UNIVERSITÉ DU QUÉBEC À MONTRÉAL

COMMUNICATION, GOUVERNANCE ET CYBERSÉCURITÉ: SUITE À LA CYBERATTAQUE CONTRE TV5 MONDE, QUELS SONT POUR LA FRANCE LES NOUVEAUX ENJEUX DE CYBERSÉCURITÉ ET DE CYBERDIPLOMATIE ?

MÉMOIRE DE MAÎTRISE
PRÉSENTÉ COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN COMMUNICATION

PAR
ANGÉLIQUE LAKIA-SOUCALIE

NOVEMBRE 2017

« Pour comprendre l'intuition fondamentale qui sous-tend l'oeuvre de Goffman et qui ordonne sa perception particulière du monde social, selon laquelle les rapports entre les individus sont toujours (au même titre que les rapports entre les États) des rapports de force fondés sur le simulacre »

« Les Moments et leurs hommes »
1988, Erving Goffman, Textes recueillis et présentés par Yves Winkin
Édition Broché.

REMERCIEMENTS

Après plusieurs mois de recherche et de rédaction, je souhaite particulièrement remercier diverses personnes sans lesquelles la réalisation et la concrétisation de ce mémoire auraient été difficiles.

Tout d'abord, mon directeur de recherche Claude-Yves Charron pour son soutien, ses conseils, son accompagnement et sa disponibilité tout au long de cette aventure au Québec. Merci de m'avoir fait confiance et de m'avoir donné l'opportunité de réaliser mes projets.

Aussi, je remercie ma famille, mes parents et mes amis qui ont su m'accompagner et me soutenir, dans les bons comme dans les mauvais moments. C'est avec un réel plaisir que j'ai rédigé ce mémoire et que j'ai travaillé sur ce sujet qui fût pour moi, une très belle découverte à mon arrivée à Montréal.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

Tableaux Page

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

ISIS	Islamic State in Iraq and Syria
DAECH	État islamique en Irak et au Levant
ANSSI	Agence nationale de la sécurité des systèmes d'information
CCDCOE	Cooperative cyber defense centre of excellence
ENISA	European union agency for network and information security
EI	État islamique
UE	Union européenne
OTAN	Organisation du traité de l'Atlantique nord
NATO	North atlantic treaty organization
ONU	Organisation des Nations Unies
UIT	Union internationale des télécommunications
OCDE	Organisation de coopération et de développement économique
CTIRU	Counter Terrorism Internet Referral Unit
RTI	Règlement des télécommunications internationales
TIC	Technologies de l'information et de la communication
SGDNS	Secrétariat général de la défense et de la sécurité nationale
NSA	National security agency
OSCE	Organisation pour la sécurité et la coopération en Europe
TES	Titres électroniques sécurisés
DARPA	Defense advanced research projects agency
ARPANET	Advanced research projects agency network
IETF	Internet engineering task force
IANA	Internet assigned numbers authority
IP	Internet protocol
RIR	Registres internet régionaux
ICANN	Internet corporation for assigned names and numbers
SMSI	Sommet mondial sur la société de l'information
WSIS	World summit on the information society

RÉSUMÉ

Selon une étude du PWC, le nombre de cyberattaques a augmenté partout à travers le monde de 38% en 2015 et les budgets des entreprises en matière de cybersécurité de 24%. La France est l'un des pays où les cyberattaques ont été les plus dénombrées au monde avec un taux de 51% en 2015, et 29% d'augmentation dans les budgets des entreprises, donc une perte financière de plus de 28%.

La cyberattaque contre TV5 Monde, était l'une des plus importantes attaques qu'ait connue la France. TV5 Monde est une chaîne de télévision à portée internationale. Elle représente l'un des plus grands médias télévisuels au monde par ses douze chaînes disponibles dans 200 pays et dont la diffusion atteint 291 000 foyers. Le 8 avril 2015, les réseaux sociaux de la chaîne ont été investis et diffusaient des messages faisant allusion à l'organisation de DAECH.

Le gouvernement français a aussitôt réagi publiquement. En effet, suite aux différents attentats survenus à Paris, quelques mois plus tôt dans cette même année, la population française semble toujours effrayée et heurtée par les évènements que les attaquants n'ont pas manqué de rappeler, « Je suIs IS [ISIS]...La guerre contre l'État islamique était une faute impardonnable [...] c'est pour ça que les Français ont reçu les cadeaux de janvier à Charlie Hebdo et à l'Hypercacher ».

Les cyberattaques peuvent engendrer de graves conséquences, pas uniquement en cas de crises majeures touchant les infrastructures critiques d'un pays, mais également, dans le cadre des relations diplomatiques bilatérales ou multilatérales entre différents États s'affrontant dans le cyberespace.

Suite à la cyberattaque contre TV5 Monde, quels sont pour la France les nouveaux enjeux de cybersécurité et de cyberdiplomatie ?

Mots clés: communication, gouvernance, cybersécurité, cyberdiplomatie, stratégies nationales

INTRODUCTION

Internet est devenu « le réseau omniprésent et multifacétique de canalisation de l'énergie et de l'expression humaine »[1]. Accessible par tous, le réseau permet à tout individu, quelle que soit sa position géographique sur le globe, d'accéder à un flux d'informations, de contenu important, avec la possibilité d'y contribuer et d'en créer lui-même.

Le réseau Internet se développe et se propage très rapidement à travers le monde à un tel point que « dans la première décennie du XXIe siècle, on est passé de 350 millions à plus de 2 milliards d'individus connectés à Internet dans le monde »[2]. À l'avenir, le monde que nous connaissons sera divisé en deux parties à la fois distinctes et complémentaires: le monde physique et le monde virtuel. Tous, organismes, États, individus ou associations devront s'adapter et composer avec ces deux mondes parallèles « sous peine d'obsolescence et d'inattention à la société moderne. »[3]. Dans ce monde parallèle où il paraît moins aisé de mettre en place des règles et de faire respecter des lois, les individus auront donc plus de facilité à accéder à certaines informations et parfois même à les détourner, les gouvernements devront prendre les précautions nécessaires grâce à de nouvelles mesures politiques.

---

[1] Schmidt, E. et Cohen, J. (2014). The New Digital Age. *Reshaping the Future of People, Nations and Business (p.11)*. France: Edition Broché.

[2] Schmidt, E. et Cohen, J. (2014). The New Digital Age. *Reshaping the Future of People, Nations and Business (p.12-13)*. France: Edition Broché.

[3] Schmidt, E. et Cohen, J. (2014). The New Digital Age. *Reshaping the Future of People, Nations and Business (p.15)*. France: Edition Broché.

Dans ce nouvel espace présentant également de nouvelles menaces, nous nous attacherons particulièrement à analyser le processus de cyberattaques et les notions de cybersécurité, de cyberdéfense et de cyberdiplomatie qui en découlent sur le territoire français et au travers de ses différentes alliances internationales.

Nous prendrons comme étude de cas la cyberattaque contre TV5 Monde, qui fût l'une des plus importantes en France, non pas uniquement de par les conséquences matérielles qu'elle a causée, mais surtout pour les conséquences morales qu'elle a entraînées. Nous le rappelons, la France déjà fragile lors de cette cyberattaque, a subi quelques mois auparavant plusieurs attentats terroristes qui fût de nombreux morts. Ces pertes humaines ont laissé de graves séquelles morales au sein de la société française, et les menaces extrémistes qui planent sur la France effraient toujours.

Au sein de cet objet d'étude, ce qui nous semble le plus pertinent sont les différentes perspectives en présence et ses divers acteurs (TV5 Monde, l'ANSSI, le gouvernement français, DAECH et le gouvernement russe) qui ont participé a cette mise en scène et dont les conséquences ont affecté les relations diplomatiques et bilatérales entre certains États. Elle a également touché, l'image de la France et de la francophonie à l'internationale.

Dans un premier chapitre, nous identifierons nos problématiques centrales et sectorielles qui nous guideront tout au long de notre étude. Nous expliciterons de quelles façons cette cyberattaque s'est produite et nous définirons les concepts clés utilisés durant notre analyse. Enfin, nous détaillerons et analyserons toutes les perspectives présentes au sein de cette cyberattaque.

Dans un second chapitre, nous développerons notre cadre théorique, portant particulièrement sur le simulacre dans les rapports étatiques. Ainsi, nous utiliserons principalement l'approche constructiviste de Berger et Luckmann et les perspectives foucaldiennes d'analyse de discours et celle de conflit d'Adam Segal.

Dans un troisième chapitre, nous analysons d'une part le concept de « mise en scène » que présente particulièrement notre étude, de par ses nombreux acteurs et d'autre part, nous développerons les différentes notions nous permettant l'analyse de nos discours. De plus, nous étudierons le discours conflictuel également présent au sein de notre étude et particulièrement utilisé lors de l'analyse de « la mise en scène de la menace ».

Dans un quatrième chapitre, nous tâcherons de présenter nos résultats grâce à l'analyse du discours de nos différentes perspectives en présence et des deux stratégies nationales établies par le gouvernement français suite à la cyberattaque contre TV5 Monde. Nous ajouterons une analyse comparative de ces deux stratégies afin de mettre en évidence les nouveaux enjeux de cybersécurité et de cyberdiplomatie de la France.

Enfin dans un cinquième chapitre, nous présenterons notre conclusion portant principalement sur un rapport des faits concernant la cybersécurité en France, également sur le principe de riposte, que nous abordons dans notre étude. Nous terminerons notre étude en évaluant quels ont été les nouveaux enjeux de cybersécurité et de cyberdiplomatie de la France, suite à cette cyberattaque.

CHAPITRE I

PROBLÉMATIQUE D'ENSEMBLE

1.1 Questions centrales et sectorielles

Notre question centrale se formulerait donc ainsi: suite à la cyberattaque contre TV5 Monde, quels sont pour la France, les enjeux de cyberdiplomatie et de cybersécurité?

Notre hypothèse est que la France a mis en place une nouvelle stratégie de cyberdéfense, dont l'un des objectifs principaux serait de protéger les entreprises publiques et privées, telle que TV5 Monde. Mais également, de sécuriser l'ensemble de son territoire, de sa population et d'étendre cette protection sur l'ensemble de l'Union européenne, notamment en passant par diverses alliances internationales et bilatérales.

Et nos trois questions sectorielles, portant respectivement sur la cyberattaque d'abord, puis sur la nouvelle stratégie nationale de sécurité et enfin, sur les efforts de coopération internationale de la France avec l'Union européenne et l'OTAN sur le plan de la cybersécurité, constituant chacun un chapitre au sein du mémoire, se distribueraient ainsi, sur la cyberattaque, avec comme point d'ancrage, le concept de perspectives:

1) Comment s'articule le discours des différentes perspectives en présence au sein de cette cyberattaque ?

Lors de cette cyberattaque, les discours publics n'allaient pas toujours dans le même sens puisque chaque organisation souhaitait défendre ses propres intérêts auprès de l'opinion publique. Dans cette étude de cas, ce qui nous semble être le plus intéressant, c'est qu'il a été particulièrement ardu pour les enquêteurs de trouver quels étaient les auteurs de cette cyberattaque. Avec l'État islamique comme première piste c'est ensuite la Russie qui apparaît comme potentiel accusé. Cependant, même suite aux enquêtes, le doute plane toujours sur cette attribution.

TV5 Monde: Quelles ont été les réactions et dispositions prises par TV5 Monde suite à la cyberattaque ? Le directeur de la chaîne de télévision a été mis en avant auprès des médias français suite à cette affaire. En effet, il a livré au cours de ces différentes entrevues un témoignage bouleversant, pensant qu'il s'agissait bel et bien d'une fin définitive pour TV5 Monde. Suite à la cyberattaque de nombreuses dispositions techniques ont été prises au sein des bureaux de la chaîne, les employés ont été formés sur les gestes à ne pas produire pour éviter les risques d'attaques. Enfin TV5 Monde a travaillé de près avec l'ANSSI afin qu'une sécurisation et un contrôle constant des réseaux soit mise en place.

DAECH et le Cyber Califat: en quoi DAECH représente-t-ils une menace pour la France aujourd'hui ? Suite aux dramatiques attentats ayant eu lieu à Paris, la France prend conscience du risque réel que représente l'État islamique aujourd'hui. En effet, l'EI a menacé publiquement la France puisque cette

organisation existe fortement au sein du cyberespace et peut représenter une potentielle menace. Lors de l'attaque de TV5 Monde, en apparence, tout laissait croire qu'il s'agissait de l'EI.

Le gouvernement russe: Si les Russes étaient responsables de cette cyberattaque, se seraient-ils fait passer pour DAECH, et pourquoi s'en prendre à la France ? Beaucoup de cyberattaquants se cachent derrière une toute autre identité. En effet, au vu de la structure initiale d'Internet il n'est pas aisé de retracer l'identité d'un individu. Cette technique est surnommée « false-flag » ou « faux-drapeaux »: se cacher derrière la façade d'un tout autre pays permet de commettre l'attaque sans forcément en assumer les conséquences, qu'elles soient politiques ou diplomatiques.

2) Quels sont les nouveaux enjeux de cybersécurité auxquels s'adresse la nouvelle stratégie nationale de cybersécurité, lancée publiquement par le Premier ministre et le directeur de l'ANSSI suite à cette cyberattaque contre TV5 Monde? Contrairement à l'ancienne, la nouvelle stratégie française se concentre principalement sur la protection de ses infrastructures, de ses entreprises et de ses citoyens. Également elle veut intégrer la France au sein de la coopération européenne.

3) La coopération internationale: Quels sont les nouveaux enjeux de cyberdiplomatie qu'explore la France en terme de coopération internationale avec l'UE et l'OTAN ? La nouvelle stratégie souhaite faire de la France un leader au sein de la coopération européenne. Mais pas uniquement, elle souhaitent également l'impliquer au sein de différentes agences internationales telles que

l'OTAN ou encore l'ONU, afin de mettre en place des dispositifs de cybersécurité et de sensibilisation à la sécurité.

Cette cyberattaque constitue donc un point tournant, conduisant à la nouvelle stratégie française, à de nouvelles pistes et à la recherche d'une coopération au niveau des organisations internationales et multilatérales.

1.2 Comment s'articule le discours des différentes perspectives en présence au sein de cette cyberattaque ?

1.2.1 La cyberattaque contre TV5 Monde: mise en contexte

Le 8 avril 2015 aux alentours de 21h, le directeur de TV5 Monde, Yves Bigot, est averti de l'invasion des réseaux de la chaîne de télévision par de possibles hackers. En effet, un des comptes Twitter a été détourné et diffusait des messages faisant allusion à l'organisation de DAECH. Les cyberattaquants ont par la suite investi l'ensemble des réseaux sociaux et la totalité des chaînes de télévision qui affichaient, partout à travers le monde, un écran noir. D'un point de vue du réseau interne de l'entreprise, les boites e-mail de la chaîne ne fonctionnaient plus, de même pour l'ensemble du réseau informatique.

Cette cyberattaque a été revendiquée par un groupe nommé « Cyber Califat » et se présentant comme djihadistes de DAECH. Sur les réseaux sociaux de la chaîne, étaient explicitement affichés « Je suIS IS » (« Je suis ISIS »). De plus, des messages ont été directement adressés au Président de la République, François Hollande, ainsi qu'aux soldats combattant l'organisation à l'étranger.

Quelles ont alors été les réactions et dispositions prises par TV5 Monde suite à la cyberattaque ?

Yves Bigot, le directeur de TV5 Monde a spécifiquement déclaré qu'il s'agissait d'une « première dans l'histoire de la télévision ». Pour Yves Bigot, la cyberattaque a été pensée à des fins de destruction: « nous avons été des cobayes, les premiers atteints dans notre domaine, les médias ». Suite à l'attaque, la chaîne de télévision a immédiatement contacté l'agence nationale de cybersécurité française, l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information). Le directeur de la chaîne s'interroge également sur la raison de cette attaque, encore méconnut à cette période et met en garde les autres médias français:

> « Tout dépend de la nature de la cyberattaque. Si nous sommes la vraie cible, cela recommencera. Si les hackers ont simplement voulu passer un message, nos collègues devraient être très vigilants ».[4]

Le gouvernement français réagit publiquement au lendemain de la cyberattaque et suite aux revendications du Cyber Califat, le Premier ministre Manuel Valls déclare qu'il s'agissait d' « une atteinte inacceptable à la liberté d'expression et d'information »[5]. Fleur Pellerin, le ministre de la Culture et de la Communication, qualifie cette attaque de « véritable acte terroriste »[6].

---

4 Bigot, Y. (2015, octobre). Conférence stratégie nationale pour la sécurité du numérique. *Cyberattaque: quand tout s'arrête*. Maison de la Chimie, 16 octobre 2015. Paris: Agence nationale de la sécurité des systèmes d'information.

5 Valls, M. (2015). Récupéré de http://www.bfmtv.com/politique/valls-le-piratage-de-tv5-est-une-atteinte-inacceptable-a-la-liberte-d-information-et-d-expression-875657.html

6 Pellerin, F. (2015). Récupéré de http://www.leparisien.fr/faits-divers/piratage-de-tv5monde-le-gouvernement-denonce-un-acte-terroriste-09-04-2015-4677963.php

1.3 Les différents processus en présence

Afin d'appréhender plus aisément les notions que nous aborderons tout au long de notre étude, nous vous proposons les définitions des différents processus que nous emploierons le plus souvent, à savoir: la cybersécurité, la cyberdéfense, la cyberdiplomatie, les cyberattaques, le piratage et le hacking, la cybercriminalité, le cyberterrorisme et la cyberpropagande.

1.3.1 Cybersécurité

La cybersécurité est un terme global qui permet de considérer la sécurité du cyberespace en général. En effet, ce terme qualifie tant les systèmes techniques mis en place, les dispositifs de sensibilisation que la protection des infrastructures critiques. Il va s'agir de tous les dispositifs proposés pour défendre, sécuriser les citoyens, le territoire, au travers du cyberespace et des TIC. L'Union International des Télécommunications nous propose une définition précise:

> « On entend par cybersécurité l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à

> garantir que les propriétés de sécurité des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants:
> • Disponibilité;
> • Intégrité, qui peut englober l'authenticité et la non-répudiation; »[7]

1.3.2 Cyberdéfense

Contrairement au terme de cybersécurité plus global, la cyberdéfense va également concerner la défense, la sécurité des citoyens et du territoire au travers du cyberespace, des technologies de l'information et de la communication, mais il va cependant être consacré au domaine de l'État, de son agence de cybersécurité, telle que l'ANSSI en France ou encore le domaine militaire, avec l'armée.

1.3.3 Cyberdiplomatie

Quand nous parlons de « cyberdiplomatie », nous parlons bien de diplomatie au sens strict du terme. Il s'agit d'assumer une fonction de représentation du pays d'attache à l'étranger, également au sein des relations internationales et au travers du cyberespace. En effet, la diplomatie va se servir des technologies de l'information et de la communication pour établir le contact, exercer son rôle auprès des individus, organisations ou États.

---

[7] Union International des télécommunications (UIT). Récupéré de http://www.itu.int/net/itunews/issues/2010/09/20-fr.aspx

1.3.4 Cyberattaque, piratage et hacking

Une cyberattaque est une attaque qui serait lancée par des individus malveillants, souvent appelés « pirates informatiques » à un site internet, un ordinateur, un serveur au travers de diverses techniques informatiques afin d'effectuer une action de vol, de destruction de données, ou encore à des fins d'espionnage:

> « Le piratage constitue le principal vecteur des actes criminels et représente le danger le plus inquiétant. C'est un phénomène qui n'est pas récent, mais dont la prolifération est préoccupante. Hier réservé à une élite, il s'est démocratisé et est aujourd'hui à la portée de n'importe qui possédant un micro-ordinateur raccordé à l'Internet, car de multiples outils assurant le hacking sont accessibles sur le réseau. [...] Il s'agit en fait de l'action d'accéder et/ou de se maintenir frauduleusement dans un système d'informations, de prendre connaissance des logiciels, des fichiers, des données, éventuellement d'altérer le fonctionnement du système, de supprimer ou de modifier des données, d'y introduire des virus, vers, bombes logiques, chevaux de Troie. »[8]

1.3.5 Cybercriminalité

Quand nous parlons de cybercriminalité, il va s'agir de toutes actions entrainant un délit qui serait préjudiciable, tel qu'un vol d'identité. Daniel Martin et Frédéric-Paul Martin nous en donnent une définition très claire, nous rappelant notamment celle élaborée par l'OCDE:

---

[8] Martin, D. et Martin, F-P. (2001). Cybercrime-menaces, vulnérabilités et ripostes (p.43). France: Edition Broché.

> « Toute action illégale dans lequel un ordinateur est l'instrument ou l'objet du délit; tout délit dont le moyen ou le but est d'influencer la fonction de l'ordinateur; tout acte intentionnel, associé d'une manière ou d'une autre à la technique informatique, dans laquelle une victime a subi ou aurait pu subir un préjudice et dans laquelle l'auteur a tiré ou aurait pu tirer un profit. [...] Les lignes directrices de l'OCDE, dès 1986, ont posé des principes de base de la criminalité informatique: accès frauduleux, interception des systèmes, violation des règles de sécurité dans une intention malhonnête ou nuisible, violation du droit exclusif du détenteur d'un programme, entrée, altération, effacement ou suppression de données, entrave ou fonctionnement des systèmes. »[9]

1.3.6 Cyberterrorisme et cyberpropagande

Le cyberterrorisme représente les actions malveillantes des organisations terroristes au travers le cyberespace. En effet ces groupes malveillants lancent des cyberattaques vers des individus, des organisations ou encore des gouvernements. Ils mettent également en place de la « cyberpropagande »: ils font de la propagande en ligne profitant de l'anonymat et de l'audimat que peuvent procurer le cyberespace pour mener leurs actions:

> « Les organisations terroristes ont recours depuis plusieurs années déjà à l'informatique pour stocker ou transmettre les données concernant leur action et aussi pour réaliser la propagande relative à la cause qu'elles défendent. [...] Internet est un vecteur privilégié et efficace pour transmettre les idées. Terroristes et sectes ont bien compris qu'ils pouvaient utiliser des serveurs implantés hors de France et échapper ainsi au harcèlement des autorités nationales. [...]

---

9 Martin, D. et Martin, F-P. (2001). Cybercrime-menaces, vulnérabilités et ripostes (p.13). France: Edition Broché.

> Compte tenu des moyens existant sur le marché, en vente libre, avec des investissements ridicules, par rapport à ceux correspondant aux armements classiques, il est tout à fait possible pour pratiquement n'importe qui d'attaquer ou de détruire les systèmes d'information d'un pays, de mettre à genoux une grande puissance ou une multinationale. »[10]

1.4 DAECH et le Cyber Califat

Suite à la cyberattaque contre TV5 Monde, les autorités françaises se sont directement orientées vers une piste djihadiste de par la propagande signée DAECH sur les réseaux sociaux (Facebook, Twitter) avec la diffusion de messages explicites tels que « Je suIS IS ». En quoi DAECH représente-t-elle une menace pour la France aujourd'hui ?

Les réseaux sociaux sont devenus un outil indispensable pour la fonction et les relations diplomatiques. Notamment pour établir un lien plus proche entre les gouvernements et la société civile. Cependant, ils peuvent servir aux individus malveillants. Selon Adam Segal, c'est d'ailleurs le cas pour l'État islamique, qui depuis quelques années se développe, et n'utilise plus seulement les sites internet, mais également une large palette de réseaux sociaux, « It is also an attempt to forge narratives that undermine the arguments an attractiveness of adversaries, especially radical Islamists ».[11]

---

[10] Martin, D. et Martin, F-P. (2001). Cybercrime-menaces, vulnérabilités et ripostes (p.68-70). France: Edition Broché.

[11] Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.46)*. Etats-Unis: 1st Edition.

En plus de mener un combat sur le terrain, DAECH mène également un combat dans le cyberespace. La radicalisation est devenue aujourd'hui un fait important en France et en Europe. Comme l'auteur Adam Segal le précise, les individus défendant les valeurs de l'organisation de DAECH dans le cyberspace sont devenus de véritables « experts en communication », en utilisant notamment la brutalité et la violence, « ISIS conquests on the ground were accompanied by an information campaign so slick that the online magazine Vice called the group « total social media pros » »[12]. Pour cela, il nous donne un exemple concret et révélateur de l'influence et de l'impact de DAECH dans le monde virtuel:

> « ISIS tweeted almost 40,000 times in on day; ISIS followers and others around the world retweeted those tweets. ISIS also developed its own app for the web and Android phones called The Dawn of Glad Tidings ».[13]

Néanmoins, DAECH n'est pas la première et la seule organisation à utiliser la connectivité pour propager son idéologie à des fins de recrutement et de radicalisation. Adam Segal précise que le groupe d'Al-Qaeda l'utilisait aussi. Face à cette menace, l'Europe a réagi en essayant d'empêcher ces utilisateurs d'accéder au réseau et de publier des messages ou du contenu faisant allusion à l'organisation. Cependant, ces mesures sont difficilement applicables de par les notions importantes en Europe, de liberté d'expression et de respect des droits humains. Des mesures contraignantes ont néanmoins vu le jour:

---

12 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.185)*. Etats-Unis: 1st Edition.

13 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.186)*. Etats-Unis: 1st Edition.

> « In March 2015, the European Union proposed the creation of an Internet Referral Unit that, as part of the law enforcement agency Europol, would remove extremist material from the Internet. This model is based on the Counter Terrorism Internet Referral Unit (CTIRU) set up by the UK government in 2010 [...] By March 2015, CTIRU had removed 75,000 pics of online extremist material».[14]

De nos jours, les cyberattaques venant de groupes terroristes sont très peu destructrices, puisque ces groupes ne possèdent pas les moyens humains et matériels nécessaires pour conduire des attaques qui auraient un fort impact. Cependant avec le « dark web », ce marché noir ouvert sur Internet, il devient plus aisé d'accéder à des programmes malveillants. Adam Segal, souligne notamment le fait que l'organisation de DAECH, a réussi à faire ce qu'aucune autre organisation a pu faire, « to unite Egypt, the Gulf States, Iran, Iraq, the Kurds, Saudi Arabia, Syria, Turkey, and the United States in destroying a common enemy».[15]

Dans leur ouvrage *The New Digital Age: Reshaping the Future of People, Nations and Business* (2014), Eric Schmidt et Jared Cohen abordent l'avenir du terrorisme au sein de nos sociétés. Ils l'annoncent très clairement: « C'est une vérité incontournable: la connectivité profite aussi aux terroristes et aux extrémistes ».[16]

---

[14]Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.189)*. Etats-Unis: 1st Edition.

[15] Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.188)*. Etats-Unis: 1st Edition.

[16] Schmidt, E. et Cohen, J. (2014). The New Digital Age: Reshaping the Future of People, Nations and Business (p.224). Etats-Unis: Vintage USA

Nous l'avons constaté durant ces dernières années, les terroristes profitent fortement du monde virtuel pour s'immiscer dans nos sociétés. En effet, du recrutement, en passant par les menaces, jusqu'à la mise en exécution de celles-ci, Internet et les nouvelles technologies y jouent un rôle important. Les attentats du 13 novembre et de janvier 2015 à Paris nous le démontrent bien, les terroristes font de la cyberpropagande. Des vidéos incitant à rejoindre l'organisation sont postées régulièrement sur des plateformes telles que YouTube. Aussi avec les réseaux sociaux, les malfaiteurs peuvent plus facilement entrer en contact avec certains individus déjà influencés par ces mêmes vidéos. Les États devront trouver des solutions plus efficaces pour contrer le terrorisme. Les auteurs définissent le cyberterrorisme comme « toute attaque à motivation politique ou idéologique portée contre l'information, les données des usagers ou les systèmes informatiques dans le but d'aboutir à un dénouement violent »[17]. Au fur et à mesure de l'évolution technologique, les terroristes peuvent améliorer leurs compétences techniques, ce qui représenterait un grand risque, puisqu'ils pourraient prendre en otage nos sociétés et les paralyser au moins pour quelques instants. Les conséquences tant psychologiques que matérielles seront graves pour les populations.

La connectivité est un avantage pour les terroristes. Cependant, elle peut aussi comporter certains inconvénients puisque du fait de la structure d'Internet, des traces sont continuellement enregistrées dans le réseau et les malfaiteurs sont ainsi facilement traçables à partir du moment où ils vont commettre le moindre faux pas. Les auteurs prennent l'exemple très explicite d'Oussama Ben Laden, qui lui, au contraire, s'est complètement coupé de toute connectivité pouvant paraitre compromettante. Or, à l'heure du numérique, ne pas être connecté parait

---

17 Schmidt, E. et Cohen, J. (2014). The New Digital Age: Reshaping the Future of People, Nations and Business (p.227). Etats-Unis: Vintage USA

suspicieux. Et c'est donc ainsi qu'il s'est fait repérer et arrêter par les autorités américaines. La technologie évoluant, les États auront de nouveaux dispositifs de contrôle. Aussi, puisque des traces sont constamment laissées, « s'ils sont en ligne, ils sont trouvables. Et s'ils sont trouvables, le réseau de tous leurs collaborateurs l'est aussi »[18].

1.5 L'Agence de Sécurité des Systèmes d'Information: ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est l'organisation gouvernementale française de cybersécurité créée en juillet 2009. D'après le directeur général de l'ANSSI, Guillaume Poupard, l'organisation détient diverses missions. En effet, elle permet avant tout de répondre aux attentes que représentent les différents enjeux de cybersécurité et de cyberdiplomatie en France. De la protection des réseaux informatiques, de la souveraineté du pays en matière de décision dans un cadre politique, militaire et diplomatique, en passant par la sécurité, la protection des citoyens, notamment au vu de l'augmentation de la cybercriminalité, en finissant par les enjeux primordiaux de souveraineté et d'autonomie pour la France, même dans le cyberespace. L'ANSSI travaille autour de trois principales notions: la prévention, la défense et la sensibilisation.

L'agence de sécurité s'adresse à différents publics, à savoir aux administrations, aux petites et aux grandes entreprises, aux particuliers. L'organisation est également présente sur la scène internationale. En effet, elle a participé aux négociations du Règlement des télécommunications internationales (RTI) qui se sont déroulées à Dubaï en 2012 et organisées par l'Union internationale des

---

[18] Schmidt, E. et Cohen, J. (2014). The New Digital Age: Reshaping the Future of People, Nations and Business (p.270). Etats-Unis: Vintage USA

télécommunications (UIT). Elle fait partie de la Première Commission de l'ONU sur la sécurité internationale de l'information et des télécommunications. L'ANSSI est également présente à travers l'OTAN étant donné son statut d'autorité nationale de sécurité des systèmes d'information et au sein de l'Union européenne où elle représente la France au conseil d'administration de l'agence européenne pour la sécurité des réseaux et de l'information: l'ENISA (European Union Agency for Network and Information Security). De par les nouveaux enjeux que représentent les communications, l'ANSSI a coordonné, en collaboration avec le gouvernement une « Stratégie nationale pour la sécurité du numérique » (2015).

Suite à la cyberattaque contre TV5 Monde, où l'ANSSI est directement intervenue, le directeur Guillaume Poupard, qualifie clairement cette cyberattaque « d'un acte de sabotage »[19]. Pour lui, la France a un réel besoin de « réflexion et d'organisation »[20] pour le développement du « territoire cybernétique nationale, même si ce territoire est bien plus compliqué que le territoire physique »[21].

Durant la conférence du 16 octobre 2015 intitulée « Stratégie nationale pour la sécurité du numérique », en présence du Premier ministre ainsi que du Directeur de TV5 Monde. Guillaume Pourpard, directeur de l'ANSSI, annonce les

---

19 Poupard, G. Stratégie nationale pour la sécurité du numérique. (2015, octobre). *Conférence. Des chiffres à la sécurité du numérique*. 16 octobre 2015, Maison de la Chimie. Paris: Agence nationale de la sécurité des systèmes d'information.

20 Poupard, G. Stratégie nationale pour la sécurité du numérique. (2015, octobre). *Conférence. Des chiffres à la sécurité du numérique*. 16 octobre 2015, Maison de la Chimie. Paris: Agence nationale de la sécurité des systèmes d'information.

21 Poupard, G. Stratégie nationale pour la sécurité du numérique. (2015, octobre). *Conférence. Des chiffres à la sécurité du numérique*. 16 octobre 2015, Maison de la Chimie. Paris: Agence nationale de la sécurité des systèmes d'information.

ambitions françaises pour le numérique et la cybersécurité. En effet, selon lui, la France se dessine en trois principales communautés qui agissent au sein et pour le développement du cyberespace. Tout d'abord, « la communauté des chercheurs, des inventeurs de produits qui détiennent une responsabilité de premier plan. Étant donné que ceux qui bâtissent le numérique doivent également penser à sa sécurité »[22]. Pour lui l'ANSSI, représente une aide à ce développement est non un obstacle.

> « L'ANSSI s'inscrit dans cette communauté [...] elle accompagne le développement du numérique, nous ne sommes pas là pour freiner ce développement du numérique, nous sommes là pour l'accompagner, pour continuer à le rendre possible, pour le pérenniser, pour faire en sorte que le numérique ne soit pas un feu de paille qui tombe sous le coup de ces attaques ».[23]

La deuxième communauté concerne les États, les gouvernements, ainsi que les personnalités politiques. En effet, il est nécessaire pour l'ANSSI que la France se protège de la présence et de l'influence d'individus malveillants, d'attaquants. De plus, le pays doit imposer son principe de souveraineté pour se protéger des grandes firmes multinationales exploitant les données à des fins commerciales.

> « Ce que nous appelons l'article 22 [...] positionne la France dans les pionniers en matière de protection des infrastructures critiques, nous sommes le premier pays au monde à avoir le courage de passer par la

---

[22] Poupard, G. Stratégie nationale pour la sécurité du numérique. (2015, octobre). *Conférence. Des chiffres à la sécurité du numérique*. 16 octobre 2015, Maison de la Chimie. Paris: Agence nationale de la sécurité des systèmes d'information.

[23] Poupard, G. Stratégie nationale pour la sécurité du numérique. (2015, octobre). *Conférence. Des chiffres à la sécurité du numérique*. 16 octobre 2015, Maison de la Chimie. Paris: Agence nationale de la sécurité des systèmes d'information.

voie juridique ».[24]

Enfin, la troisième communauté s'adresse aux dirigeants d'entreprises, d'administrations, d'institutions, puisqu'une cyberattaque peut être réellement dévastatrice pour une entreprise et pour son personnel. Il est donc important selon Guillaume Poupard de prendre des dispositions de sécurité avant qu'un évènement dramatique ait lieu.

1.6 Le gouvernement russe

Suite aux investigations de l'agence gouvernementale de cybersécurité française (ANSSI), la piste des enquêteurs se dirige plus tard, vers des hackers russes. Si les Russes étaient responsables de cette cyberattaque, pourquoi se seraient-ils fait passer pour DAECH, et pourquoi s'en prendre à la France ?

Selon l'ANSSI, les preuves techniques montreraient que l'attaque proviendrait de Russie. Il s'agirait d'un groupe nommé « APT28 », aussi surnommé « Pawn Storm », ou « Tempête de pions». La cyberattaque a eu lieu alors que des tensions se faisaient ressentir entre la France et la Russie de par les conflits en Ukraine et les sanctions européennes qui ont suivis, contre les intérêts russes. La Russie représente pour les autres puissances un danger potentiel dans le cyberespace. En effet, Adam Segal le précise:

> « The Kremlin's theory of influence also relies greatly on mass disinformation. Russia has mobilized an army of trolls, part of a larger

---

[24] Poupard, G. Stratégie nationale pour la sécurité du numérique. (2015, octobre). *Conférence. Des chiffres à la sécurité du numérique.* 16 octobre 2015, Maison de la Chimie. Paris: Agence nationale de la sécurité des systèmes d'information.

> information war to legitimize its actions and divide, distract, and disturb its opponents in and out of Russia ».[25]

La Russie a toujours tenu une place importante dans le cyberespace depuis la création d'Internet. Selon Kevin Limonier, la Russie a toujours exprimé l'envie d'un « Internet indépendant »[26]. Le cyberespace représente un réel enjeu de pouvoir, que la Russie souhaite acquérir. Elle exprime également le besoin de protéger sa souveraineté, avec « la mise en valeur d'une certaine forme de patriotisme fondée sur la célébration de la puissance et de la souveraineté de l'État »[27]. La Russie détient les capacités matérielles pour imposer sa puissance dans le cyberespace puisque les Russes sont « les premiers producteurs de données numériques d'Europe »[28]. Ces envies sont également liées au fait que le pays ne souhaite pas être dépendant des États-Unis. Une plateforme a notamment été spécialement développée pour le territoire russe, le *Runet* « il s'agit très concrètement de tous les sites Internet, de tous les serveurs et de toutes les adresses mails qui utilisent la langue russe pour diffuser de l'information »[29].

Les hackers russes utilisent souvent la technique de piratage connue sous le nom de « spear-phishing », où des e-mails sont envoyés avec une pièce jointe, donnant l'apparence d'un destinataire et d'un message familier au récepteur. Ainsi la pièce

---

25 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.184).* Etats-Unis: 1st Edition.

26 Limonier, K. (2014). La Russie dans le cyberespace: représentations et enjeux. (Herodote, n° 152-153). France: La Découverte.

27 Limonier, K. (2014). La Russie dans le cyberespace: représentations et enjeux (p.141). (Herodote, n° 152-153). France: La Découverte.

28 Limonier, K. (2014). La Russie dans le cyberespace: représentations et enjeux. (Herodote, n° 152-153). France: La Découverte.

29 Limonier, K. (2014). La Russie dans le cyberespace: représentations et enjeux (p.145). (Herodote, n° 152-153). France: La Découverte.

jointe ouverte, le *malware* se propage au sein du réseau et peut effectuer un grand nombre d'actions. Il s'agit de la technique utilisée lors de la cyberattaque contre TV5 Monde. Ce qui a permis aux enquêteurs français d'émettre l'hypothèse que cette attaque a été longuement pensée, étant donné qu'il faille une certaine préparation à cela. Kevin Limonier précise que dans cette nouvelle ère du numérique, les attaques peuvent provenir de n'importe où au vu du grand nombre d'appareils connectés. Aussi, les attaquants peuvent se cacher derrière une tout autre identité. Ce qui fut le cas lors de l'attaque contre TV5 Monde:

> « Hackers can conduct « false flag » operations, attacks designed to look like they are coming from another group or nation-sate. In April 2015, for example, attackers claiming to be from the Islamic State's Cyber Caliphate shut down transmissions from France's TV5 Monde television channel and posted jihadist propaganda on websites. Two months later, French investigators and cybersecurity experts reported that Internet addresses liked to be the Cyber Caliphate website and techniques used in the attack pointed Russian group as responsible for the attack, though the motive remained elusive »[30]

Adam Segal précise que la Russie représente une menace considérable pour les autres États, puisque de nombreuses attaques y ont été reliées:

> « Putin has relied heavily on what some have termed hybrid or « nonlinear » war. He has used espionage, sabotage, economic coercion, and propaganda, as well as special forces or militias ».[31]
>
> « Unlike the United States, Russia relies on criminals, patriotic

---

30 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.12-13).* Etats-Unis: 1st Edition.

31 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.45).* Etats-Unis: 1st Edition.

> hackers, and other proxies, as seen in the conflicts with Estonia, Georgia, and Ukraine ».[32]

Adam Segal nous éclaire également sur le fait que ces types d'attaques, quand elles sont orchestrées par un État, n'ont pas pour but de détruire, mais d'influencer les relations diplomatiques et politiques bilatérales ou multilatérales. Adam Segal citera Eric Rosenbach, assistant du secrétaire de la défense du Pentagone:

> « The space between [...] You have diplomacy, economic sanctions... and then you have military action. In between there's this space, right ? In cyber, there are a lot of things that you can do in that space between that can help us accomplish the national interest [...] This gives states a whole lot of room to maneuver, to push the other side up to the point of violent conflict »[33].

Afin de se protéger contre les cyberattaques, l'auteur semble convaincu qu'il faille que les gouvernements coopèrent avec le secteur privé, « private firms own the vas majority of telecom, energy, and transportation networks »[34]. Cependant, il précise également que cette coopération entre « publique » et « privé » ne se tiendra pas sur un pied d'égalité. Le secteur public dévoilera forcément moins d'informations, pour la protection de leurs sources et méthodes d'actions « Government only inhales, it never exhales »[35].

---

32 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.93).* Etats-Unis: 1st Edition.

33 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.45).* Etats-Unis: 1st Edition.

34 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.36).* Etats-Unis: 1st Edition.

35 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.105).* Etats-Unis: 1st Edition.

D'après Adam Segal dans le cyberespace, deux puissances tiennent réellement le pouvoir. En effet, il s'agit de la Chine et des États-Unis. Il va d'ailleurs citer Barack Obama, ancien Président des États-Unis:

> « We have owned the Internet. Our companies have created it, expanded it, perfected it in ways that can't compete. And oftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interest »[36]

Cependant, la Russie semble se tenir juste derrière. Les meilleurs hackers du monde se trouvent en Russie, laissant rarement de traces détectables dans leurs opérations de cyberattaques: « I worry a lot more about the Russians [...] than the Chinese [...] The Russian cyber threat is more severe than we have previously assessed »[37]. Tandis que la France, semble détenir un potentiel en matière d'attaque, elle se montre encore sceptique à ce sujet.

1.7 Le rapport dialectique entre territoire physique et territoire virtuel (cyberspatial)

Les rapports entre le territoire physique et le territoire virtuel font souvent l'objet de certaines connivences. En effet le « cyberspatial », tel que le nomme Pierre-Léonard Harvey, représente un aspect qu'il est nécessaire de prendre en compte à la mise en place de quelconque plan de cybersécurité. Au sein du cyberespace les

---

36 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.151).* Etats-Unis: 1st Edition.

37 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.40).* Etats-Unis: 1st Edition.

frontières peuvent parfois paraître floues, puisque contrairement au territoire physique elles ne sont pas explicitement délimitées. Or, même si le cyberespace est régi selon le droit international, les lois varient selon les pays. Pierre-Léonard Harvey, mettait en évidence l'impact du territoire avec les « communautiques », c'est-à-dire, les communautés virtuelles:

> « Nous allons essayer de mieux cerner les rapports que les groupes humains entretiennent avec l'espace, pour tenter d'apprécier ensuite en quoi l'appropriation des médias interactifs comporte un impact significatif sur la structuration des ensembles humains et sur les collectivités. »[38]

Quels sont les impacts de la connectivité sur les communautés ? Il semble qu'il s'agit bien là, d'un aspect important à prendre en compte, au vu de la mise en place d'une stratégie de cyberdéfense, d'autant plus si elle est directement adressée au grand public.

Selon Pierre-Léonard Harvey, dépourvu de connectivité, le territoire, l'espace physique, la proxémique permettaient en grande partie la construction de communautés. Les technologies de l'information et de la communication (TIC) ont, en quelque sorte apportées de nombreux changements à ce fonctionnement.

> « Quels sont les traits et les caractéristiques d'une communauté de l'avenir où le face à face, lié au rapprochement des corps, n'est plus obligatoirement la condition nécessaire de la proximité des esprits ? »[39]

---

[38] Harvey, P-L. (1999). Cyberespace et communautique. *Appropriation, réseaux, groupes virtuels (p.34).* Canada: Les presses de l'Université Laval.

[39] Harvey, P-L. (1999). Cyberespace et communautique. *Appropriation, réseaux, groupes virtuels (p.39).* Canada: Les presses de l'Université Laval.

Aussi, l'auteur apporte un autre aspect que présente le cyberespace et qui nous semble pertinent dans ce contexte. Il s'agit de celui de l'identité et du statut. Nous le savons, au sein du cyberespace il peut parfois être difficile de tracer l'identité d'un individu. Le monde virtuel détient cette capacité de permettre à ses utilisateurs de garder leur anonymat, ou à l'inverse de se donner une toute autre identité, un tout autre statut. L'auteur va citer Meyrowitz en précisant qu'il qualifiait « ce phénomène par l'expression no sens of place. » [40] C'est-à-dire que dans la plupart des cas, nous constatons souvent l'absence, premièrement, de territoire, et deuxièmement de hiérarchie au sein de cet espace.

> « L'évolution des médias a changé la logique de l'ordre social et des regroupements humains. Elle a restructuré les relations entre la place physique et la place sociale à l'intérieur des communautés virtuelles. »[41]

Cela modifie les rapports sociaux et entraine donc un tout nouvel ordre social auquel il faut s'adapter. Selon l'auteur avant cette montée de la connectivité, des groupes sociaux étaient créés selon leurs tendances respectives. À l'heure de la connectivité, nous allons plutôt sur une uniformisation de ces tendances, et donc des différents groupes:

> « En d'autres mots, voici peut-être le réel impact de l'autoroute électronique qui intégra des territoires virtuels et des voies d'accès pour toutes les instances physiques et sociales traditionnelles:

---

[40] Harvey, P-L. (1999). Cyberespace et communautique. *Appropriation, réseaux, groupes virtuels (p.51).* Canada: Les presses de l'Université Laval.

[41] Harvey, P-L. (1999). Cyberespace et communautique. *Appropriation, réseaux, groupes virtuels (p.52).* Canada: Les presses de l'Université Laval.

> éducation, santé, gouvernements, industrie, domicile, groupes communautaires, armés, police, etc. »[42]

Des corrélations se font donc ressentir entre la « géographie physique » et la « géographie sociale ». Cet anonymat, ce bouleversement social que présentent Internet et la connectivité entraînent également la création de nouvelles formes de rapports sociaux entre les différents groupes:

> « C'est l'idée de settings complexe au sens que lui donne Goffman (1973) dans ses « mises en scène de la vie quotidienne ». La notion de situation sociale a généralement été conçue en termes de coordonnées espace/temps: où est l'individu, à quel moment y est-il ? L'impact des nouveaux médias électroniques modifie les frontières des situations en incluant et en excluant les participants de façon tout à fait nouvelle. »[43]

---

[42] Harvey, P-L. (1999). Cyberespace et communautique. *Appropriation, réseaux, groupes virtuels (p.53).* Canada: Les presses de l'Université Laval.

[43] Harvey, P-L. (1999). Cyberespace et communautique. *Appropriation, réseaux, groupes virtuels (p.52).* Canada: Les presses de l'Université Laval.

CHAPITRE II

CADRE THÉORIQUE

2.1 Simulacre des rapports étatiques et organisationnels dans le cyberespace

2.2 « L'approche constructiviste comme construction sociale » de Berger et Luckmann

L'approche constructiviste de Berger et Luckmann (1996) considère « la réalité comme une construction sociale ». Ils envisagent la réalité sociale en lien avec les acteurs sociaux. Cette réalité se construit autour de deux notions: l'externalisation (l'homme construit la réalité sociale) et l'internalisation (l'homme intériorise la réalité sociale à travers la socialisation)[44].

Berger et Luckmann nous définissent précisément ce qu'ils entendent par réalité. Il va s'agir des actions qui ont lieu et que nous ne pouvons prévoir:

> « Il nous suffira, dans le cadre de notre propos, de définir la « réalité » comme une qualité appartenant à des phénomènes que nous reconnaissons comme ayant une existence indépendante de notre propre volonté (nous ne pouvons pas les « souhaiter »), et de définir la

---

44 Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité. Etats-Unis: Doubleday & Company Inc.

> « connaissance » comme la certitude que les phénomènes sont réels et qu'ils possèdent des caractéristiques spécifiques. »[45]

Selon les auteurs, notre monde serait composé de plusieurs réalités dont l'Homme aurait conscience. Ainsi, la réalité vers laquelle l'Homme serait le plus attiré inconsciemment, est celle de la réalité quotidienne:

> « En conséquence il est nécessaire de lui accorder toute notre attention. Je vis la vie quotidienne dans un état d'éveil aigu. Cet état qui permet d'exister à l'intérieur de cette réalité quotidienne, et de l'appréhender, je le considère comme normal allant de soi, c'est-à-dire qu'il constitue mon attitude naturelle. »[46]

La réalité de la vie quotidienne est donc appréhendée par la l'Homme de façon naturelle. Cette réalité, il doit la partager avec autrui: « En effet, je ne peux pas exister dans le monde de la vie quotidienne sans interagir et communiquer continuellement avec les autres. »[47]. Au sein de cette réalité, la plupart des Hommes auront en commun leur comportement et leurs connaissances, une « routine allant de soi du quotidien. »[48]

Berger et Luckmann se servent de la métaphore de la pièce de théâtre pour

---

[45] Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité (p.39). Etats-Unis: Doubleday & Company Inc.

[46] Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité (p.68). Etats-Unis: Doubleday & Company Inc.

[47] Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité (p.70). Etats-Unis: Doubleday & Company Inc.

[48] Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité (p.71). Etats-Unis: Doubleday & Company Inc.

expliciter cette réalité de la vie quotidienne. En effet au théâtre, chaque acte séparé par la tombée du rideau pourrait représenter chacune des réalités de la vie quotidienne. Ainsi, quand le rideau est levé le spectateur entre dans une toute autre réalité qu'il est libre d'interpréter personnellement et quand le rideau retombe c'est un retour à la réalité:

> « Des « commutations » similaires prennent place entre le monde de la vie quotidienne et le monde du jeu, qu'il soit enfantin, ou, plus subtilement, adulte. Le théâtre fournit une excellente illustration d'un tel jeu de la part des adultes. La transition entre les réalités est marquée par le rideau qui se lève et tombe. Quand le rideau se lève, le spectateur est « transporté dans un autre monde », avec ses propres significations et son ordre personnel qui n'est pas nécessairement le même que celui de la vie quotidienne. Quand le rideau tombe, le spectateur « retourne à la réalité », c'est-à-dire à la réalité souveraine de la vie de tous les jours, en comparaison de laquelle la réalité présentée sur scène apparaît maintenant ténue et éphémère même si elle a pu paraître frappante quelques instants auparavant. »[49]

Mise à part la réalité qui se produit à l'instant même, ce que les auteurs appelleront le « ici et maintenant », l'Homme est également conscient d'autrui, et des activités d'autrui: ils sont « capables d'objectivisation ». Si l'Homme est capable d'objectivisation, le langage est le moyen qui lui permet de partager sa réalité et les actions qu'il vit ou qu'il a vécues, avec autrui:

> « Les transcendances possèdent des dimensions spatiales, temporelles et sociales. Grâce au langage, je peux transcender le fossé qui sépare ma zone de manipulation de celle d'autrui; je peux synchroniser ma séquence temporelle personnelle (biographie) avec la sienne; et je peux parler d'individus et de collectivités qui sont pourtant absents de

---

[49] Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité (p.73). Etats-Unis: Doubleday & Company Inc.

> notre interaction en face à face. En conséquence de ces transcendances le langage est capable de « rendre présent » une diversité d'objets qui sont à la fois spatialement, temporellement et socialement absent du « ici et maintenant » ».[50]

Ces actions accomplies et partagées avec autrui vont permettre à l'Homme de prendre part à la société et notamment de détenir une place au sein de celle-ci, une sorte de hiérarchie va apparaître et c'est ainsi que va prendre place « les origines de tout ordre institutionnel »[51]. L'Homme va construire le monde qui l'entoure selon son ouverture d'esprit et son évolution, c'est ainsi que les institutions existent, grâce aux individus et leurs actions au sein de la société. L'homme construit son histoire et se rapporte continuellement aux évènements prenant part au sein de cette même histoire pour rendre compte des institutions existantes:

> « L'univers symbolique prend sa racine dans la constitution de l'homme. Si l'homme en société est un bâtisseur du monde, c'est que cela est rendu possible grâce à son ouverture au monde constitutionnellement donnée, qui implique déjà le conflit entre l'ordre et le chaos. L'existence humaine est, ab initio, une extériorisation continuelle. Au fur et à mesure que l'homme s'extériorise, il construit le monde dans lequel il s'extériorise. Dans le processus d'extériorisation, il projette ses propres significations dans la réalité. Les univers symboliques, qui proclament que toute réalité est signifiante humainement et en appellent au cosmos entier pour signifier la validité de l'existence humaine, constituent les domaines les plus vastes de cette protection. »[52]

---

50 Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité (p.90). Etats-Unis: Doubleday & Company Inc.

51 Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité (p.135). Etats-Unis: Doubleday & Company Inc.

52 Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité (p.178). Etats-Unis: Doubleday & Company Inc.

L'identité est également une notion importante de ce processus de construction sociale de la réalité. En effet, un individu va bâtir son identité de par les relations sociales qu'il entretient avec autrui dans la société. Vice et versa cette société va être sujette à différents changements de par le processus de construction d'identité de l'individu:

> « La société possède une histoire au cours de laquelle des identités spécifiques émergent; cette histoire est, cependant, produite par des hommes détenant une identité spécifique. »[53]

De plus selon les auteurs, l'identité psychologique d'un individu sera également définie par les relations sociales et la réalité que connaît cet individu. Ainsi, les auteurs se questionnent sur la place des diverses psychologies dans l'histoire:

> « Pourquoi une psychologie devrait-elle en remplacer une autre dans l'histoire ? La réponse générale consiste à affirmer qu'un tel changement surgit quand l'identité apparaît comme problématique pour une raison ou pour une autre. [...] Des changements radicaux dans la structure sociale [...] peuvent entraîner des changements parallèles dans la réalité psychologique. Dans ce cas, de nouvelles théories psychologiques peuvent apparaître parce que les anciennes ne permettent plus d'expliquer de façon adéquate les phénomènes empiriques en cours. [...] La manipulation idéologique délibérée effectuée par des groupes d'intérêts politiques constitue une de ces possibilités historiques. »[54]

---

[53] Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité (p.271). Etats-Unis: Doubleday & Company Inc.

[54] Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité (p.270-280). Etats-Unis: Doubleday & Company Inc.

2.3 La perspective foucaldienne du discours contrôlé

Nous envisageons notre étude dans perspective foucaldienne d'analyse du discours avec le principe que dans toute société le discours soit contrôlé, afin de réduire, voire d'éliminer l'influence du contre-pouvoir:

> « Voici l'hypothèse que je voudrais avancer pour fixer le lieu – ou peut-être le très provisoire théâtre – du travail que je fais : je suppose que dans toute société la production du discours et à la fois contrôlée, sélectionnée, organisée et redistribuées par un certain nombre de procédures qui ont pour rôle d'en conjurer les pouvoirs et les dangers, d'en maîtriser l'évènement aléatoire, d'en esquiver la lourde, la redoutable matérialité ».[55]

Nous le constatons particulièrement dans le cas des discours politiques qu'il s'agit d'une procédure bien rodée. Les protagonistes, auteurs et orateurs de ces discours, mettent tout en oeuvre afin de légitimer leurs allocutions aux yeux de leurs publics cibles et ainsi, dans cette visée de les convaincre. Michel Foucault met en avant les différentes embûches que rencontre un orateur lors de l'élaboration et de la mise en scène de son discours, dont celui de « l'exclusion »:

> « Dans une société comme la nôtre, on connaît, bien sûr, les procédures d'exclusion. La plus évidente, la plus familière aussi, c'est l'interdit. On sait bien qu'on n'a pas le droit de tout dire, qu'on ne peut pas parler de tout dans n'importe quelles circonstances, que n'importe qui, enfin, ne peut pas parler de n'importe quoi. »[56]

---

55 Foucault, M. (1971). L'ordre du discours (p.11). France: Gallimard.

56 Foucault, M. (1971). L'ordre du discours (p.11). France: Gallimard.

2.3.1 Le discours : entre domination et vérité

Le discours peut dans certains cas être synonyme de pouvoir et de domination. L'auteur d'un discours, grâce à ses paroles va influencer son public pour le rattacher à sa propre cause. D'après Michel Foucault, nous nous trouvons dans cette nouvelle ère, où les capacités oratoires ne suffisent plus, mais où le public va prendre en compte le sens et l'intérêt du message qui va être transmis. Une nouvelle ère donc, particulièrement portée sur le contenu du message, à la recherche d'une certaine vérité:

> « Entre Hésiode et Platon un certain partage s'est établi, séparant le discours vrai et le discours faux; partage nouveau puisque désormais le discours vrai n'est plus le discours précieux et désirable, puisque ce n'est plus le discours lié à l'exercice du pouvoir. Le sophiste est chassé. »[57]

Or, d'après Michel Foucault, cette recherche de vérité au sein des discours est hypocrite. En effet, le public peut paraître satisfait que son orateur ait fait preuve de vérité au sein de ses propos. Cependant, cette vérité sert également à l'exclusion:

> « Ainsi n'apparaît à nos yeux qu'une vérité qui serait richesse, fécondité, force douce et insidieusement universelle. Et nous ignorons en revanche la volonté de vérité, comme prodigieuse machinerie destinée à exclure. »[58]

---

[57] Foucault, M. (1971). L'ordre du discours (p.18). France: Gallimard.

[58] Foucault, M. (1971). L'ordre du discours (p.22). France: Gallimard.

Michel Foucault met aussi l'accent sur le rôle de l'auteur. Un discours peut-être interprété de différentes façons selon chaque individu. C'est ainsi, que l'auteur va jouer un rôle primordial, puisque de par son interprétation il va donner un sens à son discours: « L'auteur est ce qui donne à l'inquiétant langage de la fiction, ses unités, ses noeuds et cohérence, son insertion dans le réel. »[59]

2.3.2 Le rôle de l'acteur

Michel Foucault précise également que l'auteur d'un discours doit respecter diverses règles qui encadrent ce discours même, que seuls les experts les plus aguerris sont capables de déceler: « nul n'entrera dans l'ordre du discours s'il ne satisfait à certaines exigences ou s'il n'est, d'entrée de jeu, qualifié pour le faire. »[60]. Ces règles se nomment d'après lui des « rituels ». Ces rituels contiennent toutes les composantes du discours de l'individu:

> « La forme la plus superficielle et la plus visible de ces systèmes de restriction est constituée par ce qu'on peut regrouper sous le nom de rituel; le rituel définit la qualification que doivent posséder les individus qui parlent (et qui, dans le jeu d'un dialogue, de l'interrogation, de la récitation, doivent occuper telle position et formuler tel type d'énoncés); il définit les gestes, les comportements, les circonstances, et tout l'ensemble de signes qui doivent accompagner le discours; il fixe enfin l'efficace supposée ou imposée des paroles, leur effet sur ceux auxquels elles s'adressent, les limites de leurs contraignantes. »[61]

---

[59] Foucault, M. (1971). L'ordre du discours (p.30). France: Gallimard.

[60] Foucault, M. (1971). L'ordre du discours (p.39). France: Gallimard.

[61] Foucault, M. (1971). L'ordre du discours (p.41). France: Gallimard.

Pour l'auteur la doctrine par exemple est un discours qui sert à la fois à réunir les individus faisant partie d'une certaine idéologie et d'en exclure le reste:

> « Au premier regard, c'est l'inverse d'une « société de discours » que constituent les « doctrines » (religieuses, politiques, philosophiques): là le nombre des individus parlants, même s'il n'était pas fixé, tendait à être limité; et c'est entre eux que le discours pouvait circuler et être transmis. La doctrine, au contraire, tend à se diffuser; et c'est par la mise en commun d'un seul et même ensemble de discours que des individus, aussi nombreux qu'on veut les imaginer, définissent leur appartenance réciproque. »[62]

2.3.3 Prendre part à « L'ordre du discours »

La solution pour entendre une large majorité des discours prononcés dans la société serait selon l'auteur, l'éducation. En effet, l'éducation nous permettrait d'acquérir certaines bases nous permettant de différencier et de comprendre les rouages d'une diversité de discours, puisque tel qu'il le précise:

> « Le discours n'est rien de plus qu'un jeu, d'écriture dans le premier cas, de lecture dans le second, d'échange dans le troisième, et cet échange, cette lecture, cette écriture ne mettent jamais en jeu que les signes. Le discours s'annule ainsi, dans sa réalité, en se mettant à l'ordre du signifiant. »[63]

2.4 La perspective d'Adam Segal: The Hacked World Order et les nouveaux enjeux de gouvernance

---

[62] Foucault, M. (1971). L'ordre du discours (p.43-44). France: Gallimard.

[63] Foucault, M. (1971). L'ordre du discours (p.51). France: Gallimard.

2.4.1 Les affrontements au sein du cyberespace

Adam Segal au sein de son ouvrage *« The Hacked World Order »*, nous livre un récit des affrontements entre les différentes nations au sein du cyberespace à l'heure de l'ère du numérique. En effet, il commence son ouvrage avec une comparaison surprenante, celle du commencement de la Guerre Froide avec celle du commencement des affrontements dans le cyberespace, qu'il surnomme « year zero »:

> « Just as historians consider 1947 as the year that two clear sides in the Cold war emerged, we will look back at the stretches roughly from June 2012 to June 2013 as year zero in the battle over cyberspace. »[64]

L'une des plus importantes cyberattaques au monde, a eu lieu en Iran, quant un virus, nommé *Stuxnet* a pénétré le réseau des centrales nucléaires iraniennes et a engendré de graves conséquences sur celui-ci. Adam Segal précise qu'auparavant les virus s'incrustaient dans les systèmes pour dérober ou détruire des informations. Mais depuis *Stuxnet* un virus peut désormais entraîner des modifications sur toute une infrastructure physique.

Plusieurs techniques sont utilisées par les hackers lors de cyberattaques. Souvent, beaucoup moins dangereuses que celles qui ont eu lieu en Iran, mais plus facilement réalisables. Comme le processus nommé « spear-fishing » utilisé lors de la cyberattaque contre TV5 Monde. En effet, comme nous l'avions précisé

---

64 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.1).* Etats-Unis: 1st Edition.

précédemment il s'agit d'un e-mail envoyé à un individu, donnant l'apparence dans le contenu du message, de quelqu'un de connu de la personne. Un message qui peut être amical ou d'apparence professionnelle, avec une pièce jointe rattachée. Cette pièce jointe, quand elle sera ouverte par l'individu va libérer un virus qui se propagera non seulement au sein de l'ordinateur, mais également au sein de tout le réseau informatique lié à cet ordinateur, dans l'optique d'un vol de données:

> « Opening an attachment or clicking on a link downloads software that allows attackers to gain control of your computer. They then gradually expand their access and move into different computers and networks, sending files back to computers »[65]

Les cyberattaques ne sont pas uniquement lancées par des groupes de hackers qui se disent agir positivement pour la nation (aussi surnommés les « White Hat »), tel que le célèbre groupe *Anonymous* ou négativement (les individus aussi surnommés « Black Hat »). Les États, même s'ils ne le déclarent évidemment pas, participent également à ces affrontements au sein du cyberespace, selon leurs propres intérêts:

> « A group of Russian hackers used the malware for espionnage directed at NATO, the European Union, Poland, Ukraine, private energy organisations, and European telecommunications companies. Yet they could also reprogram it as an attack tool capable of crippling energy supplies, water-distribution and water-filtration systems, or

---

65 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.7).* Etats-Unis: 1st Edition.

financial transactions. »[66]

2.4.2 « The battle over cyberspace »

Dans cette « bataille au sein du cyberespace », de nombreux États et organisations internationales, comme la France ou l'Union européenne se battent pour garder une certaine notion de souveraineté. En effet, les États-Unis détenant les infrastructures physiques du réseau Internet détiennent également un certain contrôle sur celui-ci.

L'autre challenge pour certain pays, et particulièrement la France, est de mettre en place divers partenariats entre l'État, les entreprises privées travaillant sur la connectivité et les nouvelles technologies de l'information et de la communication. Non pas uniquement, dans une visée économique, mais également afin de fournir divers processus et outils performants à l'État:

> « The challenge for governments wanting to harness the energy and innovation of the private sector is that technology compagnies increasingly do more business abroad than they do at home. »[67]

Également, la France souhaiterait une mise en place d'un partenariat solide entre l'État et les entreprises privées afin de combattre les différentes menacent qui

---

66 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.13).* Etats-Unis: 1st Edition.

67 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.37).* Etats-Unis: 1st Edition.

planeraient sur son territoire:

> « US and European governments expect tech companies to help them deliver their diplomatic messages and disrupt those of extremists, jihadists, and rogue states [...] In an interview before he traveled to Silicon Valley, after the January 2015 terrorist attacks in Paris, French interior minister Bernard Cazeneuve said « We are facing a new threat. We need tech companies to realize that they have an important role to play. »[68]

Le cyberespace devenu une potentielle menace pour les États, ceux-ci ont créés différentes agences de protection au sein du gouvernement, parfois rattachées à la branche militaire du pays, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en France, directement rattachée au Secrétaire général de la Défense et de la Sécurité nationale (SGDSN):

> « Forty-one nation-states have cyber warfare doctrine; seventeen reportedly have offensive capabilities. It is cheap and easy to break into machines, but much more difficult to design an attack that creates real impact. »[69]

2.4.3 La France et le principe de protection des données personnelles

Au cours de cette bataille au sein du cyberespace, la France et l'Union européenne

---

[68] Adam Segal, The Hacked World Order. How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age, 1st Edition, 2016, p.173

[69] Adam Segal, The Hacked World Order. How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age, 1st Edition, 2016, p.37

souhaitent également détenir une position de leader. Cependant, elle peine à y arriver puisque ne possédant pas les moyens matériels et humains suffisant, contrairement à certaines puissances comme les États-Unis ou la Russie. Néanmoins, elle détient un atout important, celui de son histoire. En effet, la France, pays des Lumières, des libertés individuelles et des Droits de l'Homme s'est toujours battue dans ce sens et elle souhaite également le faire au sein du cyberespace. C'est ainsi qu'elle se positionne comme leader des libertés individuelles dans ce monde parallèle:

> « European diplomats have been instrumental in generating UN resolutions and other international declarations that question the legitimacy of mass surveillance and promote the protection of online rights. »[70]

En effet, un nouvel enjeu important apparaît avec la collecte des données personnelles, tant pour les entreprises privées que pour les États. Comment les États peuvent-ils protéger leurs citoyens et sécuriser leurs territoires sans pour autant empiéter sur la vie personnelle de chaque individu ? Cette problématique est notamment pertinente dans le contexte des attaques terroristes ou dans le cas d'agissement de groupuscules aux idéologies controversées, puisque comme nous l'avions précisé précédemment ils utilisent particulièrement Internet et la connectivité, pour propager leurs idéologies:

> « Many liberal democracies prevent the flows of certain types of content, [...] France demanded information from Twitter about users who violated French law by publishing anti-Semitic comments under the hashtag

---

70 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.40).* Etats-Unis: 1st Edition.

#UnBonJuif (a good Jew) and #UnJuifMort (a dead Jew) »[71]

Adam Segal aborde également la notion de « contrat social ». En effet, dans les démocraties libérales la relation entre l'État et le pouvoir qu'il détient sur le cyberespace serait parfois épineuse. Jusqu'à quel point un État serait-il prêt à étendre son pouvoir pour défendre son point de vue, ses valeurs au sein du cyberespace ? Cette notion du contrat social va particulièrement apparaître en Europe, où l'auteur nous citera divers grands philosophes:

> « These visions of the social contract, drawn from British philosopher John Locke and French Enlightenment thinker Jean-Jacques Rousseau, emphasize the recognition of human rights online, government transparency, and checks and balances. »[72]

À l'opposé des démocraties libérales, les États totalitaires pourraient se servir du cyberespace afin d'étendre leur pouvoir et de servir leurs propres intérêts, tant au niveau de leurs populations respectives, qu'à l'international:

> « By contrast, the narrative in one-party an authoritarian states is primarily about how to optimize data collection to serve national goals, including economic development and national security. »[73]

---

71 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.43).* Etats-Unis: 1st Edition.

72 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.48).* Etats-Unis: 1st Edition.

73 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.48).* Etats-Unis: 1st Edition.

Les cyberattaques plus que des dégâts techniques entraînent des conflits au sein des relations diplomatiques. Mais pas uniquement, certains pays ont été soupçonnés d'avoir espionné leurs alliés, parfois même certaines personnalités politiques dans le cadre de leurs vies personnelles. Ce fut le cas, comme le précise Adam Segal lors de l'affaire WikiLeaks:

> « June 2015, WikiLeaks posted documents purporting to show that the NSA had monitored the communications of hight-level French officials, including President François Hollande, Nicolas Sarkozy, and Jacques Chirac »[74]

C'est à partir de cet évènement, que l'Europe et les États-Unis ont soudainement arrêté de coopérer mutuellement. Cependant, en 2015 de nombreuses attaques terroristes sont survenues en France avec les attentats de janvier 2015 à Charlie Hebdo et ceux du 13 novembre 2015 faisant des explosions et des fusillades dans tout Paris, du 10e au 11e arrondissement en passant par la salle de concert, le Bataclan fréquenté au moment même, jusqu'au Stade de France. Ces attaques ont notamment beaucoup marqué la France et le monde entier qui l'a rendue hommage. Cette menace du terrorisme islamiste extrémiste ne cesse toujours pas en 2017 sur le territoire français et européen, avec de nouvelles attaques qui se produisent régulièrement. C'est ainsi que la relation entre la France et les États-Unis s'est progressivement rétablie. Adam Segal nous le rappelle également:

> « The continuing chaos in the Middle East, particularly the rise of the Islamic State in Iraq and Syria (ISIS), heightened the sens of interdependence with the United States. Thousands of French and

---

74 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.144).* Etats-Unis: 1st Edition.

> German citizens have traveled to Iraq, Syria, and Yemen. The real fear that they would return and commits acts of violence played out when two brothers armed with assault rifles burst into Paris offices of Charlie Hebdo, killing eleven and injuring twelve. »[75]

L'Europe fortement engagée au sein de la protection des données personnelles et de leur usage, se sent même prête à faire le pas sur la protection des données si cela permettait d'aider la lutte contre le terrorisme:

> « Most European, by contrast, were likely to view the terrorist threat as a criminal matter, allowing the maintenance of individual privacy [...] European and US intelligence collaborated closely, and in several instances, German, French, and other European security officials sidestepped privacy protections and sideline privacy advocates. »[76]

En effet, le terrorisme est désormais une réelle menace et comme nous l'avions précisé précédemment, les terroristes islamistes sont des professionnels de la communication, ils savent très bien comment agir au sein du cyberespace afin de conquérir leur public cible:

> « As ISIS approached the Iraqi capital, users who searched for « Bagdad » in Arabic on Twitter found the top image showed ISIS's black flag flying over Baghdad and warning « Baghdad, we're coming » »[77]

---

75 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.150).* Etats-Unis: 1st Edition.

76 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.148).* Etats-Unis: 1st Edition.

77 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.185).* Etats-Unis: 1st Edition.

Les techniques de DAECH sont de plus en plus sophistiqués et le groupuscule détient une technique bien à lui pour propager son idéologie:

> « ISIS's social media usage has a strategic logic. As Berger writes, « Fear and brutality are a crucial part of its strategy to win on the ground, by amplifying fear and demoralizing those who might stand up to it. »[78]

Les États-Unis et l'Union européenne ont donc réagi ensemble contre la menace et ont tenté un blocage de DAECH sur le réseau Internet, avec des résultats positifs qui se sont fait ressentir très rapidement:

> « The US and European governments have vacillated between blocking ISIS and other groups from using Internet platforms to radicalize, recruit, and motivate and disrupting or competing with the Islamic State's narrative. For liberal democracies, taking down content and accounts raises obvious sensitives about free speech rights, which the line of protected speech [...] By March 2015, CTIRU had removed 75,000 pics of online extremist material. »[79]

Nous l'avons donc constaté, contrairement aux États-Unis, le droit au respect des données personnelles en Europe est un réel enjeu et un principe fondamental qui semble ancré et immuable dans la société:

---

78 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.187-188).* Etats-Unis: 1st Edition.

79 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.189).* Etats-Unis: 1st Edition.

> « The divide between Europe and United States on privacy is real, and it would be a mistake to characterize the impulse to protect government secrets and the data of citizens against espionage and foreign surveillance simply as a mask for European protectionism. The idea of privacy as a humain rights is a basic European principle. »[80]

Il y a fondamentalement en France et en Europe, une forte envie de détenir un réseau Internet complètement indépendant, notamment vis-à-vis des États-Unis, qui, nous le rappelons, détiennent la majorité des infrastructures physiques permettant le fonctionnement d'Internet. L'Europe essaie maintenant depuis plusieurs années de mettre en place des lois afin de limiter cette utilisation des données personnelles, surtout à l'étranger:

> « The original directive went into effect in 1995 and landed that every member of the European Union create national privacy regulations and a Data Protection Authority to protect citizens' privacy. [...] The directives requires that companies ask for permission before they gather private information and gives users the right to review the data and correct inaccuracies. [...] Companies cannot share personal information with each other or accros borders without express permission from users. Any company that collects information must register its activities with the government. »[81]

Les lois concernant la protection des données personnelles sont encore très floues, plus précisément en France et en Europe, laissant parfois la porte ouverte à certaines organisations:

---

80 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.151).* Etats-Unis: 1st Edition.

81 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.157).* Etats-Unis: 1st Edition.

> « If the NSA wants access to data in the United States, it needs the permission of the Foreign Intelligence Surveillance Court. Foreign user data in Europe can be collected without a court order. Moreover, the British, French, and German intelligence agencies do not require a court order for national surveillance. »[82]

Adam Segal nous rappelle un point qui semble primordial dans cette bataille autour de la protection des données personnelles et de l'indépendance de l'Europe au sein du cyberespace. En effet, il va s'agir comme le précise l'auteur de « two cultures of privacy ». L'Union européenne et les États-Unis n'ont tout simplement pas la même estimation de ce qui doit être considéré comme étant personnel et privé, et de ce que l'on pourrait se permettre de dévoiler et de partager. Il y a donc bien là, une différence importante de culture entre ces deux puissances:

> « The finding emerge from two major cultural differences between the United States and Europe. The first has to do with different ideas about regulation [...] privacy is a humain right in Europe, and government is expected to actively regulate technology companies to protect it. In the United States, the cliché goes the users do not care about privacy. »[83]

L'auteur nous explique que cette tendance à vouloir protéger les données personnelles et cette vision européenne du respect personnel est en train de conquérir le reste du monde et pourrait devenir dans les années à venir un standard au sein de la réglementation du cyberespace:

---

82 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.159).* Etats-Unis: 1st Edition.

83 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.161).* Etats-Unis: 1st Edition.

> « European Union standards already have a global reach, and privacy standards are only the latest regulations to migrate from Brussels to the rest of the world. [...] On global stage, Europe is convincing many countries around the world to implement privacy laws that follow the European model. The facts speak for themselves: in the last year alone, a dozen countries in Latin America and Asia have adopted European-style privacy law. Not a single country, anywhere, has followed the U.S model. »[84]

Ainsi pour Adam Segal, ce qui semblerait se dessiner dans le futur contexte de cette « bataille au sein du cyberespace » est que chaque parti continuera à défendre sa position: les États-Unis souhaitent garder la main mise qu'ils ont sur le cyberespace au détriment du continent européen, qui tout de même ne se laissera pas faire, en créant de nouvelles alliances pour défendre et propager ses valeurs concernant les libertés individuelles et les droits de l'Homme et surtout pour se défendre contre leur principal ennemi, la Russie:

> « In Asia and Europe, it built alliances to combat and contain the Soviet Union. It advocate for the expansion of participatory democracies, a free press, and the protection of humain rights, unless they undermined the interest of clients states perceived to be on the front lines in the competition with Moscow. »[85]

Enfin, l'auteur termine son ouvrage sur une note plutôt optimiste. En effet, il nous rappelle avant tout que le cyberespace bien plus que représentatif de nouvelles menaces et de nouveaux conflits nous a beaucoup apporté, et que le danger dans ce monde parallèle pourrait bel et bien diminuer grâce au changement de

---

84 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.164).* Etats-Unis: 1st Edition.

85 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age.* Etats-Unis: 1st Edition.

comportement des États:

> « In a description of the emerging conflict in cyberspace, the negative effects on stability and security can overshadow the immense benefits to humanity of a global platform for the sharing of information and knowledge. [...] If states agree to some basic norms of behavior, the hacked world order may also be more human. »[86]

---

86 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.231).* Etats-Unis: 1st Edition.

CHAPITRE III

MÉTHODOLOGIE

3.1 Le concept de « mise en scène » d'Erving Goffman

Erving Goffman nous présente dans son ouvrage *« La mise en scène de la vie quotidienne: la présentation de soi »* l'individu et les actions qu'il entreprend au sein de la société comme une représentation théâtrale. Il s'agit de comprendre les relations sociales et humaines grâce au principe de la mise en scène, normalement utilisée au théâtre:

> « J'examinerai de quelle façon une personne, dans les situations les plus banales, se présente elle-même et présente son activité aux autres, par quels moyens elle oriente et gouverne l'impression qu'elle produit sur eux, et quelles sortes de choses elle peut ou ne peut pas se permettre au cours de sa représentation. »[87]

Cependant, l'auteur nous avertit dès le début de son ouvrage que même si le principe de mise en scène théâtrale et les activités de la vie quotidienne présentent de nombreux points en commun, il y a néanmoins un aspect qui diverge: les prestations scéniques au théâtre sont des fictions, donc préparées, répétées et

---

87 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.9). France: Les éditions de Minuit.

jouées au préalable. Puisque « Le monde, en vérité, est une cérémonie »[88]. E.Goffman nous présente différentes composantes qui permettent aux représentations dramaturgiques de prendre forme. Ces différentes composantes sont également applicables aux situations de la vie quotidienne et plus encore aux organisations et aux États.

3.1.1 Au centre de la représentation: le jeu de l'acteur

Au sein de la représentation, le jeu de l'acteur semble primordial. En effet, l'auteur va nommer cela « la conviction de l'acteur »[89]. L'acteur au sein d'une situation se doit pour qu'elle paraisse réelle et véritable de croire en son rôle et parvenir à faire croire au public qu'il représente le personnage qu'il tente de jouer. Il s'agit comme sur scène, d'un contrat implicite entre le public et les acteurs. Puisque le public a évidemment conscience qu'il s'agit là d'une pièce de théâtre, donc d'une représentation, d'une situation et non d'événements réels. Cependant, il y a de fortes chances qu'il se laisse entraîner si le jeu de l'acteur fusionne parfaitement au rôle.

3.1.2 Définition de la « façade »

E.Goffman explicitera le procédé qu'il nomme « façade ». En effet, il va tout

---

88 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.41). France: Les éditions de Minuit.

89 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.25). France: Les éditions de Minuit.

d'abord distinguer le terme de « représentation » et celui de « façade ». Pour lui, une représentation qualifie l'ensemble des activités de l'acteur sur scène face à son public. Tandis qu'une façade est:

> « La partie de la représentation qui a pour fonction normale d'établir et de fixer la définition de la situation qui est proposée aux observateurs. La façade n'est autre que l'appareillage symbolique, utilisé habituellement par l'acteur, à dessein ou non, durant sa représentation. »[90]

Cette façade serait composée selon l'auteur de trois éléments étant: le décor, l'apparence et la manière. Pour le décor il s'agit tout simplement des éléments d'ornementation présents sur la scène et permettant de former et de créer un certain contexte. Pour l'apparence, ce sont tous les « stimuli dont la fonction à un moment donné est de nous révéler le statut social de l'acteur »[91]. Enfin la manière, va compléter l'apparence et va aider le public à cerner quel est le rôle que joue l'acteur.

Aussi, il semble nécessaire de préciser qu'une façade peut convenir à plusieurs rôles. En effet, E. Goffman explicite que les différents éléments composants la façade, que nous avons vu précédemment, sont calqués sur une image que le public serait capable de reconnaître aisément:

---

90 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.29). France: Les éditions de Minuit.

91 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.31). France: Les éditions de Minuit.

> « Différents rôles peuvent ainsi utiliser la même façade; d'autre part, on notera qu'une façade sociale donnée tend à s'institutionnaliser en fonction des attentes stéréotypées et abstraites qu'elle détermine et à prendre une signification et une stabilité indépendante de tâches spécifiques qui se trouvent être accomplies sous son couvert, à un moment donné. La façade devient une « représentation collective » et un fait objectif. »[92]

3.1.3 « La réalisation dramatique »

Tout autour du jeu de l'acteur, celui-ci va faire en sorte de mettre en évidence ses activités afin qu'elles soient correctement perçues par son public. Il s'agit de « rendre visibles les coûts invisibles »[93]. L'acteur va accorder ses actions avec ses paroles au sein de l'interaction:

> « L'élève attentif » comme l'écrit Jean-Paul Sartre, « qui veut *être* attentif, l'oeil rivé sur le maître, les oreilles grandes ouvertes, s'épuise à ce point à jouer l'attentif qu'il finit par ne plus rien écouter. » C'est ainsi que nombre de personnes se heurtent au dilemme crée par *l'antinomie* qui se produit entre l'expression et l'action. »[94]

3.1.4 Le procédé de « l'idéalisation »

---

92 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.33). France: Les éditions de Minuit.

93 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.38). France: Les éditions de Minuit.

94 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.39). France: Les éditions de Minuit.

Comme son nom l'indique, le procédé de l'idéalisation consiste à rendre idéaliste la représentation et les activités qui en découlent. Comme nous l'avions précisé précédemment, les actions sont basées sur des stéréotypes connus de tous. C'est ainsi que l'acteur s'entend au cours de sa représentation à exagérer ces stéréotypes afin de les rendre plus réalistes:

> « Si quelqu'un se propose d'exprimer des normes idéales au cours de sa représentation, il doit dissimuler ou renoncer à toute action incompatible avec ces normes. Une conduite inadéquate qui procure en elle-même, d'une façon ou d'une autre, des satisfactions continue, en règle générale, à être pratiquée en secret. De cette façon l'acteur est en mesure d'avoir « le beurre, et l'argent du beurre » »[95].

3.1.5 « La cohérence de l'expression »

Il semble important que la totalité de la représentation soit effectuée avec une certaine cohérence. En effet, l'objectif principal d'une telle tâche est de continuer à faire croire au public en la représentation et maintenir cette impression de réalité:

> « Ce qui importe ici, ce n'est pas que la définition momentanée, provoquée par une maladresse, soit en elle-même particulièrement répréhensible, mais c'est plus simplement le fait qu'elle est *différente* de la définition officielle. »[96]

---

95 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.49). France: Les éditions de Minuit.

96 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.55). France: Les éditions de Minuit.

Il arrive bien évidemment que des erreurs se produisent, comme le précise E. Goffman. Dans ce cas l'ensemble de la représentation pourrait en subir les conséquences. Néanmoins, nous pouvons faire en sorte qu'elles se produisent moins fréquemment:

> « Cette indispensable cohérence de l'expression fait apparaître une opposition essentielle entre notre moi intime et notre moi social. En tant qu'êtres humains, nous sommes probablement des créatures dont les démarches varient selon l'humeur et l'énergie du moment. Au contraire, en tant que personnages représentés devant un public, nous devons échapper à ces fluctuations. »[97]

3.1.6 « La représentation frauduleuse »

Comme nous l'avions précisé précédemment, les acteurs sont souvent amenés à mentir à leur public. Il s'agit là d'un jeu très périlleux puisque si le public en vient à découvrir le mensonge de ceux-ci, il y a alors une sorte de rupture du contrat de confiance entre les deux partis et le public aura par la suite beaucoup de mal à croire à nouveau en l'acteur et en ses actions:

> « Non seulement les personnes prises en flagrant délit de mensonge perdent la face pour la durée de l'interaction, mais encore leur façade peut en être ruinée, car beaucoup de publics estiment que, si quelqu'un se permet de mentir une seule fois, on ne doit plus jamais lui faire pleinement confiance. »[98]

---

97 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.59). France: Les éditions de Minuit.

98 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.64). France: Les éditions de Minuit.

3.1.7 « La mystification »

Quand l'auteur aborde le concept de la « mystification », il nous indique en quelque sorte que dans cette relation entre le public et l'acteur, celui-ci doit garder et entretenir une partie de mystère: « Il y a ici une relation entre l'information et le rituel »[99]. En effet, il ne doit pas dévoiler trop ou dévoiler trop peu. Il s'agit en fait d'avoir la capacité de réguler l'information transmise entre les deux partis dans l'interaction. Erving Goffman va d'ailleurs citer E. Durkheim:

> « Émile Durkheim fait une remarque semblable:
> « La personnalité humaine est chose sacrée; on n'ose la violer, on se tient à distance de l'enceinte de la personne, en même temps que, le bien par excellence, c'est la communication avec autrui. » »[100]

3.1.8 L'opposition entre « réalité et simulation »

Erving Goffman dans cette composante, expose le fait que tout individu est capable de mentir, de cacher sa véritable apparence et ainsi de faire croire à son public ce que bon lui semble, s'il joue correctement son rôle: « On voit par là que, bien que les gens soient en général ce qu'ils ont l'apparence d'être, leur apparence pourrait bien, néanmoins, avoir été habilement arrangée ».[101]

---

99 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.69). France: Les éditions de Minuit.

100 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.70). France: Les éditions de Minuit.

101 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.72). France: Les éditions de Minuit.

Bien évidemment cela nécessite beaucoup de travail de la part de l'acteur, qui doit mettre en place cette représentation théâtrale:

> « Et il en est ainsi, semble-t-il, parce que les relations sociales ordinaires sont elles-mêmes combinées à la façon d'un spectacle théâtral, par l'échange d'actions, de réactions et de répliques théâtralement accentuées. »[102]

3.1.9 « Les équipes » au sein de la mise en scène

L'auteur nous présente le terme « d'équipe » pour une situation particulière. En effet, il s'agit d'une situation qui ne serait pas totalement conforme aux représentations ordinaires que nous avons notamment étudiées précédemment. Il va d'ailleurs le définir ainsi:

> « Le terme « équipe de représentation » ou, plus brièvement, « équipe » désignera tout ensemble de personnes coopérant à la mise en scène d'une routine particulière. »[103]

Dans ce contexte, il faudra tout d'abord identifier l'acteur et ses actions, puis le public et les autres protagonistes participant à la représentation ainsi que les différentes actions qui en découlent. Le fait qu'il y ait plusieurs participants à l'interaction change la donne. En effet, « les gens se trouvent placés dans une

---

102 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.73). France: Les éditions de Minuit.

103 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.81). France: Les éditions de Minuit.

étroite relation d'interdépendance mutuelle »[104]. Ainsi afin de donner une représentation qui sera cohérente devant le public-témoin, il paraît essentiel que les acteurs se mettent d'accord sur les actions et les propos qui auront lieu lors de la représentation. E. Goffman nous précise également que souvent dans ces rapports d'équipe, l'un des protagonistes va vouloir prendre la place du leader et va ainsi prendre le contrôle de la représentation. L'étude de la représentation d'équipe est nécessaire puisqu'elle est:

> « La meilleure référence de base, lorsqu'on s'attache particulièrement à l'étude de la maîtrise des impressions, à celle des événements imprévus qui se produisent pendant le développement d'une impression, et à celle des techniques permettant de remercier à ces accidents. »[105]

Enfin, les acteurs faisant partie d'une équipe mettent en place un plan en vue de la mise en scène. Ce plan n'est évidemment pas connu du public. L'auteur nous présente trois types de « secrets » auxquels les protagonistes d'une équipe font souvent appel.

a) Les « secrets inavouables »:

Il s'agit des secrets que l'équipe veut à tout prix occulter puisqu'ils ne correspondraient pas à l'image qu'elle véhicule auprès de son public témoin. Ainsi, le dévoilement de ces informations pourrait ternir son image.

---

104 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.83). France: Les éditions de Minuit.

105 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.82). France: Les éditions de Minuit.

b) Les « secrets stratégiques »:

Ce sont les capacités de l'équipe qui sont gardées secrètes afin de ne pas subir de remontrances de la part du public, au vu de la possible inaptitude de l'équipe à mettre en place les idées qu'elle propose:

> « Les secrets stratégiques sont ceux que les milieux d'affaires et de l'armée utilisent lorsqu'ils préparent un plan d'action contre l'adversaire. » [106]

c) Les « secrets d'initiés »:

Dans ce cas ce sont les secrets qui ont permis aux participants de l'équipe de se réunir. En effet, les protagonistes de l'équipe détiennent un ou plusieurs secrets en commun. Ces secrets qu'ils partagent ont fortement contribué à les réunir et donc à former une équipe qui se différencierait des autres équipes.

3.2 Le discours conflictuel d'Uli Windisch

Notre étude présente de nombreux aspects se rapprochant du discours conflictuel de par nos diverses perspectives et cadrages en présence étant ceux de TV5 Monde, du gouvernement français, de DAECH et du gouvernement russe. Ainsi, il nous semble intéressant de prendre en compte l'aspect conflictuel du discours tel que le perçoit Uli Windisch dans *« Le K-O verbal. La communication conflictuelle »*. Nous étudierons principalement les éléments nous permettant d'affirmer que notre étude comporte bel et bien les composantes rendant compte

---

106 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.138). France: Les éditions de Minuit.

du discours conflictuel. Ces différents éléments sont le « démasquage et le masquage », « la concession », « l'ironie et la simulation », « la représentation fantasmatique » ainsi que « la stratégie de guerre invisible ».

Uli Windisch nous annonce dès le début de son ouvrage que la communication sert bien évidemment à se faire comprendre, mais pas uniquement. Les participants à une interaction utilisent d'autres stratagèmes linguistiques leur permettant d'exprimer des sentiments, de la tristesse, de la joie, de la peur ou encore de la colère: « On peut parler en vue de dominer, de se distinguer, d'exclure. La prise de parole peut servir à lutter, à combattre, à vaincre, à résister, à se révolter »[107]. Selon l'auteur, il ne faut pas confondre la notion de conflit et le discours conflictuel, qui sont deux choses distinctes:

> « Il faut distinguer un conflit d'un discours conflictuel. Parler de conflit revient à faire référence à au moins deux personnes, deux groupes (sociaux, politiques ou autres qui sont en conflit). Le terme de discours conflictuel, en revanche, renvoie de manière plus précise:
>
> 1. À la réalité spécifiquement langagière et discursive d'abord, et à la partie de cette réalité langagière qui est traversée par un conflit.
> 2. Au discours de l'*une* seulement des parties en conflit, au discours du désaccord, d'une divergence, politique ou autre. La personne interpellée devient l'*adversaire* du premier sujet parlant. [...] Ces interventions langagières successives constituent autant de discours conflictuels. Et chaque discours conflictuel se compose d'un ensemble d'énoncés conflictuels. »[108]

---

[107] Windisch, U. (1987). Le K-O verbal: La communication conflictuelle (p.18). France: Edition Broché.

[108] Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.23). France: Les éditions de Minuit.

La composante principale nous permettant de qualifier un discours de « conflictuel » est la relation qu'entretiennent l'interlocuteur et le récepteur au sein d'une interaction. En effet, U.Windisch précise que cette relation est très bien représentée par l'expression bien connue : « l'Autre, c'est l'enfer ». Pour qu'il y ait discours conflictuel, il faut que la relation et les rapports entretenus avec l'Autre soient de nature « négative ».

Avec cet apport négatif dans la conversation, il ne s'agira plus de communiquer pour informer le récepteur, mais à l'opposé, il s'agira de communiquer pour réfuter l'information transmise par le récepteur. Il s'agira donc d'une tentative de destruction de sa face et de production d'un « contre-discours »[109]. Le but ultime de cette action résidera dans le fait de contredire l'information donnée par le récepteur, de la renier et de la qualifier comme étant fausse ou encore sans intérêt. Autre notion très importante dans le discours conflictuel, est celle du « public-témoin »[110]. En effet, bien plus que le fait d'argumenter contre le discours de l'adversaire afin de défendre sa propre opinion et ses propres idées, l'un des principaux objectifs est de rendre compte au public-témoin de la thèse défendue par l'interlocuteur. Afin de défendre ses idées, il se pourrait qu'une mise en scène soit nécessaire:

> « Quel est l'objectif essentiel d'un discours conflictuel si ce n'est de séduire, de rendre complice et de prendre à témoin le public ? C'est la raison pour laquelle un discours conflictuel doit presque automatiquement revêtir un air de mise en scène, un aspect

---

109 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.25). France: Les éditions de Minuit.

110 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.25). France: Les éditions de Minuit.

spectaculaire, théâtral et parfois ludique. »[111]

Au sein de cet affront linguistique entre au moins deux protagonistes, l'un des stratagèmes les plus violents consistera à transformer et à détourner à son avantage les propos de l'adversaire. Cela constitue pour U. Widisch « un véritable viol du discours de l'Autre et, par conséquent, aussi de son identité »[112]. Il s'agit donc à ce moment-là, d'un véritable « K.O verbal ». Cependant, l'auteur précise que ce K.O n'est pas pour autant définitif. En effet, l'adversaire mit K.O a la possibilité de riposter pour ne pas perdre la face devant son public-témoin, puisque « l'issue du combat ne peut, en effet, connaître que deux solutions totalement contradictoires: le rayonnement de la victoire ou l'humiliation de la défaite »[113].

En ordre général quand nous faisons allusion à un discours conflictuel, il y a toujours au sein de l'interaction des rapports d'inégalités et de hiérarchie: « Les rôles, les places, les positions s'échangent d'un discours à l'autre, mais l'élément moteur, à savoir l'établissement d'un rapport hiérarchique et inégalitaire à des fins de domination, subsiste »[114].

3.2.1 « Le démasquage et le masquage »

---

111 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.26). France: Les éditions de Minuit.

112 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.27). France: Les éditions de Minuit.

113 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.27). France: Les éditions de Minuit.

114 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.30). France: Les éditions de Minuit.

Cette stratégie telle que son nom l'indique sert à démasquer les propos cachés de l'adversaire et ainsi à les dévoiler au public-témoin comme étant le véritable discours. Cela est fait encore une fois, dans l'optique de disqualifier l'adversaire. Le masquage est un procédé qui est utilisé tout autant que celui du démasquage au sein de la communication conflictuelle. En effet, autant que l'interlocuteur va essayer de dévoiler les faces cachées du discours de son adversaire, il va essayer dans la même visée de cacher les différentes facettes de son propre discours qu'il ne souhaite pas partager et dévoiler à son public-témoin:

> « Dans un conflit discursif entre deux systèmes d'idées, politiques ou autres, un auteur de discours pourra chercher à supprimer, à taire, à masquer les aspects de son idéologie qui ne correspondent pas à la sensibilité du moment ».[115]

3.2.2 « La concession »

Avec « la concession », l'interlocuteur va tenter de détourner les propos de son adversaire. En effet, suite au démasquage entrepris par celui-ci, il va dans une première phase accepter les propos malveillants à son encontre, puis dans une deuxième phase, va mettre en place un processus de manipulation de la parole de l'adversaire et va détourner ses propos à son avantage. Comme l'auteur le précise:

> « On concède pour mieux agresser. Aux éléments concédés, on

---

115 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.50). France: Les éditions de Minuit.

> donnera progressivement une signification différente, on leur fera dire autre chose, le contraire, et on en tirera finalement des conclusions diamétralement opposées. »[116]

Le but ici, est une fois de plus d'obtenir et de maintenir le soutien du public-témoin. En plus de cela, il s'agira d'élargir son public cible et si possible de rallier à sa propre cause le public adverse:

> « Ce sont bien ces assauts qui constituent l'élément fondamental du discours et non la concession qui n'est effectivement qu'une stratégie. On valide « l'argument-choc » de l'adversaire pour passer à l'attaque en règle de l'ensemble de son argumentation. »[117]

3.2.3 « L'ironie et la simulation »

Les protagonistes vont également tenter de ridiculiser l'adversaire et ses propos afin de légitimer son propre discours devant le public-témoin:

> « L'ironie est le traitement du discours rival sur le *mode ludique*. Il s'agit d'un ensemble de moyens et de procédés discursifs à l'aide desquels on veut ridiculiser à la fois la personne du rival et son discours. [...] on ne cherche pas à contre-argumenter, à construire un

---

116 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.50). France: Les éditions de Minuit.

117 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.51). France: Les éditions de Minuit.

contre-discours, mais à tourner en ridicule. »[118]

Uli Windisch précise que l'on distingue cette forme d'ironie dans le discours conflictuel grâce à des « marques graphiques » dans le discours écrit. Quand ces marques ne sont pas présentes, mais que le discours présente néanmoins un aspect ironique, alors on passe du processus d'ironie à celui de la « simulation »:

> « Le discours manipulateur reprend le discours manipulé en l'intégrant à son propre discours sans le marquer. Seule la connaissance du *contexte* et de la *situation extralinguistique* dans lequel se déroule le conflit permet de comprendre l'aspect ironique du propos. On fait comme si l'on était d'accord avec l'adversaire; mais ce n'est que pour mieux le rejeter, en faisait rire. »[119]

3.2.4 « La représentation fantasmatique »

En marche vers le K.O verbal, l'interlocuteur va tenter au cours d'une « représentation fantasmatique » d'abattre son adversaire radicalement. En effet, il s'agira encore une fois de détourner le discours de l'adversaire, de donner un nouveau sens à ses propos afin de transmettre un nouveau message: « Plutôt que de parler de l'Autre et de son discours, on fabule et on fantasme à son sujet »[120].

---

118 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.52). France: Les éditions de Minuit.

119 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.53). France: Les éditions de Minuit.

120 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.55). France: Les éditions de Minuit.

Une tout autre image et identité sera donc conférée à celui-ci face au public-témoin: « Tout se passe comme si l'on voulait liquider définitivement l'adversaire, en finir une fois pour toutes : on veut mettre fin au conflit discursif en liquidant l'adversaire, en le transformant en un Autre monstrueux »[121].

3.2.5 « La stratégie de la guerre invisible »

Entre apparence et réalité, bien des messages peuvent être transmis implicitement. C'est ainsi que nous assistons au sein du discours conflictuel à un « simulacre de discours didactique »[122]. En effet, au sein d'un cycle de communication à part entière à vocation informative où l'interlocuteur va énoncer la thèse qu'il défend, il va en l'énonçant, également critiquer implicitement la thèse de son adversaire, « Restitué dans le contexte qui lui donne sens, un tel discours n'est qu'un simulacre de discours didactique »[123].

3.2.6 Une mise scène du discours conflictuel

Selon Uli Windisch, le discours conflictuel présente également les caractéristiques

---

121 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.55). France: Les éditions de Minuit.

122 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.57). France: Les éditions de Minuit.

123 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.57). France: Les éditions de Minuit.

d'une mise en scène. Toutes les composantes de ce type de discours dont nous avons pu rendre compte précédemment nous montrent que l'interlocuteur joue un rôle et se donne en spectacle devant un public. Tout cela a été pensé afin de pouvoir transmettre une image de soi qui correspondrait à l'identité qu'on souhaite véhiculer, une identité capable de plaire au public. « N'a-t-on pas été jusqu'à dire que le monde social n'était qu'un *théâtre* »[124].

> « Le discours conflictuel n'offre-t-il pas une illustration très concrète de ce travail et de cette lutte pour être reconnu ? Cette lutte suppose bien une mise en scène à laquelle aucun moyen n'échappe. Point essentiel: pour jouer avec le social, il faut bien le connaître. »[125]

---

124 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.64). France: Les éditions de Minuit.

125 Goffman, E. (1973). La Mise en scène de la vie quotidienne: La présentation de soi (p.64). France: Les éditions de Minuit.

CHAPITRE IV

PRÉSENTATION DES RÉSULTATS

4.1 Vers une mise en scène de la menace

Nous tenterons dans cette partie d'appliquer le principe de « mise en scène » d'Erving Goffman (1973) à la notion de « menace » que notre étude semble présenter avec les différentes menaces exprimées par DAECH et les Russes, et pour ainsi mettre en évidence une « mise en scène de la menace ».

Pour Goffman, dans la société chaque personne est un acteur jouant un rôle et utilisant ainsi dans son jeu de rôle une « façade ». Aussi, l'acteur utilisera le procédé de « l'idéalisation », il va cacher son jeu et se faire passer pour une toute autre personne face à son public, puisque son image ne correspond pas à celle qu'il souhaite renvoyer. Il y a donc une opposition entre « réalité et simulation », avec d'un côté une représentation honnête et de l'autre une représentation inventée. Bien qu'une personne semble correspondre parfaitement à l'apparence qu'elle souhaite se donner, cette apparence peut bel et bien avoir été préfabriquée.

« Pour comprendre l'intuition fondamentale qui sous-tend l'œuvre de

> Goffman et qui ordonne sa perception particulière du monde social, selon laquelle les rapports entre les individus sont toujours (au même titre que les rapports entre les États) des rapports de force fondés sur le simulacre, sans doute faudrait-il pouvoir remonter, dans la genèse de l'œuvre, en amont de l'instant relativement arbitraire où elle s'objective dans l'écrit et même en amont du temps où, par l'apprentissage rationnel du métier, son auteur acquiert l'habitus scientifique, pour accéder aux expériences sociales antérieures qui sont constitutives de l'habitus de classe : un habitus scientifique n'est jamais en effet totalement autonome par rapport à l'habitus de classe qui lui préexiste et sur lequel il se construit, en sorte qu'une œuvre scientifique enferme toujours, comme une œuvre littéraire, la trace de la trajectoire sociale de son producteur ».[126]

4.1.1 Le simulacre dans le discours politique: analyse du discours

Dans cette étude de cas, nous constatons deux postures qui s'opposent diamétralement. En effet, il va s'agir de celle de DAECH et de la Russie, tous deux soupçonnés d'avoir attaqué TV5 Monde.

Ainsi selon les discours respectifs de DAECH et grâce à leurs différentes déclarations sur les réseaux sociaux ainsi que les discours des ministres qui ont réagi à la cyberattaque et avec les discours des représentants de TV5 Monde, nous allons tenter de comprendre en quel sens cette cyberattaque fut peut-être l'œuvre de la Russie et pourquoi se serait-elle cachée derrière le drapeau de l'État islamique ? Aussi, pourquoi la chaîne de télévision fût particulièrement prise à partie lors de cette cyberattaque ?

4.1.2 Le discours de DAECH

---

[126] Goffman, E. (1998). Les Moments et leurs hommes. France: Edition Broché.

Tel que nous l'avions précisé précédemment, un message particulièrement violent de la part de l'organisation de DAECH a été publié sur les réseaux sociaux de TV5 Monde, accusant ainsi la France de lutter contre l'EI et rappelant les dramatiques attaques terroristes contre Charlie Hebdo et l'Hypercacher, qualifiant ces événements de « cadeaux » délivrés à la France:

> « Je suIs IS...La guerre contre l'État islamique était une faute impardonnable, c'est pour ça que les Français ont reçu les cadeaux de janvier à Charlie Hebdo et à l'Hypercacher »[127]

Yves Bigot intervient dans une courte vidéo mise en ligne quelques heures après la cyberattaque. Cette vidéo fût analysée par les autres médias comme résultant de l'état de la chaîne de télévision au moment même: une résolution d'image dégradée, une seule caméra et un micro qui ne semblait pas fonctionner, il déclare alors:

> « Le 8 avril à 22h, heure de Paris, TV5 Monde a été victime d'une cyberattaque extrêmement puissante. Ce piratage a conduit l'ensemble de nos onze chaînes, les neuf généralistes et les deux thématiques à virer à l'écran noir et nous avons donc en même temps perdu le contrôle de nos réseaux sociaux et de nos sites internet. L'ensemble de nos équipes travail d'arrache-pied depuis pour rétablir les programmes auxquels vous êtes habitués. »[128]

Au lendemain de la cyberattaque et durant les jours qui ont suivi, de nombreuses

---

[127] 20 minutes. (09/04/2015). [Article de presse] Récupéré de http://www.20minutes.fr/societe/1582663-20150409-piratage-djihadistes-passe-tv5-monde

[128] C à vous. (09/04/2015). Récupéré de https://www.youtube.com/watch?v=ZiOUxzOchBo:

personnalités politiques et médiatiques ont pris la parole publiquement. En effet, cet événement a entraîné de nombreuses réactions de par le message implicitement renvoyé lors de cette cyberattaque, comme l'expliquait Hélène Zemmour la directrice de TV5 Monde:

> « Je crois que c'est avant tout une menace contre la culture, TV5 Monde est le premier diffuseur culturel francophone, c'est d'abord cela qui a été attaqué et je pense que c'est ce qui explique la réaction de tout le gouvernement. C'est la France qui a été attaquée, et au-delà de la France TV5 Monde c'est la francophonie, les Suisses, les Belges, les Canadiens et c'est tout ce réseau de francophones qui souhaitent diffuser la culture, au sens large, la langue française et ses valeurs »[129]

Laurent Fabius, ministre des affaires étrangères s'est rendu au siège de TV5 Monde au lendemain de la cyberattaque et déclare publiquement: « C'est à ma connaissance la première fois qu'on s'attaque à un média mondial, en piratant et en utilisant les armes les plus contemporaines de la technologie »[130]. Le ministre des Affaires étrangères ajoute également:

> « Je condamne avec fermeté la cyberattaque qui a frappé hier soir TV5 Monde, chaîne francophone internationale fruit d'un partenariat unique entre plusieurs pays. Je me suis rendu ce matin au siège de la chaîne, avec M. Bernard Cazeneuve et Mme Fleur Pellerin, pour exprimer ma solidarité à l'équipe de TV5 Monde. Tout sera mis en œuvre pour identifier les auteurs de cette attaque et les traduire en justice. Une fois de plus, les terroristes prennent pour cible la liberté

---

[129] C à vous. (09/04/2015). Récupéré de https://www.youtube.com/watch?v=ZiOUxzOchBo:

[130] C à vous. (09/04/2015). Récupéré de https://www.youtube.com/watch?v=ZiOUxzOchBo:

> d'expression et d'information. Notre détermination pour combattre le terrorisme est totale. »[131]

De plus, de nombreux messages d'officiels ont suivi sur les réseaux sociaux, particulièrement Twitter. Tous qualifiant cet acte comme inacceptable, notamment envers le droit à la liberté d'expression et de presse, comme ce fût le cas lors des attaques terroristes contre Charlie Hebdo, et exprimant leur soutien à TV5 Monde.

Fleur Pellerin, ministre de la Culture et de la Communication déclare: « J'exprime tout mon soutien et ma solidarité aux équipes de la chaîne @TV5Monde, victimes d'un véritable acte terroriste @YvesBigot ».

Laurent Fabius apporte « Solidarité et soutien à @TV5Monde: la liberté de la presse reste debout, malgré les attaques ».

Manuel Valls, Premier ministre déclare que « L'attaque du réseau #TV5Monde est une atteinte inacceptable à la liberté d'information et d'expression. Soutien total à la rédaction. »

Annick Girardin, Secrétaire d'État chargée du Développement et de la Francophonie, assiste sur le fait que « Pirater #TV5Monde est écoeurant et lâche. Elle véhicule la langue française, célèbre sa diversité, crée des ponts entre

---

[131] Gouvernement Français. (2015). Récupéré de http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-culturelle/les-actualites-et-evenements-2015-de-la-diplomatie-culturelle/article/tv5-monde-cyberattaque-declaration:

francophones du monde. »

Enfin Christiane Taubira, ministre des Outres-mers déclare: « Pas de doute, ils ne supportent ni éducation ni culture ni libre information ni libertés. Soutien aux équipes de @TV5Monde ».

Du côté de la Russie, même après les résultats de l'enquête française dirigée par l'ANSSI, prouvant que l'hébergeur de la cyberattaque se situait sur le territoire russe, aucun officiel ne s'est prononcé. De même pour les médias russes qui ne répondent pas aux accusations, même si elles proviennent directement du gouvernement français étant donné que l'ANSSI est une agence gouvernementale.

Nous constatons donc de par ces différentes perspectives et les événements qui y sont liés: une mise en scène tel que le définissait Goffman. En effet, au sein de cette mise en scène réside plusieurs acteurs: TV5Monde, DAECH, le gouvernement français avec notamment, l'ANSSI et le gouvernement russe. Ces différents acteurs vont mettre en place un jeu de scène, propre à chacun afin que le public puisse correctement les identifier. De plus, ils vont tenter de se construire une « façade » au travers de leur représentation afin de faire valoir leur point de vue et leurs arguments.

Dans le cyberespace, tous, organismes ou individus ont la possibilité de choisir l'image qu'ils souhaitent renvoyer à leurs publics-témoin, grâce ce procédé de « façade » et donc, grâce à l'apparence qu'il donne à leurs identités et la manière dont leurs actions sont construites. Également, chacun va tenter au travers de la

« réalisation dramatique » de mettre en avant ce qui n'est pas visible aux premiers abords. En effet, comme nous l'avions précisé auparavant, les cyberattaques sont lancées, la plupart du temps, non pas dans le but de détruire, mais d'avoir un impact sur les relations diplomatiques. Dans cette cyberattaque contre TV5 Monde, beaucoup d'actions ont été réalisées à l'abri du regard du public, elles ont ensuite été rapportées par les médias. Le procédé de l' « idéalisation » est utilisé dans ce contexte pour que les acteurs en présence puisque cacher le jeu de scène. Particulièrement les Russes envers le gouvernement français. En utilisant la technique de « faux-drapeaux », et en se cachant derrière le drapeau de l'EI, la Russie a souhaité renvoyer une tout autre image. Cela s'est également construit avec une « cohérence de l'expression », puisque que les messages diffusés sur les réseaux sociaux et adressés directement aux officiels, vont tous dans la même direction en accusant la France d'avoir agit contre l'EI, c'est ainsi que les Français en subissent aujourd'hui les conséquences. Si les Russes ont réellement commis cette cyberattaque, et ont donc délivré ces messages, ils ont mis en place une représentation dont ils se doutaient du fort impact que cela pourrait entraîner. En effet, la menace islamiste extrémiste en France est prise très au sérieux, notamment de par les nombreuses et douloureuses attaques qui ont été dénombrées jusqu'à présent. Cette représentation est également « frauduleuse » puisque la Russie aurait menti en se cachant derrière l'EI. Le gouvernement français et TV5 Monde, n'ont également pas tout dévoilés sur l'affaire, notamment à cause des raisons de sécurité nationale, nous remarquons donc aussi une certaine « mystification » des actions, en gardant une part de mystère tout au long de cette représentation. Nous constatons également une certaine opposition entre « réalité et simulation » puisque d'un côté nous avons une représentation dans la réalité qui serait en quelque sorte véridique et honnête puisque DAECH représente bel et bien une menace concrète pour la France, et de l'autre côté nous avons une représentation qui aurait été inventée puisque se serait en fait, la Russie le véritable auteur de cette attaque. Enfin, au

niveau de la formation d' « équipe » nous le constatons particulièrement dans le cas du gouvernement français et son agence de cybersécurité, l'ANSSI. En effet, les protagonistes faisant partie du gouvernement et de l'organisation se sont tous mis d'accord sur un message en particulier à délivrer. Nous nous en rendons compte de par les différents Tweets des officiels: tous apportent leurs soutiens à TV5 Monde et se disent profondément choqués par cette attaque visant la liberté d'information et de presse et rapportent également une attaque directement dirigée contre l'image de la francophonie dans le monde. Il y a donc eu des « secrets stratégiques » qui ont été mis en place, le gouvernement et son agence n'ont pas dévoilé leurs capacités, puisqu'il s'agit de sécurité nationale, mais également, tel que Goffman le précisait, pour ne pas montrer l'éventuelle inaptitude de l'équipe face à un certain problème. Enfin, des « secrets d'initiés », puisque ces personnalités se sont regroupées autour d'un secret commun, qui a permis la formation de l'équipe.

4.1.3 Une mise en scène de la Russie ?

Au sein de cette mise en scène, nous constatons un rapport conflictuel entre le gouvernement français, l'EI et le gouvernement russe. Dans cette représentation les rapports entre récepteurs et interlocuteurs sont de nature négatives: l'EI et le gouvernement russe ont tous deux tenté d'attaquer la France dans ce contexte. Le gouvernement français suite aux menaces de l'EI n'a pas communiqué avec son public-témoin dans le seul but de l'informer, mais également pour réfuter les informations transmises sur les réseaux sociaux et pour le rassurer. Il y a donc une tentative de destruction de la face de l'adversaire, en contredisant et en reniant les propos publiés. Il est important pour le gouvernement français de rétablir sa vérité

et la thèse qu'il défend devant son public-témoin. C'est ainsi, selon U.Windisch, que la mise en scène est nécessaire: pour défendre ses idées. L'auteur évoque également le stratagème le plus violent du processus, entraînant le K.O verbal: la transformation des propos au vu d'un détournement. La Russie a détourné les propos de l'EI afin de renverser la situation à son avantage. Le plus surprenant est que l'EI n'a pas réagi pour se défendre et se dissocier suite à cette cyberattaque.

De plus, au sein de cette attaque il y a un procédé de « démasquage » puisqu'il s'agissait pour l'ANSSI et le gouvernement français de démasquer l'auteur qui se cachait derrière cette cyberattaque et aussi d'une opération de « masquage » pour ne pas dévoiler la totalité du discours et de la vérité derrière celle-ci. Le concept de « concession » apparait quant la Russie a voulu détourner les propos de l'EI pour se faire passer pour l'organisation et ainsi attaquer la France indirectement et sans compromettre son image.

Nous constatons que les attaquants ont voulu ridiculiser le discours de la France dans le contexte de cette cyberattaque. Notamment par le message publié sur le réseau social Facebook, disant que « les cadeaux de l'Hypercacher et de Charlie Hebdo » ont été délivrés de par les actions de la France envers l'EI. Le terme « cadeaux », de nature ironique, est utilisé ici pour qualifier les attaques terroristes antérieures, il s'agit bien d' « ironie et de simulation ». Pour la « représentation fantasmatique » elle a lieu puisqu'une fois de plus, la Russie a détourné les propos de l'EI pour transmettre un message nouveau, à son avantage, en appui aux attaques terroristes qui ont eu lieu précédemment à Paris. Enfin la « stratégie de la guerre invisible » prend forme quand la France va critiquer ouvertement la thèse de ses attaquants, en déclarant par le biais de ses officiels, qu'il s'agissait d'une atteinte inacceptable à la culture française certes, mais également à l'ensemble des

pays francophones.

Nous pouvons donc supposer qu'au sein de cette mise en scène de la cyberattaque contre TV5 Monde *(voir Annexe D)*, que le véritable K.O verbal a été ironiquement délivré par celui dont nous avons le moins perçu la parole, mais qui n'a pas pour autant agi moindrement. En effet, il va s'agir de la Russie puisque nous supposons que son jeu de faux drapeaux à fonctionner correctement en constatant la situation de la France au moment de l'attaque et suites aux enquêtes. En effet, comme nous le précisions auparavant la France avait déjà été profondément blessée par les attaques de l'EI, le fait que la Russie est choisie de se cacher derrière ce drapeau en particulier, n'était pas un hasard. Cela a été envisagé dans le but de faire ressentir un plus grand impact. De plus, au sein de TV5 Monde, les conséquences de la cyberattaque, qu'elles soient matérielles ou morales, se sont également fait fortement ressentir. Au sein du gouvernement français et de l'ANSSI, les officiels se sont précipités le jour même de l'attaque et le lendemain pour déclarer publiquement, au travers des médias qu'il s'agissait bel et bien de l'EI, rappelant ainsi aux Français les dramatiques événements antérieurs. Or, suite à l'enquête, il s'avérait qu'il s'agissait de la Russie. Ce qui nous paraît surprenant, c'est que même suite à ce nouvel élément déterminant dans l'enquête, le gouvernement français ne s'est plus prononcé, la Russie n'a pas réagi publiquement et enfin l'EI n'a pas démenti. Nous constatons donc une situation de flou total, qui laisse planer le doute et le mystère sur cette affaire, avec néanmoins quelques pistes délivrées par les médias et les enquêteurs assurant bel et bien qu'il s'agissait d'un ou de plusieurs hacker(s) se situant sur le territoire russe. Le plan de départ des Russes a donc bien fonctionné dans le sens où, nous imaginons que leur objectif était d'attaquer leur cible implicitement, sans utiliser leurs propres identités. Il s'avère suite à l'attaque que les conséquences morales et diplomatiques, plus que matérielles, voulues, se sont avérées justes.

4.2 Première stratégie de cybersécurité française : « Défense et sécurité des systèmes d'information: la stratégie de la France » (2011)

Une première stratégie de cybersécurité nationale a été publiée en 2008 *(voir Annexe A)* dans le *Livre Blanc sur la défense et la sécurité nationale* annoncé par le Président de la République. La stratégie est présentée par un discours de Francis Delon, ancien Secrétaire général de la défense et de la sécurité nationale, rappelant l'importance de la souveraineté de la France dans ce domaine. Il qualifie également le cyberespace comme étant: « la nouvelle tour de Babel [...] un lieu de partage des cultures du monde, de diffusion des idées et d'informations en temps réel, un lieu d'échanges entre personnes ».[132]

Francis Delon, explique la méconnaissance et le manque d'information concernant l'importance des enjeux de sécurité du cyberespace. Pour lui, le cyberespace est « devenu un lieu d'affrontement », dont la France a besoin de se défendre, notamment en s'armant d'une stratégie nationale. Il précise également la création de l'ANSSI (Agence nationale de la sécurité des systèmes d'information), en 2009, amorcée par le Président de la République.

L'ancienne stratégie se construit en quatre « objectifs stratégiques » et se présente en « sept axes d'effort ». En effet, le premier objectif concernera la France comme « puissance mondiale dans le cyberespace ». Il s'agit pour la France de coopérer sur la scène internationale en s'intégrant au sein d'instances internationales, notamment celle de l'Union européenne afin de représenter un allié ou un adversaire conséquent en matière de cybersécurité, en protégeant ses réseaux, son

---

[132] Défense et sécurité des systèmes d'information. *Stratégie de la France*. (2011). France: ANSSI. Récupéré de https://www.ssi.gouv.fr

territoire et ses citoyens des acteurs non étatiques ou étatiques lançant des attaques directes ou indirectes ainsi que les potentielles menaces terroristes. Également dans l'optique de devenir un leader dans le domaine du numérique. Pour le second objectif, il s'agira de « garantir la liberté de la France par la protection de l'information de souveraineté ». En effet, la sécurité de la souveraineté semble représenter un enjeu important en France, et notamment dans le cyberespace. Il s'agira d'élaborer un processus de défense pour la protection d'une information souveraine, synonyme de « fraction de l'information diplomatique, militaire, scientifique, technique et économique qui permet la liberté d'action et conditionne la prospérité des nations »[133]. Le troisième objectif est le renforcement de « la cybersécurité des infrastructures vitales nationales ». De nos jours, la France n'est pas la seule à s'en soucier. Les infrastructures critiques peuvent représenter un risque important si elles ne sont pas correctement sécurisées, puisque:

> « Dans la rencontre, ancienne et pourtant inédite parce que bousculée par l'interconnexion des systèmes, entre le monde industriel et le monde de l'informatique, le premier manque de formation et de sensibilisation à la sécurité des systèmes d'information, tandis que le second méconnaît souvent les contraintes et le fonctionnement des systèmes industriels ».[134]

La sécurisation des infrastructures critiques est donc une des « priorités nationales» pour la France. En effet, le risque associé à ces infrastructures peut également toucher le domaine de l'économie ou plus grave encore, entraîner des pertes humaines. Enfin, le quatrième et dernier objectif rend compte de la «

---

133 Défense et sécurité des systèmes d'information. *Stratégie de la France (p.12)*. (2011). France: ANSSI. Récupéré de https://www.ssi.gouv.fr

134 Défense et sécurité des systèmes d'information. *Stratégie de la France (p.13)*. (2011). France: ANSSI. Récupéré de https://www.ssi.gouv.fr

sécurité dans le cyberespace ». Il s'agira avant tout de la protection du citoyen et de ses données personnelles. Pour cela, il est nécessaire de sensibiliser la population française aux risques que peut présenter le cyberespace, ainsi que de protéger les entreprises et les administrations françaises. La France prévoit donc la mise en place de mesures juridiques, avec l'appui du droit international afin de contrer la criminalité et les attaques, mais également dans l'optique de mettre en place de potentielles sanctions.

Les « sept axes d'effort » sont essentiellement composés de différentes actions, illustrées dans cette stratégie par divers verbes à l'infinitif. Primo, l'axe consistant à « anticiper et analyser » l'activité et les actions futures de personnalités publiques afin de prévoir tous propos pouvant entraîner de potentielles actions revendicatrices. Secundo, « Détecter, alerter, réagir », comme ces verbes l'indiquent, il s'agira de détecter la menace ou l'attaque. Les victimes seront ensuite directement alertées, et un processus de gestion de crise sera mis en place immédiatement par l'ANSSI et sa « salle d'opération » qui se doit de réagir contre la menace, surtout si elle touche les principales infrastructures administratives ou d'importance vitale. Tertio, il s'agira « d'accroître et pérenniser » les centres d'expertise en la matière. En effet, la France représente une potentielle puissance dans le domaine du cyberespace des technologies de l'information et de la communication. Et elle se dit détenir les moyens matériels pour supporter un tel projet. En revanche, sa faille viendrait principalement du manque d'effectif humain. Et pour cela, elle préconise la création de formations et l'orientation des jeunes étudiants dans ce domaine. Quarto, « protéger » les principaux réseaux administratifs et les infrastructures critiques sur le territoire national. Cette mesure s'applique principalement par l'apport de nouveaux moyens techniques tels que des cartes à puce ou encore des systèmes de visioconférence protégée. Également, pour la protection des entreprises vitales, étant à dominance privées, une alliance

entre le secteur privé et public est envisagée pour un partage des connaissances et des processus de sécurité. Quinto, « adapter » la législation et la réglementation française au fur et à mesure de l'évolution des technologies. Sexto, « développer » un réseau d'alliés internationaux. En effet, pour la protection contre la cybercriminalité, grâce au partage de données entre différents États sur cette même problématique. Enfin septimo, « communiquer », où il s'agira d'informer et de sensibiliser le public sur les risques que présentent le cyberespace et les technologies de l'information et de la communication. Cette mission sera menée par l'ANSSI, tant pour l'aide à la protection des réseaux que pour la communication sur les risques.

4.3 Nouvelle stratégie de cybersécurité française: « La stratégie nationale pour la sécurité du numérique » (2015)

Un nouveau plan stratégique de cybersécurité français a vu le jour en 2015 *(voir Annexe B)* et débute avec un discours rédigé par le Premier ministre, Manuel Valls qui déclare que:

> « Le numérique est également un espace de compétition et de confrontation. Concurrence déloyale et espionnage, désinformation et propagande, terrorisme et criminalité trouvent dans le cyberespace un nouveau champ d'expression ».[135]

Le plan stratégique national pour la sécurité du numérique se construit en cinq étapes. En effet, la France s'est munie d'une nouvelle stratégie nationale, pour protéger son gouvernement, sécuriser ses citoyens et pour développer son secteur

---

135 Stratégie nationale pour la sécurité du numérique. (2015). France: ANSSI. Récupéré de https://www.ssi.gouv.fr

économique dans ce domaine. Mais également afin de rayonner sur la scène internationale dans cette nouvelle ère du numérique.

Cette stratégie que nous avions analysée précédemment et qui apparaît quatre ans après la première (2011), bien qu'ayant évoluée, présente de nombreux points en communs avec la seconde. Points communs que nous rappellerons au fur et à mesure de notre analyse et dont nous avons résumé sous forme de tableau comparatif *(voir Annexe C)*.

La stratégie est annoncée par un texte introductif nous rappelant d'abord, l'importance et l'influence du numérique et de la connectivité dans nos vies quotidiennes tant personnelles que professionnelles. Précisant également que le numérique peut être un avantage considérable à prendre en compte, comme un inconvénient dangereux duquel il faudrait se protéger. Ce texte introductif évoque également la première stratégie de cybersécurité parue en 2011, suite à la découverte d'une cyberattaque majeure en France, contre les ministères économiques et financiers dans la même année, entraînant le piratage de milliers de documents secrets et de 150 ordinateurs. D'autres crimes sont également abordés tels que le vol d'information personnelle, les escroqueries, le crime organisé, des actes de sabotages, le harcèlement ou encore des défigurations de sites internet. La stratégie prend explicitement l'exemple de TV5 Monde étant la deuxième cyberattaque majeure que la France ait connue. Plus les technologies vont évoluées, plus les attaques seront dangereuses et dévastatrices, la stratégie le précise: « ce qu'il est convenu d'appeler « l'état de la menace » établi en 2010 s'est ainsi révélé juste »[136]. Autre menace annoncée par la France, celle des

---

136 Stratégie nationale pour la sécurité du numérique (p.8). (2015). France: ANSSI. Récupéré de https://www.ssi.gouv.fr

grandes entreprises mettant en place des services permettant de créer toute une économie autour des données personnelles des individus. Enfin la France rend légitime les diverses dispositions qu'elle a entreprises de par le soutien de ses alliances internationales et bilatérales, notamment celle avec l'ONU. Pour clôturer ce texte introductif, la stratégie rappelle les trois principales communautés citées par le directeur de l'ANSSI précédemment, celle des « chercheurs, les inventeurs de produits et de services », celle des « élus, du gouvernement, des administrations centrales et territoriales et des syndicats », et celle des « usagers, responsables d'entreprises, acteurs de la société civile et citoyens ».

La première étape concerne les intérêts fondamentaux, c'est-à-dire la défense et la sécurité des systèmes d'information de l'État. L'objectif est de protéger les intérêts français au sein du cyberespace. Avec les cyberattaques, les attaquants peuvent dérober des informations confidentielles et s'installer au sein des réseaux. Après les attentats de janvier 2015 à Paris, la France a ressenti les conséquences de ces attaques dans le cyberespace avec les « défigurations de sites Internet [...] [qui] ont eu un impact technique faible, mais une portée symbolique souhaitée par les attaquants »[137]. Plus que le pillage de données, les cyberattaques visent dans certains cas à affecter l'opinion publique en touchant certains éléments à fortes valeurs symboliques. Aussi, le pays souhaite maintenir sa souveraineté, mais exprime son envie d'agir à un niveau international par le biais des nombreux accords multilatéraux dont elle fait partie (Union européenne, OTAN, ONU). Cette étape est notamment très proche du troisième objectif de la stratégie de 2011 (« Renforcer la cybersécurité des infrastructures vitales nationales »).

Le deuxième objectif, proche du deuxième axe d'effort de la stratégie de 2011 (« Détecter, alerter, réagir »), concerne la vie privée, les données personnelles et la

---

[137] Défense et sécurité des systèmes d'information. Stratégie de la France (p.14). (2011). France: ANSSI. Récupéré de https://www.ssi.gouv.fr

malveillance au sein du cyberespace. Dans ce cas précis, il s'agira de protéger le citoyen tout en respectant les valeurs que porte la France. La charte précise que les attaques visant des particuliers sont pour la plupart d'entre elles à but financier. En effet, il s'agit pour les malfaiteurs de dérober des ressources financières. Contrairement au gouvernement qui détient le support de l'ANSSI, les citoyens français ne disposent pas d'organisation pour aider à la lutte contre la cybercriminalité. Des mesures sont néanmoins mises en place pour leur protection. Par exemple, les utilisateurs des réseaux sociaux transmettant des informations allant à l'encontre des valeurs de la République française seront punis par la loi, puisque ces réseaux étant fortement fréquentés par un public parfois peu avisé pourraient influencer l'opinion publique. Le plan stratégique se montre contre la libre circulation de l'information parce que cela « masque difficilement la volonté de captation de ces données par des oligopoles dont les valeurs et les pratiques ne correspondent ni à la conception de la vie privée française ou européenne ni à son encadrement juridique »[138]. Afin de mettre en place ce second objectif, la France met l'accent sur la prévention. En effet, le fait que les lois applicables dans la vie réelle soient également applicables en ligne apparait explicitement et le gouvernement français souhaite faire valoir son autorité dans le cyberespace. Par exemple, suite aux attentats de janvier 2015, une plateforme de prévention a été mise en place, de même pour les autres « phénomènes de propagande ou de déstabilisation »[139].

Le troisième objectif concerne la sensibilisation et la formation à la sécurité du numérique. Il s'agira avant tout de sensibiliser les Français et notamment les plus

---

138 Défense et sécurité des systèmes d'information. Stratégie de la France (p.21). (2011). France: ANSSI. Récupéré de https://www.ssi.gouv.fr

139 Défense et sécurité des systèmes d'information. Stratégie de la France (p.21). (2011). France: ANSSI. Récupéré de https://www.ssi.gouv.fr

jeunes aux dangers que peuvent présenter Internet. Désormais, la sensibilisation à la cybersécurité fera partie intégrante des programmes de formations supérieures et continues. Ce troisième objectif se rapproche fortement du quatrième objectif de l'ancienne stratégie concernant la sécurité dans le cyberespace.

Le quatrième objectif rend compte des enjeux économiques liés au numérique. La France souhaite développer son secteur du numérique, notamment à l'international. La majorité des infrastructures des réseaux de communication français sont conçues à l'étranger. De même concernant l'hébergement des données où « les infrastructures physiques [sont] situées hors du territoire national et [sont] non soumises au droit européen »[140]. La France souhaite développer en partenariat avec l'Union européenne des services de sécurité concernant le numérique. Aussi, elle souhaite que ses connaissances acquises soient partagées avec les entreprises privées, pour qu'elles puissent elles aussi, se protéger contre d'éventuelles attaques informatiques. Elle souhaite également soutenir les PME et start-ups désireuses de se lancer dans le domaine de la cybersécurité, même à l'international. Nous constatons donc que cette étape détient de nombreux points communs avec le troisième axe d'effort de la stratégie de 2011, étant « accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines ».

Le cinquième objectif concerne plus généralement l'Europe et la question de la souveraineté française. Il s'agit dans ce dernier point de positionner la France et les États membres de l'Union européenne comme « moteur d'une autonomie stratégique ». En effet, la charte le précise clairement, le cyberespace représente un enjeu majeur pour les organisations internationales. Souvent considéré comme

---

140 Défense et sécurité des systèmes d'information. Stratégie de la France (p.30). (2011). France: ANSSI. Récupéré de https://www.ssi.gouv.fr

un espace moins gouverné, le cyberespace est néanmoins soumis au droit international. Nous l'avons souvent constaté durant ces dernières années, la compétitivité des États dans ce monde parallèle apparait clairement, notamment à des fins d'espionnage, et cela parfois même par des pays alliés. Aussi, il arrive que des groupes d'individus à motivations politiques ou idéologiques controversées infiltrent les réseaux gouvernementaux à des fins de déstabilisation, d'espionnage, de propagande, ou encore de pillage de données. Ce dernier objectif se rapproche fortement du premier objectif de l'ancienne stratégie étant « être une puissance mondiale de cyberdéfense ».

La gouvernance d'Internet apparaît également comme une question primordiale. La France met en avant l'Europe, en précisant qu'elle propose des idées pour la réglementation du cyberespace. Cependant, malgré ces efforts, elle peine à mettre en place les mesures nécessaires afin de devenir autonome. De plus, la France insiste sur l'importance de sa présence au sein de ces négociations. Pour concrétiser ce dernier objectif, elle propose l'élaboration d'une feuille de route pour l'autonomie en partenariat avec les États membres, tout en respectant la souveraineté de chacun, « il s'agira de faire de l'Europe le territoire numérique le plus respectueux des droits fondamentaux et individuels »[141]. La France exprime le souhait de vouloir participer aux discussions sur la scène internationale à propos de la sécurité du cyberespace, par le biais de ses différentes alliances multilatérales (ONU, OSCE). La France soutiendra les pays en voie de développement désireux d'agir pour la cybersécurité sur leur propre territoire. Enfin, même si nous constatons de nombreux points communs entre les différentes étapes de ces deux stratégies, nous remarquons également que l'ordre dans lequel se situaient les étapes de la stratégie a changé. Ainsi nous supposons,

---

141 Défense et sécurité des systèmes d'information. Stratégie de la France (p.39). (2011). France: ANSSI. Récupéré de https://www.ssi.gouv.fr

que les priorités de la France dans ce domaine ont été repensées et que l'objectif principal n'est plus pour elle de devenir une puissance en matière de cyberdéfense, mais de sécuriser son territoire et ses infrastructures critiques. Notamment de par les différentes menaces (islamiques, russes, etc.).

4.4 La mise en scène au sein du discours politique

Afin de comprendre plus aisément la nouvelle stratégie mise en place, nous allons analyser le discours du Premier ministre Manuel Valls *(voir Annexe E)* qui a été produit le 16 octobre 2015 à la Maison de la Chimie, à Paris, lors du lancement de la nouvelle stratégie de cybersécurité française, publiée quelques mois auparavant. Nous utiliserons pour cette analyse, le concept de mise en scène d'Erving Goffman.

Nous constatons tout d'abord au sein du discours de Manuel Valls un jeu d'acteur très présent. Nous supposons qu'il souhaite légitimer sa position et son discours. Il va, au début de celui-ci saluer spécifiquement certaines personnes dans l'assemblée. Nous supposons que ces personnes forment une « équipe », partageant un « secret commun », étant tous liés au domaine de l'État, et particulièrement à celui de la cybersécurité et de la nouvelle stratégie. Également dans son discours la « façade » est employée à plusieurs reprises, il va dire les choses d'une certaine façon: dans un langage très soutenu, il va souvent utiliser la première personne afin de montrer son implication dans le projet, son apparence et celle de son discours sont très soignées, quant au décor il s'agit d'un lieu très prestigieux dans la capitale française, étant la Maison de la Chimie, à Paris. De plus, à de nombreuses reprises nous remarquons que le Premier ministre va

utiliser le procédé de « l'idéalisation ». En effet, il va sans cesse rappeler les efforts de la France dans ce domaine et les éventuels changements qui pourraient voir le jour suite à cette stratégie, le plus souvent de façons positives, semblant s'éloigner de la réalité, comme s'il souhaitait légitimer la création de cette stratégie de cybersécurité et de ses acteurs. Quand il parle de dangers dans ce domaine sur le territoire français, nous remarquons qu'une note positive suit automatiquement la remarque (« Les menaces non plus, vous ne les ignorez pas [...]. Nous y répondons avec une très grande lucidité, avec les moyens adaptés »)[142]. Il va rassurer son public-témoin, en évoquant les dangers et en apportant de suite, une solution adaptée.

La « réalisation dramatique » tient une place importante au sein de ce discours. Beaucoup d'éléments du domaine de la cybersécurité ne sont pas connus du public présent, notamment ceux qui ont permis l'élaboration de cette nouvelle stratégie. C'est ainsi que Manuel Valls, n'hésite pas à reprendre ces éléments: ceux qui ont amenés à la création de la stratégie (il va d'ailleurs citer explicitement la cyberattaque contre TV5 Monde)[143], les acteurs qui ont participé, les organismes participants ainsi que les publics concernés. Il n'oublie personne et s'adresse même parfois directement à eux. Ce qui nous permet aussi de constater la présence, et même la formation « d'équipe », puisque le Premier ministre va intégrer dans les différents groupes cités un certain nombre de personnes, notamment par catégories.

---

142 Valls, M. (2015). Stratégie nationale pour la sécurité du numérique. Conférence. Maison de la chimie. Paris: ANSSI. [Annexe E, p.1]

143 Valls, M. (2015). Stratégie nationale pour la sécurité du numérique. Conférence. Maison de la chimie. Paris: ANSSI. [Annexe E, p.1]

Aussi, la « cohérence de l'expression » au sein de ce discours est évidente. Tout au long de celui-ci Manuel Valls aborde la cybersécurité et la stratégie. Cependant, à deux reprises il va comparer celle-ci avec la loi sur le renseignement qui a fait beaucoup débat en France et dont il ne se cache pas: « Cette opposition caricaturale, nous l'avons vue, nous l'avons entendue, à l'occasion du débat sur la loi sur le renseignement »[144].

En ce qui concerne « l'opposition entre réalité et simulation », elle est également très présente. Le Premier ministre grâce à son jeu d'acteur va constamment rassurer son public, le féliciter et le remercier. Il va, premièrement constamment justifier ces arguments grâce à des événements ou des actions réelles qui se sont produites ou qu'il prévoit. Deuxièmement, en intégrant constamment les personnalités faisant partie de cette stratégie (ANSSI, personnalités politiques faisant partie du projet) et en s'adressant directement à son public cible. Enfin, troisièmement en s'impliquant personnellement, notamment en utilisant constamment, tout au long du discours la premièrement personne du singulier.

Enfin, un processus de « mystification » apparaît légèrement. En effet, Manuel Valls va la plupart du temps évoquer ouvertement les projets du gouvernement en lien avec cette stratégie. Mais nous supposons que, la cybersécurité étant un domaine parfois très secret, une certaine part de mystère peut éventuellement être gardée et non dévoilée au public.

---

144 Valls, M. (2015). Stratégie nationale pour la sécurité du numérique. Conférence. Maison de la chimie. Paris: ANSSI. [Annexe E, p.1]

CHAPITRE V

CONCLUSION

5.1 La cybersécurité en France

La cybersécurité étant un domaine récent, les États mettent progressivement en place leurs propres stratégies de cyberdéfense. La France en fait de même et va dévoiler publiquement sa première stratégie de cyberdéfense en 2011, suite à une cyberattaque de grande ampleur qui a touchée les ministères des Affaires économiques et financiers. En effet, la Direction des Trésors était la principale cible et les réseaux ont été investi pendant quatre mois grâce à la technique du « spearfishing », comme ce fut le cas lors de la cyberattaque contre TV5 Monde. 150 ordinateurs ont donc été piratés au sein du ministère, un important nombre de documents ont été dérobés et le ministère fut coupé de toute connexion Internet le temps d'un week-end. Suite aux enquêtes des autorités françaises, une piste se dirigeant vers la Chine commence à se dessiner, mais le gouvernement français ne se prononcera pas publiquement. Il s'agissait en faite d'une tentative d'espionnage pour tenter de récupérer des informations concernant le sommet du G20, qui avait eu lieu en France dans la même année. François Baroin ancien ministre de l'Économie, des Finances et de l'Industrie a d'ailleurs déclaré que ce sont les dossiers concernant le G20 qui « intéressaient les hackers »[145].

---

[145] Le Monde [article de presse]. (2017). Récupéré de http://lemonde.fr

Dans leur ouvrage « Cybercrime: menaces, vulnérabilités et ripostes », Daniel Martin et Frédéric-Paul Martin nous exposent les différentes menacent qui planent sur la France au sein du cyberespace. En effet, selon les auteurs notre monde se trouve dans une « nouvelle ère » où nous constatons une « nouvelle donne mondiale », qui donne naissance à trois différents types de révolutions, technologique, géographique et financière:

> « On assiste en fait à la conjugaison de trois révolutions simultanées: une révolution technologique par le développement des technologies de la communication, une révolution géographique par la création de nouveaux marchés pour les entreprises, une révolution financière par la mondialisation des flux de capitaux et de la gestion de l'épargne» (« Une nouvelle donne mondiale »).[146]

Au sein de cette « nouvelle donne mondiale » la société de l'information et de la communication va impacter de nombreux domaines et cela pas uniquement de façon positive:

> « Cette nouvelle ère mondiale où la concurrence touche tous les domaines: économiques, politiques, financiers, sociaux, linguistiques, consacre le rôle primordial de l'information, de la connaissance et de l'intelligence. [...] Dans ce nouveau contexte, notre société est devenue particulièrement vulnérable. À la fois au niveau des pouvoirs publics par les failles relatives aux infrastructures sensibles, mais aussi et surtout à celui des entreprises où le risque informatique devient le danger numéro un, sans oublier le niveau des citoyens dont les droits fondamentaux peuvent être violés notamment dans leur vie

---

[146] Martin, D. et Martin, F-P. Cybercrime-menaces, vulnérabilités et ripostes. (2001). France: Edition Broché.

privée ou comme consommateur. »[147]

5.2 La France et le principe de riposte

La cybersécurité étant un sujet sensible, très peu de médias ou de personnalités politiques ont abordé le sujet publiquement. Cependant, récemment un reportage diffusé sur une des chaînes nationales françaises (France 2) nous livre des informations exclusives concernant la cyberdéfense en France. En effet, le reportage précise tout d'abord que le nombre de cyberattaques en 2016 était d'environ 24 000. Le ministre de la Défense Jean-Yves Le Drian déclare que « L'espace cyber est devenu un espace de combat, c'est devenu un enjeu de souveraineté pour la France ».[148]

La France a connue des attaques majeures dont celle contre le ministère des fiances en 2011 ou celle de TV5 Monde qui selon Guillaume Poupard, le directeur de l'ANSSI, représentent autant de conséquences pour la sécurité nationale que concernant les retombées économiques.

Le reportage nous dirige également vers une autre piste, celle d'une victime potentielle, qui pourrait entraîner de graves conséquences pour la France: l'armée

---

147 Martin, D. et Martin, F-P. Cybercrime-menaces, vulnérabilités et ripostes. (2001). France: Edition Broché.

148 France 2. (22/01/2017). La riposte de la France contre les cyberattaques & le cyberespionnage [reportage télévisé]. Récupéré de https://www.youtube.com/watch?v=tqVcdIvaTGQ

française. En effet, les équipements de l'armée tels que les navires de guerre, les avions de chasse ou encore les sous-marins, sont tous liés par des systèmes électroniques au réseau Internet et pourraient, d'une certaine façon être sensible aux cyberattaques. Selon France 2, l'armée française relèverait chaque jour des tentatives d'intrusions, c'est pour cela que « la France ne cesse d'étoffer sa cyberarmée »[149].

Bien plus que cela, ce reportage de France 2 nous livre une information qui n'a jamais était dévoilée publiquement auparavant, notamment par un officiel: « la France mène ses propres cyberattaques »[150]. En effet, le plus pertinent reste la conversation entre le journaliste de la chaîne de télévision et le ministre de la Défense, Jean-Yves le Drian.

À la question est-ce que « la France se donne les moyens et la possibilité et le droit de mener elle-même ses propres cyberattaques ? »[151]. Le ministre va répondre que « si c'était nécessaire cela peut arriver »[152]. La France dirige donc elle-même ses propres opérations de cyberattaques, envers des organisations ou des États.

---

149 France 2. (22/01/2017). La riposte de la France contre les cyberattaques & le cyberespionnage [reportage télévisé]. Récupéré de https://www.youtube.com/watch?v=tqVcdIvaTGQ

150 France 2. (22/01/2017). La riposte de la France contre les cyberattaques & le cyberespionnage [reportage télévisé]. Récupéré de https://www.youtube.com/watch?v=tqVcdIvaTGQ

151 France 2. (22/01/2017). La riposte de la France contre les cyberattaques & le cyberespionnage [reportage télévisé]. Récupéré de https://www.youtube.com/watch?v=tqVcdIvaTGQ

152 France 2. (22/01/2017). La riposte de la France contre les cyberattaques & le cyberespionnage [reportage télévisé]. Récupéré de https://www.youtube.com/watch?v=tqVcdIvaTGQ

De plus, la chaîne de télévision va faire le lien entre ces informations précédemment dévoilées, et les documents classés secrets défense des autorités canadiennes, qui ont été rendus publics par *Wikileaks*. Ces documents attestent qu'« Ottawa soupçonne la France d'espionnage de certaines institutions au Canada, mais aussi en Iran, en Algérie et en Côte d'Ivoire », ils vont également préciser que derrière les espions se cachent une agence française de renseignement. France 2 consolidera ces informations en déclarant que ces propos ont été confirmés par un ancien directeur de la DGSE (La Direction générale de la Sécurité extérieure).

5.3 Cyberattaque contre le parti « En marche ! »

Résultant de la course à la présidentielle Française de 2017, Emmanuel Macron jeune candidat de son propre parti « En marche ! » fut élu le 6 avril 2017 face à Marine Le Pen candidate d'extrême droite. Suite à la campagne politique du nouveau président, celui-ci déclare que son parti a été victime de plusieurs cyberattaques visant leur site Internet accompagné de tentative d'espionnage et de vol de données de par la technique du « spear-phishing ».

Trend Micro, une compagnie japonaise va alors avertir le parti en l'informant qu'il s'agirait d'un groupe de hackers nommés « *Pawn Storm* », aussi nommée « *APT 28* », le même groupe qui avait infiltré auparavant, les réseaux de TV5 Monde.

Pourquoi des hackers russes voudraient venir troubler les élections présidentielles

françaises, alors que le parti de l'extrême droite se retrouve au deuxième tour ? Les médias français ont très vite réagit et soupçonnent fortement *APT 28* d'être directement en lien avec le Kremlin et insistent particulièrement sur l'hypothèse que Moscou voudrait en quelque sorte, influencer les scrutins occidentaux.

5.4 Les fichiers TES

Le ficher du « titre électronique sécurisé », autrement dit le « ficher TES », est un projet du ministère de l'Intérieur, qui de nos jours a d'ores et déjà pris forme. En effet, il s'agit d'une base de données qui est composée de nombreuses informations personnelles sur le citoyen à savoir: la couleur des yeux, l'identité, la taille, le sexe, l'adresse de domicile, l'adresse courriel, les empreintes digitales, la photo d'identité et la signature.

Beaucoup de débats ont surgi à ce sujet étant donné que cette base de données représente un danger considérable pour l'ensemble des citoyens français, puisque s'il s'avérait que ces fichiers soient piratés, l'identité de milliers de citoyens pourrait être dérobée, et cela avec des informations plus que précises. C'est d'ailleurs pour cette raison que le Conseil national du numérique a suspendu le projet le 7 novembre 2016, mais a déclaré par la suite que:

> « Le Conseil s'interroge sur la nécessité de stocker de manière centralisée des informations aussi sensibles. [...] Un travail d'anticipation détaillé reste dans tous les cas à conduire. [...] Au-delà des questions spécifiques au fichier TES, le Conseil conclut qu'il y a

> urgence à réformer la gouvernance des choix technologiques au sein de l'État dans le sens d'une transparence et d'une ouverture accrues. »[153]

C'est ainsi que le projet voit le jour et se met en place concrètement sur l'ensemble du territoire français le 30 mars 2015.

5.5 La coopération internationale: l'Union européenne et l'OTAN

L'ancêtre du réseau informatique mondial, ARPANET est le premier réseau interconnecté qui a été développé aux États-Unis par la DARPA (Defense Advanced Research Projects Agency). Chargée de la recherche et du développement des nouvelles technologies pour l'armée américaine, l'agence a financé ce projet qui a vu le jour en 1969. C'est à partir des années 1990 qu'Internet est découvert par le grand public grâce au World Wide Web (WWW). En effet, Internet est désormais omniprésent dans nos vies, et notamment à l'heure du WEB 2.0. Tom O'Reilly, l'initiateur du Web 2.0, a déclaré que:

> « Le web 2.0 repose sur un ensemble de modèles de conception : des systèmes architecturaux plus intelligents qui permettent aux gens de les utiliser, des modèles d'affaires légers qui rendent possibles la syndication et la coopération des données et des services. Le web 2.0 c'est le moment où les gens réalisent que ce n'est pas le logiciel qui fait

---

153 Le conseil national du numérique. CCNNum, Fichier TES : le Conseil national du numérique publie son avis. (12/12/2016). Récupéré de https://tes.cnnumerique.fr/blog/fichier-tes-le-conseil-national-du-numerique-publie-son-avis

le web, mais les services ».[154]

Suite à la création d'ARPANET, la DARPA met en place l'*Internet Configuration Control Board* en 1979 afin d'assurer la sécurité du réseau, qui sera renommé ensuite *Internet Architecture Board* en 1992. Puis, il y a eu la création par les États-Unis d'un groupe de recherche afin de développer la messagerie électronique: Internet Engineering Task Force (IETF). Vient ensuite la création de l'Internet Assigned Numbers Authority (IANA) qui a pour rôle d'assigner les noms de domaines et les adresses IP (numéro d'identification permettant à un appareil de se connecter au réseau Internet). Depuis, l'IANA attribue les adresses IP selon les zones géographiques avec les Registres Internet régionaux (RIR) crées en 1990. En 1998, ces fonctions seront attribuées à un nouvel organisme, l'ICANN (*Internet Corporation for Assigned Names Numbers*).

De nombreux États se sont alors interrogés sur la gouvernance de ce réseau mondial commençant tout juste à prendre forme. Cela a donné lieu à divers Sommets mondiaux sur la société de l'information et la gouvernance d'Internet (SMSI), organisés par l'Union internationale des télécommunications (UIT), une instance liée à l'Organisation des Nations Unies (ONU). Pour Adam Segal, « WSIS was the first « battle for the soul of Internet », one of the rare occasions when the conflict between worldview on how the Internet should be governed»[155]. Ces sommets se sont déroulés en deux phases. La première phase a eu lieu à Genève en 2003. Selon l'UIT, il s'agissait durant ce sommet de:

---

154 O'Reilly, T. Récupéré de http://www.internetactu.net/2005/09/29/quest-ce-que-le-web-20/

155 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.211).* Etats-Unis: 1st Edition.

> « Formuler de façon parfaitement claire une volonté politique et prendre des mesures concrètes pour poser les bases d'une société de l'information accessible à tous, tout en tenant pleinement compte des différents intérêts en jeu ».[156]

La deuxième phase s'est tenue à Tunis en 2005, avec pour objectif de:

> « Mettre en oeuvre le Plan d'action de Genève et aboutir à des solutions et parvenir à des accords sur la gouvernance de l'Internet, les mécanismes de financement, et le suivi et la mise en oeuvre des documents de Genève et Tunis ».[157]

Les deux sommets ont été suivis d'un forum à Athènes en 2006, pour discuter de la Gouvernance d'Internet et d'un sommet à Dubaï en 2014, où la question de la suprématie américaine a été abordée, notamment en lien avec les enjeux que représentent les assignations des noms de domaine par l'ICANN. Pour sa sécurité et son développement au sein du cyberespace, l'Europe agit également au travers de diverses instances internationales telles que l'ENISA (European Union agency for network and information security), et le CCDCOE (Cooperative cyber defense centre of excellence).

Quels sont les nouveaux enjeux de cyberdiplomatie qu'explore la France en termes de coopération internationale avec l'UE et l'OTAN ?

---

156 Union internationale des télécommunications. Récupéré de http://www.itu.int/fr/about/Pages/default.aspx

157 Union internationale des télécommunications. Récupéré de http://www.itu.int/fr/about/Pages/default.aspx

Tout comme la France, de nombreux États-nations commencent à mettre en place des stratégies nationales de cybersécurité. En effet, dans ce contexte, la notion de souveraineté semble jouer un rôle primordial. Même au sein du cyberespace, les nations souhaitent garder leur souveraineté et faire valoir leur droit à un niveau national:

> « « Digital sovereignty » is an evocative if vague term that harkens back to twentieth-century conceptions of regulation and state control. It represents the old world imposing itself on the hacked world. » [158]

Cette notion de souveraineté semble nettement s'opposer à celle de la gouvernance globale d'Internet. De plus, les États-nations n'ont souvent pas les moyens techniques afin d'exercer cette autorité nationale. Plus qu'un enjeu concernant les droits humains fondamentaux, cette souveraineté serait également le moyen pour les États de développer une économie liée au numérique:

> « For some, digital sovereignty is synonymous with the de-Americanization of the Internet. One French Foreign Ministry official described the US technology companies to me as « the gatekeepers of the digital economy, absorbing the value an ensuring European companies act as subcontractors »[159]

Les valeurs fondamentales de l'Union européenne et des pays qui la composent, telles que la liberté d'expression, le respect des droits de l'Homme et la

---

158 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.21).* Etats-Unis: 1st Edition.

159 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.21-22).* Etats-Unis: 1st Edition.

souveraineté, sont également des valeurs qu'elle souhaite faire valoir au sein du cyberespace. L'un des enjeux pour l'UE est de se positionner internationalement comme modèle porteur des valeurs des droits humains dans le cyberespace. L'Union européenne ne pourra peut-être pas devenir un adversaire puissant en matière de gouvernance du cyberespace, mais elle peut apporter beaucoup concernant les droits démocratiques fondamentaux:

> « The question for US policymakers is wether to continue to fight the battle over competing vision of cyberspace or to design polices that mediate and respond to the splintering of the global Internet into national sovereignties ».[160]

Ces valeurs ont notamment été mises de l'avant de par les révélations de *Wikileaks* sur la collecte des données par la NSA. En effet la NSA « had been collecting the phone and e-mail metadata of millions of European users, the ignition official reaction was fairly muted »[161]. Cela a entraîné une détérioration des rapports européens et américains.

La circulation des données personnelles et la liberté d'expression font beaucoup débat en Europe, et plus encore depuis les récents attentats de Paris à Charlie Hebdo. Cette menace terroriste amène l'Europe à coopérer avec les États-Unis, même si les deux puissances détiennent des différents sur les notions de circulation et d'accès aux données personnelles.

---

160 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.223).* Etats-Unis: 1st Edition.

161 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.143).* Etats-Unis: 1st Edition.

Cette vision des droits humains, remonte bien avant l'apparition du cyberespace et a depuis longtemps tenue un rôle un important en France et en Europe. Quant au droit à la souveraineté des États, il s'est manifesté avec les travaux de Thomas Hobbes et va se renforcer notamment à l'intérieur de l'espace Schengen:

> « This concept of the role of the state echoes Thomas Hobbes, whereby the state acts to defend and protect the nation interest and, at times, violates individual rights, if necessary, for state preservation.»[162]

La Convention de Budapest a fait beaucoup dans ce sens pour le territoire Européen, où il a été décidé que les crimes commis dans le cyberespace subiront pratiquement les mêmes sanctions que dans la vie réelle. Le respect des données personnelles est une question de droit, mais elle concerne également les intérêts économiques:

> « The Snowden revelations fanned and reinforced a growing unease in Europe with the size and dominance of US technology companies reflected in the acronym « GAFA » — Google, Apple, Facebook, and Amazon — often deployed by French critics. »[163]

La France souhaite s'imposer sur le marché économique lié au numérique, mais ne détient pas les capacités humaines et matérielles nécessaires face aux grandes entreprises multinationales, venant principalement des États-Unis, telle que les

---

162 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.49).* Etats-Unis: 1st Edition.

163 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.159).* Etats-Unis: 1st Edition.

« GAFA ».

Ces tensions sur la protection et la circulation des données personnelles entre l'Europe et les États-Unis, s'expliquent par le fait que ces deux puissances ne détiennent pas la même culture des libertés individuelles fondamentales. En effet, Adam Segal souligne qu'en Europe il s'agit d'un droit humain tandis qu'aux États-Unis, les contraintes et les attentes sont moins fortes. Il y a également en Europe « le droit à l'oubli », tel qu'il le laisse entendre, le droit pour chaque individu de demander le retrait définitif d'Internet d'informations le concernant, même si cela reste encore difficile à appliquer:

> « In November 2014, Europe's privacy regulators argued that the right to be forgotten should go global. Google was removed links from the local version of Google in France (www.google.fr) and Germany (www.google.de) but not from the primary Google site (www.google.com) ».[164]

L'Europe devient donc un modèle dans ce domaine, et inspire de nombreux autres États. Le modèle européen renvoie une image « general, aspirational, horizontal and concise »[165].

Les échanges au sein de l'Union européenne passent principalement par les réseaux d'information et de communication. C'est ainsi que l'organisation prend conscience du danger que peut représenter une négligence au niveau de la

---

164 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.164).* Etats-Unis: 1st Edition.

165 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.164).* Etats-Unis: 1st Edition.

cybersécurité.

Vincent Joubert et Jean-Loup Samaan nous rappellent en quoi consiste la politique de cybersécurité européenne. Selon les deux auteurs, cette politique se construit en deux phases. La première consiste à « renforcer la sécurité des systèmes d'information et des réseaux de l'ensemble des institutions »[166] de l'organisation. La deuxième « doit permettre d'améliorer la cybersécurité de l'ensemble de l'Union, c'est-à-dire, sur les réseaux et systèmes de ses États membres »[167]. Les auteurs nous rappellent également l'importance qu'accorde l'UE aux respects des libertés individuelles au sein du cyberespace.

L'ENISA a été créée en 2004 par le Parlement Européen et le Conseil de l'Europe dans le but de développer, avec les États membres européens la protection, la sécurité des systèmes d'informations et des réseaux, surtout à un niveau d'expertise technique dont manquait l'Europe jusqu'à présent. L'agence a pour rôle de donner des conseils d'expertises à l'Union européenne concernant la cybersécurité. Plus qu'à un niveau gouvernemental, l'agence travaille également avec le secteur privé. L'ENISA détient trois principales missions étant, la recommandation en conseillant et préconisant les États, le partenariat qui permet à l'agence de coopérer activement avec d'autres organismes et la mise oeuvre de politiques pour le renforcement de la sécurité.

La République d'Estonie, pays de l'Europe du Nord, membre de l'Union

---

166 Joubert, V. et Samaan, J-L. (2014).L'intergouvernementalité dans le cyberespace: étude comparée des initiatives de l'OTAN et de l'UE. France: Hérodote.

167 Joubert, V. et Samaan, J-L. (2014).L'intergouvernementalité dans le cyberespace: étude comparée des initiatives de l'OTAN et de l'UE. France: Hérodote.

européenne, de l'Organisation des Nations Unies et de l'OTAN, est l'un des plus grands usagers du réseau Internet au monde, d'où son surnom *E-stonie*. En avril 2007, l'Estonie connaît la première cyberattaque de l'histoire, souvent représentée comme étant la « Première Guerre informatique mondiale ». En effet, une série de cyberattaques a déferlé sur le pays touchant les réseaux gouvernementaux, financiers et médiatiques. L'attaque a même entraîné la déconnexion du pays au réseau Internet pendant quelques instants. Cela a débuté de par le déplacement, d'une statue représentant un soldat soviétique de la seconde guerre mondiale, de la capitale estonienne vers l'extérieur de la ville. Ce soldat représentait un symbole de la Russie, et son déplacement a été perçu comme une attaque. Le but de cette action par le gouvernement estonien était de se détacher de la puissance russe et de se rapprocher de l'Union européenne, Vladimir Poutine a d'ailleurs déclaré « defile the monuments to the heroes of this war are insulting their own peoples »[168].

Ce déplacement et les cyberattaques qui ont suivi ont entrainé de violentes émeutes dans la capitale estonienne et des conséquences sur les relations diplomatiques entre les deux pays. Les autorités estoniennes ont immédiatement demandé l'aide de l'Union européenne et de l'OTAN. Des preuves techniques ont montré que les cyberattaques étaient directement reliées au bureau du Kremlin, ce qui a fait réagir ouvertement le Premier ministre estonien qui a accusé le gouvernement russe, contrairement à l'Union européenne qui ne s'est pas prononcée publiquement.

Suite à ces cyberattaques sur l'Estonie, l'OTAN a créé le « Cyber Defense

---

168 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.62).* Etats-Unis: 1st Edition.

Management Authority » et le « Cooperative cyber defense center of excellence » (CCDCOE) dans la ville de Tallinn. Cette organisation est chargée de développer avec les pays membres les problématiques liées au cyberespace en matière de sécurité, d'éducation ou encore de sensibilisation.

Adam Segal souligne une des problématiques à laquelle fait face l'OTAN aujourd'hui. En effet, malgré les nombreux efforts faits par l'organisation, notamment durant les sommets de 2012 et 2014, l'alliance ne détient pas ses propres armes pour défendre ses États membres:

> « NATO met again in the summer 2014 [...] Cyberattacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defense is part of NATO's core task of collective defense ».[169]

En parallèle à l'ouverture du centre d'expertise en Estonie, a été ouverte en 2008 dans la capitale belge, à Bruxelles, une autorité pour la défense du cyberespace. Néanmoins, la problématique majeure au sein de l'OTAN et des organisations qui y sont liées reste la persistance des États membres à vouloir affirmer leur souveraineté, ce qui n'aide pas dans le processus d'échange.

Ces deux instances internationales, l'Union européenne et l'OTAN montrent l'envie et le besoin de développer des politiques de cybersécurité qui se sont manifestés par la création de ces deux centres d'expertises représentés par

---

169 Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (p.76).* Etats-Unis: 1st Edition.

l'ENISA et le CCDCOE. Néanmoins de nombreux efforts restent encore à faire pour permettre d'établir un procédé de défense efficace. De plus, les inégalités entre les États membres entraînent des contradictions dans la mise en place des politiques. Le manque d'infrastructures tant pour l'UE que pour l'OTAN est une condition importante, puisque de nos jours la plupart des organismes relevant du numérique et possédant les infrastructures critiques sont privées.

5.6 Décision des ministres des Finances du G7

Le dernier sommet du G7 s'est tenu dans une petite ville de 11 000 habitants sur les côtes sicilienne de l'Italie. Les membres du Groupe des Sept sont: les États-Unis, le Japon, l'Allemagne, la France, le Royaume-Uni et le Canada, avec leurs représentants respectifs: Donald Trump, Shinzo Abe, Angela Merkel, Emmanuel Macron, Theresa May et Justin Trudeau.

Plusieurs problématiques ont été abordées lors du sommet, telles que le commerce international, l'Accord de Paris sur le climat, l'autonomisation économique des femmes, ainsi que l'attentat de Manchester et la lutte contre le terrorisme.

Au sein de son programme l'Italie souhaite particulièrement s'attarder sur la cybersécurité et la lutte contre le financement du terrorisme. De plus, le Premier ministre italien Paolo Gentiloni souhaite faire des relations avec la Russie, une priorité.

Ainsi, il a été adopté par le Groupe des Sept une déclaration contre le terrorisme et notamment contre la cyberpropagande terroriste. Faisant dans cette visée, écho aux récents attentats qui ont eu lieu en Grande-Bretagne.

La cybersécurité ne cesse donc d'être un sujet d'actualité, et les pays au sein des alliances internationales mettent en place des procédures afin d'assurer la sécurité de leurs réseaux et de leurs territoires. Le terrorisme semble aujourd'hui représenter la menace la plus importante, et les États-nations s'unissent afin de lutter contre l'État islamique tant bien sur le terrain que dans le cyberespace.

5.7 Les nouveaux enjeux de cyberdiplomatie et de cybersécurité pour la France

La cyberattaque contre TV5 Monde s'articule donc autour de différents discours et perspectives. En effet, la première perspective de TV5 Monde nous précise les réactions et les dispositions immédiates mises en place suite à la cyberattaque. Une attaque, qui selon le directeur de la chaîne, a été pensée à des fins de destruction et représentait également une atteinte à certains droits fondamentaux français étant la liberté d'expression et d'information. L'agence de cybersécurité française, l'ANSSI a immédiatement été contacté et une enquête a par la suite abouti avec de nouvelles dispositions de cybersécurité.

Une première piste s'est dirigée vers l'organisation de DAECH, de par les messages explicites laissés sur les réseaux sociaux par le Cyber Califat. De plus,

suite aux attentats de Paris, la menace de l'État islamique pesait toujours sur la France et représentait ainsi un risque à considérer par les autorités françaises. Cependant quelques jours plus tard, l'enquête plus approfondie de l'agence de cybersécurité française révèle de nouvelles preuves techniques avec une deuxième piste visant la Russie. Pour quelles raisons les russes seraient-ils à l'origine de cette cyberattaque envers la France et pourquoi se feraient-ils passer pour des djihadistes de DAECH ? De par cette opération de « faux drapeaux », les suppositions vont dans le sens que la Russie aurait entrepris cette attaque à cause des conflits ukrainiens et des sanctions prises par l'Union européenne.

Suite à la stratégie française de 2011, les nouveaux enjeux de cybersécurité que présente la nouvelle stratégie nationale parue en 2015, notamment de par la cyberattaque de TV5 Monde, concernent avant tout la sécurité des systèmes d'information de l'État. Aussi, la sensibilisation des citoyens aux risques présents dans le cyberespace et la protection de leurs données personnelles. La stratégie aborde également les différents avantages économiques que présente le numérique de nos jours et dont la France peut en tirer parti. Enfin, la question de la coopération internationale apparaît avec la place que souhaite tenir la France au sein des différentes instances internationales dont elle fait partie.

La France explore de nouveaux enjeux de cyberdiplomatie sur la scène internationale par le biais de l'UE et l'OTAN. L'agence européenne de cybersécurité l'ENISA, lui permet d'acquérir une expertise technique pour la cybersécurité de son territoire. Quant au CCDCOE, il lui permet de développer de nombreux axes concernant les problématiques de cybersécurité, d'éducation et de sensibilisation.

Cette cyberattaque constitue donc un point tournant, conduisant à la nouvelle stratégie française, et à de nouvelles pistes en émergence à la recherche d'une coopération plus marquée au niveau des organisations internationales et multilatérales, de l'Union européenne à l'OTAN, au Internet Governance Forum, à l'Union Internationale des Communications et au Groupe des experts gouvernementaux de l'ONU. Cet essai d'analyse des « ordres du discours » diplomatique et médiatique constitue donc une tentative d'analyse de ces enjeux, un peu comme dans une valse à trois temps: la cyberattaque, la nouvelle stratégie nationale, et de nouvelles pistes potentielles de coopération.

ANNEXE A

PREMIÈRE STRATÉGIE NATIONALE DE CYBERSÉCURITÉ FRANÇAISE

(2009)

Prologue

Sans doute n'en avons-nous pas encore pris collectivement la mesure : dans le *Livre blanc sur la défense et de la sécurité nationale* présenté par le Président de la République en juin 2008, la sécurité des systèmes d'information émergeait, avec la dissuasion, comme un domaine dans lequel la souveraineté de la France devrait s'exprimer pleinement.

Le cyberespace peut pourtant apparaître bien éloigné du champ de la défense et de la sécurité nationale. En vingt ans, les technologies du numérique ont fusionné nos vies personnelles et professionnelles, porté la compétitivité des entreprises à un niveau inédit, rapproché les administrations des usagers et favorisé la transparence de la vie des institutions de notre pays.

Le cyberespace, nouvelle tour de Babel, est un lieu de partage des cultures du monde, de diffusion des idées et d'informations en temps réel, un lieu d'échanges entre personnes. L'exclusion du numérique condamne les individus à l'isolement, les entreprises à la décroissance et les nations à la dépendance.

Dans le monde matériel, les destructions causées par les guerres ou le terrorisme comme les exactions des criminels sont visibles et souvent médiatisées. Dans le cyberespace, monde immatériel, les conséquences des attaques informatiques contre les systèmes d'information des États, des entreprises ou contre les ordinateurs des citoyens ne sont le plus souvent visibles que des spécialistes et restent ignorées du grand public.

Le cyberespace, nouvelles Thermopyles, est devenu un lieu d'affrontement : appropriation de données personnelles, espionnage du patrimoine scientifique, économique et commercial d'entreprises victimes de leurs concurrents ou de puissances étrangères, arrêt de services nécessaires au bon fonctionnement de l'économie ou de la vie quotidienne, compromission d'informations de souveraineté et même, dans certaines circonstances, perte de vies humaines sont aujourd'hui les conséquences potentielles ou réelles de l'imbrication entre le numérique et l'activité humaine.

Devant l'irruption du cyberespace dans le champ de la sécurité nationale et à la mesure des enjeux, le Gouvernement a décidé de doter la France d'une capacité structurée de défense et de sécurité. Il a ainsi créé en 2009 l'Agence nationale de la sécurité des systèmes d'information (ANSSI), autorité au service des pouvoirs publics, des entreprises et des citoyens. Le Président de la République a décidé en juillet dernier de confier à l'Agence, en complément de sa mission de sécurité, une mission de défense des systèmes d'information.

L'objectif de ce document est de préciser les grandes lignes de la stratégie poursuivie par la France depuis la publication du *Livre blanc sur la défense et la sécurité nationale* afin de garantir, dans le cyberespace, la sécurité de nos compatriotes, de nos entreprises et de la Nation.

Francis DELON

Secrétaire général de la défense et de la sécurité nationale

Les mots suivis d'un astérisque sont définis dans le glossaire

Crédits Photos

couverture	Jean [illegible] (CC BY-NC-ND 2.0) ou libres de droits
page 8	[illegible] (CC BY-NC-SA 2.0)
page 12	Simon [illegible] (CC BY-NC-ND 2.0)
page 13	[illegible] (CC BY-NC-ND 2.0)
page 14	[illegible] (CC BY-SA 2.0)

Sommaire

Synthèse

4. Assurer la sécurité dans le cyberespace

Les menaces qui pèsent sur les systèmes d'information touchent tout à la fois les administrations, les entreprises et les citoyens.

L'administration doit être exemplaire et améliorer la protection de ses systèmes d'information et des données qui lui sont confiées.

S'agissant des entreprises et des particuliers, un travail d'information et de sensibilisation doit être engagé.

En matière de lutte contre la cybercriminalité, la France encouragera le renforcement du droit et l'entraide judiciaire internationale.

Pour atteindre ces objectifs, sept axes d'effort sont retenus :

1. Mieux anticiper et analyser l'environnement afin de prendre les décisions adaptées.
2. Détecter les attaques et les contrer, alerter les victimes potentielles et les accompagner.
3. Accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines dans l'objectif de conserver l'autonomie nécessaire.
4. Protéger les systèmes d'information de l'État et des opérateurs d'infrastructures vitales pour une meilleure résilience nationale.
5. Adapter notre droit afin de prendre en compte les évolutions technologiques et les nouveaux usages.
6. Développer nos collaborations internationales en matière de sécurité des systèmes d'information, de lutte contre la cybercriminalité et de cyberdéfense pour mieux protéger les systèmes d'information nationaux.
7. Communiquer, informer et convaincre afin de permettre aux Français de prendre la mesure des enjeux liés à la sécurité des systèmes d'information.

Ce document résume la partie publique des orientations et actions approuvées par le comité stratégique de la sécurité des systèmes d'information institué par le décret n° 2009-834 du 7 juillet 2009 portant création de l'agence nationale de la sécurité des systèmes d'information" (ANSSI).

Quatre objectifs stratégiques

I. Être une puissance mondiale de cyberdéfense

Le développement de la société de l'information, porté par les réseaux de communications électroniques, parce qu'il crée de la valeur et de nombreux emplois, est un formidable moteur de notre croissance. Il contribue fortement à la compétitivité du tissu économique national et donc au rang de la France dans le monde.

Or, les réseaux de communications électroniques font l'objet d'activités illicites menées directement ou indirectement par des États. Certains se livrent à des opérations massives d'espionnage via ces réseaux et cherchent à obtenir des informations de souveraineté, comme celles relevant du secret de la défense nationale ou encore du patrimoine scientifique, technologique, commercial ou financier des entreprises de nos secteurs stratégiques.

De leur côté, des groupes terroristes utilisent ces mêmes réseaux de communications électroniques pour propager leurs idées, diffuser de l'information opérationnelle à leur organisation et se livrer à des activités de propagande.

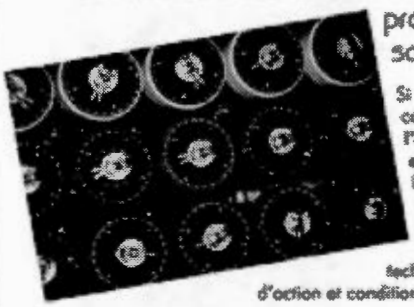
Dans un avenir proche, États ou groupes terroristes pourraient attaquer les infrastructures vitales d'État considérés comme idéologiquement hostiles.

Il est donc indispensable que la France se dote d'une capacité de cyberdéfense.

Or, contrairement à ceux du monde matériel, les affrontements dans le cyberespace ne connaissent pas les frontières. Ainsi, une cyberdéfense crédible ne peut être uniquement nationale et doit s'appuyer sur un réseau d'alliés avec lesquels il est possible d'échanger, en temps réel, des informations sur les vulnérabilités, les dispositifs de protection, les attaques et les parades à mettre en œuvre face aux agressions menées dans le cyberespace directement ou indirectement par des États ou des groupes terroristes. La France renforcera ses partenariats opérationnels avec ses alliés les plus proches et mettra à profit son expertise pour contribuer activement à la formulation des politiques de cyberdéfense au sein des organisations internationales, et notamment au sein de l'Union européenne.

Quatre objectifs stratégiques

2. Garantir la liberté de décision de la France par la protection de l'information de souveraineté



Si l'évolution de la société tend à imposer comme règle l'existence et le partage de l'information et son accès, à la fois instantané et sous de multiples formes, une part de l'équilibre du monde réside toujours dans la capacité à maintenir secrète « l'information de souveraineté », fraction de l'information diplomatique, militaire, scientifique, technique et économique qui permet la liberté d'action et conditionne la prospérité des nations.

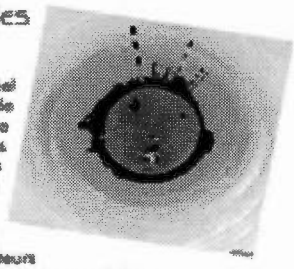
Comme par le passé, les services de renseignement du monde entier, parmi d'autres acteurs, tentent d'obtenir l'information de souveraineté. Les réseaux de télécommunications, notamment Internet, les informations qui y circulent, celles disponibles sur les réseaux ou les terminaux qui s'y connectent, sont devenus à la fois sources d'information et vecteurs de collecte.

Le moyen le plus efficace pour protéger l'information de souveraineté est d'utiliser des techniques de cryptographie* qui rendent impossible, ou du moins retardent, sa compréhension si cette information venait à être altérée, divulguée ou interceptée. Les progrès de la cryptanalyse*, qui suivent notamment ceux de la puissance de calcul des ordinateurs, obligent à concevoir et utiliser des méthodes et techniques plus difficiles à analyser et renouvelées régulièrement.

Le maintien de notre autonomie stratégique repose sur notre capacité à maîtriser les techniques cryptographiques et les technologies clés nécessaires à la conception de produits de sécurité* qui les utilisent, ce qui implique de veiller à ce que le domaine de la sécurité des systèmes d'information reste attractif pour les jeunes diplômés afin d'éviter le tarissement progressif des compétences.

Parallèlement à la nécessité de pouvoir communiquer de manière sûre et confidentielle, les décideurs comme les organismes associés à la gestion des situations de crise doivent avoir à leur disposition des moyens de communication disponibles en toutes circonstances. Ces moyens d'échanges électroniques, de téléphonie et de visioconférence sécurisés ont été conçus et développés. Leur déploiement va se poursuivre dans les années qui viennent, notamment au profit des opérateurs d'importance vitale*.

3 Renforcer la cybersécurité des infrastructures vitales nationales



Par la convergence de multiples technologies, le monde réel et les réseaux s'interpénètrent. De nombreux objets du monde réel — de l'étiquette de supermarché à la raffinerie, de la photocopieuse au drone de combat — embarquent des systèmes d'information et s'y intègrent. À distance, via les réseaux, il est possible de collecter les informations transmises par ces objets, de les maintenir en fonction et de les piloter.

La France a défini dans son code de la défense des secteurs d'activités d'importance vitale dans lesquels agissent des opérateurs qui concourent à la satisfaction des besoins indispensables à la vie des populations, à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la Nation, dès lors que ces activités sont difficilement substituables ou remplaçables.

La plupart des opérateurs d'importance vitale utilisent largement les réseaux de télécommunications, et singulièrement Internet, tant pour leur gestion que pour l'exercice de leur métier. Pourtant, dans la rencontre, ancienne et pourtant inédite parce que bouleversée par l'interconnexion des systèmes, entre le monde industriel et le monde de l'informatique, le premier manque de formation et de sensibilisation à la sécurité des systèmes d'information, tandis que le second méconnaît souvent les contraintes et le fonctionnement des systèmes industriels.

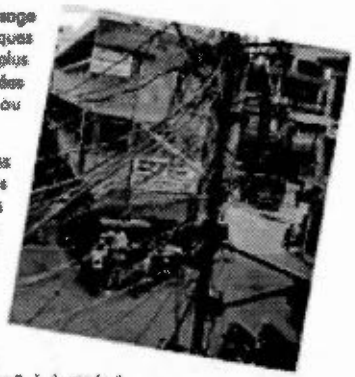
La dépendance de chacun des acteurs vis-à-vis d'Internet est accrue par des tendances lourdes de notre organisation économique et sociale : l'externalisation et l'informatique en nuage, la mutualisation des services supports, la gestion en temps réel et en flux tendus, le nomadisme, le transfert de tâches vers les clients ou les administrés, la création ou la réingénierie de nombreux processus.

En cas d'interruption du fonctionnement des réseaux de télécommunications ou d'Internet, les moyens de substitution peuvent s'avérer très insuffisants, notamment par manque de personnels qualifiés susceptibles de remettre en fonction les processus antérieurs à l'avènement de l'ère numérique. Dans le cas de processus directement issus de nouveaux usages liés aux technologies de l'information, les moyens de substitution n'existent pas.

Comme le démontre régulièrement l'actualité mondiale, les conséquences possibles d'actes de malveillance contre les systèmes automatisés de contrôle des processus industriels déployés par les opérateurs d'importance vitale sont aujourd'hui insuffisamment mesurées. Ainsi, la protection des réseaux de communications électroniques — et notamment d'Internet — comme la sécurisation des systèmes critiques des opérateurs d'importance vitale constituent des priorités nationales.

Quatre objectifs stratégiques

1 Assurer la sécurité dans le cyberespace



Pour une part croissante de nos concitoyens, l'usage des réseaux de communications électroniques comme Internet imprègne les fonctions les plus courantes de la vie quotidienne comme celles liées au commerce, aux démarches administratives ou aux échanges interpersonnels.

Parallèlement, les techniques utilisées dans le cyberespace par des individus ou groupes d'individus malveillants sont de plus en plus performantes et visent à usurper des identités, à se procurer les informations nécessaires à l'accès à des comptes bancaires ou à collecter et revendre des données personnelles. On observe également une multiplication des cas de prises de contrôle malveillantes à distance d'ordinateurs visant à les intégrer dans des réseaux de machines compromises (« botnets ») destinés à accomplir des actes illicites tels que des attaques informatiques ou des envois de courriels malveillants.

Dans ce contexte, les administrations doivent montrer l'exemple en protégeant le cyberespace public. Les usagers doivent utiliser en confiance les services électroniques proposés par les autorités publiques, notamment au regard de la protection de leurs données personnelles. Le référentiel général de sécurité (RGS) publié début 2010 offre un cadre réglementaire susceptible de renforcer cette sécurité. Son respect et sa mise en œuvre par les autorités publiques sont prioritaires.

La sécurisation du cyberespace passe par une démarche systématique d'information des entreprises et des citoyens sur les risques encourus et les moyens de s'en protéger. L'objectif est qu'à terme, chaque citoyen puisse être sensibilisé aux questions de cybersécurité au cours de son éducation. Cette démarche appelle la mise en place d'une politique de communication gouvernementale active.

Enfin, Internet est un espace de droit. La France doit encourager le renforcement ou l'édiction de règles juridiques dans le cyberespace lorsque le droit existant est insuffisant et amplifier l'entraide judiciaire internationale en matière de répression des infractions commises sur ou à travers les réseaux de communications électroniques.

Afin de remplir les quatre objectifs stratégiques, 7 axes d'effort ont été retenus.

Sept axes d'effort

1 Anticiper, analyser

Risques et menaces évoluent rapidement dans le cyberespace. La parution d'un nouveau produit ou d'une nouvelle version d'un logiciel, la publication d'une faille* non corrigée d'un logiciel largement utilisé, l'apparition d'une nouvelle technologie ou d'un nouvel usage, une déclaration politique, peuvent entraîner, dans des délais très courts, une mise en danger de la sécurité des systèmes d'information.

- Dans ce contexte, la défense et la sécurité de nos systèmes d'information passe en premier lieu par un suivi de l'actualité des technologies et par une analyse, une bonne compréhension voire une anticipation du jeu des acteurs publics ou privés.

2 Détecter, alerter, réagir

Compte-tenu de la dépendance croissante à Internet des entreprises, des infrastructures et des services, et en raison des risques systémiques portés par certaines faiblesses, il est nécessaire d'être en mesure de détecter au plus tôt failles et attaques, d'alerter les victimes potentielles ou avérées et de leur proposer dans un délai bref une aide à l'analyse et à l'élaboration de parades.

- Comme l'a prévu le *Livre blanc sur la défense et la sécurité nationale*, la France développe une capacité de détection des attaques sur les systèmes d'information. Notamment déployés dans les réseaux des ministères, des dispositifs permettent d'alerter leurs responsables, d'aider à élucider la nature des attaques et d'élaborer des parades adaptées.
- Pour gérer l'ensemble des informations recueillies par les outils de détection, par les dispositifs de veille ou transmises par nos partenaires, afin de présenter une image en temps réel de la situation des réseaux nationaux et pour être capable de gérer une situation de crise, l'ANSSI se dote d'une « salle d'opération » à la hauteur des enjeux.
- Pour répondre aux crises majeures affectant ou menaçant la sécurité des systèmes d'information des autorités administratives ou des opérateurs d'importance vitale, l'État doit être en mesure de prendre rapidement les mesures nécessaires. Dans cette optique, l'ANSSI assure la fonction d'autorité nationale de défense des systèmes d'information.

4. Protéger les systèmes d'information de l'État et des opérateurs d'infrastructures vitales

Comme le souligne le *Livre blanc sur la défense et la sécurité nationale*, nous devons disposer « d'une offre de produits de très haute sécurité totalement maîtrisés, pour la protection des secrets de l'État, ainsi que d'une offre de produits et de services de confiance labellisés, à laquelle recourront les administrations et qui seront largement accessibles au secteur économique ». Des réseaux sécurisés résilients* pour « l'ensemble de la chaîne de décision et de commandement sur le territoire métropolitain » doivent être utilisés.

- Relevant de l'information classifiée*, la stratégie française en matière de produits de sécurité et de composants a été redéfinie. Elle prend notamment pleinement en compte le retour de la France dans le commandement intégré de l'OTAN.
- Dans les réseaux ministériels, la mise en place de systèmes d'authentification forte reposant, par exemple, sur l'utilisation de cartes à puce, domaine d'excellence française, va permettre d'en améliorer très significativement la sécurité.
- Les autorités gouvernementales disposent aujourd'hui d'un intranet sécurité interministériel, d'un réseau de téléphonie à forte disponibilité qui sera totalement équipé de nouveaux terminaux chiffrants d'ici 2012, et d'une solution de visio-conférence protégée, en particulier destinée à équiper les centres de décision ministériels. Le déploiement de ces différents réseaux se poursuivra, notamment dans les administrations territoriales.
- Dans le domaine de la sécurité des systèmes d'information des opérateurs d'importance vitale, un partenariat public-privé sera mis en place afin, d'une part, de faire profiter les opérateurs de l'information dont dispose l'État en matière d'analyse des menaces, et d'autre part, de permettre à l'État de s'assurer que les infrastructures essentielles au bon fonctionnement de la Nation disposent d'un niveau de protection adéquat. Un travail sera également engagé avec les équipementiers.

5. Adapter notre droit

Les nouveaux usages portés par le développement du cyberespace peuvent, si l'on n'est suffisamment vigilant, présenter des dangers pour nos libertés individuelles, le fonctionnement des infrastructures vitales ou l'équilibre de nos entreprises.

Notre cadre législatif et réglementaire doit suivre l'évolution des techniques. Les textes seront adaptés en fonction de l'apparition de nouvelles technologies ou de nouveaux usages, afin de renforcer la sécurité des particuliers et avec le souci du

3 Accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines

La sécurité des systèmes d'information repose sur une maîtrise de technologies et de savoir-faire, également accessibles aux organisations et individus qui veulent y porter atteinte. Si les acteurs étatiques de la sécurité des systèmes d'information doivent connaître « l'état de l'art », ils doivent également être en mesure d'anticiper voire de créer les évolutions technologiques en maintenant leurs capacités de recherche, seules capables de permettre de limiter l'avantage tactique de l'attaquant sur le défenseur.

La France dispose d'équipes de recherche de niveau mondial dans les domaines de la cryptologie et des méthodes formelles. Dans d'autres domaines, comme celui des architectures de sécurité des systèmes d'information, elle rattrape le niveau des nations les plus avancées.

- Pour catalyser ces travaux, la création, avec des partenaires industriels, d'un centre de recherche consacré à la cyberdéfense est à l'étude. Ce centre mènera des activités de recherche scientifique (recherche en cryptologie, étude des groupes d'attaquants et de leurs méthodes, expertise sur les logiciels malveillants et les failles informatiques, développement de logiciels libres sécurisés, élaboration de concepts de défense informatique, etc.), et des actions d'expertise et de formation.

Le développement de la société de l'information crée pour les entreprises un marché d'ampleur mondiale, aujourd'hui préempté par des acteurs situés hors d'Europe. S'agissant de la sécurité des systèmes d'information, cette situation n'est ni souhaitable ni tenable. La France dispose pourtant d'un tissu industriel de pointe unique en Europe, qui lui permet potentiellement de maîtriser une grande partie des technologies nécessaires à la conception de produits de sécurité, y compris en matière de composants. De nombreuses PME innovantes composent ce tissu. Elles n'ont cependant pas aujourd'hui la taille critique nécessaire et ne sont pas portées par une demande suffisante.

- Les consolidations industrielles seront favorisées par les différents moyens de l'État, notamment par les fonds d'investissement stratégique.

Pour une meilleure efficacité, les concepteurs de produits informatiques et de systèmes d'information doivent prendre en compte les questions de sécurité dès l'origine de leurs développements. L'imprégnation du tissu industriel par des experts en sécurité des systèmes d'information doit donc être renforcée. L'orientation de jeunes vers ces métiers sera encouragée afin d'accroître le vivier national de compétences.

De manière générale, les formations scientifiques et techniques dans les domaines des technologies de l'information devront intégrer un volet relatif à la sécurité des systèmes d'information.

respect de l'équilibre entre la volonté de peser le moins possible sur la compétitivité des entreprises et la nécessité pour l'État d'être en mesure d'intervenir dans le cadre de l'intérêt supérieur de la Nation.

- S'agissant des opérateurs de communications électroniques, la transposition en droit français des directives européennes va permettre d'édicter de nouvelles règles de protection des systèmes d'information et d'obliger des autorités gouvernementales en cas d'incident.
- En ce qui concerne les autorités publiques, la mise en œuvre du « référentiel général de sécurité » (RGS) et son évolution permettront de relever significativement le niveau de protection de leurs systèmes d'information, notamment dans leurs relations avec les usagers.

6 Développer nos collaborations internationales

La sécurité des systèmes d'information repose en partie sur la qualité de l'échange d'informations entre les services compétents des divers États. La France cherchera à établir un large tissu de partenaires étrangers afin de favoriser le partage des données essentielles, comme, par exemple, les informations concernant les vulnérabilités ou les failles des produits et services.

Elle renforcera également ses échanges avec ses partenaires en matière de lutte contre la cybercriminalité.

De la même manière, les relations fortes entre alliés sont la base d'une cyberdéfense efficace. La France construit un cercle très restreint de partenaires de confiance avec lesquels des échanges opérationnels très approfondis seront menés.

7 Communiquer pour informer et convaincre

La sécurité des systèmes d'information repose tant sur la vigilance personnelle que sur l'organisation, les choix et mesures techniques portés par les entreprises et l'action des États.

Devant les conséquences potentielles d'une attaque majeure contre les systèmes d'information sur la vie du pays et de ses citoyens, la sensibilisation et la motivation des personnes et des organisations doivent être assurées.

Or, en France, l'information et le débat public sur les menaces que font peser les atteintes à la sécurité des systèmes d'information sur la défense et la sécurité nationale

Glossaire

Botnet

Un botnet, autrement dit un réseau de robots, est un réseau de machines compromises à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son maître de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise.

Remarques : certains réseaux peuvent atteindre un nombre considérable de machines (plusieurs millions). Celles-ci peuvent faire l'objet de commerce illicite ou d'actions malveillantes contre d'autres machines.

Cryptanalyse

Processus de déchiffrement de données protégées au moyen de cryptographie sans être en possession des clés de chiffrement.

Cryptographie

Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification ne passe inaperçue et/ou d'empêcher leur utilisation non autorisée (ISO 7498-2).

Cryptologie

Science englobant la cryptographie et la cryptanalyse.

Cybercriminalité

Actes contrevenant aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Cyberdéfense

Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

Cyberespace

Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

Cybersécurité

État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Faille

Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Information classifiée

L'article 413-9 du code pénal indique que « les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation ou auxquels l'accès est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale » font l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.

Nétiquette

Charte établie en 1995 par l'Internet Engineering Task Force (IETF) présentant les règles de bienséance recommandées pour les échanges ayant lieu dans le cyberespace (voir charte : http://tools.ietf.org/html/rfc1855 ou http://www.ari.ucl.ac.be/rfc/1855.fr.html pour une traduction française).

Glossaire

Opérateur d'importance vitale (OIV)

L'article R. 1332-1 du code de la défense précise que les opérateurs d'importance vitale sont désignés parmi les opérateurs publics ou privés mentionnés à l'article L. 1332-1 du même code, ou parmi les gestionnaires d'établissements mentionnés à l'article L. 1332-2.

Un opérateur d'importance vitale :
- exerce des activités mentionnées à l'article R. 1332-2 et comprises dans un secteur d'activités d'importance vitale ;
- gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population.

Produit de sécurité

Dispositif matériel ou logiciel conçu pour protéger la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que les systèmes d'information offrent ou qu'ils rendent accessibles.

Résilience

En informatique, capacité d'un système d'information à résister à une panne ou à une cyberattaque et à revenir à son état initial après l'incident.

Référentiel général de sécurité (RGS)

Ensemble des règles établies par l'ANSSI et prévues par l'ordonnance n° 2005-1516 du 8 décembre 2005 « relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives » que doivent respecter certaines fonctions contribuant à la sécurité des informations, parmi lesquelles la signature électronique, l'authentification, la confidentialité ou encore l'horodatage.

Les règles formulées dans le RGS s'imposent et sont modulées en fonction du niveau de sécurité retenu par l'autorité administrative dans le cadre de la sécurisation des services en ligne dont il est responsable. Ses conditions d'élaboration, d'approbation, de modification et de publication sont fixées par le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance citée relative à la sécurité des informations échangées par voie électronique. (voir http://www.ssi.gouv.fr/rgs).

Sécurité des systèmes d'information

Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Système d'information

Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information.

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.

En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr

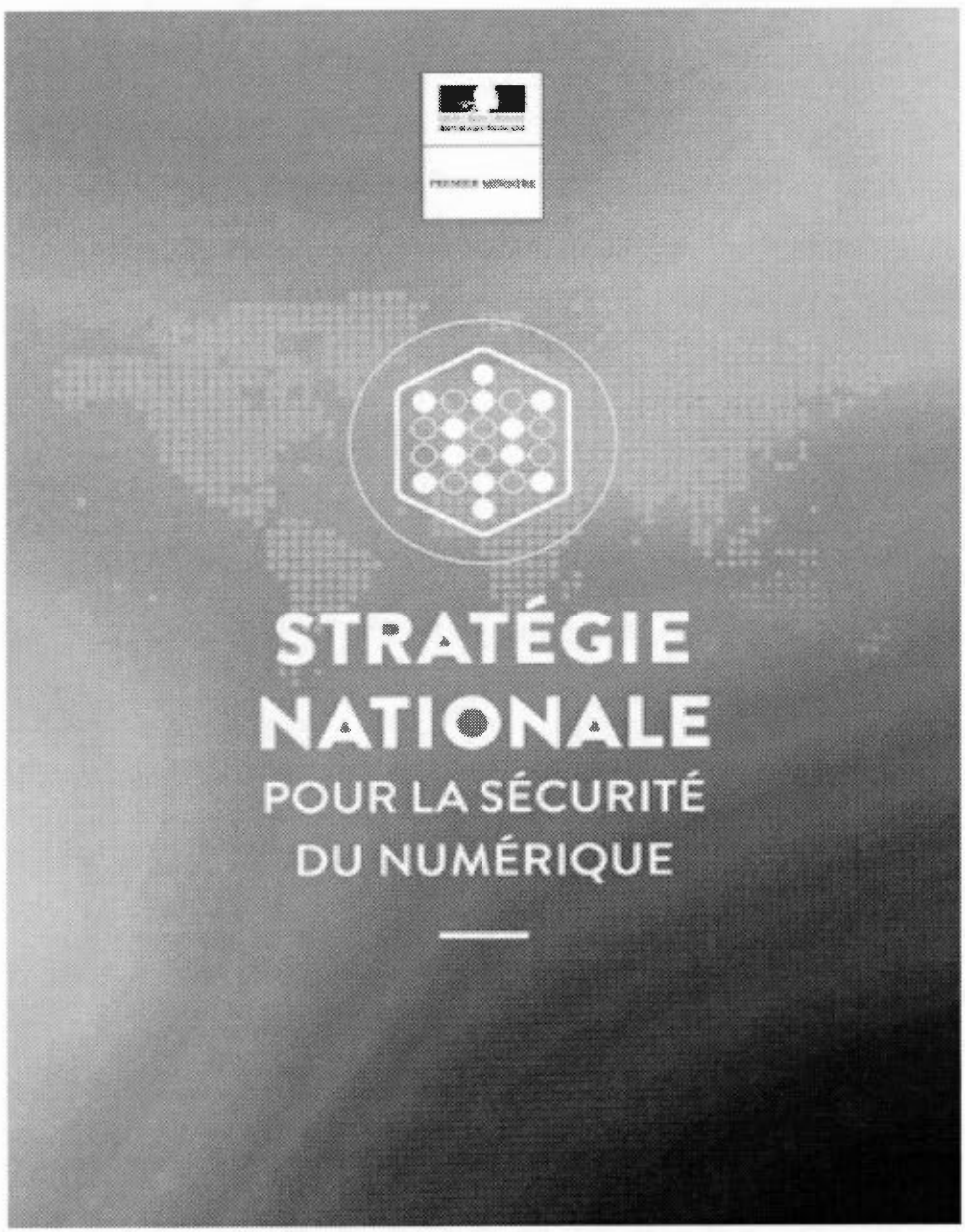
Février 2011

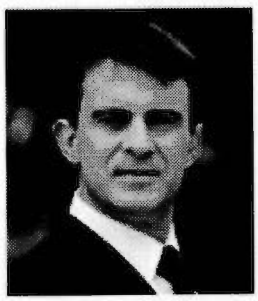
Agence nationale de la sécurité des systèmes d'information

ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
Messagerie : communication [at] ssi.gouv.fr

ANNEXE B

DEUXIEME STRATEGIE DE CYBERSECURITE FRANÇAISE (2015)





La France est pleinement engagée dans la transition numérique. Forte d'une population très largement connectée et portée par une économie numérique en croissance soutenue, la France dispose de talents et d'atouts à la pointe de l'innovation européenne et mondiale.

Le numérique est également un espace de compétition et de confrontation. Concurrence déloyale et espionnage, désinformation et propagande, terrorisme et criminalité trouvent dans le cyberespace un nouveau champ d'expression.

La « République numérique en actes », voulue par le gouvernement, doit promouvoir nos valeurs, notre économie et protéger les citoyens. Œuvrer pour la sécurité du numérique, c'est favoriser le développement d'un cyberespace gisement de croissance pérenne et lieu d'opportunités pour les entreprises françaises, c'est affirmer nos valeurs démocratiques, c'est enfin préserver la vie numérique et les données personnelles des Français.

Mon ambition dans le domaine est élevée. La stratégie nationale pour la sécurité du numérique doit s'appuyer en particulier sur la formation et sur la coopération internationale et doit être portée par l'ensemble de la communauté nationale : le gouvernement, les administrations, les collectivités territoriales, les entreprises et plus largement, tous nos compatriotes. Elle est l'affaire de tous.

Répondre aux enjeux de sécurité du monde numérique est un facteur clé de succès collectif. Je souhaite que cette stratégie nationale pour la sécurité du numérique enclenche une dynamique à la fois protectrice et libératrice d'énergies.

Manuel Valls

Manuel Valls
Premier ministre

STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE

La numérisation de la société française s'accélère : la part du numérique dans les services, les produits, les métiers ne cesse de croître. Réussir la transition numérique est devenu un enjeu national. Vecteur d'innovation et de croissance, la numérisation présente aussi des risques pour l'État, les acteurs économiques et les citoyens. Cybercriminalité, espionnage, propagande, sabotage ou exploitation excessive de données personnelles menacent la confiance et la sécurité dans le numérique et appellent une réponse collective et coordonnée selon cinq objectifs stratégiques.

 # Intérêts fondamentaux, défense et sécurité des systèmes d'information de l'État et des infrastructures critiques, crise informatique majeure.

En développant une pensée stratégique autonome, soutenue par une expertise technique de premier plan, la France se donnera les moyens de défendre ses intérêts fondamentaux dans le cyberespace de demain. Parallèlement, elle continuera à renforcer la sécurité de ses réseaux critiques et sa résilience en cas d'attaque majeure en développant des coopérations tant à l'échelle nationale avec les acteurs privés qu'internationale.

 # Confiance numérique, vie privée, données personnelles, cybermalveillance.

Afin que le cyberespace reste un espace de confiance pour les entreprises de toutes tailles et les particuliers, des mesures de protection et de réaction seront adoptées. La protection passera par une vigilance accrue des pouvoirs publics sur l'utilisation des données personnelles et par le développement d'une offre de produits de sécurité numérique adaptée au grand public. La réaction s'articulera autour d'un dispositif d'assistance aux victimes de cybermalveillance qui apportera une réponse technique et judiciaire à de tels actes.

 # Sensibilisation, formations initiales, formations continues.

La prise de conscience individuelle des risques liés à la numérisation de la société reste insuffisante. Face à ce constat, la sensibilisation des écoliers et des étudiants sera renforcée. En outre, afin de répondre aux demandes croissantes des entreprises et des administrations en matière de cybersécurité, la formation d'experts dans ce domaine sera développée.

 # Environnement des entreprises du numérique, politique industrielle, export et internationalisation.

La croissance des marchés du numérique à l'échelle mondiale, et des exigences de sécurité qu'ils porteront constituent une opportunité de différenciation pour les produits et services français ayant un niveau de sécurité numérique adapté aux usages. Par le soutien à l'investissement, à l'innovation, et à l'export, par le biais de la commande publique, l'État développera un environnement favorable aux entreprises françaises du numérique proposant une offre de produits et de services sécurisés.

 # Europe, souveraineté numérique, stabilité du cyberespace.

La régulation des rapports dans le cyberespace est devenue un sujet majeur des relations internationales. La France promouvra, avec les États membres qui le souhaitent, une feuille de route pour l'autonomie stratégique numérique de l'Europe. Elle renforcera également son influence dans les instances internationales et soutiendra les pays volontaires les moins protégés dans la mise en place de capacités de cybersécurité afin de contribuer à la stabilité globale du cyberespace.

La sécurité du numérique conforte le projet de République numérique. L'État y joue un rôle majeur en élaborant cette stratégie et en lançant une dynamique dans laquelle les professionnels du numérique, les décideurs publics et privés et les citoyens sont invités à s'investir.

*La stratégie nationale pour la sécurité du numérique a été élaborée avec l'ensemble des ministères. Elle a été soumise par le secrétaire général de la défense et de la sécurité nationale à l'approbation du Premier ministre en application du 7° de l'article R*1132-3 du code de la défense.*

SOMMAIRE

INTRODUCTION

La France accomplit sa transition numérique. Les réseaux sont omniprésents dans le fonctionnement de l'État, dans l'activité économique et la vie quotidienne des citoyens.

Porteur de nouveaux usages, de nouveaux produits et de nouveaux services, le numérique est facteur d'innovation. Il engendre une mutation de la plupart des métiers. Il transforme des secteurs d'activités et des entreprises pour leur apporter plus de souplesse et de compétitivité. Enrichis par l'apport du numérique, ces secteurs sont simultanément plus exposés aux menaces issues du numérique.

Se priver du numérique ou ne pas pouvoir y accéder conduit à une forme d'exclusion économique et sociale. De même, un État qui ne disposerait pas de l'autonomie nécessaire dans le secteur du numérique verrait sa souveraineté menacée.

Pour que le numérique demeure un espace de liberté, d'échanges et de croissance, il est nécessaire que la confiance et la sécurité y soient établies et défendues. Seul un effort collectif et coordonné peut permettre d'atteindre cet objectif.

* *
*

Une première stratégie de cybersécurité de la France a été élaborée début 2010 et publiée début 2011, peu après la découverte d'une attaque informatique à des fins d'espionnage contre les entreprises économiques et financiers. Présents depuis plusieurs mois, les attaquants avaient pris le contrôle du cœur d'un des réseaux des ministères et collectaient régulièrement des informations de nature politique, économique et financière.

Ce type d'attaque informatique vise de nombreuses entreprises françaises, de toutes tailles, dans tous les secteurs d'activité. Les entreprises sont également la cible d'escroqueries de toutes sortes comme, par exemple, l'infection par un logiciel malveillant qui rend les fichiers de l'entreprise inutilisables jusqu'au paiement d'une rançon effectuée par des moyens difficilement traçables.

Parallèlement, les intrusions informatiques destinées à dérober des informations personnelles (identité, données d'identification à des sites marchands, données bancaires) se multiplient. Il s'agit le plus souvent pour des criminels de commettre des délits identiques à ceux connus dans le monde matériel — vols, escroqueries, chantage —, mais de manière industrialisée, une part du risque d'être identifié et poursuivi en moins. Le crime organisé s'est saisi de l'avantage procuré par les réseaux de communications électroniques. Ses capacités techniques sont croissantes au point d'être désormais en mesure de pratiquer, pour lui-même ou en sous-traitance par hybridation, des actes de sabotage ou de prise en otage d'outils de production.

Des campagnes de harcèlement se développent sur les réseaux sociaux, comme des cas d'escroqueries aux sentiments destinés à amener les victimes crédules à transférer de l'argent vers l'étranger.

Les nombreuses défigurations de sites Internet, notamment ceux de collectivités territoriales, ayant suivi les attentats de janvier 2015 ou, quelques semaines plus tard, l'attaque informatique contre un média français

à vocation internationale, ont montré la volonté et la capacité de groupes organisés de rendre indisponibles des ressources informatiques qui soutiennent notre vie quotidienne.

Ce qu'il est convenu d'appeler « l'état de la menace » établi en 2010 s'est ainsi révélé juste. La menace est aujourd'hui accentuée par l'accroissement des capacités des attaquants, la prolifération des techniques d'attaques et le développement dans le cyberespace de la criminalité organisée.

Mais un défi d'une autre nature est apparu. Celui de la captation de richesses numériques par un oligopole d'entreprises utilisant leur position dominante pour gêner l'arrivée de nouveaux entrants et capter la valeur ajoutée de cette économie naissante qui exploitera les données pour inventer de nouveaux services, améliorer notre vie quotidienne ou rendre plus accessibles les services publics. Parmi ces données figurent au premier plan nos données personnelles, y compris celles relatives à notre vie privée. La maîtrise de ces masses de données ouvre la porte à la déstabilisation économique et à des formes sophistiquées de propagande ou d'orientation des convictions ou des habitudes. En ce sens, ce défi relève, par son ampleur nationale et ses enjeux stratégiques, de la défense et de la sécurité nationale.

* *
*

Face à ces risques malheureusement avérés, beaucoup a déjà été accompli.

Comme l'annonçait le livre blanc sur la défense et la sécurité nationale de 2008, une agence nationale a été créée dès 2009 pour traiter les attaques informatiques et protéger les systèmes d'information de l'État et des infrastructures critiques.

Une politique industrielle en faveur de l'industrie nationale de cybersécurité est notamment portée par le programme des investissements d'avenir et dans le cadre du plan « Industrie du futur ».

Le Parlement a voté en 2013 les mesures proposées par le gouvernement qui visent à renforcer la sécurité informatique des opérateurs d'importance vitale et de ceux qui participent à leurs systèmes d'information les plus critiques.

Les positions de la France sont soutenues dans toutes les instances internationales, et notamment à l'Organisation des Nations Unies (ONU) qui a reconnu en 2013 l'application au cyberespace du droit international. Des relations bilatérales opérationnelles avec plusieurs pays ont par ailleurs été engagées par les services de l'État.

Les ministères ont pris conscience de l'impact politique et technique des technologies de l'information sur leurs missions et l'activité de leur administration et se dotent de coordonnateurs en charge des questions liées au numérique et à sa sécurité. Une politique de sécurité des systèmes d'information de l'État a été élaborée et est progressivement mise en œuvre.

Les années qui viennent doivent permettre de recueillir les bénéfices des actions engagées et d'élargir le périmètre de l'action publique et des acteurs impliqués. Le constat doit maintenant être établi et partagé que la défense et la sécurité du numérique relèvent de la communauté nationale et pas seulement de l'action de l'État.

* *
*

Jusqu'à ces dernières années, notre défense et notre sécurité nationale reposaient sur l'expertise, le comportement et les décisions des hommes et femmes ayant accès aux installations et équipements les plus sophistiqués, les plus protégés, les plus secrets. Alors qu'émerge une société massivement connectée, cette responsabilité est désormais en partie partagée par l'ensemble des Français. Un objet connecté ou un service insuffisamment sécurisé par ses développeurs, la négligence d'un décideur en matière de sécurité des systèmes d'information, le comportement dangereux d'un prestataire ou celui d'un salarié mélangeant sans précaution vie privée et vie professionnelle peuvent entraîner pertes de disponibilité, de confidentialité ou d'intégrité d'informations essentielles, ruptures d'activité et pertes écono-

majeurs, accidents industriels et pertes de vies humaines ou catastrophes écologiques et troubles à l'ordre public, susceptibles d'affecter la vie de la nation.

Jamais, en effet, la stabilité de notre avenir, porté par le numérique, n'a été aussi dépendante des responsabilités de chacun et de celles, collectives, de trois communautés d'acteurs.

Une première communauté a la responsabilité de proposer et de mettre en œuvre des technologies, des produits et des services dotés du niveau de sécurité adapté aux usages et capables de parer les risques identifiés. Les principaux acteurs de cette communauté sont les chercheurs, les inventeurs de produits et services et leurs intégrateurs, les entreprises du secteur de la cybersécurité, les opérateurs de réseaux de communications électroniques, les fournisseurs d'accès à internet ou les fournisseurs de services informatiques distants.

La deuxième communauté a pour responsabilité de protéger la nation des prédateurs du numérique. Outre la mise en œuvre des politiques de cybersécurité, il s'agit notamment de conduire de façon volontariste une politique de développement des compétences techniques nécessaires et de mettre en place un écosystème de confiance qui accompagne la transformation numérique de la société, en défendant les citoyens, nos valeurs et nos intérêts dans le cyberespace. Cette responsabilité engage celui qui la porte à exprimer sa position en faveur de solutions de sécurité qualifiées et à promouvoir l'industrie nationale, y compris à l'export. Cette communauté est constituée des élus, du gouvernement, des administrations centrales et territoriales et des syndicats.

La troisième communauté a pour responsabilité d'utiliser de manière réfléchie les services et technologies disponibles, d'effectuer des choix raisonnés et d'éviter les comportements à risque dans les actes de la vie numérique. Cette communauté est constituée de tous les usagers, responsables d'entreprises, acteurs de la société civile et citoyens.

Ce sont ces engagements synallagmatiques pris par chacun des acteurs qui permettront à la France de bénéficier pleinement des apports du numérique, de transformer en avantage concurrentiel national les choix liés à la sécurité du numérique, souvent vécus aujourd'hui exclusivement comme une contrainte économique et comportementale, et de promouvoir nos valeurs, nos produits et nos services.

L'État a pour rôle dans le cyberespace de garantir la liberté d'expression et d'action de la France et d'assurer la sécurité de ses infrastructures critiques en cas d'attaque informatique majeure (objectif 1), de protéger la vie numérique des citoyens et des entreprises, de lutter contre la cybercriminalité (objectif 2), d'assurer la sensibilisation et la formation nécessaires à la sécurité du numérique (objectif 3), de favoriser le développement d'un écosystème favorable à la confiance dans le numérique (objectif 4) et de promouvoir la coopération entre États-membres de l'Union dans un sens favorable à l'émergence d'une autonomie stratégique numérique européenne, garante sur le long terme d'un cyberespace plus sûr et respectueux de nos valeurs (objectif 5).

CINQ
OBJECTIFS
STRATÉGIQUES

1

#INTÉRÊTS FONDAMENTAUX, DÉFENSE ET SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ÉTAT ET DES INFRASTRUCTURES CRITIQUES, CRISE INFORMATIQUE MAJEURE

ENJEUX

La France est la cible d'attaques informatiques qui portent atteinte à ses intérêts fondamentaux.

Aujourd'hui, lorsqu'un attaquant cible l'État, les opérateurs d'importance vitale ou des entreprises stratégiques, il cherche à s'installer durablement dans le système d'information visé pour y voler des données confidentielles (politiques, diplomatiques, militaires, technologiques, économiques, financières ou commerciales). Demain, un attaquant pourrait prendre le contrôle d'objets connectés, interrompre à distance une activité industrielle ou détruire sa cible. Depuis 2011, une centaine d'attaques informatiques d'importance ont été traitées, le plus souvent en toute confidentialité, par les administrations et les prestataires de service compétents.

Parallèlement, des attaques informatiques destinées à frapper l'opinion publique accompagnent les prises de position de la France sur la scène internationale, ses opérations militaires ou certains débats publics. À titre d'exemple, les défigurations de sites internet qui ont suivi les attentats ayant visé la France début 2015 ont eu un impact technique faible, mais une portée symbolique soubaitée par les attaquants. Dans le même ordre d'idée, l'attaque informatique ayant entraîné l'interruption de service d'un média français à vocation internationale visait également à frapper les esprits et favorise la radicalisation conduisant à des actes terroristes. Cette attaque a également montré la capacité d'attaquants déterminés à perturber le fonctionnement d'une infrastructure à forte valeur symbolique.

Depuis plusieurs années, plusieurs États ont mis en œuvre leur volonté politique et des moyens humains, techniques et financiers considérables afin de nuire, à notre encontre, des opérations informatiques à grande échelle dans le cyberespace.

Qu'elles soient connues par des documents publiquement révélés ou mis en évidence lors du traitement d'attaques informatiques, les excès de telles pratiques entament la crédibilité de certains de ces États sur la scène internationale et ruinent la confiance qu'il serait naturel d'attribuer aux produits et services numériques de leurs entreprises.

« Les excès de telles pratiques entament la crédibilité de certains de ces États sur la scène internationale et ruinent la confiance qu'il serait naturel d'attribuer aux produits et services numériques de leurs entreprises. »

Ainsi, le risque cybernétique, placé en troisième position des menaces majeures pour la France par le Livre blanc sur la défense et la sécurité nationale de 2013, est aujourd'hui renforcé et constitue un défi majeur posé à la France.

OBJECTIF

La France se donnera les moyens de défendre ses intérêts fondamentaux dans le cyberespace. Elle consolidera la sécurité numérique de ses infrastructures critiques et œuvrera pour celle de ses opérateurs essentiels à l'économie.

ORIENTATIONS

> **Détenir les capacités scientifiques, techniques et industrielles nécessaires à la protection de l'information de souveraineté, à la cybersécurité et au développement d'une économie numérique de confiance.**

Un groupe d'experts pour la confiance numérique sera créé, sous l'égide du secrétariat d'État au numérique et de l'autorité nationale de sécurité des systèmes d'information.

Le groupe d'experts pour la confiance numérique réunira très régulièrement les administrations compétentes du premier ministre, des ministères de l'Éducation nationale, de l'Enseignement supérieur et de

la Recherche, de la Justice, de la Défense, des Affaires sociales, de la Santé et des droits des femmes, de l'Intérieur, de l'Économie, de l'Industrie et du numérique, le commissariat général à l'investissement, l'agence nationale de la recherche et les organismes de recherche concernés. Le groupe pourra associer à ses travaux des acteurs du secteur privé et des personnalités qualifiées.

La mission de ce groupe sera notamment d'identifier les technologies-clés dont la maîtrise est nécessaire pour les métiers de la cybersécurité et plus largement pour le développement d'un environnement numérique de confiance. Il évaluera les besoins en formations initiales et continues, suivra les travaux de recherche et en accompagnera la valorisation, participera à l'amélioration de l'accompagnement des jeunes docteurs. Il contribuera, dans le domaine des technologies numériques, à la définition des axes stratégiques des dispositifs de financement et d'accompagnement des travaux de recherche et de développement industriel. Ces travaux seront réalisés en cohérence avec ceux des structures déjà en place tel que le comité de filière des industries de sécurité (CoFIS).

Plus largement, les choix d'acteurs privés majeurs en matière de modèle économique, de technologie, parfois hors de tout cadre de normalisation, ou plus simplement certaines innovations dans les usages du numérique peuvent consolider la confiance ou susciter la défiance. Le groupe d'experts pour la confiance numérique organisera la veille technologique et économique permettant d'anticiper les évolutions des questions liées au numérique. Le cas échéant, des mesures adaptées seront proposées pour accompagner ou cadrer ces évolutions. Ces mesures pourront, par exemple, concerner la protection du potentiel scientifique et technique de la Nation ou le contrôle des investissements étrangers dans des entreprises nationales critiques.

Une commission du groupe d'experts réunira les coordinateurs ministériels des questions liées au cyberespace autour du secrétaire général de la défense et de la sécurité nationale pour les sujets relevant de sa compétence.

Ce groupe d'experts rendra compte annuellement de ses activités au Premier ministre.

> **Assurer au profit de l'État, des entreprises et des citoyens une veille active en matière de sécurité des technologies et des usages.**

Dans la perspective d'évolutions technologiques majeures, comme les télécommunications mobiles de 5e génération (5G) ou les « réseaux définis par le logiciel », la France restera vigilante sur la nature et les capacités des équipements matériels et logiciels installés au cœur de ses réseaux de communications électroniques, pour protéger le secret des correspondances, la vie privée de ses citoyens et la résilience de ces infrastructures, et poursuivra l'adaptation de son cadre réglementaire aux nouvelles technologies émergentes.

L'autorité nationale de sécurité des systèmes d'information informera régulièrement les ministères, les entreprises, les collectivités territoriales et les citoyens, par des moyens adaptés au public visé, des éléments susceptibles de présenter un danger dans leur utilisation du numérique. Le cas échéant, ces informations auront au préalable été consolidées avec les administrations compétentes.

> **Accélérer le renforcement de la sécurité des systèmes d'information de l'État.**

Depuis 2010, plusieurs actions destinées à élever le niveau de sécurité des systèmes d'information de l'État ont été conduites. Une politique de sécurité des systèmes d'information de l'État (PSSIE) a été élaborée, un réseau interministériel de communications électroniques est en cours, le déploiement de terminaux mobiles sécurisés a été initié. Ces actions, comme celles destinées à produire les équipements de sécurité destinés à protéger l'information de souveraineté, mobilisent des ressources humaines et budgétaires. Elles seront poursuivies afin d'offrir au gouvernement et à nos capacités militaires le niveau de sécurité adapté à une préservation à long terme de l'autonomie de décision et d'action de la France.

L'application de la politique de sécurité des systèmes d'information de l'État et l'efficacité des mesures adoptées seront évaluées annuellement. Un bilan annuel confidentiel sera transmis au Premier ministre et le Parlement sera informé au moyen d'indicateurs.

Dans le même objectif d'informer le Parlement, les projets de loi comporteront dans leur étude d'impact dès 2016 un volet consacré au numérique et, au sein de ce volet, à la cybersécurité, établi sous l'égide des hauts fonctionnaires chargés de la qualité de la réglementation. Plus largement, les hauts fonctionnaires chargés de la qualité de la réglementation veilleront à prendre en compte les questions liées au renforcement de la sécurité des systèmes d'information de l'État dans le cadre du pilotage de l'activité normative.

> Préparer la France et les organisations multilatérales dont elle est membre à faire face à une crise informatique majeure.

Annoncé par le Livre blanc sur la défense et la sécurité nationale de 2013, le renforcement de la sécurité des systèmes d'information les plus sensibles des opérateurs d'importance vitale a fait l'objet de mesures législatives (articles 21 et 22 de la loi n° 2013-1168 du 18 décembre 2013). Les travaux engagés avec ces opérateurs se poursuivront durablement, notamment par la mise à jour régulière des textes réglementaires. Ces travaux seront progressivement étendus, comme le précise la loi, aux opérateurs publics ou privés qui participent à ces systèmes d'information sensibles.

Ce choix fait par la France aura permis de participer activement à l'élaboration des orientations de la proposition de directive européenne concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union et d'anticiper sa transposition. Le moment venu, la France définira ses opérateurs essentiels à l'économie conformément aux orientations de la directive et participera aux initiatives européennes destinées à renforcer leur sécurité numérique.

Les exercices de gestion de crise cybernétique menés au niveau national concerneront progressivement l'ensemble du territoire et des secteurs d'activité d'importance vitale. Le ministère de la Défense, en lien avec l'autorité nationale de sécurité des systèmes d'information, poursuivra la mise en place d'une réserve de cyberdéfense à vocation opérationnelle destinée à faire face à une crise informatique majeure.

En parallèle, la France continuera de concourir à l'émergence d'un cadre de coopération volontaire de gestion de crises cybernétiques à l'échelle européenne, en soutenant en particulier les travaux de l'agence européenne ENISA.

Il appartient au CERT-EU (capacité de réponse aux incidents informatiques des institutions, entités et agences de l'Union européenne - UE) et au NCIRC (capacité de réponse aux incidents informatiques de l'Organisation du Traité de l'Atlantique Nord - OTAN) d'assurer la cyberdéfense de leurs institutions respectives. Active lors des exercices de gestion de crises cybernétiques organisés par ces organisations et fortement représentée dans les instances qui orientent les choix de l'UE et de l'OTAN en matière de technologies numériques sécurisées, la France continuera à apporter son concours à ces institutions et à leurs membres dans le respect des compétences de chacun.

La France contribuera également à renforcer la cybersécurité d'autres organisations internationales dont elle est membre, au niveau politique et au niveau technique, notamment celles hébergées sur le territoire national qui bénéficient de l'écosystème technique national.

> Développer une pensée autonome et conforme à nos valeurs.

Les choix stratégiques effectués par la France au lendemain de la Deuxième Guerre mondiale ont entraîné l'émergence d'une pensée stratégique autonome et l'élaboration d'une doctrine qui a donné à la France une place singulière sur la scène internationale et irrigue aujourd'hui encore sa diplomatie et les concepts d'emploi de ses forces armées.

Si le numérique modifie en profondeur nos sociétés, il reste à mesurer son impact sur d'autres réalités comme celles de souveraineté, de territoire national, de monnaie ou d'intérêts fondamentaux de la Nation et à repenser l'organisation et les moyens de l'action publique pour y faire appliquer la loi ou pour assurer leur protection. Une réflexion sera conduite sous la coordination du secrétaire général de la défense et de la sécurité nationale, pour élaborer un corpus intellectuel relatif au cyberespace.

2

CONFIANCE NUMÉRIQUE, VIE PRIVÉE, DONNÉES PERSONNELLES, CYBERMALVEILLANCE

ENJEUX

S'ils ont de manière générale confiance dans le numérique, les Français ont, en revanche, une certaine défiance quant à son impact sur leur vie quotidienne, notamment personnelle. Généralement soucieux de l'utilisation et de la conservation de leurs données personnelles, ils les confient toutefois à des plates-formes dont les conditions d'utilisation sont léonines au détriment des utilisateurs.

Le mode opératoire constaté lors de certaines attaques informatiques contre des entreprises ou des administrations montre également une réelle difficulté à dissocier vie privée et vie professionnelle dans l'utilisation des équipements comme des services.

Les attaques informatiques qui touchent les particuliers ont généralement pour objectif le gain financier. Par la prise de contrôle de l'équipement personnel utilisé — ordinateurs, tablette, ordiphone —, l'usurpation d'identité et le vol d'identifiants à des comptes bancaires ou à des sites commerciaux, par l'engagement d'une relation affective virtuelle débouchant sur une demande de transfert d'argent, par le chiffrement de données à l'insu de l'utilisateur conduisant au paiement d'une rançon, le racket est aujourd'hui pratiqué à grande échelle par une criminalité qui s'est organisée et a gagné en efficacité.

Bien qu'il ne fasse appel à aucune technique d'attaque particulière, le harcèlement, facilité et amplifié par les réseaux de communications électroniques est une agression informatique contre les personnes dont l'issue est parfois dramatique.

Si l'agence nationale de la sécurité des systèmes d'information (ANSSI) est l'interlocuteur étatique identifié en cas d'incident informatique grave affectant les administrations et les opérateurs d'importance vitale, la lisibilité de l'offre publique est nettement moindre en matière d'assistance aux victimes d'actes de cybermalveillance pour les autres acteurs, qu'il s'agisse d'entreprises de taille intermédiaire, de petites et moyennes entreprises, de professions libérales, de collectivités territoriales ou de particuliers.

Les victimes d'actes de cybermalveillance sont encouragées à déposer une plainte, auprès des services de police et de gendarmerie qui se sont adaptés au traitement de tels contentieux. Toutefois, la réponse qui leur est apportée dans ce cadre est centrée sur l'identification des auteurs présumés de la cybermalveillance et sur l'engagement éventuel de poursuites contre ces auteurs. Les victimes doivent pouvoir être orientées vers un service d'assistance au traitement de l'incident informatique à l'origine de l'acte de cybermalveillance.

Plus insidieusement, les plates-formes numériques et notamment les réseaux sociaux peuvent façonner l'opinion et parfois être vecteurs de valeurs qui ne sont pas celles de la République. Dans certains cas, ils peuvent être instrumentalisés à des fins de désinformation et de propagande envers les citoyens français, notamment les plus jeunes. Les opinions diffusées vont alors à l'encontre des intérêts fondamentaux de la France et relèvent d'une atteinte à la défense ou à la sécurité nationale sanctionnée par la loi.

Dans un registre différent, les développements récents et simultanés de nouveaux usages et de nouvelles techniques de stockage et de traitement des données favorisent l'émergence de risques de déséquilibre économique et d'atteinte à la sécurité individuelle des personnes ainsi qu'à celle des nations. Le souhait de voir instaurer, par exemple au travers de traités commerciaux, la libre circulation des données, dont les données personnelles collectées par

« Les plates-formes numériques et notamment les réseaux sociaux peuvent façonner l'opinion et parfois être vecteurs de valeurs qui ne sont pas celles de la République »

« Le développement numérique ne peut être durable dans un cyberespace où les États ne respectent pas les bonnes pratiques nécessaires à une transition numérique équilibrée et profitable à toutes les nations »

des objets connectés, risque difficilement la volonté de captation de ces données par des oligopoles dont les valeurs et les pratiques ne correspondent ni à la conception de la vie privée française ou européenne ni à son encadrement juridique. La captation massive et illicite de certains types de données personnelles, comme par exemple les données de santé, peut en effet entraîner des atteintes à la sécurité individuelle et collective, ou plus simplement une exploitation commerciale abusive (revente à des compagnies d'assurance, par exemple).

Le développement numérique ne peut être durable dans un cyberespace où les États ne respectent pas les bonnes pratiques nécessaires à une transition numérique équilibrée et profitable à toutes les nations et où quelques acteurs économiques s'accaparent la richesse que constituent les données numériques, notamment les données personnelles, véritables ressources des générations futures.

■ OBJECTIF

La France développera un usage du cyberespace conforme à ses valeurs et y protégera la vie numérique de ses citoyens. Elle accroîtra sa lutte contre la cybercriminalité et l'assistance aux victimes d'actes de cybermalveillance.

■ ORIENTATIONS

> **Promouvoir et défendre nos valeurs sur les réseaux de communications électroniques et dans les instances internationales.**

Les droits des personnes s'appliquent de la même manière « en ligne » et « hors ligne ». Le cyberespace doit ainsi rester un lieu de libre expression pour tous les citoyens, où les abus ne peuvent être prévenus que dans la mesure des limites fixées par la loi et en conformité avec nos engagements internationaux. La France promeut cette approche destinée à préserver un cyberespace libre et ouvert dans les instances internationales.

Il appartient à l'État d'informer les citoyens sur les risques de manipulation et les techniques de propagande utilisées par des acteurs malveillants sur Internet. Après les attentats perpétrés contre la France en janvier 2015, le gouvernement a mis en place une plateforme d'information sur les risques liés à la radicalisation islamiste via les réseaux de communication électroniques. « Stop-djihadisme.gouv.fr ». Cette approche pourrait être étendue pour répondre à d'autres phénomènes de propagande ou de désinformation. Il appartiens aux services compétents en matière de défense et de sécurité de détecter ces phénomènes et de proposer au gouvernement la mise en œuvre de ces moyens.

> **Apporter une assistance de proximité aux victimes d'actes de cybermalveillance.**

Copiloté par le ministère de l'Intérieur et l'agence nationale de sécurité des systèmes d'information, avec l'appui des ministères de la Justice, des Finances et des comptes publics, de la Défense, de l'Économie, de l'Industrie et du numérique, un dispositif national sera mis en place dès 2016 destinés à porter assistance aux victimes d'acte de cybermalveillance.

Ce dispositif aura également une mission de sensibilisation aux enjeux de protection de la vie privée numérique et de prévention qui s'appuiera localement sur l'action des préfets et des services de l'État. Le réseau territorial de l'ANSSI, les délégués régionaux à l'intelligence économique et les services du ministère de l'Intérieur compétents en matière de sécurité économique, le réseau « transition numérique », celui de la Banque de France — qui pourrait à terme intégrer dans sa cotation des entreprises un critère lié à la prise en compte du risque cybernétique —, participeront à cette

mission. Les chambres de commerce et d'industrie, les chambres des métiers et plus largement tous les réseaux professionnels seront également sollicités.

Le dispositif adoptera une forme juridique et une organisation lui permettant de bénéficier de l'apport des acteurs économiques du secteur de la cybersécurité — éditeurs de logiciels, plates-formes numériques, fournisseurs de solutions. Grâce aux technologies mises en œuvre, le dispositif devra proposer aux victimes des solutions techniques s'appuyant sur des acteurs de proximité et facilites les démarches administratives, notamment afin de favoriser le dépôt de plainte.

> Mesurer la cybercriminalité.

Les travaux interministériels menés à l'initiative du ministère de l'intérieur depuis 2013 ont conduit au constat qu'il n'existe pas *aujourd'hui* de statistiques fiables relatives spécifiquement à la délinquance ou à la criminalité informatique, la plupart des infractions concernées étant enregistrées sous une appellation qui ne rend pas compte de cette dimension, aujourd'hui absente des référentiels utilisés.

L'absence de telles statistiques est préjudiciable à la conception par les pouvoirs publics de politiques constamment réévaluées et à la mise en place des moyens adaptés. C'est pourquoi le ministère de l'intérieur mettra en œuvre de nouveaux instruments de suivi de l'évolution de la cybercriminalité afin d'éclairer l'action publique. L'Observatoire national de la délinquance et des réponses pénales y contribuera également en consacrant un volet de ses travaux à l'examen statistique de la cybercriminalité. Ce volet intégrera les données transmises par l'autorité nationale de sécurité des systèmes d'information et le dispositif d'assistance aux victimes d'actes de cybermalveillance, qui auront participé à son élaboration.

> Protéger la vie numérique, la vie privée et les données personnelles des Français.

À la faveur du règlement européen en matière d'identité électronique (eIDAS), la France se dotera d'une feuille de route claire en matière d'identité numérique délivrée par l'État. Cette feuille de route sera élaborée avant la fin de l'année 2015 sous l'égide du mi-

nistère de l'intérieur et des secrétariats d'État chargés du numérique et de la réforme de l'État, appuyés par les services du Premier ministre, et devra comprendre un volet qui définira un cadre de référence pour l'utilisation au profit des collectivités territoriales de l'identité numérique délivrée par l'État.

Cette feuille de route prendra en compte la stratégie numérique du Gouvernement qui prévoit le déploiement de dispositifs de fédération d'identité permettant d'utiliser une même identité numérique pour s'authentifier sur différents services. Grâce à ces dispositifs, les identités numériques peuvent avoir été fournies par des entités différentes tant que le tiers chargé de la gestion de la fédération d'identité est capable de déterminer le niveau de confiance associé à l'identité.

Sous réserve de respecter des exigences de sécurité adaptées aux usages et aux menaces, ces dispositifs sont de nature à renforcer la confiance des utilisateurs dans leur vie numérique, à en favoriser la fluidité tout en limitant le risque d'une exploitation non désirée de leurs données personnelles. Pour les usages les plus sensibles, tels que ceux concernant la vie démocratique ou les échanges internationaux relatifs à la justice, des niveaux de confiance élevés dans les dispositifs et services seront systématiquement employés. Ces niveaux élevés de confiance s'appuieront sur le tissu industriel national et le schéma de certification de sécurité en place.

La France protégera la vie privée et les données personnelles de ses ressortissants. Les droits à la vie privée et à la maîtrise individuelle et collective des données personnelles seront réaffirmés chaque fois que nécessaire et notamment à l'occasion des négociations commerciales entre États, qu'elles soient bilatérales ou multilatérales.

Pour informer les Français sur l'utilisation faite des données confiées aux services numériques, une signalétique adaptée et partagée avec les États volontaires et en cohérence avec les travaux européens effectués dans le cadre du règlement européen relatif à la protection des données à caractère personnel sera mise en place courant 2016. Cette signalétique permettra de visualiser les caractéristiques essentielles des conditions d'utilisation des plates-formes et services numériques ou des moyens de paiement utilisés.

> **Proposer des solutions techniques destinées à sécuriser la vie numérique, accessibles à toutes les entreprises et au grand public.**

Les services de l'État labelliseront des solutions de sécurisation des terminaux personnels. Une signalétique cohérente avec celle proposée ci-dessus permettra aux utilisateurs d'être informés d'éventuelles transmissions d'informations à un tiers dans le cadre de cette protection. Une fois créé, le dispositif d'assistance aux victimes d'actes de cybermalveillance évoqué ci-dessus fera, au titre de sa mission de prévention, la promotion de ces dispositifs auprès des publics concernés.

Par ailleurs, et comme cela a pu être engagé par le programme des investissements d'avenir, l'offre de solutions accessibles et adaptées destinées à sécuriser la vie numérique des petites et moyennes entreprises sera soutenue.

Un soutien au développement de solutions françaises sera apporté ainsi qu'aux communautés du logiciel libre développant des solutions de sécurité.

> **Renforcer les mécanismes opérationnels d'entraide judiciaire internationale et universaliser les principes de la Convention de Budapest sur la lutte contre la cybercriminalité.**

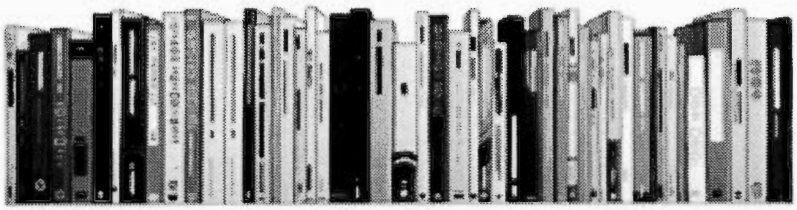
Adoptée en 2001 dans le cadre du Conseil de l'Europe, la Convention de Budapest est devenue un instrument de référence qui permet la coopération dans la lutte contre la cybercriminalité entre États des cinq continents. Ratifié par 46 États, dont 7 non membres du Conseil de l'Europe, cet instrument rassemble d'ores et déjà 125 États à un titre ou à un autre (signataires, États invités à adhérer, États recevant de l'assistance technique en vue d'une future adhésion, États ayant adopté leur loi interne sur le modèle de la Convention).

Il est aujourd'hui essentiel d'universaliser et de consolider aussi bien le socle de normes que l'outil de coopération que constitue ce texte.

Par ailleurs, la France fera la promotion au sein de l'Union européenne de la définition d'un dispositif de coopération judiciaire simplifié entre États membres afin d'accélérer la transmission des données et de mettre un terme aux activités illégales.

3

SENSIBILISATION, FORMATIONS INITIALES, FORMATIONS CONTINUES



ENJEUX

La France est en retard par rapport à ses partenaires en matière de sensibilisation de sa population aux risques associés aux usages du numérique et de formation à la cybersécurité.

Les Français négligent en général les bonnes pratiques lors de l'utilisation des réseaux de communications électroniques.

Dans l'usage privé des réseaux de communications électroniques, les enfants et adolescents, confrontés à des contenus inadaptés, exposés au harcèlement ou à la prédation, sont les premières victimes. Afin de rompre le silence et de permettre les poursuites, les plus jeunes devraient être initiés à la conduite à tenir lorsqu'ils sont victimes de malveillance numérique.

La sensibilisation de tous est un préalable nécessaire pour que les élus, les dirigeants d'administrations ou d'entreprises puissent prendre en compte le « risque cyber » à son juste niveau et décider des mesures susceptibles de protéger les citoyens qu'ils représentent ou les organismes qu'ils dirigent, face à des menaces de vol d'informations ou de propriété intellectuelle, d'atteinte aux données personnelles, voire l'exposition à des ruptures d'activité, d'accidents de production, avec des impacts technologiques ou environnementaux auxquels ils sont potentiellement exposés.

Outre la sensibilisation des plus jeunes, la formation aux métiers du numérique doit permettre aux futurs professionnels du domaine de bénéficier d'un enseignement poussé en sécurité des systèmes d'information, aujourd'hui encore absent de nombreuses formations supérieures.

Par ailleurs, le contenu et le nombre de formations initiales et supérieures aux métiers de la cybersécurité ne permettent pas de satisfaire la demande des entreprises et des administrations.

OBJECTIF

La France sensibilisera dès l'école à la sécurité du numérique et aux comportements responsables dans le cyberespace. Les formations initiales supérieures et continues intégreront un volet consacré à la sécurité du numérique adapté à la filière considérée.

ORIENTATIONS

> Sensibiliser l'ensemble des Français.

Un programme ambitieux de sensibilisation de l'ensemble des Français doit être engagé.

Sous la conduite du ministre de l'Éducation nationale, de l'enseignement supérieur et de la recherche et du secrétariat d'État au numérique, avec l'appui du service d'information du Gouvernement et de l'agence nationale de la sécurité des systèmes d'information, un appel à manifestation d'intérêt pour la réalisation de contenus de sensibilisation à destination du grand public sera lancé.

Le ministère de l'intérieur poursuivra l'opération « Permis Internet » initiée en 2014 par la gendarmerie nationale en partenariat avec une fondation privée, et relayée depuis le début de l'année 2015 par la Police nationale. Cette opération permet de sensibiliser aux risques et de conseiller plus de 300 000 élèves de CM2 chaque année pour les protéger dans leur navigation sur Internet.

La visibilité du portail « une éducation numérique

pour tous » de la Commission nationale informatique et libertés (CNIL) sera renforcée.

Les associations seront invitées à élaborer des projets de campagnes de communication visant à renforcer la confiance dans le numérique susceptibles de rentrer dans le cadre d'une « grande cause nationale ».

> Intégrer la sensibilisation à la cybersécurité dans toute formation supérieure et dans les formations continues.

Le ministère de l'Éducation nationale, de l'enseignement supérieur et de la recherche, avec l'aide de la Conférence des présidents d'université, de la conférence des grandes écoles et des administrations compétentes, incitera à ce que, dès la rentrée 2016, des sensibilisations à la cybersécurité correspondant à la filière de formation soient mises en place dans toute formation initiale supérieure.

Le ministère du travail, de l'emploi, de la formation professionnelle et du dialogue social, appuyé par les administrations de l'État compétentes en matière de cybersécurité, engagera les consultations nécessaires afin que, dès 2016, les organismes dispensateurs de formation continues intègrent dans les différents cursus une sensibilisation aux questions de cybersécurité adaptée à la formation.

Enfin, sous la coordination du secrétariat d'État chargé du numérique, avec les ministères concernés et l'appui de l'ANSSI, la sensibilisation de catégories professionnelles pour lesquelles une imprégnation des questions de cybersécurité est particulièrement nécessaire au regard de leurs responsabilités sociétales sera engagée. Ces catégories seront précisées par le comité stratégique pour la confiance numérique.

> Intégrer la formation à la cybersécurité dans toute formation supérieure intégrant une part d'informatique.

L'initiative « CyberÉdu » lancée en 2013 a permis de confirmer l'intérêt des enseignants intervenants dans les cursus de formations supérieures aux métiers de l'informatique pour les sujets de sécurité des systèmes d'information. Cette initiative doit être confortée.

Le ministère de l'Éducation nationale, de l'enseignement supérieur et de la recherche, avec l'aide de la conférence des présidents d'universités, la conférence des grandes écoles, les administrations et les organisations professionnelles compétentes, veillera à ce que dès la rentrée 2016, une formation à la sécurité des systèmes d'information adaptée à la filière soit dispensée dans toute formation initiale supérieure comprenant des questions liées au numérique. Une intégration de ces éléments de sécurité dans les cours existants devra être recherchée en priorité et s'inscrire de manière pertinente dans le contexte plus large de chaque spécialité enseignée. Ces démarches pourront utilement s'appuyer sur les contenus pédagogiques en cours d'élaboration, en lien étroit avec la communauté enseignante, dans le cadre du projet CyberÉdu.

Le ministère de la Décentralisation et de la Fonction publique s'attachera à ce que les formations aux postes de responsabilités de la fonction publique comportent des éléments de sensibilisation à la cybersécurité. En lien avec le ministère de l'Intérieur, il veillera à ce que le concours de recrutement dans le corps des ingénieurs des systèmes d'information et de communication prévu par le décret n°2015-576 du 27 mai 2015 ainsi que les formations qui seront dispensées à ses membres comportent un volet cybersécurité.

Face à une demande croissante de nos partenaires, il conviendra, dans la mesure du possible, d'adapter une partie de l'offre de formation et de sensibilisation à un public international, en proposant notamment des programmes en langue anglaise.

> Recenser et anticiper les besoins en formations initiales et continues.

Sous l'égide du groupe d'experts pour la confiance numérique, les besoins en formations initiales à court, moyen et long terme seront établis, en lien avec l'ensemble des acteurs concernés de l'administration et du secteur privé.

Les syndicats professionnels seront sollicités pour l'élaboration et la mise en place de formations continues adaptées aux besoins des salariés et des entreprises.

4

ENVIRONNEMENT DES ENTREPRISES DU NUMÉRIQUE, POLITIQUE INDUSTRIELLE, EXPORT ET INTERNATIONALISATION

ENJEUX

Le cyberespace est en construction rapide. 100 000 objets nouveaux se connectent chaque heure à Internet. La présence de nombreuses entreprises françaises sur les salons internationaux comme le succès de l'initiative « French Tech » montre un réel dynamisme de l'innovation française en matière de produits et services numériques. Cette réalité ne doit cependant pas masquer une certaine perte de maîtrise et une réelle dépendance technologiques.

Les grands équipements qui assurent le fonctionnement des réseaux de communications électroniques dont les infrastructures sont situées en France sont souvent conçus, développés et administrés depuis des centres situés hors de l'Europe. Il en est de même pour l'essentiel des équipements de communications et de sécurité informatique de nos opérateurs d'importance vitale. Le fonctionnement d'un nombre croissant d'entreprises repose sur l'utilisation d'applications et le traitement de données hébergés dans des espaces immatériels non maîtrisés, portés par des infrastructures physiques situées hors du territoire national et non soumises au droit européen.

Les évolutions en cours tant au niveau des technologies que dans les modèles économiques, avec par exemple la multiplication des objets connectés ou la concentration des plates-formes de service en ligne entre les mains de quelques acteurs seulement, sont de nature à amplifier cette perte de maîtrise du cyberespace national. En cas de crise internationale, l'accès à des pans entiers du cyberespace pourrait nous être contesté.

La réponse à cet enjeu de souveraineté nécessite en premier lieu le maintien d'une industrie nationale et européenne forte et compétitive dans le domaine spécialisé des produits et services de cybersécurité. Plus généralement, elle passe par le développement, en France et en Europe, d'une offre d'équipements et de services numériques qui apportent à leurs clients les garanties de sécurité et de confiance adaptées aux enjeux et aux usages.

« Le développement, par les entreprises nationales du secteur numérique, d'une offre de produits et de services sécurisés doit également être vu comme un facteur essentiel de compétitivité pour ces entreprises. »

Les utilisateurs n'ont pas le moyen de s'assurer eux-mêmes du niveau de sécurité des objets et services numériques. La promotion de la sécurité dans le discours commercial des fournisseurs se généralise sans toutefois permettre une évaluation objective du niveau de sécurité réellement atteint. Le développement d'une plus grande lisibilité sur le plan de la sécurité de l'offre numérique, fondée sur des éléments objectifs et vérifiables par un tiers, constitue un défi majeur pour assurer la confiance dans l'économie numérique.

Le développement, par les entreprises nationales du secteur numérique, d'une offre de produits et de services sécurisés doit également être vu comme un facteur essentiel de compétitivité pour ces entreprises. Le domaine des moyens de paiements (cartes à puce, terminaux de paiement, etc.) est l'archétype d'un secteur économique dans lequel un niveau de sécurité adapté à la menace et vérifiable par un tiers constitue un argument commercial de premier plan. Plusieurs entreprises nationales disposent dans ce secteur d'une position concurrentielle au niveau mondial qui doit beaucoup à l'excellence qu'elles ont su développer et démontrer en matière de sécurité.

La multiplication des menaces cybernétiques et la prise de conscience de plus en plus large de la réalité de ces menaces conduiront dans quelques années à faire de la sécurité un critère d'achat essentiel dans de nombreux autres secteurs. Agir dès à présent pour améliorer la sécurité et la transparence de l'offre nationale de solutions numériques, c'est aussi préparer leur compétitivité à venir.

En 2015, la part des entreprises françaises et singulièrement des PME-PMI utilisant largement

le numérique n'est que dans la moyenne des pays européens. Le rattrapage de ce retard doit s'accompagner d'une meilleure sécurisation de la vie numérique des entreprises et en premier lieu d'une meilleure sécurité de leurs systèmes d'information. Il en va de notre compétitivité et donc de nos emplois.

Le défi posé aux entreprises françaises est de concilier recherche de productivité, d'économies, de rentabilité et utilisation ou développement de produits et services numériques ne mettant pas en danger leur compétitivité ou leur sécurité, celles de leurs partenaires ou celles de leurs clients.

La plupart des équipements, objets et services numériques disponibles aujourd'hui sur le marché n'ont pas le niveau de sécurité informatique leur permettant d'éviter un incident — fuite de données, dysfonctionnement ou rupture de service. Pour les entreprises françaises l'ergonomie, la protection des données personnelles, le niveau de sécurité des produits et services numériques qu'elles développent et produisent, doivent devenir à court terme un différenciateur, un avantage concurrentiel pour ces entreprises et en retour pour la nation.

Par ailleurs, si la contrefaçon ne relève pas directement de la sécurité des systèmes d'information, des produits de sécurité informatique contrefaits peuvent mettre en danger l'activité des organisations qui les acquièrent.

« Pour les entreprises françaises l'ergonomie, la protection des données personnelles, le niveau de sécurité des produits et services numériques qu'elles développent et produisent, doivent devenir à court terme un différenciateur, un avantage concurrentiel pour ces entreprises et en retour pour la nation. »

En matière d'internationalisation des entreprises et d'export, face à une concurrence internationale exacerbée où nos partenaires accordent un soutien appuyé et structuré à leur industrie, les services de l'État doivent s'organiser de manière pérenne pour soutenir les entreprises françaises de la cybersécurité.

La mobilisation et la coordination de toutes les ressources publiques et privées disponibles sont essentielles pour accroître la visibilité et la compétitivité de l'offre française à l'international, mutualiser les connaissances, les retours d'expérience et ainsi favoriser le partage d'informations entre les différents acteurs de la filière.

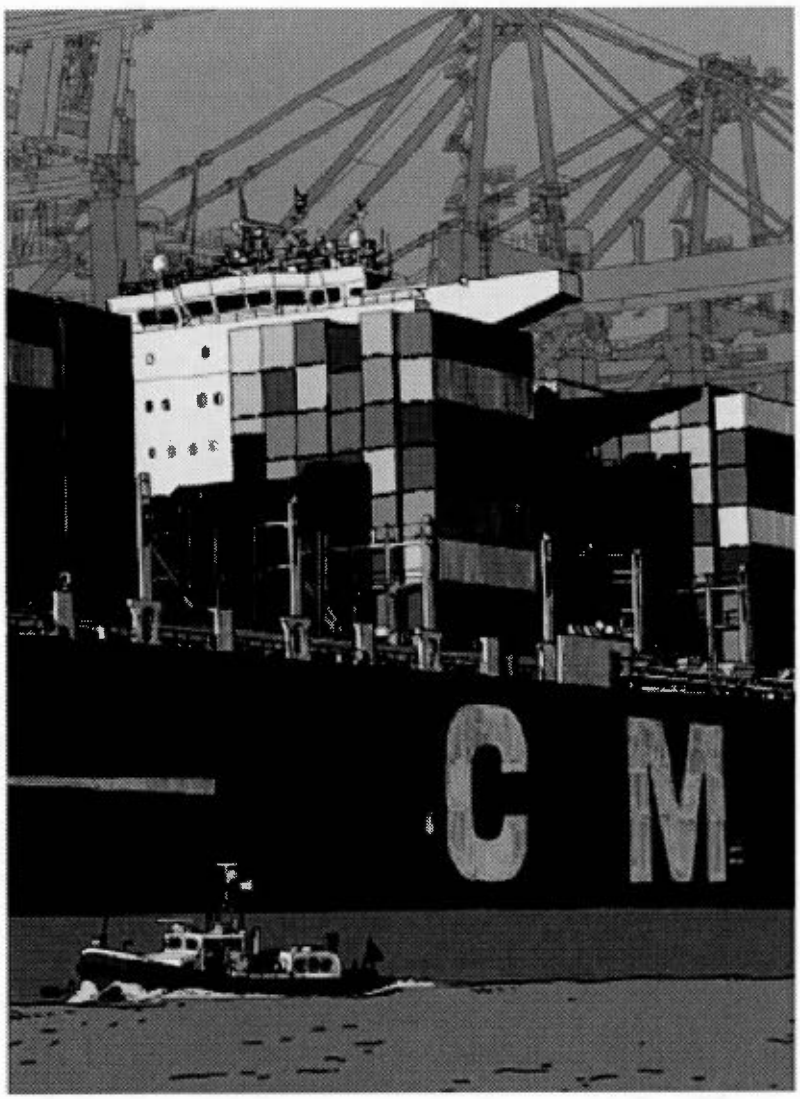
■ OBJECTIF

La France développera un écosystème favorable à la recherche et à l'innovation et fera de la sécurité du numérique un facteur de compétitivité. Elle accompagnera le développement de l'économie et la promotion internationale de ses produits et services numériques. Elle s'assurera de la disponibilité pour ses citoyens, ses entreprises et ses administrations, de produits et services numériques présentant des niveaux d'ergonomie, de confiance et de sécurité adaptés aux usages et aux cybermenaces.

■ ORIENTATIONS

> Développer et valoriser l'offre nationale et européenne de produits et services de sécurité.

En lien avec les administrations compétentes du ministère de l'Économie, de l'Industrie et du numérique et du ministère de la Défense, l'agence nationale de la sécurité des systèmes d'information a engagé en 2012 une politique industrielle afin de développer le tissu national des entreprises développant des produits et services de sécurité informatique.


C M

Le lancement en 2013 du plan « cybersécurité » de la Nouvelle France industrielle, désormais englobé dans la solution « Confiance numérique » accompagné de l'appui du commissariat général à l'investissement et de BpiFrance ont permis d'organiser la filière et de lancer des appels à projets visant à créer une offre d'équipements de confiance pour la détection d'attaques informatiques, essentiellement destinés aux opérateurs d'importance vitale, et de produits de mobilité sécurisée à l'intention de toutes les entreprises.

Les services de l'État vont accentuer leur effort en matière de qualification et de suivi de produits et de services de sécurité informatique, ainsi que de soutien au développement de nouveaux produits de sécurité répondant à l'évolution des usages. Ils soutiendront également la valorisation et la pérennisation de ces offres par le biais d'une commande publique privilégiant les produits et services de sécurité qualifiés au bon niveau, ainsi que par des actions de communication et de sensibilisation à destination du secteur privé.

Par ailleurs, les services de l'État chercheront à diffuser les résultats des travaux de recherche en développement qu'ils financent pour des équipements de haut niveau de sécurité afin d'élever celle des produits destinés aux entreprises et au grand public.

Enfin, la France s'attachera à tirer pleinement parti des leviers offerts par l'Union européenne afin de soutenir, promouvoir et défendre les compétences scientifiques, technologiques et industrielles françaises dans les domaines de la cybersécurité. Elle encouragera par ailleurs l'UE à ne pas se limiter à un rôle de consommateur, mais à s'imposer comme un acteur global incontournable de l'offre dans ce secteur.

> Transférer les savoir-faire acquis vers le secteur privé pour favoriser la prise en charge de sa sécurité informatique.

La France s'est dotée depuis cinq ans d'une capacité de détection et de traitement des attaques informatiques, comme l'annonçait le Livre blanc sur la défense et la sécurité nationale de 2008. Si cet effort doit être poursuivi, notamment par l'ANSSI, il appartient au secteur privé d'assurer sa propre sécurité dans le domaine informatique comme dans d'autres domaines, les services de l'État ne devant intervenir qu'en cas de crise grave.

Appuyée par le transfert de savoir-faire acquis par les administrations vers le secteur privé, la labellisation de prestataires compétents et de confiance devrait permettre de détecter et de traiter l'inévitable croissance du nombre d'attaques informatiques subies par les entreprises.

> Préparer un monde numérique plus sûr par une meilleure anticipation des usages, un accompagnement adapté et une information des acteurs.

Pour les cinq ans à venir, la priorité des administrations compétentes en matière de sécurité des systèmes d'information doit être l'anticipation et la prévention.

Il s'agira d'obtenir que les produits et services numériques ou intégrant du numérique, conçus, développés et produits en France, soient parmi les plus sûrs au monde. Pour atteindre cet objectif, les administrations compétentes devront orienter leurs efforts de communication vers la communauté scientifique, publique et privée, et les lieux d'innovation — pôles de compétitivité, instituts de recherche technologiques, incubateurs, « fab labs », en y consacrant au besoin des moyens spécifiques, comme c'est le cas au ministère de la Défense, et, plus récemment, au ministère de l'intérieur.

Lorsque les produits et services numériques hébergeront des données personnelles ou seront destinés aux secteurs d'activité d'importance vitale, les services de l'État apporteront les éléments utiles à l'analyse des risques ou les conseils nécessaires à l'obtention du niveau de sécurité correspondant à l'usage du produit ou du service en cours de conception ou de développement. Ils contribueront également, pour les usages qui le justifient, à mettre en place des dispositifs permettant d'évaluer de manière indépendante le niveau de sécurité et de confiance de ces produits et services, et d'offrir à leurs utilisateurs potentiels des garanties adaptées par le biais d'une labellisation.

Parallèlement, l'environnement juridique d'accueil des nouveaux produits et services devra être anticipé. À titre d'exemple, la prochaine arrivée de véhicules autonomes doit inciter le régulateur à préparer les conditions assurant la sécurité de leur circulation. La cybersécurité doit être prise en compte dans les groupes de travail internationaux définissant le référentiel et les procédures techniques de contrôle.

Pour d'autres types de produits ou services, une signalétique adaptée devra informer le consommateur de leurs caractéristiques numériques essentielles et notamment du traitement qui est réalisé des données collectées. Pour certains secteurs, comme celui de la santé, une labellisation systématique des produits et services numériques sera étudiée.

La France cherchera à associer d'autres États membres de l'Union européenne à la mise en œuvre de ces pratiques afin de créer une zone de confiance et de sécurité numériques. Les travaux engagés avec l'Allemagne en matière d'informatique en nuage ou de messageries sécurisés vont en ce sens.

> Intégrer l'exigence de cybersécurité dans la commande et le soutien publics.

Pour la protection de sa souveraineté et notamment la protection de ses informations relevant du secret de la défense nationale, la France conservera sa capacité financière et industrielle à développer des solutions atteignant les plus hauts niveaux de sécurité.

Plus généralement, l'ensemble de l'administration devra démontrer son exemplarité dans le cadre de la commande publique, en intégrant des critères de sécurité au juste niveau dans ses choix des produits et services numériques.

Enfin, dès 2016, tout produit ou service embarquant ou s'appuyant sur un système d'information et souhaitant répondre à un appel d'offres, à un appel à projets publics, ou accéder à des fonds publics bénéficiera d'un facteur de bonification s'il est accompagné d'une analyse de risque en matière de cybersécurité correspondant à l'usage prévu du produit ou service et de la réponse technique apportée.

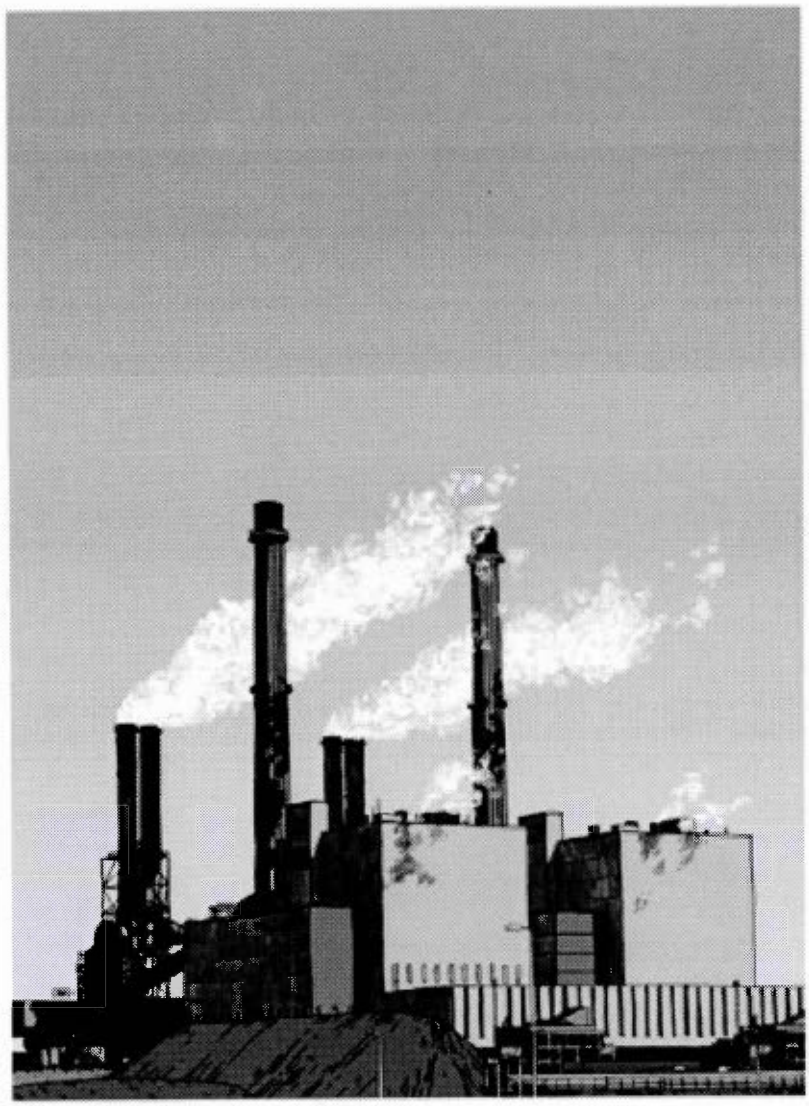
> Soutenir l'export et l'internationalisation des entreprises du secteur.

Afin de soutenir le développement économique de la filière industrielle de cybersécurité, la France s'attachera donc à renforcer la visibilité et la compétitivité de l'offre française à l'international et à faciliter l'accès des PME et des start-ups notamment aux marchés internationaux.

La coordination interministérielle sera structurée et renforcée. Une organisation adaptée en soutien des entreprises françaises sera mise en œuvre au-delà des actions ponctuelles et souvent isolées actuellement menées par les différents ministères et entités étatiques.

En sus de la création possible de dispositifs de soutien spécifiques aux acteurs de la filière cybersécurité, les conditions d'accès aux dispositifs de soutien existants, ainsi que leurs modalités de mise en œuvre seront clarifiées et optimisées. Les procédures de contrôle des exportations de solutions de cybersécurité seront clarifiées et optimisées.

Par ailleurs, à l'image des réalisations de « French Tech », les initiatives collaboratives issues du secteur privé et destinées à favoriser l'accompagnement des PME et des start-ups à l'international seront soutenues.



ENJEUX

Le cyberespace est devenu un sujet majeur de négociation au sein des organisations internationales dont les travaux portent désormais sur l'ensemble du champ du numérique.

En 2013, les États ont reconnu que loin d'être d'un espace sans règle, le cyberespace était régi par le droit international existant. Pour autant, le cadre normatif international est encore en début, ce qui, en l'absence d'avancée des négociations, pourrait nuire à la préservation d'un cyberespace stable et sûr, respectueux des droits fondamentaux et propice au développement d'une économie prospère et de confiance à l'ère numérique.

Tandis qu'un nombre croissant de pays déclarent se doter de capacités offensives, la conflictualité entre États trouve à s'exprimer de manière croissante dans le cyberespace. Par ailleurs, les révélations de pratiques massives et de techniques d'espionnage menées par de grands États ou des alliances d'États contre d'autres — parfois alliés —, des personnes et des entreprises, ont accru la défiance politique contre les pays à l'origine de ces pratiques et la méfiance technique vis-à-vis de leurs produits et services. Ces révélations favorisent aussi la prolifération de moyens techniques similaires.

Parallèlement, des groupes d'individus aux motivations et soutiens divers, mercenaires recrutés mondialement et associés au gré des circonstances, recourent régulièrement à des attaques informatiques dans le cyberespace pour tenter de déstabiliser les autorités gouvernementales de nombreux pays ou des entreprises qui les incarnent symboliquement. Des organisations terroristes profitent par ailleurs de l'audience portée par les réseaux sociaux pour diffuser une propagande destinée à attirer des volontaires et terroriser des populations. Ces différents groupes bénéficient d'un impact médiatique constant.

Sur le plan économique, la tendance du début de la décennie se confirme. Un petit nombre d'entreprises, portées par les États qui ont permis leur développement, utilisent leur avance technologique, leur domination sur le marché et leurs capacités financières pour préempter l'innovation numérique. Cette privatisation du cyberespace au profit de quelques monopoles condamne les autres acteurs du numérique à la dépendance et capte une part trop importante de la valeur ajoutée du numérique pour que cette situation soit supportable par les économies des autres pays.

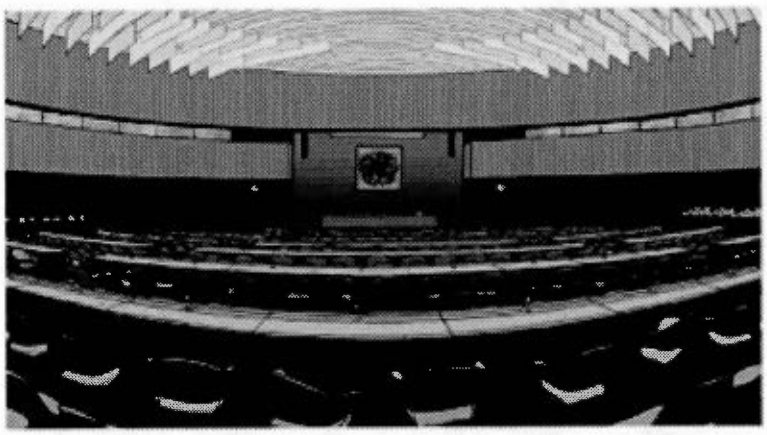
« S'il porte la croissance du monde, le cyberespace est devenu un lieu de compétition souvent déloyale et de conflits »

S'il porte la croissance du monde, le cyberespace est devenu un lieu de compétition souvent déloyale et de conflits, jusqu'à présent de basse intensité informatique, de déstabilisation politique et d'hégémonie économique.

L'Europe a su identifier ces enjeux et tente d'apporter par le discours et la réglementation des idées et des solutions plus respectueuses d'un développement numérique durable, tant en matière de gouvernance d'Internet que de protection des données personnelles ou de sécurité informatique des opérateurs essentiels à l'économie. L'Europe, qui a adopté en 2013 une stratégie de cybersécurité, peine toutefois à oser une autonomie stratégique numérique et à se doter des outils nécessaires à un rééquilibrage du cyberespace en sa faveur, bien que ce sujet soit désormais inscrit à l'ordre du jour de nombreuses enceintes de discussions et négociations européennes.

Parce qu'elle partage des valeurs communes avec d'autres États membres de l'Union européenne, la France doit y avoir avec eux un rôle moteur en matière de numérique.

La France veut participer à la transformation numérique de l'Europe par des alliances. L'Europe s'est construite hier par une alliance autour de matières premières. L'Europe numérique se construira sur des alliances, de la confiance et la maîtrise des données, matières premières des prochaines décennies.



OBJECTIF

La France sera, avec les États membres volontaires, le moteur d'une autonomie stratégique numérique européenne. Elle jouera un rôle actif dans la promotion d'un cyberespace sûr, stable et ouvert.

ORIENTATIONS

> Établir avec les États-membres volontaires une feuille de route pour l'autonomie stratégique numérique de l'Europe.

Ouverte aux États membres de l'Union européenne, cette feuille de route déterminera les facteurs-clés de succès de la mise en place à court terme des politiques propices à l'émergence d'une autonomie stratégique numérique européenne, notamment en matière de réglementation, de normalisation et de certification, de recherche et développement, de confiance dans le numérique, — en veillant au respect de la souveraineté des États-membres, de protection de la vie privée et des données personnelles conçues comme un bien d'intérêt public.

De la même manière, la France veillera à ce que les traités internationaux négociés au nom de l'Europe ne conduisent pas à la dépendance technologique ou économique des acteurs européens et à l'aliénation des données personnelles de ses citoyens ou des données sensibles de ses administrations, sources de déstabilisation du cyberespace.

Il s'agira de faire de l'Europe le territoire numérique le plus respectueux des droits fondamentaux et individuels et de mettre en place, dans le sens des travaux précurseurs entre la France et l'Allemagne relativement à l'informatique en nuage ou à l'échange chiffré de courriels entre les deux pays, une zone de confiance et de prospérité économique.

> Renforcer la présence et l'influence françaises dans les discussions internationales sur la cybersécurité.

Afin de renforcer la confiance à l'échelle internationale et d'explorer de nouveaux mécanismes de régulation visant à prévenir les conflits dans le cyberespace, la France renforcera ses contacts avec toutes les parties prenantes disposées à engager le dialogue sur les enjeux de cybersécurité.

La participation aux négociations multilatérales sur la cybersécurité (ONU, OSCE) sera accentuée afin de consolider un socle global d'engagements de bonne conduite pour les États dans le cyberespace, dans le respect du droit international.

Les contacts bilatéraux seront renforcés, dans le cadre notamment des dialogues diplomatiques à vocation interministérielle sur les enjeux relatifs au cyberespace, pilotés par le ministère des Affaires étrangères et du Développement international.

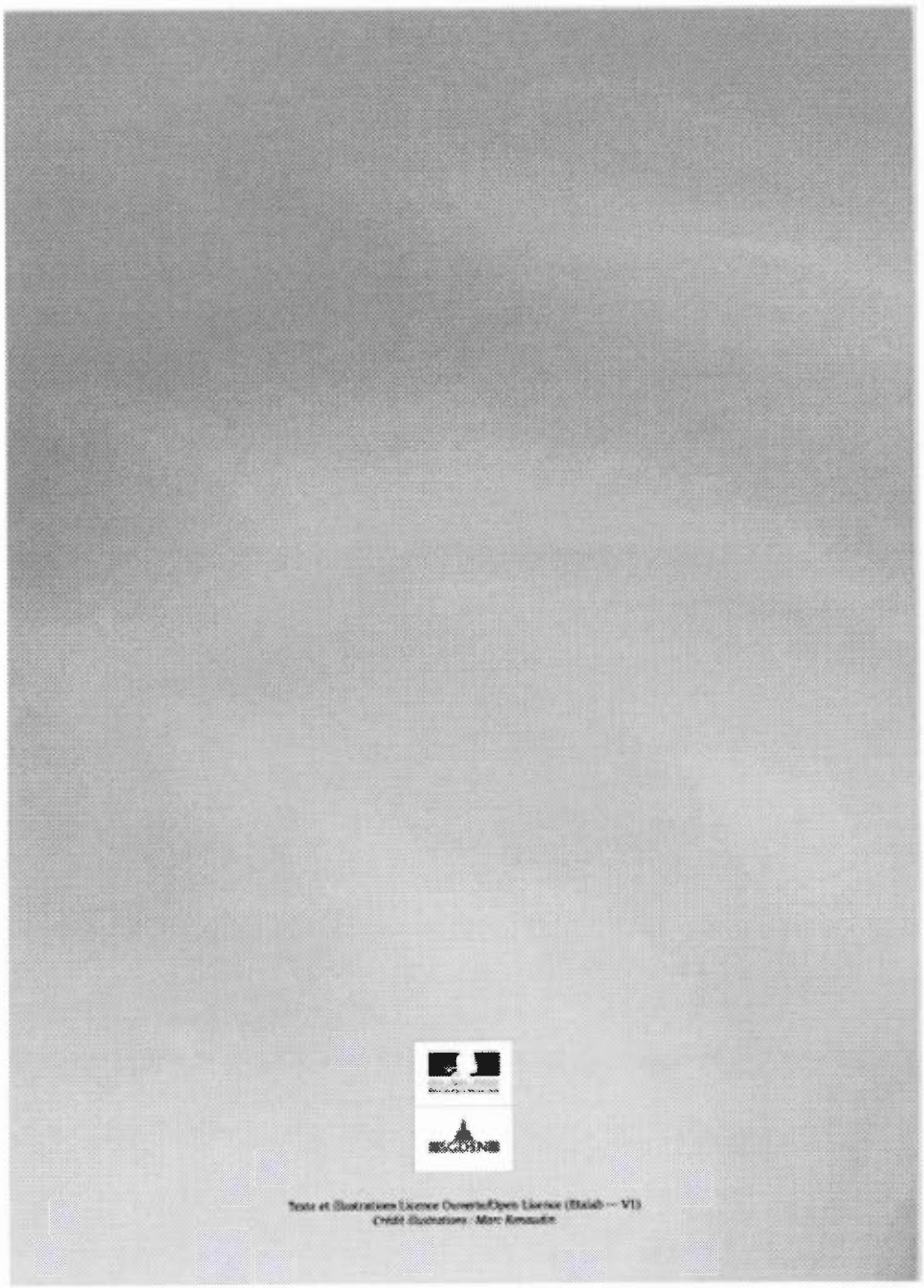
Enfin, dans une logique d'influence, la France investira davantage les forums internationaux plus informels dans lesquels les communautés techniques et académiques et les décideurs politiques pensent ensemble les équilibres à venir.

> Contribuer à la stabilité globale du cyberespace en soutenant les pays volontaires dans la mise en place de capacités de cybersécurité.

La transition numérique, porteuse d'opportunités politiques, sociales et économiques, est loin d'être maîtrisée de manière homogène dans tous les pays. Cela porte préjudice à la sécurité et au développement des États les moins protégés, et fragilise à l'échelle internationale, l'ensemble de l'écosystème numérique.

Afin de contribuer à un déploiement fiable et soutenable des technologies numériques dans l'ensemble des pays, et en particulier les pays en voie de développement, la France se doit de contribuer au renforcement capacitaire des pays souhaitant accroître la résilience et la sécurité de leurs systèmes d'information, notamment en matière de protection des infrastructures critiques et de lutte contre la cybercriminalité.

Afin d'assurer la durabilité et la soutenabilité des projets de renforcement des capacités, la France inscrira de préférence son action dans des partenariats de confiance à long terme. Cette action devra également permettre à la France de renforcer sa propre cybersécurité.



ANNEXE C

TABLEAU COMPARATIF DES STRATEGIES NATIONALES DE CYBERSECURITE FRANÇAISES (2009 & 2015)

Objectifs:	Stratégie de cybersécurité française de 2011:	Nouvelle stratégie de cybersécurité de 2015:
1	Coopérer sur la scène internationale, devenir une « puissance mondiale dans le cyberespace »	Défense et sécurité des systèmes d'informations de l'Etat: protéger les intérêts français dans le cyberespace
2	« garantir la liberté de la France par la protection de l'information de souveraineté »	Protéger le citoyen français concernant la vie privée, les données personnelles et la malveillance au sein du cyberespace tout en respectant les valeurs que porte la France
3	renforcement de la cybersécurité des infrastructures vitales nationales »	La sensibilisation et la formation à la sécurité du numérique, notamment concernant les dangers que représentent le cyberespace
4	La « sécurité dans le cyberespace »: protection du citoyen et de ses données personnelles	Rendre compte des enjeux économiques liés au numérique
5		L'Europe et la question de la souveraineté française: positionner la France et l'UE comme « moteur d'une autonomie stratégique »

ANNEXE D

TABLEAU REPRESENTATIF DE LA « MISE EN SCENE DE LA MENACE »

	Concepts:	Mises en situations:
1	Le jeu de l'acteur	TV5Monde, DAECH, le gouvernement français, l'ANSSI et le gouvernement russe.
2	La façade	Dans le cyberespace, tout organisme ou individu a la possibilité de choisir l'image qu'il souhaite renvoyer à son public, grâce à l'apparence qu'il donne à son identité et la manière dont ses actions sont construites.
3	La réalisation dramatique	Les cyberattaques sont lancées, la plupart du temps, non pas dans le but de détruire, mais d'avoir un impact sur les relations diplomatiques. Dans cette cyberattaque contre TV5 Monde, beaucoup d'actions ont été réalisées à l'abri du regard du public, elles ont ensuite été rapportées par les médias.
4	L'idéalisation	En utilisant la technique de « faux-drapeau », et en se cachant derrière le drapeau de l'EI, la Russie a souhaité renvoyer une tout autre image.

	Concepts:	Mises en situations:
5	La cohérence de l'expression	Les messages diffusés sur les réseaux sociaux et adressés directement aux officiels: accusent la France d'avoir agi contre l'EI, c'est ainsi que les français en subissent aujourd'hui les conséquences. Si les russes ont réellement commis cette cyberattaque, et ont donc délivrés ces messages, ils ont mis en place une représentation dont ils se doutaient du fort impact que cela pourrait entraîner: la menace islamiste extrémiste en France est prise très au sérieux, notamment de par les nombreuses et douloureuses attaques qui ont été dénombrées jusqu'à maintenant.
6	La représentation frauduleuse	La Russie aurait menti en se cachant derrière l'EI. Le gouvernement français et TV5 Monde, n'ont également pas tout dévoilés sur l'affaire, notamment à cause des raisons de sécurité nationale.
7	La mystification	Une part de mystère est gardée tout au long de cette représentation, puisque le gouvernement français et l'ANSSI ne dévoilent pas tout sur l'affaire.
8	L'opposition réalité/ simulation	D'un côté: représentation dans la réalité qui serait véridique et honnête puisque DAECH représente bel et bien une menace concrète pour la France. De l'autre côté: représentation qui aurait été inventée puisque se serait en fait, la Russie qui serait le véritable auteur de cette attaque.

	Concepts:	Mises en situations:
9	Les équipes + les secrets	Particulièrement dans le cas du gouvernent français et son agence de cybersécurité, l'ANSSI: les protagonistes faisant partie du gouvernement et de l'organisation se sont tous mis d'accord sur un message en particulier à délivré, nous nous entraidons particulièrement compte de par les différents Tweets des officiels. - « secret stratégiques »: le gouvernement et son agence n'ont pas dévoilé leurs capacités, puisqu'il s'agit de sécurité national et pour ne pas montrer l'inaptitude de l'équipe face à un certain problème. - « secret d'initiés »: ces personnalités se sont regroupés autour d'un message commun à délivré au publique témoin, celui-ci a permis la formation de l'équipe.

ANNEXE E

DISCOURS DU PREMIER MINISTRE MANUEL VALLS

GOUVERNEMENT.fr

16 octobre 2015 - Discours

Discours du Premier ministre - Présentation de la Stratégie nationale pour la sécurité du numérique

Contenu publié sous le Gouvernement *Valls II* du *26 Août 2014* au *10 Février 2016*

Madame la ministre, chère Axelle LEMAIRE,
Mesdames et messieurs les ambassadeurs,
Monsieur le Secrétaire général de la Défense et de la Sécurité nationale,
Monsieur le Directeur général de l'Agence nationale de la Sécurité des Systèmes d'Information,
Monsieur le Président du Conseil national du Numérique,
Mesdames et messieurs,

La formule est bien connue : nous sommes dans un monde globalisé, un monde qui est, grâce au numérique, plus ouvert, avec beaucoup d'opportunités, mais qui doit faire face aussi à de nombreuses menaces.

Les opportunités, vous les connaissez : créations d'emplois et de richesses, simplification de l'administration, débat public et engagement citoyen, accès à la culture. Nous essayons tous, et mon Gouvernement aussi, de les saisir.

Les menaces aussi, vous ne les ignorez pas : mouvements protestataires, idées de plus en plus se détournement du numérique par des individus malveillants et des organisations criminelles ou terroristes. Nous y répondons avec une très grande lucidité, avec les moyens adaptés.

Début 2011, une première stratégie de cyber-sécurité a été publiée ; c'était peu après une attaque informatique visant le ministère de l'Economie et des Finances.

En quatre ans – parce que le monde va très vite – la donne a profondément évolué. Le numérique s'est plus encore imposé partout, dans le fonctionnement de l'Etat, dans l'activité économique ou dans la vie quotidienne de nos concitoyens.

Les cyberattaques peuvent aussi avoir des effets dévastateurs. Celle contre TV5 MONDE en avril dernier et le témoignage précis, vivant, empreint aussi d'Yves BIGOT il y a quelques instants en sont

la meilleure illustration.

Ces cyberattaques sont susceptibles de désorganiser les activités vitales de notre pays, de déstabiliser les entreprises, de vampiriser leur savoir faire. La conséquence directe est alors la destruction de nombreux emplois, de valeur industrielle et culturelle aussi.

Nos concitoyens sont également exposés, que ce soit à des tentatives d'escroquerie, qui s'accompagnent parfois de chantage, ou à la captation de leurs données personnelles.

Dans cet espace numérique comme ailleurs, la responsabilité de l'Etat est donc de se protéger – de protéger les citoyens, le tissu économique –, d'anticiper les menaces, et de réprimer les actes et les auteurs délictueux.

Alors qu'une société plus encore massivement connectée émerge, il nous faut aller vite, aller plus loin et bâtir une nouvelle stratégie pour notre cyber-sécurité.

Le document présenté ce matin est le résultat d'un travail inédit et ambitieux – Louis GAUTIER le rappelait il y a quelques minutes. Je veux remercier Guillaume POUPARD, très dynamique directeur général de l'ANSSI, de l'avoir initié, ainsi que tous ceux qui, par leur participation aux groupes de travail ou au travers de leurs auditions, ont contribué à son élaboration.

De façon souvent caricaturale, certains opposent le numérique, qui devrait être le monde de la liberté absolue, à la sécurité, qui se traduirait nécessairement par une restriction dangereuse de nos libertés fondamentales ...

Cette opposition caricaturale, nous l'avons vue, nous l'avons entendue, à l'occasion du débat sur la loi sur le renseignement.

La réalité est à mille lieues de cela, ou en tout cas elle est plus complexe : sans sécurité, c'est vrai dans le monde numérique comme dans le monde – si j'ose dire – réel, il n'y a pas de liberté possible. C'est quand il n'y a pas de règle, quand il n'y a personne pour les faire respecter, que prospère la loi du plus fort et qu'il y a l'asservissement des petits par les grands.

La force de notre démocratie, de notre Etat de droit, c'est justement de garantir cet équilibre, cette dynamique, entre sécurité et liberté. Et c'est tout le sens de cette stratégie nationale pour la sécurité du numérique, et des cinq objectifs stratégiques qui vous ont été présentés.

Je souhaite revenir rapidement sur certains d'entre eux.

Le premier objectif est de donner à la France les moyens de défendre ses intérêts fondamentaux dans le cyberespace.

S'il reste encore des progrès à faire, le Gouvernement a déjà pris un certain nombre de mesures fortes pour notre cyber-sécurité. Tout d'abord, en affectant des ressources à la hauteur des enjeux. Ainsi l'ANSSI, qui comptait une centaine d'agents lors de sa création en 2009, sera forte de 500 agents à l'horizon 2017. Les ministères de la Défense et de l'Intérieur ont eux aussi augmenté le nombre d'effectifs consacrés à ces missions.

Il faudra poursuivre dans ce sens, ce qui pose d'ailleurs une question plus générale sur l'engagement de nos finances publiques – engagement incontournable pour notre sécurité. Toutes les sociétés vont devoir faire des efforts majeurs pour se défendre, à l'intérieur de nos frontières ou à l'extérieur, ce qui va nous obliger à réfléchir sur nos priorités budgétaires dans les années qui viennent.

Notre pays a la chance de disposer d'un vivier de compétences de très haut niveau. Ses filières de formation et de recherche en informatique et en mathématiques sont mondialement reconnues et vous êtes nombreux, ici, dans cette salle, à en être issus.

Ce n'est pas toujours facile pour l'Etat, et donc pour l'ANSSI, d'être compétitifs en termes salariaux face aux possibilités des grandes entreprises. Mais nous faisons des efforts pour qu'une partie de ces talents s'engagent, même si ce n'est que pour une part de leur carrière, au sein de ces services publics.

Par ailleurs, la loi de programmation militaire de 2013 a prévu un renforcement de la sécurité des systèmes d'information des opérateurs d'importance vitale, et non plus uniquement de ceux de l'Etat. Le travail de concertation entre ces opérateurs, les ministères coordonnateurs et l'ANSSI aboutira avant la fin de cette année à la publication d'arrêtés. Ils préciseront par secteur d'activité les mesures techniques qui devront être mises en œuvre et les délais à respecter.

En matière de politique industrielle, Bpifrance, en lien avec le ministère de l'Economie, de l'Industrie et du Numérique et l'ANSSI, a lancé des appels à projets consacrés à la cyber-sécurité. Le but est d'accompagner les entreprises françaises pour développer des dispositifs fiables de détection d'attaques informatiques ou des équipements de protection destinés aux PME.

Deuxième objectif sur lequel je veux insister à mon tour : la protection des Français, en particulier de leurs données personnelles.

Si le développement du e-commerce, l'émergence des objets connectés et l'explosion des échanges sur les réseaux sociaux sont de véritables progrès, et sont désormais incontournables, ils sont aussi source de vulnérabilité. Les données numériques dévoilent notre vie personnelle et professionnelle et contiennent des éléments, souvent, qui relèvent de l'intime. Il est donc indispensable de protéger la vie numérique de nos concitoyens.

Le 8 décembre dernier, devant l'ensemble des CNIL européennes, je formulais des engagements pour faire du modèle européen de protection des données personnelles un argument d'attractivité, voire de compétitivité. La toute récente décision de la Cour de justice des communautés européennes montre bien l'écart qui peut exister par rapport à d'autres législations. Et je partage l'analyse de Benoît THIEULIN : nous sommes là face à un basculement historique – mais il faut être capable, désormais, d'être à la hauteur de cette décision.

Je veux insister sur un autre point fondamental : celui de la confiance.

Je suis fier d'avoir porté, je l'évoquais il y a un instant, la loi sur le renseignement, quasiment intégralement validée par le Conseil constitutionnel – ce qui lui donne une légitimité plus grande encore ; et nous verrons ultérieurement ce qu'il adviendra au niveau de la Cour de Strasbourg.

Mais s'il était nécessaire de donner à nos services de renseignement les outils indispensables pour assumer leurs missions dans la société numérique, mon Gouvernement reste favorable à ce que les acteurs privés continuent de bénéficier pleinement, pour se protéger, de toutes les ressources qu'offre la cryptologie légale.

Par ailleurs, comme le rappelait Louis GAUTIER, la France est en retard par rapport à ses partenaires en matière de sensibilisation de sa population aux risques associés aux usages du numérique. La sensibilisation de tous au "risque cyber" est indispensable. Jeunes, élus, dirigeants d'administration et d'entreprise, professionnels du numérique doivent être sensibilisés, associés, mobilisés – et c'est aussi, au fond, le sens de cette rencontre.

Il est également essentiel de soutenir et d'accompagner les entreprises françaises – beaucoup sont

présentes ici et je les salue – notamment celles de la "French Tech", dont on connaît le dynamisme et la force d'innovation.

Je souhaite, à ce titre, saluer le lancement, la semaine dernière, par Axelle LEMAIRE, d'un appel à projets du programme d'investissements d'avenir pour soutenir les technologies innovantes en matière de protection de la vie privée. Doté de 10 millions d'euros, il permettra à des entreprises françaises de développer une expertise et des produits de niveau mondial, qui leur ouvriront des marchés importants, en même temps qu'ils contribueront à la protection de nos concitoyens.

Les métiers de la cyber-sécurité sont des métiers d'avenir et des gisements d'emplois importants. C'est vrai pour les entreprises qui développent ces outils, mais c'est vrai aussi pour toutes les structures, aussi bien publiques que privées, qui sont amenées à protéger leurs systèmes d'information.

Ma présence ce matin, c'est l'occasion de livrer quelques recommandations à ceux qui parmi vous seront chargés de la mise en œuvre de cette stratégie.

Je vous invite tout d'abord à l'ouverture.

Nous sommes tous impliqués, je le disais, et nous devons tous être mobilisés. L'Etat doit accomplir sa part en matière de formation, de prévention et de défense – mais rien que sa part. Cette action doit aussi s'appuyer, chaque fois que possible, sur le secteur privé et associatif.

Je me félicite d'ailleurs de la diversité de vos profils et de vos parcours, vous qui êtes présents ici, ce matin, et témoignez donc de cette mobilisation collective : fonctionnaires, cadres et chefs d'entreprise, de grands groupes industriels comme de PME, acteurs associatifs, élus, représentants de pays étrangers.

Je me félicite, aussi, qu'un dialogue constructif s'opère désormais entre les pouvoirs publics et les professionnels du numérique, pour mieux sécuriser Internet et défendre également nos valeurs sur les réseaux sociaux.

La signature, en marge de cette journée, en présence d'Axelle LEMAIRE, d'une charte par laquelle les principaux opérateurs de télécommunications français s'engagent à protéger les échanges de mails entre leurs serveurs respectifs en est, me semble-t-il, le témoignage. Cela permettra de mieux sécuriser les échanges de nos concitoyens tout en préservant les impératifs de sécurité nationale.

Par ailleurs, le numérique ne connaît pas de frontière et la dimension internationale, sur ces sujets, est essentielle. Nous n'agissons pas seuls. Une coopération opérationnelle existe entre nos plus proches alliés, dont je veux saluer les représentants ici. Et je me réjouis que le document qui nous a été remis soit aussi traduit dans plusieurs langues : anglais, allemand, espagnol.

L'Etat doit lui aussi faire preuve d'ouverture ! Comme dans notre vie quotidienne, toutes les politiques publiques doivent désormais impérativement intégrer la dimension numérique, aussi bien dans leur définition que dans leur mise en œuvre.

Je vous invite aussi à la vigilance et à l'anticipation. Anticipation des nouvelles menaces, bien évidemment, mais également vigilance quant au risque de dispersion des moyens.

L'effort collectif pour nous doter des moyens nécessaires à la sécurisation de l'espace numérique est significatif. Il arrive toutefois que différentes entités travaillent sur des sujets comparables ou complémentaires, et je vous demande donc d'échanger, de mutualiser le cas échéant et de partager les travaux de recherche.

Enfin, vigilance et anticipation sur le cadre juridique relatif à la sécurité du numérique s'imposent. Cela est vrai au niveau français, mais aussi à l'échelon international, lorsqu'il s'agit de traités qui engagent notre pays ou de travaux menés à l'ONU ou au niveau européen. C'est le cas, actuellement, dans le cadre des négociations relatives au projet de directive sur la sécurité des systèmes d'information, dite directive NIS.

Mesdames, Messieurs,

Je l'ai dit précédemment : la responsabilité de l'Etat, sur les territoires numériques comme ailleurs, est de se protéger et de protéger ses citoyens.

Le défi de la sécurité dans l'espace numérique est pris en compte depuis plusieurs années. Mais aujourd'hui, l'ampleur des menaces et l'importance du numérique dans notre société nous obligent à monter en puissance et adapter constamment notre dispositif.

La stratégie nationale pour la sécurité du numérique qui vous est présentée aujourd'hui est un bon équilibre entre prise en compte de la sécurité et dynamisme économique. La présentation de cette stratégie n'est toutefois qu'un commencement, qu'une première étape. Et je souhaite, monsieur le Secrétaire général, que vous me présentiez régulièrement un état de sa mise en œuvre afin de lever les difficultés éventuelles ou d'apporter les adaptations, les inflexions nécessaires.

Vous pouvez être assurés de la détermination du Gouvernement à poursuivre l'effort pour faire face aux menaces issues du cyberespace. L'époque le commande, l'exige, nous l'impose.

L'espace numérique doit être un espace de confiance, de sécurité et de responsabilité. La "République numérique", voulue par le Gouvernement, portée par vous, madame la ministre, mais aussi par vous, cher Benoît THIEULIN, doit promouvoir nos valeurs, développer notre économie et protéger nos concitoyens. C'est le sens du projet de loi porté par la ministre, qui sera débattu au Parlement dans quelques semaines, dans quelques mois.

Je souhaite que cette stratégie nationale pour la sécurité du numérique soit le point de départ d'une dynamique à la fois protectrice et libératrice, et qui permettra à la France aussi d'être en pointe sur ces sujets.

Et je sais que je peux compter sur votre engagement à tous.

Je vous remercie.

DISCOURS DU 16 OCTOBRE 2015 - PRÉSENTATION DE LA STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE

BIBLIOGRAPHIE

ANSSI. (2011). Défense et sécurité des systèmes d'information. *Stratégie de la France.*

ANSSI. (2015). La stratégie nationale pour la sécurité du numérique.

Berger, P. et Luckmann, T. (1996). La construction sociale de la réalité. Doubleday &Compagny Inc.

Chambet, P. Le cyber-terrorisme. Récupéré de http://www.chambet.com/publications Cyberterrorisme.pdf

Daniel, M. et Martin, F-P. (2001). Cybercrime-menaces, vulnérabilités, ripostes. Édition Broché.

Foucault, M. (1971). L'Ordre du discours. Gallimard.

Goffman, E. (1973). La Mise en scène de la vie quotidienne. *La Présentation de soi.* Les éditions de Minuit, Le sens commun.

Goffman, E. (1988). Les Moments et leurs hommes. Textes recueillis et présentés par Yves Winkin. Édition Broché.

Harvey, P-L. (1999). Cyberespace et communautique. *Appropriation, réseaux, groupes virtuels.* Les Presses de l'Université Laval.

Joubert, V. et Samaan, J-L. (2014). L'intergouvernementalité dans le cyberespace: étude comparée des initiatives de l'OTAN et de l'UE. Hérodote. Cyberespace: enjeux géopolitiques.

Le Conseil de l'Europe. (1997). Apprendre et enseigner dans la société de communication. Edition Levy.

Limonier, K. (2014). La Russie dans le cyberespace: représentations et enjeux. La Découverte. 2e trimestre. Héridote, n° 152-153.

Schmidt, E. et Cohen, J. (2014). The New Digital Age. *Reshaping the Future of People, Nations and Business*. Édition Broché.

Segal, A. (2016). The Hacked World Order. *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. 1st Edition.

Windisch, U. (1987). Le K.-O. Verbal: la communication conflictuelle. Édition Broché.