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

ETUDE PROSPECTIVE ET STRATEGIQUE

LES EVOLUTIONS DE LA CYBERSECURITE : CONTRAINTES, FACTEURS, VARIABLES…

Juin 2015

N° 1506388759

M. Daniel VENTRE

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

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

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

Les évolutions de la cybersécurité : contraintes, facteurs, variables…

Daniel Ventre, CNRS (Laboratoire CESDIP. UMR 8380). Titulaire de la Chaire de Cybersécurité & Cyberdéfense (Ecoles Militaires de Saint-Cyr Coëtquidan)

Juin 2015

Résumé de 2 pages

De la lecture des multiples stratégies, politiques, plans, programmes de cybersécurité et cyberdéfense publiés de par le monde ces dernières années, paraît émerger un consensus, une convergence de tous, reconnaissant la nécessité d'organiser et assurer la sécurité et la défense du domaine cyber, c'est-à-dire tout d'abord la sécurité et défense de l'ensemble des systèmes techniques eux-mêmes, et celles des sociétés qui sont traversées par ces systèmes. De la sécurité des systèmes dépend celle de l'Etat-nation.

Le consensus prend forme dans l'acceptation par tous de la trame d'un récit relativement simple, constitué de quelques briques élémentaires. Ce récit tourne autour de trois protagonistes : il y a « nous », «La menace », et « le cyberespace ».
Ce « nous » c'est l'Etat, la nation, notre société, l'ensemble des acteurs qui partagent nos valeurs, nos intérêts aussi. Ce « nous » assoit son développement, son progrès, son économie, sur un socle technologique. Or la sécurité n'a pas été intégrée à l'origine dans ce socle, de sorte que « nous » sommes toujours en train de poursuivre une sécurité idéale qui n'existera probablement jamais pour deux raisons : remettre de la sécurité dans l'ensemble du socle technologique reviendrait à tout démonter et tout reconstruire ; en face, il y a des adversaires/ennemis/opportunistes, qui partagent de plus en plus les mêmes dépendances technologiques mais pas nécessairement les mêmes valeurs, intérêts, objectifs, et ont appris à tirer parti de nos fragilités. Notre dépendance a atteint un tel degré, que plane sur nous la menace d'une attaque dont les effets seraient destructeurs (cyber Armageddon). « Nous » est alors confronté aux « autres », « la menace » : ils peuvent même être parmi nous (*insider threat*), et font peser sur notre modèle des menaces vitales. Ces adversaires sont indénombrables, ne connaissent pas les frontières. La menace mobilise toutes les catégories du crime et du conflit (crime organisé, délinquance, gangs, mafias, terrorisme, guérillas, services de renseignement, insurrection…). La mise en évidence des attaques menées par des alliés et partenaires ne contribue pas à réduire le sentiment de menace globale. Dans certains Etats le citoyen lui-même est une menace (cyberactivisme). Ces adversaires sont souvent invisibles, agissent par surprise, sont asymétriques. Le « nous » menacé doit donc légitimement se protéger, se défendre, apprendre à répliquer, à attaquer. Il apprend à montrer sa force, il rêve de trouver des méthodes de dissuasion. Il rêve de dominer le cyberespace pour y maintenir son ordre quand il est hégémonique, ou d'y retracer ses frontières nationales de souveraineté quand il n'est pas dans la ligne tracée par l'hégémon. Certains évènements, incidents, plus médiatisés que d'autres, viennent comme autant de piqures de rappel, maintenir les consciences éveillées et conforter la justesse de la trame du récit.

Ce récit a ses auteurs, ses promoteurs, ses acteurs, ses audiences. Chacun d'entre eux, en fonction de son pouvoir, de ses intérêts, objectifs, motivations, de sa réceptivité, va contribuer à dessiner la cybersécurité.

Ainsi, l'apparente convergence des politiques/stratégies de cybersécurité (de nombreux Etats mettent en place des unités dédiées au sein des armées, des polices, créent des forces cyber, attribuent rôles et responsabilités, créent du droit, affirment la nécessité du partenariat public-privé, de la coopération internationale, adoptent une approche multi-stakeholders…) ne saurait-elle masquer les différences. Car les Etats, acteurs rationnels, poursuivent tous leurs propres objectifs sur la scène internationale ; au sein des Etats, les diverses composantes défendent également leurs propres intérêts. La cybersécurité a donc une utilité qui diffère d'un acteur à l'autre, et cela ne peut que transparaître dans ce que devient la cybersécurité à l'intérieur d'un Etat, puis au niveau régional ou international. Elle est le reflet de tensions, conflits, relations, dynamiques multiples. Elle ne sera pas instrumentalisée ou appréhendée de la même manière d'un acteur à l'autre, selon que l'on est un industriel ou un acteur étatique, que l'on est une grande puissance ou un petit Etat ; que l'on est dans un Etat démocratique ou autoritaire ; ni même à l'intérieur d'un même espace, dans le temps, car elle est appelée à évoluer. La cybersécurité peut être aujourd'hui définie comme une priorité de sécurité et défense nationale ; ce n'était pas le cas il y a quelques années ; ce ne sera peut-être plus le cas à moyen ou long terme.

Il y a donc bien « des » politiques/stratégies de cybersécurité, « des » cyberstratégies nationales. Ce sont ces différences et convergences que nous avons tenté de mettre en évidence dans ce rapport, sans prétendre bien sûr à l'exhaustivité. Nous avons essayé d'identifier les facteurs politiques, économiques, sociologiques, stratégiques, qui gouvernent à la définition et à la forme que prennent les cyberstratégies,

Les deux premiers chapitres proposent une lecture de quelques stratégies de cybersécurité et cyberdéfense. Nous n'avons pas nécessairement focalisé notre attention sur les grandes nations, dont les politiques, postures, sont très documentées par ailleurs, quand bien même seraient-elles les modèles qui les orientent toutes, ou les influencent. Nous retrouverons donc dans cette étude les stratégies de petits Etats (*small states*), dont le rôle stratégique peut cependant être majeur pour les équilibres mondiaux ou du moins régionaux. Les Etats dont les stratégies sont observées ici, classés par ordre alphabétique dans le texte, ont des destins différents, des environnements géopolitiques distincts, des dimensions, un rôle et des ambitions forts différents (rien de commun sans doute entre le Qatar et Vanuatu) ; certains sont entrés dans l'histoire du cyberconflit (Estonie, Géorgie) l'ayant expérimenté au cours de la dernière décennie ; l'expérience de ces mêmes pays a d'ailleurs fait office d'électrochoc pour la communauté internationale qui depuis (2007 pour l'Estonie, 2008 pour la Géorgie) s'est engagée dans la voie de la cybersécurité. Mais aussi différents soient-ils, tous les Etats que nous évoquerons ont ceci en commun d'avoir récemment dévoilé des politiques de cybersécurité, et de les formuler en des termes dont la similitude doit nous interroger. Y a-t-il donc un « modèle » incontournable ? Peut-être est-ce ce qu'ambitionne d'ailleurs le Commonwealth qui propose à ses Etats un canevas de cyberstratégie, énumérant tous les items de base. Ces deux premiers chapitres décrivent les stratégies dans leurs grandes lignes et en soulignent les points saillants.

Le troisième chapitre proposera ensuite une lecture des points de convergence et de différenciation des stratégies et politiques.

Introduction

De la lecture des multiples stratégies, politiques, plans, programmes de cybersécurité et cyberdéfense publiés de par le monde ces dernières années, paraît émerger un consensus, une convergence de tous, reconnaissant la nécessité d'organiser et assurer la sécurité et la défense du domaine cyber, c'est-à-dire tout d'abord la sécurité et défense de l'ensemble des systèmes techniques eux-mêmes, et celles des sociétés qui sont traversées par ces systèmes. De la sécurité des systèmes dépend celle de l'Etat-nation.

Le consensus prend forme dans l'acceptation par tous de la trame d'un récit relativement simple, constitué de quelques briques élémentaires. Ce récit tourne autour de trois protagonistes : il y a « nous », «La menace », et « le cyberespace ».
Ce « nous » c'est l'Etat, la nation, notre société, l'ensemble des acteurs qui partagent nos valeurs, nos intérêts aussi. Ce « nous » assoit son développement, son progrès, son économie, sur un socle technologique. Or la sécurité n'a pas été intégrée à l'origine dans ce socle, de sorte que « nous » sommes toujours en train de poursuivre une sécurité idéale qui n'existera probablement jamais pour deux raisons : remettre de la sécurité dans l'ensemble du socle technologique reviendrait à tout démonter et tout reconstruire ; en face, il y a des adversaires/ennemis/opportunistes, qui partagent de plus en plus les mêmes dépendances technologiques mais pas nécessairement les mêmes valeurs, intérêts, objectifs, et ont appris à tirer parti de nos fragilités. Notre dépendance a atteint un tel degré, que plane sur nous la menace d'une attaque dont les effets seraient destructeurs (cyber Armageddon). « Nous » est alors confronté aux « autres », « la menace » : ils peuvent même être parmi nous (*insider threat*), et font peser sur notre modèle des menaces vitales. Ces adversaires sont indénombrables, ne connaissent pas les frontières. La menace mobilise toutes les catégories du crime et du conflit (crime organisé, délinquance, gangs, mafias, terrorisme, guérillas, services de renseignement, insurrection…). La mise en évidence des attaques menées par des alliés et partenaires ne contribue pas à réduire le sentiment de menace globale. Dans certains Etats le citoyen lui-même est une menace (cyberactivisme). Ces adversaires sont souvent invisibles, agissent par surprise, sont asymétriques. Le « nous » menacé doit donc légitimement se protéger, se défendre, apprendre à répliquer, à attaquer. Il apprend à montrer sa force, il rêve de trouver des méthodes de dissuasion. Il rêve de dominer le cyberespace pour y maintenir son ordre quand il est hégémonique, ou d'y retracer ses frontières nationales de souveraineté quand il n'est pas dans la ligne tracée par l'hégémon. Certains évènements, incidents, plus médiatisés que d'autres, viennent comme autant de piqures de rappel, maintenir les consciences éveillées et conforter la justesse de la trame du récit.

Ce récit a ses auteurs, ses promoteurs, ses acteurs, ses audiences. Chacun d'entre eux, en fonction de son pouvoir, de ses intérêts, objectifs, motivations, de sa réceptivité, va contribuer à dessiner la cybersécurité.

Ainsi, l'apparente convergence des politiques/stratégies de cybersécurité (de nombreux Etats mettent en place des unités dédiées au sein des armées, des polices, créent des forces cyber, attribuent rôles et responsabilités, créent du droit, affirment la nécessité du partenariat public-privé, de la coopération internationale, adoptent une approche multistakeholders…) ne saurait-elle masquer les différences. Car les Etats, acteurs rationnels, poursuivent tous leurs propres objectifs sur la scène internationale ; au sein des Etats, les diverses composantes défendent également leurs propres intérêts. La cybersécurité a donc une utilité qui diffère d'un acteur à l'autre, et cela ne peut que transparaître dans ce que devient la cybersécurité à l'intérieur d'un Etat, puis au niveau régional ou international. Elle est le reflet de tensions, conflits, relations, dynamiques multiples. Elle ne sera pas instrumentalisée ou appréhendée de la même manière d'un acteur à l'autre, selon que l'on est un industriel ou un acteur étatique, que l'on est une grande puissance ou un petit Etat ; que l'on est

dans un Etat démocratique ou autoritaire ; ni même à l'intérieur d'un même espace, dans le temps, car elle est appelée à évoluer. La cybersécurité peut être aujourd'hui définie comme une priorité de sécurité et défense nationale ; ce n'était pas le cas il y a quelques années ; ce ne sera peut-être plus le cas à moyen ou long terme.

Il y a donc bien « des » politiques/stratégies de cybersécurité, « des » cyberstratégies nationales. Ce sont ces différences et convergences que nous avons tenté de mettre en évidence dans ce rapport, sans prétendre bien sûr à l'exhaustivité. Nous avons essayé d'identifier les facteurs politiques, économiques, sociologiques, stratégiques, qui gouvernent à la définition et à la forme que prennent les cyberstratégies,

Les deux premiers chapitres proposent une lecture de quelques stratégies de cybersécurité et cyberdéfense. Nous n'avons pas nécessairement focalisé notre attention sur les grandes nations, dont les politiques, postures, sont très documentées par ailleurs, quand bien même seraient-elles les modèles qui les orientent toutes, ou les influencent. Nous retrouverons donc dans cette étude les stratégies de petits Etats (*small states*), dont le rôle stratégique peut cependant être majeur pour les équilibres mondiaux ou du moins régionaux. Les Etats dont les stratégies sont observées ici, classés par ordre alphabétique dans le texte, ont des destins différents, des environnements géopolitiques distincts, des dimensions, un rôle et des ambitions forts différents (rien de commun sans doute entre le Qatar et Vanuatu) ; certains sont entrés dans l'histoire du cyberconflit (Estonie, Géorgie) l'ayant expérimenté au cours de la dernière décennie ; l'expérience de ces mêmes pays a d'ailleurs fait office d'électrochoc pour la communauté internationale qui depuis (2007 pour l'Estonie, 2008 pour la Géorgie) s'est engagée dans la voie de la cybersécurité. Mais aussi différents soient-ils, tous les Etats que nous évoquerons ont ceci en commun d'avoir récemment dévoilé des politiques de cybersécurité, et de les formuler en des termes dont la similitude doit nous interroger. Y a-t-il donc un « modèle » incontournable ? Peut-être est-ce ce qu'ambitionne d'ailleurs le Commonwealth qui propose à ses Etats un canevas de cyberstratégie, énumérant tous les items de base. Ces deux premiers chapitres décrivent les stratégies dans leurs grandes lignes et en soulignent les points saillants.

Le troisième chapitre proposera ensuite une lecture des points de convergence et de différenciation des stratégies et politiques.

I - Des politiques et stratégies de cybersécurité

1.1. La stratégie du Bangladesh

La stratégie nationale de cybersécurité du Bangladesh[1] a pour objectif d'assurer la sécurité économique et le développement démocratique. Cette stratégie est associée aux enjeux de la **sécurité nationale dont la cyberstratégie est une des composantes**. Il s'agit de **coordonner les efforts** du gouvernement, du secteur privé, des citoyens, en définissant des priorités pour la cybersécurité (démarche qui vise donc à gérer les ressources disponibles, définir les rôles, attribuer les responsabilités), en privilégiant le **partenariat public-privé** (notamment parce que le secteur privé possède des infrastructures considérées comme critiques, telles que le secteur bancaire ou les télécommunications, par exemple) et la prise en compte de la dimension internationale.
Certains affirmations sont discutables : « *Worryingly, cyber espionage and other cybercrimes are very low cost activities* »[2], oubliant que les grandes opérations d'espionnage de ces dernières années

[1] National cybersecurity strategy, Bangladesh, 15 pages, http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf
[2] National cybersecurity strategy, Bangladesh, page 4, http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf

prennent au contraire forme dans des agences étatiques disposant de capacités et financements massifs (NSA, armée chinoise, renseignements russes, etc.). Pour réaliser ce programme de cybersécurité, l'Etat envisage de **légiférer** (renforcer son corpus juridique pour lutter contre la cybercriminalité et permettre la collaboration internationale des polices et de la justice) ; de prendre des **mesures techniques** (certification, industrie) et des **mesures organisationnelles**. La cybersécurité est la responsabilité de tous les acteurs de la société, mais la politique du Bangladesh **accorde à l'Etat le rôle principal** : il dirige, coordonne, fait la loi, se dote d'agence, de responsables, etc. Le document ne fait pas référence aux valeurs fondamentales (liberté, vie privée…) qui n'apparaissent donc pas comme des enjeux essentiels. La démocratie n'est d'ailleurs elle-même évoquée qu'une seule fois.

1.2. La stratégie de l'Estonie

La stratégie pour la période 2014-2017[3], publiée par le Ministère de l'Economie et de la Communication, est une composante de la stratégie de sécurité nationale, et elle **prolonge la cyberstratégie 2008-2013.** Les pays qui ont implémenté plus tôt que les autres des stratégies de cybersécurité sont déjà amenés à **tirer les conclusions de leurs premières tentatives**.

Pour assurer le rôle de leader, de coordinateur au niveau national, des **agences** sont généralement créées. Ce fut le cas en Estonie, où dans un premier temps en 2009 un Conseil de cybersécurité fut adjoint au Comité de Sécurité du gouvernement. En 2010, l'Estonian Informatics Centre accède au statut d'agence du gouvernement. Il aura en charge la protection de l'information et des systèmes d'information du gouvernement. En son sein est créée une structure spécifiquement en charge des infrastructures critiques (le Département pour la protection des infrastructures d'information critiques), laquelle embarque à son tour en 2011 une commission en charge de la coopération public-privé (PPP). En 2012 et 2013 sont fédérées et concentrées les capacités policières d'enquête en cybercriminalité. La stratégie est donc construite autour d'un **processus d'institutionnalisation,** création de structures, d'une **bureaucratie** dédiée à la cybersécurité, où l'on voit se constituer un système, ses hiérarchies, ses procédures. La cybersécurité et la cyberdéfense ne sont pas concentrées en une seule organisation, mais comme dans la plupart des pays, leurs fonctions, missions, responsabilités, se trouvent-elles distribuées entre plusieurs ministères et agences (ministère de l'économie, ministère de la défense, autorité des systèmes d'information, ministère de la justice, ministère des affaires étrangères, ministère de l'intérieur, ministère de l'éducation et de la recherche, etc. Le secteur non-étatique est appelé à coopérer avec l'institution étatique.

Le système se prolonge dans la création de cyber-unités de réservistes (Estonian Defence League's Cyber Unit) contribuant à la cyberdéfense des systèmes du pays. Cette action contribue à la constitution de capacités de cybersécurité nationales. L'Estonie occupe bien sûr **une place à part,** étant le siège du CCD COE, et le lieu de la tenue annuelle d'exercices de cyberdéfense de l'OTAN. Cette organisation concentre l'essentiel de la coopération internationale de l'Estonie en matière de cybersécurité, mais d'autres cadres internationaux sont investis par l'Estonie (OSCE, Nations Unies, etc.)

Cette cybersécurité se construit suivant plusieurs principes : **le respect des valeurs** (le respect des droits fondamentaux, libertés individuelles, identité), la **proportionnalité** (équilibre entre la prise en compte des risques et les ressources disponibles pour les affronter), le **PPP**, la **coopération internationale** (intensive). La coopération internationale est privilégiée avec les alliés, partenaires, voisins proches, et pays qui ont une même approche politique, intellectuelle de la cybersécurité.

Cette **cyberstratégie inclue la cyberdéfense** : elle prend en compte la **contribution des militaires à la cybersécurité**. Alerte, dissuasion, défense active, sont trois des piliers de cette cyberdéfense[4] dont il est prévu d'accroître les capacités. L'Estonie souhaite que puisse devenir réalité le principe de **défense collective** en matière de cyberdéfense. Elle appelle au **partage d'information** et à la coopération internationale, dans le cadre de l'OTAN ou grâce aux institutions européennes.

---

[3] Ministry of Economic Affairs and Communication, Cyber security strategy 2014-2017, Estonie, 2014, 14 pages, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

[4] Page 10

1.3. La stratégie de l'Inde

L'Inde a publié en 2013 une stratégie nationale de cybersécurité[5]. Celle-ci, dans ses lignes directrices, définit plusieurs objectifs et moyens pour les atteindre :

- TIC et cyberespace sont parmi les **catalyseurs de l'économie** indienne les plus importants
- Les TIC ont contribué à **positionner l'Inde dans l'économie mondiale**
- Cette économie et cette position internationale de l'Inde sont menacées par les cyberattaques qui déstabilisent le cyberespace
- La cybersécurité a fait jusqu'ici l'objet de nombreux plans, programmes, initiatives, sous l'impulsion de l'Etat.
- Cette stratégie nationale vise à coordonner, **unifier les initiatives**
- L'objectif est donc de construire un cyberespace sûr et résilient. Cette notion de résilience est inscrite dans de très nombreuses stratégies nationales.
- Créer un **écosystème de cybersécurité** : une agence nationale responsable de la cybersécurité, inciter les organisations à se doter en interne de responsables de la cybersécurité, de procédures spécifiques, établir un système de **partage d'information**, promouvoir des standards ouverts, utiliser des produits de sécurité certifiés, développer les CERTs, promouvoir la R&D en cybersécurité, accroître les ressources humaines (formation), **partenariats public-privé** (créer des modèles pour la collaboration, créer des espaces de dialogue, …), développer des **relations bilatérales ou multilatérales** avec les pays étrangers pour le partage d'information,

L'Inde adopte une démarche pragmatique, technologique, fondée essentiellement sur la protection des intérêts économiques du pays. La stratégie reprend des items que partagent nombre d'approches nationales, comme la création d'agences nationales, la mise en place de processus de veille, détection, réaction, la nécessité de se doter de capacités en ressources humaines. L'Etat oriente, définit les objectifs, formule des lignes directrices, des grands principes.

1.4. La stratégie de la Géorgie

La Géorgie s'est dotée d'une stratégie pour la période 2012-2015[6]. Le document s'ouvre sur un rappel à l'histoire, récente : les cyberattaques subies par la Géorgie en 2008 lors du conflit armé avec la Russie. Cet événement a montré toute l'importance de la sécurisation du cyberespace. Cette stratégie de cybersécurité s'intègre dans le processus de **refonte des stratégies et concepts de sécurité nationale**. La cybersécurité constitue l'un des **axes majeurs de la politique de sécurité nationale**. La coopération est là encore le maître mot de la démarche : **coopération** entre tous les ministères de l'Etat, **PPP**, **coopération internationale** (bilatérale et multilatérale). Les **menaces identifiées** sont celles de cyberguerre, cyberterrorisme, cybercriminalité. La mise en œuvre passera par des actions de recherche et analyse (analyser ce qui se fait à l'étranger, les expériences, etc.) ; créer un nouveau cadre législatif (le pays ne dispose pas encore de ce cadre juridique, et n'a pas ratifié la convention de Budapest) ; se rapprocher des institutions internationales (OECD, EU, OSCE, NATO, UN, ITU).

Ce type d'approche qui implique plusieurs ministères dans la mise en œuvre de la politique de cybersécurité suppose une forte **coordination des acteurs** : ministère de la justice, de l'intérieur, des affaires étrangères, de l'éducation… ont tous une tâche à accomplir dans le cadre de ce projet.

---

[5] Ministry of Communication and Information technology, Department of Electronics and information Technology, National Cyber Security Strategy – 2013 (NCSP-2013), 2 juillet 2013, 10 pages, New Dehli, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NationalCyberSecurityPolicyINDIA.pdf

[6] Government of Georgia, Cyber Security Strategy of Georgia 2012-2015, 2012, 12 pages, http://www.dea.gov.ge/uploads/National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf

1.5. La stratégie du Montenegro

Cette stratégie 2013-2017[7] offre un exemple d'approche de la **cybersécurité nationale par un petit Etat.** Ce dernier fait les mêmes constats que les nations plus puissantes, de dépendance au cyberespace, aux réseaux, et des risques induits ; le constat d'une **nécessaire approche holistique**, impliquant quantité d'acteurs de la société, voire pratiquement toutes les composantes de la société (privé, public, civil, militaire, industriels, société civile, etc.) qui n'ont pour autant pas nécessairement les compétences, les capacités, et qui ne vont surtout pas avoir de la cybersécurité les mêmes approches. Le document fait le constat du manque de ressources : « **L'un des problèmes est le manque de compétences** indispensables à une défense efficace contre les incidents ». « Un autre problème important est qu'au Montenegro il n'y a pas de système de surveillance ou enregistrement des trafic malicieux qui visent le pays »[8], « au Montenegro il n'y a qu'un faible nombre de personnels disposant du savoir spécialisé de haut niveau dans le domaine de la cyber sécurité »[9], « il n'y a pas, à l'Université du Montenegro, de facultés ou départements qui couvrent la cybersécurité et le forensics, c'est-à-dire qui produisent les ressources humaines disposant du savoir de haut niveau dans le domaine »[10]. Le document propose des **définitions** des notions essentielles (cyberespace, sécurité de l'information, sécurité de l'internet, cyberterrorisme, cyberespionnage, cyberguerre) Pour celle de la « cybersécurité », les rédacteurs ne prennent pas position, **rappelant simplement les définitions proposées par l'ISO, par les Pays-Bas et par l'UIT**. Il en est de même pour la définition de la cyberdéfense qui s'appuie sur la définition de l'OTAN.

1.6. La stratégie du Qatar

La stratégie du Qatar[11] se concentre sur les points suivants:

- Internet a connecté le Qatar au reste du monde comme cela n'avait jamais été le cas auparavant
- Internet réduit les barrières de la communication
- Le cyberespace « enrichit nos vies »
- L'effort de cybersécurité doit être partagé par tous les Etats connectés : « *Luckily, we do not have to face this formidable task of cyber security alone* »
- Le Qatar œuvre dans le sens des Etats qui veulent un cyberespace ouvert et sûr
- La protection des **infrastructures critiques d'information est une priorité** ; répondre aux cyberattaques ; définir un cadre juridique pour sécuriser le cyberespace
- Si **l'Etat joue un rôle central**, **la responsabilité doit être partagée dans la mise en œuvre de la cybersécurité** (entreprises, institutions, citoyens…)
- La politique du Qatar en matière de cybersécurité s'exprime également dans sa **participation à des instances internationales** (UIT notamment). La dimension internationale est essentielle dans le projet qatari.
- Les objectifs de sécurisation du cyberespace doivent permettre de préserver les **droits fondamentaux** et les **valeurs de la société qatarie** (« *Establish and maintain a secure cyberspace to safeguard national interests and preserve the fundamental rights and values of Qatar's society* »).
- Le document propose une annexe de **définitions** des termes essentiels. Les définitions reprennent ainsi celles de **l'UIT** (par exemple celle de la "cybersécurité", qui reprend la formulation de la résolution 181 de l'UIT)[12].

---

[7] National cyber security strategy for Montenegro 2013-2017, juillet 2013, 27 pages, https://www.unodc.org/res/cld/lessons-learned/national-cyber-security-strategy-for-montenegro-2013-2017_html/National_Cyber_Security_Strategy_for_Montenegro_2013-2017.pdf

[8] Page 4

[9] Page 13

[10] Page 13

[11] Qatar National Cyber Security Strategy, mai 2014, 34 pages, http://www.ictqatar.qa/sites/default/files/national_cyber_security_strategy.pdf

[12] https://www.itu.int/net/itunews/issues/2010/09/20.aspx

1.7. La stratégie de la Suisse

La Suisse publie en juin 2015 sa seconde Stratégie Nationale de Protection contre les Cyber-risques (SNPC)[13]. La précédente fut publiée en 2012[14]. Les points essentiels de la stratégie de 2015 les suivants:

- Constats des cyberattaques nombreuses, étatiques et cybercriminelles
- Des failles de sécurité perdurent, nombreuses
- Le monde prend conscience des risques
- La Suisse continue de suivre sa propre voie (l'individualité de la démarche est donc revendiquée)
- Ses objectifs : combattre les menaces pour se protéger contre les cyber-risques, pour renforcer les exigences inhérentes à une infrastructure digne de confiance
- La stratégie **identifie les menaces** et propose des solutions adaptées pour y faire face
- Les menaces n'ont pas de frontières
- **Collaboration internationale essentielle**. La Suisse tire bénéfice de sa présence à des postes de responsabilité dans des instances internationales : à la présidence du comité consultatif de l'ICANN ; présidence de l'OSCE ; participation à des exercices militaires de l'OTAN lorsque la Suisse a été présidente de l'OSCE elle a élaboré des mesures de confiance, visant à « une compréhension commune de la sécurité sur Internet ». La Suisse signe des accords avec les Etats pour partager les informations sur les failles et les incidents. Le partage de données est 1) délimité à des sujets précis et 2) encadré par des accords signés bilatéraux.
- **Le partage de connaissances** est également promu à l'échelle nationale.
- L'application des mesures inscrites au SNPC est réalisée de manière sectorielle
- Pour la réaction, renforcement des centres de compétence (les CERTS) existants
- **Evaluation des politiques de sécurité** : examen de l'efficacité des mesures de la première SNPC à compter de 2015
- Comme nombre d'autres stratégies de pays occidentaux, **les valeurs fondamentales** y sont mentionnées : liberté, responsabilité individuelle, droits de l'homme, droit à la vie privée…

1.8. La stratégie de Trinidad et Tobago

Publié en décembre 2012[15], ce document propose une **définition** de la cybersécurité (reprenant celle de l'UIT)[16], définit les enjeux stratégiques, le cadre de travail (gouvernance prévoyant notamment la création d'une agence nationale ; un système de gestion des incidents, en s'appuyant sur la création

[13] Confédération Suisse, Rapport annuel 2014 du comité de pilotage de la SNPC, juin 2015, 23 pages, http://www.news.admin.ch/NSBSubscriber/message/attachments/39700.pdf

[14] Les objectifs et moyens de la SNPC de 2012 : « détection précoce des menaces et des dangers dans le cyberespace et sur l'augmentation de la capacité de résistance des infrastructures critiques. Elle vise également une réduction générale des cyber-risques liés en particulier à la cybercriminalité, au cyberespionnage et au cyber-sabotage. » « Les seize mesures portent sur quatre domaines: la prévention, la réaction, la continuité et les processus de soutien. »

[15] Government of the Republic of Trinidad & Tobago, National Cyber Security Strategy, Prepared by the Inter-Ministerial Committee for Cyber Security, décembre 2012, 29 pages, http://www.nationalsecurity.gov.tt/Portals/0/Pdf%20Files/National_Cyber_Security%20Strategy_Final.pdf

[16] Telecommunication Standardization Sector, (ITU-T) Recommendation X.1205(X.cso), http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx La définition en anglais est la suivante: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment."

d'un CSIRT ; la **collaboration** de type **PPP**[17] et **internationale** ; le **droit**, avec l'adaptation du corpus juridique pour la lutte contre la cybercriminalité ; et la **valorisation d'une culture de la cybersécurité**) et les objectifs opérationnels. Ces approches sont dans le fond communes aux stratégies nationales de biens d'autres Etats, grands et petits.
Les **références** sur lesquelles s'appuient les auteurs du document pour formuler leur stratégie sont : l'UIT (à laquelle ils empruntent des principes, des définitions), Symantec (en puisant de l'information dans le 'Norton Cybercrime Report 2011'), le Forum Economique Mondial (dont ils reprennent des données statistiques) et des documents de politique, de cadrage étatiques. La pensée emprunte donc au moins autant à des sources extérieures que nationales.

1.9. La stratégie de Vanuatu

Le République de Vanuatu a publié en décembre 2013 sa politique de cybersécurité[18]. Les moteurs et déterminants de cette politique sont les suivants :

- Le pays se voit récemment relié à un Interchange Submarine Cable, qui apporte au pays un réseau de meilleure qualité. Cette ouverture, expose désormais aussi à plus de risques (« *The arrival of the Interchange Submarine Cable project will provide a highspeed reliable link for Vanuatu to the World. This means internet users at large are exposed to risks experienced by other countries…*").
- Le pays inscrit la définition de sa politique de cybersécurité dans une démarche de **coopération internationale** : soutien d'organisations internationales et régionales (UIT, programme ICB4PAC)
- **L'économie du tourisme** doit être la bénéficiaire de de cette stratégie : assurer la cybersécurité, c'est rassurer, accroître la confiance, c'est assurer que l'économie locale reposant sur le tourisme puisse fonctionner selon les normes modernes
- La stratégie adopte des méthodes communes à la majorité des Etats : créer des **organisations**/institutions (CERTs), adapter le système **juridique**, agir par le biais de la **coopération internationale**/régionale, tirer profit des structures préexistantes (dans le pays et la région), identifier tous les acteurs publics et privés qui agissent déjà dans le champ de la cybersécurité (cet axe, selon les pays, peut viser à la mise en synergie, la fédération, la coordination, la mise en réseau…), moyens de protection des mineurs en ligne, encourager le reporting des incidents

1.10. Le modèle du Commonwealth

L'organisation des télécommunications du Commonwealth propose aux Etats un guide de gouvernance du cyberespace et d'aide à la formulation de stratégies de cybersécurité[19].
Les enjeux sont connus : assurer la sécurité et la résilience de l'infrastructure d'information, dont dépend la croissance de l'économie mondiale.

- Le préambule du chapitre 3 prend en considération la spécificité inévitable que va revêtir chaque stratégie nationale «rappelant la nécessité pour chaque pays de **prendre en considération sa culture,** ses **priorités nationales**, les risques qu'il court et l'impact de ses stratégies à la fois sur le plan régional et global » [20] (évoquant ici une notion de **responsabilité** des Etats dans les choix qu'ils définissent. La cybersécurité n'est pas neutre, ses politiques et stratégies provoquent des effets). Chaque stratégie s'inscrit donc dans un

[17] PPP: partenariat public-privé
[18] République de Vanuatu, National Cybersecurity Policy, décembre 2013, 30 pages, http://ogcio.gov.vu/Cybersecurity%20Policy/Cybersecurity-Policy-EN-FR-BI.pdf
[19] Commonwealth Telecommunications Organisation, Commonwealth approach for developing national cybersecurity strategies, 2015, 37 pages, http://www.cto.int/media/fo-th/cyb-sec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20Strategies.pdf
[20] Page 5

contexte spécifique où de multiples facteurs vont entrer en ligne de compte. Plus encore, la cyberstratégie doit être le reflet de la culture du pays : «La stratégie devrait refléter les valeurs culturelles du pays » [21].

- L'approche attendue est « **multi-stakeholders** » : **PPP**, recherche académique, société civile, communauté internationale. Cette approche nécessite un **leadership fort**. Elle est justifiée par la nature de la cybersécurité («en raison de la nature de la cybersécurité, il est aussi impératif que la stratégie de cybersécurité nationale soit développée dans un partenariat multi-stakeholder » [22]) et du cyberespace (global). Si la stratégie est guidée et placée sous la **responsabilité des gouvernements**, ces derniers ne disposant pas toujours des ressources (financières, techniques, humaines) nécessaires à sa réalisation, elle devra être implémentée suivant une logique PPP ou gérer la rareté des ressources. Certaines actions relèveront alors du secteur privé. Il faudra prendre en compte et anticiper les effets de l'intervention de l'Etat sur l'activité industrielle.
- La conception de la stratégie doit être fondée sur une **approche gestion des risques** (identifier menaces, vulnérabilités, coûts…), être guidée par les effets recherchés, les objectifs clairement définis plutôt que par la prescription des moyens à utiliser, accorder des priorités (se focaliser sur ce qui est critique, urgent), pouvoir être mise en œuvre (la stratégie doit être réaliste, être réalisable) et intégrer les normes internationales (l'un des enjeux étant l'harmonisation, qui favorisera la coopération). L'approche proposée ici se réfère à des **méthodes préconisées par Microsoft** (pages 5, 6, 7, 16, 20, 28, 36). Cette intrusion du référent industriel, qui guide la norme, dans des démarches qui relèvent initialement du politique, doit interroger.
- Des mécanismes d'évaluation, la création d'indicateurs de performance doivent être définis.
- Les termes, notions, concepts sur lesquels s'appuient les stratégies doivent être définis. D'une langue à l'autre, les termes peuvent avoir des significations différentes.

II - Des cyberstratégies de la Défense

2.1. La stratégie américaine

Le Département de la Défense américain a publié en avril 2015 sa nouvelle cyberstratégie[23]. Le DoD a trois missions principales dans le cyberespace: défendre les réseaux, les systèmes et l'information du Département de la Défense ; défendre le territoire américain et les intérêts nationaux contre toute forme de cyberattaque importante ; soutenir ses opérations militaires.
La démarche propose plusieurs objectifs stratégiques :

- Construire et maintenir des forces et capacités pour mener des opérations dans le cyberespace
- Défendre le réseau du Département de la Défense
- Sécuriser les données du Département et réduire les risques
- Se tenir prêt à défendre le territoire américain et les intérêts vitaux du pays contre des cyberattaques perturbatrices ou destructrices, aux conséquences majeures
- Elaborer et préparer des options cyber viables, et planifier leur mise en application, pour contenir l'escalade du conflit et maîtriser l'environnement du conflit à tous les niveaux

[21] Page 5
[22] Page 5
[23] The DoD Cyber Strategy, avril 2015, Washington, 42 pages, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

- Construire et maintenir des alliances et partenariats internationaux solides, pour dissuader les menaces communes et accroître la sécurité et stabilité internationale.

Les variables qui sous-tendent les choix des objectifs et les conditions de leur mise en application sont :

- La spécificité technologique : le code, notamment grâce à l'internet des objets, brouille les frontières entre le cyber et le monde physique
- les valeurs : un internet ouvert, sûr, interopérable, liberté d'expression, respect de la vie privée, créativité, innovation
- La dimension géographique : les attaques peuvent venir de n'importe où dans le monde
- L'idéologie : les politiques de sécurité et défense doivent servir plusieurs objectifs (prospérité, sécurité, libre circulation du commerce et des idées
- La nécessité de gérer un équilibre entre bienfaits du net et vulnérabilités, risques, menaces
- La dimension économique : outre les menaces qui pèsent sur l'activité économique dans son ensemble, la stratégie en appelle clairement à investir massivement dans la cybersécurité (« sans d'importants investissements en cybersécurité et cyberdéfense, les systèmes de données restent exposés à des formes rudimentaires et dangereuses d'exploitation et d'attaque »)[24]
- Une lecture alarmiste, décrivant un environnement de menaces extrêmement large, sans aucune délimitation, puisque constitué des « acteurs étatiques et non étatiques »[25], agissant de n'importe quelle région du globe. La menace est globale : elle n'a pas de catégories précises d'acteurs, elle peut venir de n'importe où, elle peut frapper n'importe quand, n'importe quoi (tout ce qui est connecté), et au-delà viser les valeurs, et toute la gamme d'objectifs/motivations est concernée (objectifs politiques, économiques, militaires).
- la désignation de la menace (il faut mettre un nom dessus) dans le cyberespace : la Corée du Nord[26],
- La nécessité de répartir les rôles, les responsabilités : si tous les acteurs doivent sécuriser leurs propres systèmes (secteur privé, gouvernement, citoyens) pour contribuer à un état général de cybersécurité, au niveau des institutions étatiques « la cybersécurité est un effort d'équipe « , « pour réussir dans sa mission le département de la défense doit opérer en partenariat avec les autres départements et agences, les alliés et partenaires internationaux, les gouvernements étatiques et locaux et, le plus important, le secteur privé ». Au moins deux questions importantes sont soulevées dans cette formulation. Tout d'abord celle, sous-jacente, non formulée ici, de la responsabilité. Car le partenariat entre le Département et les autres ministères et agences implique-t-il une coordination tierce, par exemple de la Maison Blanche ? Une coordination de l'effort par l'un des départements ou agences ? Une coordination de la cybersécurité par l'armée ? Ensuite, l'accent mis sur le PPP, désormais conforme aux approches américaines mais aussi de la plupart des pays se dotant de politiques ou stratégies cyber, qui appuie toute stratégie de défense sur les relations avec l'industrie. Enfin, ces partenariats supposent un partage d'information, qui est l'une des problématiques centrales de toute forme de coopération cyber.
- Pour l'action dans la défense des intérêts de la nation, et notamment la conduite de contre-attaques cyber, le droit exerce une contrainte.

2.2. La stratégie chinoise

[24] page 1
[25] page 1
[26] page 2

La cyberdéfense n'est pas le produit d'une démarche isolée : la stratégie de défense dans laquelle elle va s'intégrer en définit, détermine les orientations. La cyberdéfense chinoise n'échappe pas à cette logique : elle s'inscrit dans le cadre de la stratégie de défense active qui caractérise la posture de la Chine.

La notion de défense active est introduite par le ministre de la défense Peng Dehuai et Mao Zedong en 1955 pour qualifier la doctrine militaire chinoise[27]. Cette doctrine militaire est exposée le 6 mars 1957 par Peng Dehuai dans un rapport (« On the Direction of the Fatherland's Military Doctrine and National Defense Construction ») à la Commission Militaire Centrale : coordination des moyens politiques, diplomatiques et militaires ; stratégie du « no first strike » ; être prêt à contre-attaquer face à une agression impérialiste (Etats-Unis), stabiliser la ligne de front, mener une guerre « protracted », priver l'ennemi de l'initiative de l'attaque ; d'une posture défensive passer à une posture d'attaque. Cette doctrine des années 1950 désigne donc déjà les Etats-Unis comme l'ennemi impérialiste. En 1977 la stratégie devient celle de la défense active, incitant l'ennemi à pénétrer profondément à l'intérieur des lignes (stratégie visant à laisser l'ennemi s'aventurer à l'intérieur du territoire pour le prendre ensuite en tenailles). Cette stratégie suppose qu'il n'est pas nécessaire de défendre toutes les positions. En perdre certaines, temporairement, peut au contraire s'avérer productif car permet de piéger l'ennemi. Dans les années 1980 la Chine en revient à une doctrine de défense active et délaisse celle de « *tempting the enemy in deep* ». En 1985, la défense active, selon Deng Xiaoping, implique un renforcement de la dissuasion, la promotion de la paix, et se tenir prêt pour des guerres locales de petite échelle, mais aussi lutter pour forger un environnement international plus favorable à la Chine. La stratégie du tempting the enemy in deep est délaissée et on lui substitue la défense de points clefs dès les premières phases de la guerre. La défense active n'est pas de la défense pure et simple. Elle contient la stratégie de « protracted war ». C'est dans ce contexte doctrinal qu'arrive à la fin des années 1980 – début des années 1990, la notion de guerres localisées technologisées (Fighting and Winning a Localized War Under Conditions of High Technology). La doctrine se focalise sur les guerres locales et non plus sur des guerres de grande ampleur, internationales.
La défense active s'applique à toutes les forces de défense chinoises ; elle suppose que la Chine ne frappera militairement qu'après avoir été frappée (par un adversaire qui n'est pas nécessairement militaire). Le premier coup peut aussi être non militaire, mais politique et stratégique, tout en appelant une réponse militaire (qui du point de vue tactique n'est pas alors considérée comme portant le premier coup). Cette défense active n'est donc réaliste qu'en maintenant une posture opérationnelle offensive[28]. La stratégie chinoise en mer de Chine est la traduction de l'application de la doctrine de défense active[29] définie pour cette dimension navale par Liu Huaqing en 1982. Transposée à la cybersécurité, la défense active évoque l'idée de contre-attaques (hack back) visant les hackers agresseurs. La défense active repose sur 5 principes : la veille, la détection, l'attribution, la prévention (ce qui peut être fait pour empêcher les attaques), la représaille (« retribution »[30], ou vengeance).
Les pratiques de la Chine sont aussi celles des autres Etats :

- Un discours pacifique et des pratiques guerrières/militaires/agressives
- Le cyberespionnage contre des puissances étrangères

[27] Yuan Dejin, Wang Jianfei, The historical evolution in the direction of military doctrine since the founding of New China, and the lessons from it, juin 2007, http://www3.nd.edu/~pmoody/Text%20Pages%20-%20Peter%20Moody%20Webpage/Military%20Doctrine.htm
[28] Anthony H. Cordesman, Ashley Hess, and Nicholas S. Yarosh, Chinese Military Modernization and Force Development A Western Perspective, CSIS, Washington, 23 août 2013, 73 pages, http://csis.org/files/publication/130725_chinesemilmodern.pdf
[29] Stacy A. Pedrozo, China's Active Defense Strategy and its Regional Impact, U.S.-China Economic and Security Review Commission, United States House of Representatives, First Session, 112th Congress, 2011, http://www.uscc.gov/sites/default/files/1.27.11Pedrozo.pdf
[30] http://www.welivesecurity.com/2013/11/19/active-defense-good-protection-doesnt-need-to-be-offensive/

- La projection de capacités militaires, y compris via le cyberespace
- L'influence
- La désignation d'adversaires/ennemis
- Des discours guerriers

2.3. La stratégie israélienne

Cette stratégie met en évidence quelques lignes directrices [31] :

- La cyberdéfense bénéficie du soutien des hautes instances politiques du pays. Il y a une prise de conscience au plus haut niveau.
- Cet appui politique permet de soutenir un rythme intensif d'augmentation des capacités de cyberdéfense (défensives et offensives)
- La cyberdéfense bénéficie d'un environnement industriel et de recherche favorable, avec des entreprises de pointe, des programmes étatiques de financement de la R&D bénéficiant aux capacités cyber civiles et militaires, à usage dual. Une relation étroite lie secteur civil et militaire. L'armée est l'un des fers de lance de l'innovation : les forces de défense recrutent de bons ingénieurs, les forment, les affectent à des unités de cybersécurité, à des unités de renseignement ; puis ces ingénieurs/cyberdéfenseurs alimentent le secteur des start-ups de hautes technologies. Le CyberSpark dont la création a été annoncée en 2014 est un exemple de cette recherche de symbiose entre les secteurs civils, militaires, de la recherche,de l'éducation[32].
- Israël conçoit un écosystème de cyberdéfense global, c'est-à-dire impliquant un large spectre d'acteurs (approche « multistakeholders ») qui combine renseignement, alerte, défense passive et active, capacités offensives dans les domaines civils et militaires. Surtout, la cyberdéfense ne peut pas être assurée via une approche compartimentée, d'un côté les civils, de l'autre les militaires.
- En Israël, la cyberdéfense est le moteur d'une interaction stratégique entre secteurs civils et militaires. Elle sous-tend une nouvelle économie, et fait office de « liant » entre les multiples acteurs.
- La cyberdéfense s'inscrit dans un contexte sécuritaire propre à Israël qui depuis plusieurs décennies fait face à des menaces hybrides, car combinant menaces conventionnelles, asymétriques, de faible intensité, non-linéaires, menace de prolifération d'armes de destruction massive, missiles balistiques, conflits de faible intensité, terrorisme, menaces traditionnelles à la sécurité[33]. Les enjeux de cyberdéfense sont venus ajouter à l'environnement de la menace.

Le rapport de Michael Raska a identifié les défis stratégiques du cyberespace, du point de vue des experts en cybersécurité/défense israéliens. Ces défis constituent l'ensemble des déterminants, des moteurs qui orientent les choix en matière stratégique et politique de cybersécurité/défense. Trois grandes catégories de déterminants sont définies : la dimension internationale (*foreign affairs*) et la défense ; société et économie ; secteur privé. La cyberdéfense doit être construite en prenant en compte ces variables. Reprenons ici l'ensemble des variables énumérées dans le rapport[34] :

- Pour la dimension internationale et la défense : la problématique de l'attribution ; la capacité à passer outre les défenses militaires ; l'enjeu de l'effacement de la frontière qui sépare

[31] Michael Raska, Confronting cybersecurity challenges : Israel's evolving cyber defence strategy, RSIS, Policy Report, 12 pages, janvier 2015, Singapour,

[32] Olivier Danino, Un aperçu des efforts israéliens dans le domaine cybernétique, Chaire de cybersécurité et Cyberdéfense, mars 2015, article 3.21, 5 pages.

[33] Michael Raska, Confronting cybersecurity challenges : Israel's evolving cyber defence strategy, RSIS, Policy Report, 12 pages, janvier 2015, Singapour. Page 3

[34] Michael Raska, Confronting cybersecurity challenges: Israel's evolving cyber defence strategy, RSIS, Policy Report, 12 pages, janvier 2015, Singapour. Tableau page 8

temps de paix et de guerre ; la convergence avec d'autres menaces asymétriques ; l'absence de règles et de normes ; développer une connaissance opérationnelle et des concepts pour le cyberespace que l'on puisse mettre en relation avec d'autres domaines du combat ; préserver l'avantage qualitatif des forces de défense, et son niveau de sophistication ; préserver les capacités de dissuasion et capacités offensives ; partage de renseignement entre organisation de la sécurité ; développer des niveaux de défense essentiels : renseignement, alerte, défense passive, défense active, offensif

- Pour les variables sociétales et économiques : l'absence de frontières ; réguler, définir les responsabilités dans le domaine cyber ; légiférer ; prendre en compte les menaces qui pèsent contre l'informatique invisible, comme l'on en trouve dans les systèmes de navigation ou les ordinateurs embarqués dans l'automobile ; aspects psychologiques ; dégradation du moral par des moyens cyber ; accroître la conscience du public et la résilience ; surveillance nationale globale
- Pour les variables concernant le secteur privé : interdépendance entre secteurs civil, militaire et commercial ; espionnage industriel ; soutenir l'innovation dans cybersécurité ; partenariats avec le secteur militaire.

III – Points de convergence et de différenciation

3.1. Définir les objectifs de la cybersécurité et y apporter des réponses. Construire une stratégie nationale de cybersécurité

Les projets de cybersécurité/défense convergent sur un ensemble de questions, de thèmes, d'approches, que présentent les trois tableaux ci-dessous, construits sur la base de trois rapports : le premier procède d'une étude de l'OCDE, le second d'un travail publié par l'UIT, et le troisième d'une étude sur les politiques de cybersécurité au sein de l'UE.

Objectifs affichés dans les stratégies nationales de cybersécurité	
La politique de cybersécurité est devenue dans nombre de pays une priorité de la politique nationale	Priorité, car internet et les TIC sont devenus essentiels pour l'économie, le développement de la société, et des infrastructures vitales. Les stratégies visent donc à protéger la société dans son ensemble et non plus des acteurs en particulier. Devenue priorité, car internet n'est plus seulement « utile », mais il est devenu « indispensable », « essentiel ».
Quand la politique de cybersécurité est une priorité, elle est soutenue par des responsables politiques	Cette prise en main par des responsables de haut niveau, souvent même au niveau des gouvernements, est indispensable à l'approche holistique
La cybersécurité est appréhendée de manière holistique, intégrée, globale	Holistique = prend en compte les aspects économiques, sociaux, éducatifs, juridiques, techniques, diplomatiques, militaires, de renseignement
Utilisation inégale des concepts : les stratégies n'utilisent pas toutes les notions de « cyberespace », « cybersécurité ».	On peut leur préférer la notion de « critical information infrastructure »

Nombre de concepts en commun	« enhanced governmental co-ordination at policy and operation levels » “Reinforce public-private co-operation” “improved international co-operation” “respect for fundamental values”
Des notions émergent	« souveraineté » « politiques flexibles » « aspects économiques de la cybersécurité »
Plusieurs générations de politiques de cybersécurité nationale : avant et après 2011-2012.	La différence : elles deviennent généralement holistiques.
La sécurité dans le cyberespace est un moteur de la prospérité économique et du développement social	
Les nouvelles politiques font de la souveraineté une question cruciale	Cette dimension était moins évidente dans les versions précédentes.
Il faut protéger les sociétés dépendant du cyberespace, de la menace des cyberattaques	Cette préoccupation n’est pas propre aux nouvelles stratégies. Elle apparaît dans les principes de l’OCDE formulés en 1992, pour la sécurité des systèmes d’information
Traiter les objectifs (protection contre les menaces, défendre la souveraineté) tout en préservant l’ouverture de l’internet	Cette ouverture est un prérequis, car elle permet de faire du cyberespace une plate-forme pour l’innovation et la création de nouvelles sources de richesse
Economie, société, gouvernements, dépendent d’Internet	Les cybermenaces qui se sont multipliées remettent en cause les conditions du développement des sociétés modernes dépendantes du net
Les stratégies sont toutes fondées sur la perception d’un environnement cyber de plus en plus menaçant, où les acteurs se diversifient, sont de plus en plus nombreux, de mieux en mieux organisés, de plus haut niveau, où les attaques sont de plus en plus importantes, intrusives, massives, perturbatrices, destructrices…	Configuration : menace toujours plus importante, phénomène qui ne semble pas devoir reculer. Mais aucune stratégie ne s’interroge sur le paradoxe suivant : toujours plus de cybersécurité, davantage de conscience des enjeux, toujours plus d’investissements, d’organisation dans la sécurité et la défense, mais rien ne semble arrêter ou ralentir la cybermenace.
Toutes les stratégies résultent de la prise en compte des cyber-risques croissants	Les Etats sont perçus comme de nouvelles sources de menaces. Il n’est plus uniquement question de menaces criminelles (individus ou organisations) ni de terrorisme.
Les nouvelles stratégies sont pensées en fonction d’objectifs de sécurité nationale	Les stratégies des années 2000 visaient à rétablir la confiance, pour une économie numérique…
Les Etats ne se concertent pas pour organiser leurs mesures, structures, institutions, mécanismes de cybersécurité. pas d’approche universelle.	On a donc des organisations nationales, à partir desquelles devra ensuite être organisée, pensée la coopération internationale. On ne retrouve pas cet effort de concertation préalable à la mise en œuvre de structures nationales, au niveau européen. On aura donc des organisations, des rôles, responsabilités différents d’un Etat à un

	autre, d'une structure à une autre ; des hiérarchies, des rapports à l'Etat distincts ; comme on a des corpus juridiques distincts. C'est donc « chacun pour soi », en ordre dispersé. Et cette dispersion se retrouve ensuite dans des enceintes internationales (APEC, Conseil de l'Europe, Union Européenne, G8, Forum pour la gouvernance de l'internet, OTAN, OCDE, OSCE, Organisation of American States, Nation Unies, UIT)
Les nouvelles stratégies intègrent des politiques industrielles en cybersécurité.	
Les stratégies mettent en avant la nécessaire intervention de l'Etat dans la coordination de politiques de cybersécurité	
Les stratégies définissent rôles et responsabilités en matière de cybersécurité	
Les stratégies font de la coopération public-privé un outil essentiel de la cybersécurité	
Les stratégies insistent sur la défense des valeurs fondamentales : liberté d'expression, respect de la vie privée, libre flux de l'information	
Les stratégies appellent à renforcer la coopération internationale	
Certaines stratégies soulignent l'opportunité économique que créent les politiques de cybersécurité	
Certaines stratégies créent les conditions d'une prise de décision partagée en matière de définition des politiques de cybersécurité	
Les plans d'actions renforcent les priorités identifiées dans les années 2000	« sécurité du gouvernement » « protection des infrastructures critiques d'information » « lutte contre la cybercriminalité » « accroître la prise de conscience » « éducation »
Les plans d'action affichent de nouvelles priorités :	« la nécessité de la R&D » « créer les conditions d'une industrie de cybersécurité forte » « prise en compte de secteurs d'activité spécifiques, essentiels à la vie de la nation »
Monitoring temps-réel des infrastructures du gouvernement	
Créer une industrie de cybersécurité plus forte	
Identification d'acteurs du marché ou secteurs économiques critiques, vulnérables	
Partenariats avec les fournisseurs de service internet	
Encourager les exercices de cybersécurité	
Créer des systèmes de protection des mineurs (lutte contre la pédopornographie, violences, …)	

Si la cybersécurité a besoin d'industries fortes, l'existence de ces dernières a besoin de soutien (amorçage, subventionnement, fiscalité, création d'emploi, mesures économiques…), de conditions favorisant l'innovation.	Si la cybersécurité est l'objectif, si celle-ci doit s'appuyer sur une industrie forte, notamment nationale (souveraineté technologique), indirectement la cybersécurité aura besoin de conditions économiques, de mesures fiscales, afin de favoriser cette industrie.
Il faut se préparer à l'éventualité d'une cyberattaque majeure	
La cybersécurité n'est pas figée.	Les politiques de cybersécurité ne sont pas figées. Elles ont évolué depuis les années 1990-2000, elles sont appelées à poursuivre leur évolution : « this new age of cybersecurity policy making is still in its infancy and will take time to further develop »[35].
Les stratégies adressent des acteurs de la cybersécurité (qui met en place la cybersécurité, qui en est responsable, qui doit mettre en œuvre de la cybersécurité, dans quelles conditions…)	Des règles particulières sont par exemple imposées à des opérateurs d'infrastructures critiques, aux entreprises de secteurs spécifiques. Il conviendra alors de prendre en compte l'effectivité des mesures édictées, des recommandations[36], puis la différence entre les règles, les normes, la théorie et les pratiques (en observant par exemple les pratiques sectorielles de cybersécurité : dans le secteur bancaire[37], de la finance[38], de la santé[39], etc.)

Objectifs recensés d'après l'étude de l'OCDE, *Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the internet economy*, 2012, 117 pages[40]. Cette étude compare les politiques de cybersécurité de 10 pays[41], en recherche les points communs et les différences.

Objectifs et déterminants	**Commentaires**
Les TIC sous-tendent la société moderne, sa croissance. Elles sont essentielles au progrès	Il n'y a donc pas d'autre choix actuellement que de se plier à cette évolution. Caractère impératif, inévitable. Aucun retour en arrière ne peut être envisagé (déconnexion, autres modes de communication, de fonctionnement…)
La cybersécurité est essentielle à la bonne	

[35] OCDE, Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the internet economy, 2012, 117 pages, page 10.

[36] Federal Communications Commission, Cyber Security Planning Guide, 51 pages, https://transition.fcc.gov/cyber/cyberplanner.pdf

[37] Andrew M. Cuomo, Report on Cyber Security in the Banking Sector, mai 2014, New York State, 13 pages, http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf

[38] Financial Industry Regulatory Authority, Report on cybersecurity practices, février 2015, 46 pages, https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

[39] Sans Institute, New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations, 2014, 29 pages, https://www.sans.org/reading-room/whitepapers/analyst/threats-drive-improved-practices-state-cybersecurity-health-care-organizations-35652

[40] OCDE, Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the internet economy, 2012, 117 pages , http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[41] Australie, Canada, France, Allemagne, Japon, Pays-Bas, Royaume-Uni, Etats-Unis, Finlande, Espagne.

marche de ce projet	
Les menaces à la sécurité nationale peuvent se propager via les réseaux	Coupure de l'électricité, des systèmes financiers…
Les acteurs de la menace sont nombreux	
Les outils dont disposent les acteurs de la menace sont de plus en plus sophistiqués	
La cybersécurité doit accompagner le développement technologique : mais ce n'est pas encore le cas	
Pour quelles raisons la cybersécurité n'a-t-elle pas été suffisamment prise en compte ?	Il faut considérer ces raisons, car elles pourraient de nouveau freiner, empêcher la mise en œuvre des nouvelles politiques de cybersécurité. On peut voir plusieurs raisons : - L'absence de coordination, de régulation. Laisser l'initiative libre aux acteurs ne suffit pas à créer les incitations nécessaires, car la cybersécurité c'est avant tout des coûts, à intégrer - L'absence de coordination, au sein des Etats, mais encore plus à l'échelle internationale, de sorte que les cybersécurités se mettent en place en ordre dispersé et de manière éclectique (plusieurs solutions différentes)
La cybersécurité se met en place à des rythmes inégaux et de manière distincte d'un environnement à un autre	Les raisons en sont multiples : - Des taux de pénétration du net différents - Une dépendance au cyberespace variable (des sociétés sont plus connectées que d'autres) - Existence ou non d'industries de cybersécurité - Stratégies gouvernementales
La cybersécurité émerge selon un processus bottom-up	
Des disparités entre Etats	
Des disparités entre public et privé	
Des disparités entre entreprises	
Manque d'une culture globale de cybersécurité	
Nécessité de partager l'information pour lutter contre les menaces qui n'ont pas de frontières	
Les spécificités des menaces qu'il s'agit de contrer : sans frontières, …	
Nécessaire coopération	
Coopération et partage impliquent d'organiser une multitude de disciplines : juridique, technique, éducation	
Si un Etat ou un acteur a mis en place des mesures de cybersécurité efficaces, le savoir est rarement partagé	Raisons, freins au partage de données et à la coopération : - Sensibilité des données

	- Mauvaise publicité que de reconnaître avoir été attaqué (ne pas perdre la face, ne pas perdre de clients, image)
En l'absence de coopération, certains choisissent la sécurité via l'obscurité	
La cybersécurité doit être implémentée dans tous les strates de la société	D'où la difficulté, contrainte majeure
Les moteurs et incitations à la cybersécurité dans toutes les strates de la société sont inadaptés, insuffisants	- Les contraintes de coûts sont bloquantes - Conscience insuffisante
Publier des classements des Etats en fonction de leurs niveaux de cybersécurité[42] pourrait être une incitation	- Classer suffit-il à motiver ? - Tout classement repose sur des mesures, des évaluations, des processus, la définition de critères de mesures, des variables. Il y a une forte part de subjectivité. - Noter les bons élèves suffit-il à motiver les moins bons ? - Concurrence des classements portant sur la cybersécurité, avec ceux traitant de la cybermenace, ou de la cyber puissance.
Développer des capacités de cybersécurité nécessite des investissements politiques, économiques et en ressources humaines	Cette approche globale nécessite de légiférer, éduquer, sensibiliser, convaincre, et de s'adresser au politique, au secteur économique, aux développeurs de technologies, d'inciter au partenariat public-privé, à la coopération.

Objectifs de la cybersécurité, selon l'UIT et l'entreprise ABI Research[43].

Principes	
Création d'institutions	Création de l'ENISA en 2004 afin de faciliter le

[42] L'UIT et ABI Research décrivent dans ce rapport le projet GCI (Global Cybersecurity Index) qui vise à établir des mesures des niveaux de cybersécurité des Etats. Les indicateurs constituant l'indice de mesure développé par le projet, s'appuient sur les 5 axes de travail définis par l'UIT dans le cadre du Global Cybersecurity Agenda (GCA) : mesures juridiques (indispensables, car elles déterminent ce qui est légal ou non, et permettent de mettre en place les mesures de sécurité : institutions judiciaires, législation contre la cybercriminalité, régulation. Il s'agira ici d'évaluer le corpus juridique, l'existence d'institutions, de processus, d'application du droit), mesures techniques (définies dans le projet comme la première ligne de défense contre les cybermenaces, concernant l'existence de CERT/CIRT/CSIRT, de normes, de certifications), mesures organisationnelles (politiques de cybersécurité, lignes directrices pour la gouvernance, responsabilités des agences), développement de capacités (standards, ressources humaines, certification), coopération (internationale, inter-agences, public-privé). Les indicateurs de performance choisis mesurent donc les résultats atteints dans des domaines qui sont autant de variables clefs, de déterminants de la cybersécurité, les variables qu'il faut activer, idéalement, pour parvenir à une bonne cybersécurité.

[43] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Conceptual_Framework.pdf L'UIT et AB Research publient également en avril 2015 un rapport mesurant la cybersécurité dans le monde, résultat de l'application du GCI. UIT/ABResearch, Indice de cybersécurité dans le monde et profils de cyber bien-être, avril 2015, 528 pages, Genève, http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-F.pdf « L'indice GCI fournit des informations sur le niveau d'engagement des Etats souverains en matière de cybersécurité » (p.1) L'indice évalue le niveau d'engagement de chaque pays dans 5 domaines : « cadre juridique, mesures techniques, structures organisationnelles, renforcement des capacités et coopération internationale » (p.1) Sur la base de ces mesures/évaluations, un classement mondial est établi.

	partage de données, informations sur les menaces, la sécurité, et accroitre les bonnes pratiques au sein de l'UE Contraintes : l'institution seule ne répond pas à tous les besoins. L'institution est-elle utile ? Quel rôle peut-elle jouer ?
La cybersécurité s'invite à l'agenda politique de l'UE en 2007 après les attaques contre l'Estonie	Déterminant, moteur : les faits majeurs ou perçus comme tels
Dépendance de la société au cyberespace, aux réseaux, aux NTIC	Urgence, indispensable
Les NTIC sont indispensables à la stratégie de croissance de l'UE	
Contraintes : conjuguer respect des valeurs, normes, principes de l'UE et contraintes de cybersécurité, maintenir un cyberespace libre et ouvert	Pas de concessions sur les valeurs, au motif de la cybersécurité Est-ce ce qui se passe dans la réalité ?
L'UE publie de nombreux documents, formule des recommandations, crée de la norme (directives, règlements). L'UE est une machine à créer de la norme et des publications.	L'approche doit être moins fragmentée pour gagner en efficacité. Mais est-ce possible ?
Au sein même de l'institution européenne, la cybersécurité est dispersée au travers du large corpus de directives et régulations de diverses natures.	Ce phénomène n'est pas spécifique à l'Union Européenne. Le corpus réglementaire/juridique des Etats-Unis est particulièrement complexe, constitué d'un véritable entrelacs de textes, de normes, lois, directives, décisions, règles.
Le corpus de normes européennes n'intégrait pas la cyberdéfense jusqu'en 2013, date de la cybersecurity strategy de l'UE	
La stratégie de cybersécurité n'en est qu'à ses débuts. Elle devra être évaluée.	Comment évaluer l'efficacité d'une politique de cybersécurité ?
Accords de coopération internationaux	Exemple : EU-China 2020 strategic agenda for cooperation (2013) Les accords internationaux formulent des principes généraux : « *a peaceful, secure, resilient and open cyber space », » « promoting mutual trust and cooperation through such platforms as the EU-China Cyber Taskforce* ». La coopération avec la Chine est encore davantage au niveau du discours, des intentions déclarées, que de la mise en pratique, de l'effectivité. Les perspectives, objectifs, stratégies s'opposent.
Des promoteurs, responsables, acteurs de la cybersécurité émergent. Pour l'UE, la cybersécurité est surtout l'affaire de : - la DG Justice and Home Affaires, du NIS (Network and Information Security), qui traite surtout de la protection des	L'identité des promoteurs/responsables, oriente donc les perspectives, les orientations de la cybersécurité : ici les aspects juridiques/justice (*enforcement*), économique (marché intérieur), sécurité.

infrastructures critiques et des infrastructures d'information. - De la DG Connect	
Option privilégiée par l'UE : le multistakeholderism	Vision qui trouve sa raison : - dans la multiplicité des acteurs de l'internet impliqués dans sa gestion et son utilisation - dans l'idée que la responsabilité doit être partagée Plusieurs Etats font obstacle à cette approche : Russie, Chine, Iran, Inde… qui estiment être sous-représentés dans les institutions actuelles de la gouvernance, et jugent trop importante la place des Etats-Unis.

Tableau : Caractéristiques de l'UE en matière de cybersécurité[44].

3.2. Répartition des rôles, responsabilités, pouvoirs et des capacités

L'un des points récurrents des multiples projets de cybersécurité réside dans la création de nouvelles institutions, organisations : de nouvelles unités, cellules, de nouveaux commandements « cyber » sont créés au sein des forces, de nouvelles agences, des centres de surveillance, sont créés au niveau des Etats, et la cybersécurité devient aussi l'affaire du plus grand nombre dans une approche qui privilégie l'implication de services et acteurs d'horizons multiples (approche « multi-stakeholders », c'est-à-dire à plusieurs parties prenantes). Les projets de cybersécurité et défense entrainent des modifications des structures, organisations, organigrammes, de nouvelles distributions des rôles, des domaines d'attributions, des responsabilités, de nouvelles expertises.

3.2.1. Qui doit avoir le leadership sur la cybersécurité ?

Lorsque l'US Air Force, pionnière, annonce en 2007 son projet de création de Cyber Commandement, les réactions au sein de l'armée la contraignent rapidement à mettre un terme à son projet, perçu comme une volonté d'hégémonie sur le domaine cyber, une tentative en quelque sorte, de prise de pouvoir au sein de l'institution de la Défense. Chaque branche de l'armée a entamé dès les années 2005-2006 des réflexions sur la manière de gérer le cyberespace, chaque domaine se considérant comme différent, ayant ses particularités, ses contraintes, devant avoir ses propres solutions. En 2010 la création du Cyber Commandement vient apporter une réponse globale, en prenant le lead sur la dimension cyber au sein de la Défense, même si ensuite sont créées au sein de chaque arme, air, marine, terre, des cyber commandements propres. Pour l'US Air Force, la 24th Air Force assurera ce rôle. On reconnaît donc la spécificité de chaque type de force, en créant une structure transversale cyber.

Qui doit avoir le leadership dans l'organisation de la cybersécurité nationale ? Qui doit avoir le leadership dans la gestion des réponses aux cyberattaques étatiques ?[45]

Il ne semble pas y avoir de modèle de leadership de la cybersécurité bien établi mais quelques formules ressortent tout de même[46] :

[44] George Christou, The EU's Approach to Cyber Security, Policy paper series, 2014, 13 pages, http://privatewww.essex.ac.uk/~susyd/EUSC/documents/EUSC%20Cyber%20Security%20EU%20Christou.pdf

[45] Levon (Rick) Anderson, Countering State-Sponsored Cyber Attacks: Who Should Lead?, dans *Information as Power. Section Two: Information Effects in the Physical Domain*, 22 pages, file:///D:/daventre/Downloads/nps45-030210-06.pdf

[46] Kevin P. Newmeyer, Who should lead U.S. cybersecurity efforts?, PRISM 3, n°2, pp.115-126, 2014, Etats-Unis, http://cco.dodlive.mil/files/2014/02/prism115-126_newmeyer.pdf

- Selon le CSIS, la cybersécurité doit être placée sous la responsabilité d'un czar placé aux côtés du Président des Etats-Unis[47]. Il s'agit de centraliser le pouvoir au sein de la Maison Blanche.
- Une seconde approche, américaine, opte pour une responsabilité assurée au niveau des ministères (par exemple au niveau du DHS, ou du Département de la Défense en raison de la concentration de compétences et capacités que l'on trouve au niveau militaire[48], avec la NSA et désormais le cyber commandement. Le DHS ne dispose pas de telles capacités humaines et matérielles)
- Une dernière option, toujours du point de vue américain, consisterait à créer une agence, un nouveau département spécifique pour la cybersécurité et qui viendrait exister à côté du DHS et du DoD (et autres Départements). D'autant qu'il y a des précédents : le DoD fut créé en 1947 face à l'émergence des nouvelles menaces amenant à la guerre froide ; le DHS fut créé en 2002 en réponse aux attentats du 11 septembre 2001. Regrouper la cybersécurité au sein d'une même entité aurait pour avantage de regrouper les opérations défensives et offensives. Mais nécessairement puisant à diverses institutions pour se constituer, ce nouveau département devrait lui aussi être confronté aux résistances dues à la combinaison de cultures organisationnelles différentes[49].

Dans un article intitulé *Who Should Lead U.S. Cybersecurity Efforts ?*[50], publié en 2012, Kevin P. Newmeyer rappelle les quelques options qui s'offrent en matière de leadership de la cybersécurité:

- Centraliser la direction des politiques de cybersécurité en confiant la mission à un cyber czar. Cette stratégie est défendue par le CSIS (Center for Strategic and international Studies) dans son rapport *Securing Cyberspace for the 44th Presidency*[51]. Cette solution qui concentre le pouvoir au sein de la Maison Blanche n'est pas satisfaisante, selon K. P. Newmeyer. La guerre contre la drogue a adopté ce modèle, et échoué. D'autre part, cette direction de la cybersécurité pêcherait par l'absence d'autorité sur le plan budgétaire.
- La direction de la cybersécurité doit être assurée au niveau des Départements, notamment celui du DHS, ce dernier étant responsable des incidents au niveau intérieur. Certains estiment que cette option est insuffisante, que le DHS ne dispose pas des capacités et de l'expérience nécessaire (contrairement à la NSA), et n'a pas su démontrer jusque-là qu'il savait atteindre le niveau suffisant. Ce modèle manque également d'autorité sur les autres agences. Le DHS a un rôle de coordination de l'action des différents départements en matière de sécurité des systèmes et réseaux, mis à part ceux de la défense, mais chacun d'entre eux reste responsable de la sécurité de ses propres systèmes. Le Département de la Défense reste en effet responsable de la sécurité/défense de ses propres systèmes, classifiés et non classifiés, et des infrastructures critiques liées à la défense.
- La troisième option estime qu'une restructuration plus profonde s'impose pour prendre en charge la triade de la cybersécurité : gouvernement au niveau fédéral, des Etats et au niveau local. Le Département de la Défense devrait alors assumer ce rôle, notamment en raison de l'expérience dont dispose la NSA. Mais pour l'auteur cette solution ignore les limites

[47] CSIS, Securing Cyberspace for the 44th Presidency, décembre 2008, Washington, 96 pages, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

[48] Paul Rosenzweig, 10 Conservative Principles for Cybersecurity Policy, Backgrounder No. 2513, Washington, DC, The Heritage Foundation, 2011, www.heritage.org/research/ reports/2011/01/10-conservative-principles-for-cybersecurity-policy

[49] Kevin P. Newmeyer, Who should lead U.S. cybersecurity efforts?, PRISM 3, n°2, pp.115-126, 2014, Etats-Unis, http://cco.dodlive.mil/files/2014/02/prism115-126_newmeyer.pdf

[50] Kevin P. Newmeyer, *Who Should Lead U.S. Cybersecurity Efforts ?,* Institute for National Strategic Studies, Prism 3, n°2, 2012, p.115-126, Washington DC.

[51] CSIS, *Securing Cyberspace for the 44th Presidency,* décembre 2008, 96 pages, Washington DC.

juridiques imposées par le Posse Comitatus Act, qui limite juridiquement l'action militaire dans les affaires domestiques.

L'organisation de la cybersécurité dépend de plusieurs facteurs :

- Une dimension historique et juridique : la politique de cybersécurité américaine trouve ses origines dans la politique initiée sous l'administration Clinton, focalisant ses efforts sur la protection des infrastructures critiques. En 1996, l'Executive Order 13010 sur la protection des infrastructures critiques insistait déjà sur la menace que constituaient les cyberattaques pour la sécurité nationale. Cet Executive Order créait la Commission pour la Protection des Infrastructures Critiques, laquelle formula des recommandations, ensuite traduites dans la Presidential Decision Directive 63 (PPD 63). Cette directive institua le National Coordinator for Security, Infratructure Protection, and Counterterrorism, venant en soutien au Coordinator and National Infrastructure Protection Center. La directive met aussi en place des modalités de partenariat public-privé sur lesquelles s'appuient la cybersécurité (création d'Information Sharing and Analysis Center – ISACs). L'administration Bush se serait ensuite davantage focalisée sur la menace des attaques terroristes physiques, et non cybernétiques. La stratégie nationale pour la sécurité du cyberespace[52] publiée en 2003 n'aurait pas les qualités d'une véritable stratégie globale. De même, la Comprehensive National Cybersecrity Initiative de 2008 ne propose-t-elle pas de stratégie suffisamment globale, se focalisant sur le .gov. Sous l'administration Bush les responsabilités auraient été diluées (entre la Maison Blanche, le DG et le DoD). L'administration Obama publie en 2009 la « 60-Day Cyberspace Policy Review » fait un état de l'art de la cybersécurité du point de vue du gouvernement, mais ne propose pas encore de ligne directrice et de solutions. Ce travail formule l'idée clef du CSIS, sur la nécessité d'une centralisation au niveau de la Maison Blanche, qui se traduira en décembre 2009 par la nomination d'un cyber czar. L'International Strategy to Secure Cyberspace, de mai 2011, positionne les Etats-Unis sur la scène internationale mais ne formule pas de stratégie pour la politique de cybersécurité intérieure. De fait, en 2012, le gouvernement n'a toujours pas, selon K.P. Newmeyer, définit de stratégie globale de cybersécurité, définissant une organisation structurée, de leadership clair sur la politique de cybersécurité américaine.

3.2.2. Les déterminants de la création des forces cyber

C'est par analogies avec l'histoire de la création d'autres forces que l'on peut essayer d'anticiper et identifier les facteurs qui vont décider de l'orientation des forces cyber en cours de constitution depuis quelques années dans le monde. L'analogie avec les forces spéciales américaines[53], confirmée notamment par les méthodes de recrutement des forces cyber, qui s'inspireraient de celles utilisées pour les forces spéciales[54], offre un angle d'approche intéressant des défis qui attendent les forces cyber, cyber commandements et autres organisations/institutions au sein des organigrammes de la Défense.

De l'analogie avec les forces spéciales (SOF - Special Operation Forces) nous retiendrons les points suivants :

[52] The National Strategy to Secure Cyberspace, 2003

[53] Christopher Paul, Isaac R. Porche III, Elliot Axelband, The other quiet professionals, Lessons for Future Cyber Forces from the Evolution of Special Forces, Rand corporation, Etats-Unis, 2014, 84 pages, http://www.rand.org/content/dam/rand/pubs/research_reports/RR700/RR780/RAND_RR780.pdf

[54] Andrew Tilghman, As cyber force grows, manpower details emerge, 23 septembre 2014, MilitaryTimes, http://archive.militarytimes.com/article/20140923/NEWS/309230050/As-cyber-force-grows-manpower-details-emerge

- Cette organisation est aujourd'hui bien établie. Mais son histoire ne fut pas un parcours linéaire, car elle dut affronter de nombreuses résistances au cours des années 1970-1980, traverses des étapes, affronter des épreuves. L'institution s'est notamment construite dans l'action (ses interventions dans des conflits comme la guerre du Vietnam, la guerre du Golfe…), ses succès mais aussi ses échecs. Les SOF ont été confrontées dans leur histoire à des périodes de réductions drastiques (budgétaires, ressources humaines), en raison de tensions entre elles et les forces conventionnelles, mais aussi en raison de l'image qu'elles avaient auprès des politiques, décideurs. Ces difficultés sembleraient, a priori, étrangères au développement actuel des cyber-forces au sein de la défense américaine et dans les grandes nations qui ont placé le cyber au rang de priorité, de domaine transversal. L'analogie semble donc s'arrêter là, tant les conditions d'exercice et le sort réservé aux forces cyber, paraissent indispensables et bénéficient aujourd'hui de budgets en hausse quand le reste de la défense subit au contraire des réductions de ses dotations. Mais l'histoire des forces cyber, même si elle peut être inscrite dans le prolongement d'unités ou services qui ont été déplacés, renommés, restructurés (on fait du cyber, du réseau, du traitement de l'information, de la collecte de données, depuis plusieurs décennies), reste encore relativement jeune. Rien ne permet de présager de l'évolution à long terme. Retenons donc simplement de l'histoire des SOF la leçon suivante : l'histoire des organisations, des institutions, n'est pas linéaire. Celle des forces cyber n'y échappera pas. Quelles en seront alors les dynamiques, qu'est-ce qui pourrait ralentir les processus actuels, qu'est-ce qui pourrait remettre en question les investissements, l'organisation, la fonction dévolue aux cyber-commandements ? Un changement d'appréciation des priorités au niveau gouvernemental (faire reculer la cybersécurité dans le classement des priorités de sécurité et défense nationale) pourrait constituer l'un des moteurs de changements (réductions de crédits, d'effectifs, nouvelles stratégies). Il suffirait à cela des gouvernements moins réceptifs aux promoteurs du cyber désastre.
- Les cyber-forces américaines sont nouvelles et gagnent en importance dans l'organisation militaire. Mais la création de l'US Cyber Command ne fut pas, dès le départ, un parcours sans heurts, sans réticences manifestées. Aujourd'hui, rien n'assure qu'à l'avenir les forces cyber seront telles qu'elles sont aujourd'hui. Le cyber commandement gagne en autorité, en visibilité, mais des défis demeurent.
- Le choix de la taille critique, de la bonne structure, organisation des forces
- La bonne définition des rôles, missions, attributions
- Les problématiques de recrutement, formation, exercices, carrières, gestion des ressources humaines, critères de sélection, profils psychologiques des individus[55]. Sur le plan de la gestion des ressources humaines, des premières années d'expérience, on constate que les forces cyber de la défense américaine ont dû faire preuve d'imagination :
    - pour mettre en œuvre de nouvelles modalités de recrutement, de tests
    - pour s'assurer le concours de bons profils, et gérer la concurrence avec le secteur privé plus rémunérateur (en offrant par exemple des avancées de carrière plus rapides)[56]
    - pour inciter les recrues à rester au sein de l'armée suffisamment longtemps
    - pour diversifier les viviers de recrutement, en allant puiser à l'extérieur de l'armée, mais aussi de manière interne, en détectant les potentiels et les compétences

[55] Ces questions sont abordées dans l'article suivant: Isabelle Tisserand, Les ressources humaines : éléments constitutifs fondamentaux de la cyberdéfense. Anthropologie numérique et médicale, novembre 2013, article 2.5, Chaire cybersécurité et cyberdéfense, http://www.chaire-cyber.fr/IMG/pdf/article_2_5_-_chaire_cyberdefense.pdf

[56] Andrew Tilghman, As cyber force grows, manpower details emerge, 23 septembre 2014, MilitaryTimes, http://archive.militarytimes.com/article/20140923/NEWS/309230050/As-cyber-force-grows-manpower-details-emerge

    - offrir des environnements d'entraînement spécifiques
    - essayer de maintenir dans le giron militaire les officiers qui quittent l'armée (en les incitant à devenir membres de la réserve, ou devenir des civils du département de la défense).
- L'analogie se justifierait par la dimension des forces. Les forces spéciales sont de dimension réduite ; celles du cyber le seraient également[57] ; dans les deux cas, ce sont les compétences, qualités individuelles qui priment ; dans les deux cas, il y a une différence culturelle entre les forces cyber/spéciales et les forces conventionnelles, leurs missions diffèrent des opérations conventionnelles ;

Le développement des capacités militaires s'appuie fortement sur le PPP. La relation au secteur privé est particulièrement importante :

- l'armée rechigne à se substituer à un secteur privé qui n'assume pas ses responsabilités (les infrastructures critiques sont majoritairement entre les mains du privé aux Etats-Unis ; qui doit en assurer la défense ?) ;
- l'armée est un client majeur de l'industrie cyber; l'armée est un acteur économique majeur[58]. Le Département de la Défense finance l'innovation au travers de ses projets[59].

3.2.3. Les résistances de l'institution aux priorités : le cas d'IPv6

Les priorités imposées aux institutions rencontrent dans leur réalisation de multiples obstacles. Des choix stratégiques qui paraissent s'imposer, évidents, peuvent se voir totalement bloqués par ceux qui ont la responsabilité de leur implémentation, à l'exemple de la mise en œuvre programmée mais non réalisée d'IPv6 au sein de l'armée américaine. Une commission d'enquête américaine a récemment fait le constat de la réticence des responsables militaires successifs, depuis une dizaine d'années, à effectuer une migration d'IPv4 vers IPv6, objectif pourtant affiché dès le début des années 2000 comme prioritaire, utile, vital, impératif. La Défense a déjà expérimenté une transition, lorsqu'il s'est agi de passer de NCP vers TCP/IP. L'utilité et nécessité d'une migration d'IPv4 vers IPv6 est formulée au sein de la défense américaine depuis plus de 10 ans[60]. Le mémorandum publié en 2003 prévoyait d'achever la transition d'ici 2008. De nouvelles deadlines furent définies : 2012, 2014. La migration d'IPv4 vers IPv6 a plusieurs raisons :

- Offrir une solution au manque d'adresses IP (le Département de la Défense américain possède 18% des adresses IPv4 mondiales)
- Permettre aux réseaux militaires IPv6 de traiter et partager plus de données
- satisfaire à des considérations de sécurité

La stratégie de migration, choisie par le Département de la Défense américain, consistait à maintenir une architecture double, IPv4 et IPv6.

Une enquête de l'inspection générale du département de la défense conclut cependant en 2014 qu'IPv6 n'a pas été implémenté selon les recommandations au sein du DoD[61] :

- Les mesures n'ont pas été prises pour migrer vers IPv6

---

[57] Christopher Paul, Isaac R. Porche III, Elliot Axelband, The other quiet professionals, Lessons for Future Cyber Forces from the Evolution of Special Forces, Rand corporation, Etats-Unis, 2014, 84 pages

[58] Cheryl Pellerin, Carter Unveils New DoD Cyber Strategy in Silicon Valley, 23 avril 2015, US Department of Defense, http://preview.defenselink.mil/news/newsarticle.aspx?id=128659 «But in addition to the dangers there are great opportunities to be seized through a new level of partnership between the Pentagon and Silicon Valley," he added, "opportunities that we can only realize together."

[59] Cheryl Pellerin, Carter Seeks Tech-sector Partnerships for Innovation, 23 avril 2015, Washington, US Department of Defense , http://www.defense.gov/news/newsarticle.aspx?id=128655

[60] DoD Chief Information Officer (CIO), Internet Protocol Version 6 (IPv6), 9 juin 2003.

[61] DoD Needs to Reinitiate Migration to Internet Protocol Version 6 (Redacted) (Project No. D2014-D000RB-0068.000), http://www.dodig.mil/pubs/report_summary.cfm?id=6080, http://www.dodig.mil/pubs/documents/DODIG-2015-044.pdf

- Les responsables de l'information (DoD Chief Information Officer), la DISA (Defense Information Systems Agency) et le cyber commandement (USCybercom) (responsabilités définies dans le "Department of Defense Internet Protocol Version 6 Transition Plan, Version 2.0," de juin 2006), n'ont pas fait d'IPv6 une priorité ; de sorte qu'ils n'ont ni coordonné leurs efforts, ni mobilisé les ressources disponibles nécessaires ; et n'ont pas doté le département de la défense d'un plan d'action et de jalons permettant de migrer.
- Ce retard pourrait d'autre part être très couteux pour le Département, et multiplier les vulnérabilités.

Le constat semble sans appel : les institutions n'ont pas fait leur travail, les responsables n'ont pas rempli leur mission. Il semble des actions soient menées au sein des branches de l'armée mais que fasse défaut une coordination de l'ensemble : au sein de l'US Navy, la direction du C4I (Command, Control, Communications and Intelligence) des tests ont été menés ; le Space and Naval Warfare Systems Command a demandé la réalisation de tests sur les réseaux opérés par la DISA… Mais tel n'est pas le cas de toutes les armes : l'US Air Force a même fermé son bureau en charge de la transition vers IPv6 en 2012 ; l'US Army a défini un plan d'action en août 2004 mais celui-ci n'avait toujours pas été approuvé en 2014.

Le cyber commandement a donné la priorité à la défense des réseaux IPv4 et n'a pas considéré que la transition vers IPv6 soit un impératif opérationnel. Le responsable C4I de l'US Cyber Command affirme que la migration a été bloquée en raison des contraintes de limitations budgétaires. Le même cyber commandement n'a pas opté pour IPv6 car les risques potentiels de la transition sont mal connus. Il y a des conflits d'interprétations quant aux bénéfices et risques induits par la transition. Les responsables ne prendraient pas la pleine mesure des bénéfices que l'armée peut tirer d'IPv6 notamment pour l'amélioration des capacités de combat, d'autant qu'IPv4 ne serait plus suffisant dans ce contexte particulier (créer un réseau opérationnel en Irak aurait pris 2 mois, quand la même opération avec IPv6 ne nécessiterait que quelques heures). La réticence du cyber commandement réside dans le manque de maîtrise de la cybersécurité sous IPv6, qui rendrait plus vulnérable que le fait de se maintenir sous IPv4, protocole connu, maîtrisé. IPv6 soulève de nouveaux problèmes de sécurité[62], et ne résout pas tous les problèmes de sécurité d'IPv4[63]. Visiblement, la Défense ne veut pas expérimenter les vulnérabilités et imperfections de jeunesse du protocole, attendant, voire incitant les autres acteurs à l'expérimenter avant de l'adopter : ainsi pouvait-on lire en 2010 que le département de la défense américain demandait à ses fournisseurs réseaux de déployer IPv6 sur leurs propres réseaux pour l'expérimenter et corriger les bugs de leurs produits[64]. La configuration du marché pourrait donc expliquer le retard pris par le DoD dans l'implémentation d'IPv6 : ses fournisseurs ne sont pas en mesure de lui vendre des matériels ayant fait leurs preuves. Le marché ne serait donc pas encore assez mature, ne répondrait pas aux normes de la défense.

D'autres raisons de nature organisationnelle ont été avancées pour expliquer la non-réalisation du projet. Les répartitions des rôles, des responsabilités et attributions des tâches définies dans les plans d'action au milieu des années 2000 n'ont pas été mis à jour et ne prennent donc pas en compte les évolutions des organisations elles-mêmes (le Cyber Commandement par exemple n'existait pas encore). Les plans ne sont donc plus adaptés. L'inspection générale du Département de la défense réaffirme malgré les freins constatés, le caractère impérieux de cette migration[65].

---

[62] Atik Pilihanto, A complete guide on IPv6 attack and défense, Sans Institute, novembre 2011, 76 pages, http://www.sans.org/reading-room/whitepapers/detection/complete-guide-ipv6-attack-defense-33904

[63] University of Pennsylvania, A Fresh Look at Internet Protocol Version 6 (IPv6) for Department of Defense (DoD) Networks, août 2010, 33 pages, http://www.researchgate.net/publication/235071006_A_Fresh_Look_at_Internet_Protocol_Version_6_(IPv6)_for_Department_of_Defense_(DoD)_Networks

[64] Carolyn Duffy Marsan, U.S. military strong-arming IT industry on IPv6, 20 décembre 2010, Networkworld, http://www.networkworld.com/article/2197203/lan-wan/u-s--military-strong-arming-it-industry-on-ipv6.html

[65] Inspector General, U.S. Department of Defense, DoD Needs to Reinitiate Migration to Internet Protocol Version 6, 1° décembre 2014, Etats-Unis, 52 pages, http://www.dodig.mil/pubs/documents/DODIG-2015-044.pdf

3.3. Relations internationales

Une récente étude[66] publiée par le CERI s'est intéressée à l'identification des déterminants des décisions politiques en matière de défense, plus spécifiquement aux facteurs qui incitent les décideurs à opter pour la coopération internationale ou au contraire pour l'autarcie, dans le cadre des politiques d'acquisition de biens militaires. Cette étude rappelle notamment que la coopération internationale n'est qu'une option parmi d'autres. La définition de la politique de cybersécurité peut dépendre de multiples facteurs, mais la dimension internationale y joue un rôle majeur. Un Etat définit ses politiques et stratégies de sécurité et défense en fonction de sa perception des menaces, du rôle qu'il entend jouer sur la scène internationale, de l'image qu'il veut envoyer de lui-même aux autres.

3.3.1. La perception de la menace

Un Etat adapte ses politiques et stratégies en fonction de sa perception des menaces. Le dilemme de sécurité explique ainsi des choix en matière de sécurité et défense, et notamment le principe de la course aux armements. Le Japon par exemple, définit sa politique de cyberdéfense en fonction de sa perception des intentions de la Chine, dont les capacités militaires ne cessent de croître.

Une approche réaliste privilégie l'existence d'une menace extérieure. Il faut s'en protéger, et dans un système international par nature anarchique, il faut en priorité compter sur soi-même. Cet argument réaliste est omniprésent dans les discours de cybersécurité : les menaces, sans frontières, viennent de l'extérieur essentiellement. Cette logique est en œuvre lorsque les Etats-Unis ou des pays occidentaux accusent la Chine ; quand la Corée du Sud accuse Pyongyang, etc. Il faut donc protéger l'intérieur, le sanctuaire, des menaces qui viennent de l'extérieur via les réseaux. La cybersécurité ajoute la menace intérieure (*insider threat*). Mais celle-ci peut être liée au terrorisme (venu de l'étranger), ou au « traitre » (Edward Snowden s'est réfugié à l'étranger ; il est accusé de faire le jeu de la Russie et de la Chine qui auraient eu accès grâce à lui à des informations classifiées). On retrouve cette notion de « menace extérieure » dans les discours sur la souveraineté technologique, qui considère comme seules dignes de confiance les technologies issues des industries nationales, et suspectes celles qui proviennent de l'autre côté de nos frontières.

3.3.2. La place que l'Etat veut occuper sur la scène internationale et l'image qu'il entend créer

Les quelques Etats dont nous avons proposé une lecture des cyberstratégies ne sont pas tous de taille identique, de puissance identique, n'ont pas tous la même dimension, le même poids géopolitique, économique, technologique, etc.

Les Etats forts, dominants, sont susceptibles d'influencer les Etats de puissance moindre. La République de Vanuatu par exemple, a de toute évidence formulé sa stratégie au terme de dialogues avec des institutions internationales, qui ont pu orienter, volontairement ou non, la formulation finale. Cette volonté de mise en conformité avec ce qui serait une « norme » internationale, transparaît également dans la dimension juridique du projet de cybersécurité : l'objectif de la stratégie est « d'assurer que le cadre juridique des Vanuatu soit totalement en phase avec les meilleurs pratiques internationales ».

Les organisations internationales peuvent peser sur les décisions des Etats : l'appartenance à l'OTAN ou à l'UE autorise-t-elle une totale autonomie des choix politiques et stratégiques cyber ? Les pays africains vont-ils se conformer, dans la définition de leurs politiques nationales, au termes contenus

[66] Samuel B.H. Faure, La cooperation internationale dans le secteur de l'armement, CERI, Sciences Po, Paris, Questions de recherche, n°46, juin 2015, 45 pages, http://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/qdr46.pdf

dans la Convention de l'Union Africaine sur la cybersécurité et la protection des données personnelles, adoptée en 2014[67] ?

La cybersécurité peut aussi être utile à la promotion de la puissance d'un Etat, à sa reconnaissance par la communauté internationale. La cybersécurité peut jouer le rôle, pour des petits Etats, de facilitateur d'intégration dans la communauté internationale. L'Estonie[68] par exemple, par le biais de la cybersécurité, est parvenue à se faire entendre sur la scène internationale en s'impliquant dans des processus normatifs. L'Estonie a joué un rôle moteur, tout d'abord en faisant office d'exemple, de cas d'école, de démonstration des théories de la cybermenace et de risque de cyber Armageddon. La réalité a probablement été reconstruite, déformée, pour accéder au rang d'exemple, et de symbole des conflits modernes.
La prise de conscience qu'elle a contribué à développer dans les organisations internationales (OTAN, UE) a attiré les regards sur elle. L'Estonie a aidé à pousser la cybersécurité au rang d'enjeu prioritaire, a probablement contribué à accélérer la création du CCD COE. Sa voix est entendue, reconnue. Son premier ministre Andrus Ansip a été nommé Commissaire européen pour le marché unique numérique. Le Département d'Etat américain écrit sur son site[69] que l'Estonie est un allié clef des Etats-Unis et un leader reconnu pour les questions de cybersécurité et de liberté de l'internet. La cybersécurité est devenue l'un des domaines d'excellence de l'Estonie, l'un des outils de la construction de la reconnaissance de sa puissance. Le pays a probablement aussi bénéficié du rôle de promoteur qu'a joué son président, Toomas Hendrick Ilves, ce qui nous renvoie à l'importance des trajectoires individuelles des promoteurs des thèses de la cybersécurité.

La cyber sécurisation des petits Etats acquiert une dimension stratégique majeure dans le contexte actuel des relations internationales : la cybersécurité des pays baltes par exemple, où la Russie tend à faire pression, peut constituer une résistance stratégique.

On peut également formuler l'hypothèse que pour les Etats aujourd'hui les politiques ou stratégies de cybersécurité sont devenues indispensables, non seulement en raison des enjeux de sécurité qu'elles doivent traiter, mais pour leur rôle de norme : un Etat qui dispose d'une politique de cybersécurité est un Etat moderne, industrialisé, un acteur de la transformation du monde.

3.3.3. Le bilatéral

La coopération internationale en cybersécurité dépendra de plusieurs variables : l'appartenance de l'Etat à un ensemble régional, à des organisations internationales, l'existence d'accords entre pays dans d'autres domaines de sécurité et défense, le partage de normes, d'intérêts, l'influence ou attraction de grandes puissances, etc.

Rappelons ici quelques avantages du bilatéral sur le multilatéral :
- Moindre complexité de gestion que le multilatéral
- Des domaines de collaboration « à la carte », adaptables au cas par cas, calibrage des engagements respectifs
- Possibilité de choisir des partenaires qui partagent des intérêts, des organisations communes, des valeurs communes, des systèmes juridiques compatibles

[67] African Union convention on cyber security and personal data protection, 27 juin 2014, 40 pages, http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf
[68] Liina Areng, Lilliputian states in digital affairs and cyber security, The Tallinn Papers, n°4, 2014, CCDCOE, 15 pages, https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_04.pdf
[69] http://www.state.gov/r/pa/prs/ps/2013/218234.htm

- Plus rapides à négocier
- Il est plus aisé de maintenir secret un accord bilatéral que multilatéral
- Est plus adapté aux enjeux sensibles
- en matière de cybersécurité, l'un des principaux intérêts du bilatéral réside dans la nécessité de partager de l'information (plus facile à négocier qu'en multilatéral). Le bilatéral paraît particulièrement adapté à la cybersécurité, mais d'autres formats, sans oublier les relations informelles, peuvent être mobilisés utilement[70].

Partenaires	Date
Japon – Etats-Unis[71]	Juin 2011
Etats-Unis – Inde[72]	Juillet 2011
Australie – Etats-Unis[73]	Septembre 2011
Inde – Royaume-Uni[74]	Février 2013
Russie – Etats-Unis[75]	Juin 2013
Argentine – Brésil[76]	Septembre 2013
Canada – Etats-Unis[77]	2014
Inde – Corée du Sud[78]	Janvier 2014
Japon – Israel[79]	Mai 2014
Chine – Russie	Mai 2015
France – Singapour[80]	Mai 2015
Inde – Mongolie[81]	Mai 2015
USA – Japon[82]	Juin 2015

Tableau : Quelques accord, plans d'action bilatéraux de cybersécurité

3.4. Le PPP : l'enjeu du partenariat public-privé

Le principe d'un partenariat public-privé (PPP) semble généralement faire figure de passage obligé des politiques de cybersécurité. Le principe trouve probablement ses raisons dans le constat d'une

[70] James Andrew Lewis, Cyber security : turning national solutions into international cooperation, CSIS, Washington, Significant Issues Series, Vol. 25, n°4, 2003

[71] http://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-051-en.html

[72] United States and India Sign Cybersecurity Agreement, 19 juillet 2011, http://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement

[73] http://www.nbcnews.com/id/44527648/ns/technology_and_science-security/t/cyber-security-added-us-australia-treaty/#.VZOtJfntmko

[74] http://news.softpedia.com/news/UK-Prime-Minister-to-Sign-Cybersecurity-Agreement-With-India-330712.shtml

[75] Ellen Nakashima, U.S. and Russia sign pact to create communication link on cyber security, 17 juin 2013, The Washington Post, Etats-Unis, https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html

[76] Accords de défense et cyberdéfense. http://rt.com/news/brazil-argentina-cyber-defense-879/

[77] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-eng.aspx

[78] https://www.academia.edu/7531236/INDIA_STRENGTHENS_TIES_WITH_SOUTH_KOREA_IN_CYBER_SECURITY

[79] http://osnetdaily.com/2014/05/japanese-israeli-bilateral-defense-accords-cover-cyber-cooperation-against-china-north-koreairan/

[80] http://www.channelnewsasia.com/news/singapore/singapore-s-cyber/1854750.html

[81] http://www.mea.gov.in/bilateral-documents.htm?dtl/25252/List_of_AgreementsMoUs_exchanged_during_the_visit_of_Prime_Minister_to_Mongolia_May_17_2015

[82] https://threatpost.com/u-s-and-japan-to-cooperate-on-cybersecurity-information-sharing/113103

répartition inégale des capacités et compétences, au sein d'un Etat, d'un Etat à l'autre, entre secteurs privés et public ; et dans la certitude qu'un croisement de ces ressources et capacités est du meilleur effet pour la cybersécurité. Le PPP doit donc créer de la valeur-ajoutée, en l'occurrence accroître l'efficacité des politiques de cybersécurité. Le partenariat public-privé est-il synonyme en toutes circonstances d'efficacité ? Les modèles de partenariats sont multiples[83] , plusieurs options s'offrent donc théoriquement aux acteurs :

- Objectifs :
  - Recherche d'efficacité
  - Rapidité
  - Gains de coût
  - Force d'action accrue
  - Plus de flexibilité
- Conditions :
  - Confiance
  - Souplesse, adaptation, ne pas être contraint par des rigidités culturelles
  - Conception initiale (de laquelle dépend en grande partie le succès)
  - Evaluation des ressources
  - Soutien des directions des acteurs impliqués
  - Missions clairement définies
  - Des partenaires adéquats
  - Management du partenariat

Rachel Nyswander Thomas constate que nombre de PPP n'ont pas fait leurs preuves, en raison de l'absence de définitions initiales d'objectifs clairs, de stratégies de coordination, ou encore parce que le partage d'information est souvent pris comme un objectif en soi et non comme un outil[84].

Le PPP est peut-être aussi l'expression d'un Etat qui souhaite orienter la politique industrielle, garder sous sa coupe des pans entiers de l'industrie, ou au contraire refléter la volonté d'industries qui souhaitent renforcer leur présence dans le domaine étatique, pour y puiser par exemple des financements, des subventions, y trouver des marchés en cybersécurité (notamment de substitution à d'autres marchés en perte de vitesse). Le PPP peut autoriser un rééquilibrage des capacités, des ressources. L'Etat s'est longtemps lui-même présenté comme sous-dimensionné en termes de capacités techniques et humaines par rapport au secteur privé, capable de capter les meilleurs éléments (individus) par des salaires attractifs et des perspectives de carrière que n'offre généralement pas la fonction publique. Le PPP prenait donc place, il y a une dizaine d'année, en matière de cybersécurité, dans un contexte de déséquilibre au bénéfice du privé. Depuis les Etats ont renforcé leurs capacités, recruté, formé, crée des institutions et recruté pour cela des ingénieurs de haut niveau, venant accroître les ressources aussi bien civiles que militaires et de renseignement. Aujourd'hui des formations d'ingénieurs sont créées pour former des spécialistes de la cyberdéfense. Des compétitions sont organisées pour détecter les talents. L'Etat multiplie les initiatives pour créer les viviers dont il a et aura besoin pour la cybersécurité/défense.

[83] Rachel Nyswander Thomas, Securing cyberspace through public-private partnership. A comparative analysis of partnership models, mai 2012, CSIS, Washington, 62 pages, http://csis.org/files/publication/130819_tech_summary.pdf

[84] Rachel Nyswander Thomas, Securing cyberspace through public-private partnership. A comparative analysis of partnership models, mai 2012, CSIS, Washington, 62 pages, http://csis.org/files/publication/130819_tech_summary.pdf

Le partage d'information s'inscrit également dans le cadre du PPP. Le partenariat public-privé incite au partage d'information (l'expression « sharing information » revient dans les divers documents, sans toutefois en préciser les contours). Mais le partage, public-privé, ou entre institutions étatiques, au niveau national ou international, a ses limites. Le récent rapport de la Rand Corporation sur le dilemme du défenseur souligne d'ailleurs dès ses premières lignes que « la cybersécurité est, en partie, un monde du secret[85]. Les organisations chargées de protéger l'information de la divulgation sont naturellement enclines à masquer certaines des pratiques qu'elles utilisent pour cacher cette information »[86].

Le recours au PPP pour assurer la cybersécurité des infrastructures critiques américaines remonte à la fin des années 1990[87]. Pour assurer ce PPP, une structure de coordination fut alors créée, sous contrôle de la Maison Blanche. Le partage d'information est déjà requis comme instrument au service de la cybersécurité et impose la création de centres d'analyse et de partage de l'information chez les opérateurs d'infrastructures critiques. Dans la période post-11 septembre 2001, les centres d'analyse sont placés sous la responsabilité du DHS. Mais en l'absence de législation contraignant les acteurs, la création des centres d'analyse et le PPP était laissé à la libre initiative, au volontariat, du secteur privé. En 2007 l'administration Bush introduit la Comprehensive National Cybersecurity Initiative (CNCI), qui assure la transition de politiques orientées vers les infrastructures critiques, vers la cybersécurité. En 2009 la cyberspace policy review[88] (B. Obama) demande à ce que soient levées les barrières au PPP.

3.5. La cybersécurité comme moteur d'une politique économique

Les choix des politiques de cybersécurité et leur mise en application dépendent de facteurs économiques :

- L'existence ou non d'un secteur industriel de la cybersécurité, l'existence d'une industrie logicielle ou du hardware, d'opérateurs de télécommunications, d'intégrateurs, conditionnent le réalisme des ambitions formulées. La souveraineté technologique reste en effet en bien des domaines, irréaliste, en raison de l'absence d'industries propres.
- Lorsque les industries existent, constituent un tissu économique puissant, elles peuvent aussi peser de tout leur poids sur les décideurs. De sorte que la politique ou stratégie de cybersécurité qui en résulte sera tout autant le produit de décisions prises par le politique, prises dans l'intérêt des objectifs de sécurité et de défense, que la poursuite d'intérêts économiques.
- La cyberdéfense est une opportunité économique : la lutte contre les menaces alimente une économie, une industrie, crée des emplois ou promet d'en créer, de nouveaux marchés se sont ouverts, offrant des perspectives de développement conséquentes. Le marché, pour continuer à prospérer, a besoin de l'appui des politiques qui vont soutenir (subventions, politique fiscale) les industries existantes, naissantes (innovation, tissus de start-up) ou en reconversion (industries de l'armement qui trouvent dans la cyberdéfense de nouveaux débouchés). La cybersécurité/défense est parfois considérée comme une voie de reconversion pour des industries locales, régionales : la région de Long Island, aux Etats-Unis, qui fut un bastion de l'industrie de défense, pourrait, selon ses promoteurs, devenir le

[85] "secrecy" dans le texte

[86] Martin Libicki, Lillian Ablon, Tim Webb, *The Defender's Dilemma,* Rand Corporation, 162 pages, 2015, http://www.rand.org/pubs/research_reports/RR1024.htm

[87] White House, Presidential Decision Directive 63: Policy on Critical Infrastructure Protection, (Washington, DC: U.S, Government Printing Office, 1998).

[88] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).

terreau des prochaines générations d'entreprises high-tech de la cybersécurité[89]. En France, la politique portée par le Ministre de la Défense Jean-Yves le Drian, tend à concentrer les ressources de cyberdéfense en région Bretagne. Israël appuie une partie de son économie sur son industrie de hautes technologies, où la cybersécurité/défense occupe une place essentielle.

[89] Bill San Antonio, Rep. Israel writes L.I. could lead the way in cyber défense, The Island Now, 15 janvier 2015, http://www.theislandnow.com/news/rep-israel-writes-l-i-could-lead-the-way-in/article_3077e81a-9d04-11e4-b3c7-d770640f26c2.html

Conclusion

Cette première approche oublie très certainement un ensemble de variables économiques, politiques, sociologiques, stratégiques, qui mériteront une analyse plus approfondie.
Le but n'était pas de proposer une lecture exhaustive de la question, plutôt d'éclairer la complexité de l'objet « cybersécurité/défense » dans ses composantes, dans ses déterminants.
Une politique ou une stratégie peuvent être formulées en des termes quasi identiques d'un Etat à l'autre, le phénomène étant aidé en cela par les « modèles » ou « guides » proposés par des organisations internationales, ou par l'influence des acteurs majeurs de la scène internationale en matière de cybersécurité et défense. Mais la transposition de principes, de modèles, d'un contexte à un autre, ne saurait masquer les différences, les stratégies propres, les moteurs, les effets, les dynamiques qui se mettent en place.
L'objectif serait de pouvoir distinguer les objectifs de cybersécurité en tant que tels, des objectifs qui prennent la cybersécurité comme pur instrument.

Ce rapport ne fait qu'ébaucher quelques pistes de réflexion. Pour mieux saisir les différences qui se cachent derrière des discours homogènes, convergents dans la forme, il sera nécessaire de systématiser l'identification et l'analyse des principaux déterminants des politiques de cybersécurité/défense. La cybersécurité n'a pas le même sens, la même fonction, dans tous les Etats. Elle n'est pas construite sur les mêmes bases, elle ne peut donc pas fonctionner de la même manière, ni poursuivre et atteindre les mêmes objectifs. Dans son effort d'identification des déterminants, Dennis van den Berg choisit un modèle d'analyse reposant sur trois variables : le cadre juridique ; les agences et leurs responsabilités ; la coopération internationale. Les déterminants identifié sont : le développement technologique ; le taux de pénétration d'internet dans la société ; les dépenses militaires. L'étude tente d'isoler le déterminant le plus significatif des politiques de cybersécurité. Ce déterminant est la dépense militaire, qui seule expliquerait des variations dans les écarts d'appréciations des développements de politiques de cybersécurité[90]. Il n'y aurait pas de corrélation (sur la base d'une approche statistique) entre taux de pénétration de l'internet et politiques de cybersécurité, ce résultat allant à l'encontre de la littérature habituelle qui suggère au contraire que l'on attend des pays à taux de pénétration élevés qu'ils accordent plus d'importance à la cybersécurité dans leur agenda politique. L'étude est incomplète sur ce point, elle n'explique pas les raisons de cette absence de corrélation.

Les trois catégories de déterminants qui nous paraissent devoir être étudiées sont de nature politique (la gouvernance du cyberespace ; les relations internationales…), économique (stratégies industrielles ; marchés de cyberdéfense ; déterminants des investissements en cybersécurité/défense des nations…) et stratégique (pouvoir, puissance, perception de la menace, impact de la nature du régime politique prenant les décisions…) Ces approches ne devront pas écarter la dimension sociologique : Quel est le rôle des trajectoires individuelles dans la définition des politiques de sécurité nationales ? Lorsque l'Amiral Mike Rogers prend la tête de la NSA et du cyber commandement en 2014, l'une de ses recommandations consiste à rappeler l'importance d'une étroite et intense collaboration entre la défense (cyber) et l'industrie[91]. Cette recommandation semble a priori rappeler le principe qui guide les politiques de cybersécurité et défense d'un large ensemble de pays du monde (prônant pratiquement tous le PPP). Mais cette relation étroite entre le privé et le militaire, entre un secteur marchand et un secteur qui doit maîtriser les secrets de la

[90] Dennis van den Berg, Determinants of cybersecurity policies, Erasmus Universiteit Rotterdam, International Public Management and Policy (IMP), 2014, Rotterdam, 134 pages, page 70-71
[91] Dan Verton, Rogers downplays NSA moonlight controversy, 29 octobre 2014, Fedscoop, http://fedscoop.com/rogers-downplays-nsa-moonlighting-controversy

sécurité nationale, a rapidement suscité des interrogations et motivé des enquêtes, dès lors que des personnels de la NSA partageaient, tout en continuant à y exercer leurs missions, moitié de leur temps dans des entreprises privées (d'autant que l'entreprise en question, IronNet Cybersecurity Inc., avait été fondée par Keith Alexander, alors lui-même directeur de la NSA (2005-2014) et du Cyber Commandement. Son entreprise facturerait, dit-on, 1 million de $ par mois les services de cybersécurité, sur la base de technologies brevetées et développées avec le soutien de Keith Alexander lorsqu'il était directeur de la NSA). Une autre responsable au sein des services de la NSA, Teresa Shea, directrice du SIGINT, a créé son entreprise, Telic Networks, entreprise de Sigint et Elint, dont elle est la présidente. Mais elle est également employée par DRS Signals Intelligence, un contractant de Telic Networks. Outre les questions de conflit d'intérêt que cela suscite, les risques également de fuites de données professionnelles vers le secteur privé, on s'interrogera naturellement sur la portée des discours prononcés tout au long de l'exercice de leur fonction en qualité de responsables de la cybersécurité/défense. La « menace » et la « sécurité » sont-elles alors véritablement les moteurs de leurs discours, de leurs actions ? La menace n'est-elle pas un argument profitable aux intérêts personnels, privés, financiers ?

L'étude prendra aussi en compte la dimension bureaucratique, la sociologie des organisations pour appréhender les effets de la culture des organisations et leur contribution à l'émergence de forces cyber et d'une culture de la cybersécurité.

Table des matières