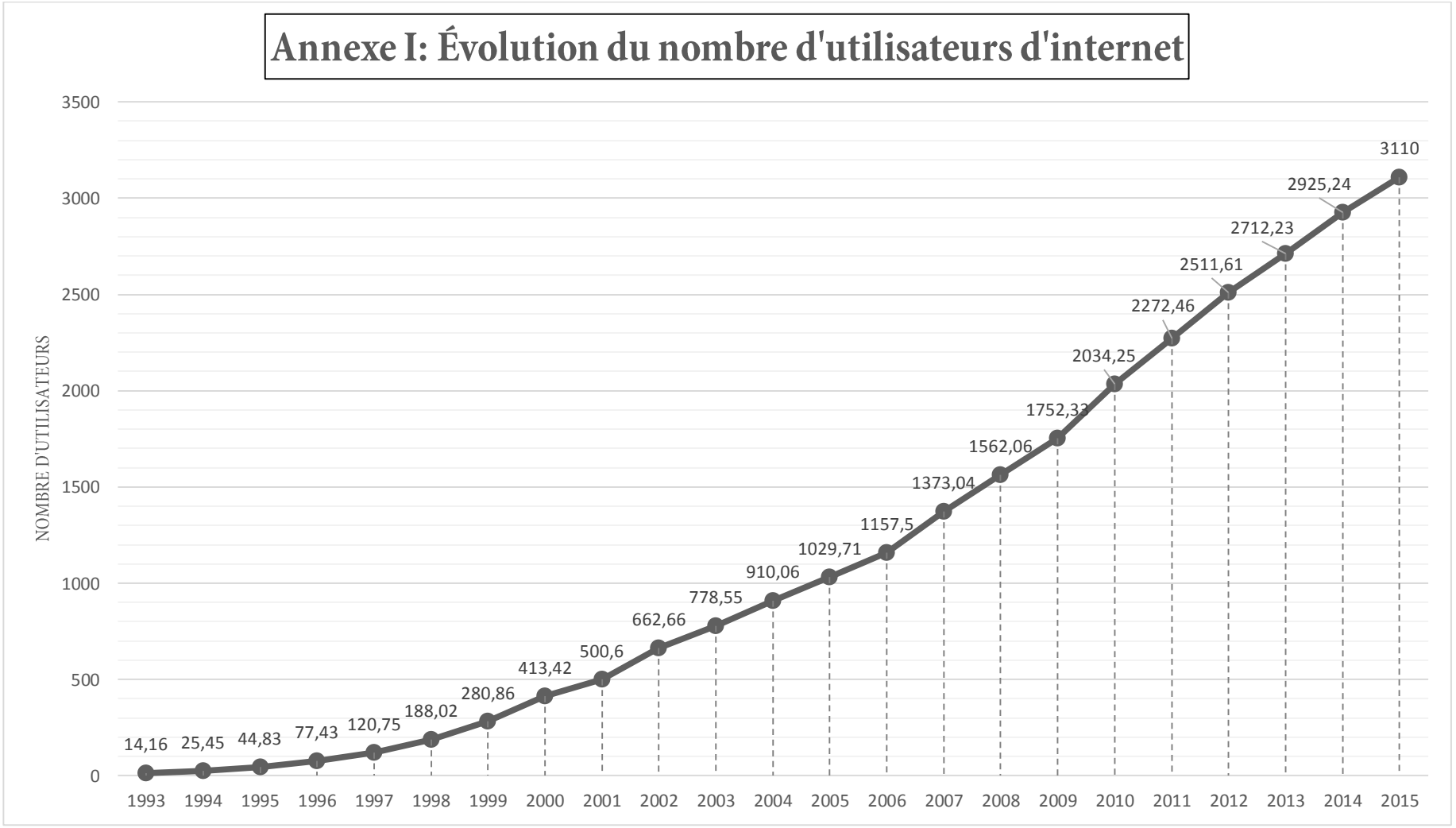


Figure dessiné par le chercheur à partir de statistiques trouvées sur : Internet Lives Stats, "internet users", http://www.internetlivestats.com/internet-users/ (accessed April 24, 2015).