CEIS

LA NOUVELLE INITIATIVE DE DÉFENSE STRATÉGIQUE AMÉRICAINE DANS LE CYBERESPACE

Guillaume Tissier

Les notes σtratégiques

Les notes stratégiques

Policy Papers – Research Papers

Les idées et opinions exprimées dans ce document n'engagent que les auteurs et ne reflètent pas nécessairement la position de la société CEIS.

A propos de CEIS

- CEIS est une société de conseil en stratégie dont les actions couvrent l'ensemble de la chaîne de valeur du circuit de décision : de la réflexion stratégique à la mise en œuvre opérationnelle.

- La spécificité de CEIS est de s'appuyer sur un fort socle informationnel pour accompagner ses clients dans le développement et la sécurisation de leurs activités en France et à l'international grâce à des solutions innovantes de business & market intelligence, de gouvernance des risques et de management de l'innovation.

- CEIS intervient à 80 % pour des clients privés (grands groupes, clusters et pôles de compétitivité, PME-PMI) et à 20 % pour des clients publics (ministères, administrations françaises et européennes, collectivités territoriales). Elle a notamment développé des expertises dans les secteurs suivants : défense et sécurité, IT, transport et logistique, énergie, industrie pharmaceutique, grande distribution, agro-alimentaire, banque et assurance.

- CEIS comprend une centaine de consultants et est implantée à Paris, Lille et Metz. Elle possède par ailleurs des bureaux ou filiales à Bruxelles, Moscou, Kiev, Pékin, Astana (Kazakhstan), Doha (Qatar) et Abou Dhabi (Emirats arabes unis).

Sommaire

Introduction

La puissance « cyber » américaine se fragilise sous l'effet combiné d'un changement de taille d'Internet et de son centre de gravité. Conséquences logiques : les nouveaux pays connectés réclament une part de gouvernance, tandis que certaines plaques du réseau mondial échappent quasi totalement aux acteurs américains.

A cette fragilisation de la domination américaine au plan « cyber » s'ajoute en toile de fond l'érosion de la puissance scientifique des Etats-Unis. « Les Etats-Unis ne sont plus le colosse de la science, dominant le paysage de la recherche mondiale et la production de publications scientifiques, comme c'était le cas il y a 30 ans. Ils partagent maintenant ce domaine, sur une base quasi égalitaire, avec l'Union européenne et la région Asie-Pacifique »[1].

Face à ces trois constats, les Etats-Unis ont engagé depuis 2009 une offensive « dans » et « par » le cyberespace qui ressemble trait pour trait à l'Initiative de défense stratégique lancée par le Président Ronald Reagan en mars 1983. On en retrouve notamment :

- La dimension idéologique (le développement d'un internet universel, libre et ouvert pour le plus grand bénéfice de l'humanité) ;
- Une certaine instrumentalisation de la menace, parfois largement fantasmée ;
- La priorité accordée à l'innovation technologique. Il s'agit de concentrer tous les moyens publics et privés pour maintenir et accentuer le « gap technologique » avec les adversaires ;
- La forte implication du secteur privé ;
- Le rôle prééminent accordé au Département de la Défense ;
- La recherche de nouveaux concepts de défense, et notamment de défense active ;
- Et enfin l'implication de pays alliés avec le développement d'une nouvelle forme de défense collective.

Quelles sont les composantes de cette nouvelle guerre des étoiles version « cyber », notamment au plan industriel et technologique ? Quels en sont les premiers résultats ? La cybersécurité est-elle le seul enjeu ? Quels enseignements pouvons-nous en tirer ?

[1] Global research report United States, Thomson Reuters, 2010

Une prise de conscience

Le cyberespace, enjeu de puissance

On a longtemps perçu le cyberespace comme un environnement universel, autorégulé et sans frontières, bref « exceptionnel » au sens premier du terme… De fait, sa gouvernance technicienne l'a pendant longtemps mis à l'abri des enjeux et rivalités politiques, laissant le moteur économique et commercial être le principal artisan de sa croissance. Les Etats avaient d'ailleurs pour la plupart largement sous-estimé l'ampleur de la révolution internet et ses conséquences globales sur la société, considérant que le sujet était purement « technique ».

Qu'on le veuille ou non, cette époque est révolue. Le cyberespace a changé de taille (2 milliards d'internautes aujourd'hui contre 250 millions début 2000) et de centre de gravité (500 millions d'internautes chinois contre 220 millions aux Etats-Unis). Les affrontements se multiplient. Signe de maturité ou rançon du succès, le fait politique envahit progressivement la « toile », tandis que les Etats cherchent aujourd'hui à s'approprier cet espace pour y exercer leur souveraineté. Le cyberespace est donc logiquement devenu un enjeu de puissance, à la fois théâtre d'affrontements numériques, mais également « objet » de conflits idéologiques, politiques, diplomatiques ou économiques.

Répartition des internautes en 2015[2] :

Ce constat conduit rapidement à s'interroger sur la notion de puissance cybernétique et sur le lien entre puissance et cyberespace. Le cyberespace constitue un vecteur de puissance à part entière mais agit surtout comme un « multiplicateur » de puissance. Principaux leviers : les infrastructures de télécommunication (points d'échange internet, connectivité internationale, datacenters…), les capacités scientifiques et techniques (centres de recherche, brevets…), la base industrielle et technologique (hardware, logiciel, services et contenus), la sécurité et la régulation des réseaux et les capacités de cyberdéfense.

[2] *http://www.conceptualdevices.com/ENG/Human%20World/Internet_Users_Animation.html*

Une réponse en deux temps

Pendant les années Bush, la réponse est d'abord sécuritaire et très militaro-centrée. Elle est par ailleurs quasi-exclusivement technologique et met de côté l'humain (d'où le traumatisme causé par l'affaire Wikileaks). Par opposition aux visions russes et chinoises qui mettent l'accent sur la composante informationnelle du cyberespace, les Etats-Unis théorisent le concept de « cyber war », d'affrontement entre machines. Le cyberespace devient le 5ème espace de bataille. On élabore une doctrine dans une sorte de bouillonnement et d'effervescence intellectuelle. On crée des premières règles d'engagement. Un Cyber Command est laborieusement mis sur les rails.
Dans un deuxième temps, avec l'arrivée de Barack Obama, la posture évolue et se veut plus équilibrée, moins militaro-centrée, et surtout globale. L'enjeu n'est pas simplement militaire ou sécuritaire : le « cyber » peut agir comme un multiplicateur de puissance globale. L'administration Obama développe donc en quelques années une vision très structurante du cyberespace avec pour objectif de maintenir et d'accentuer la suprématie américaine dans cet espace grâce au « cyber power »[3]. On y retrouve aussi la volonté d'intégrer la communauté internationale et de créer une sorte de « parapluie cyber » associant les pays alliés dans un système de défense collective.

Une approche de plus en plus décomplexée

La posture américaine est soutenue par une approche de plus en plus décomplexée du cyberespace. Les révélations, a minima tolérées par la Maison Blanche, sur l'origine de Stuxnet dans le livre écrit par le journaliste David E. Sanger[4], le lancement du projet « plan X » de la DARPA sur un système de « cyber warfare » (voir plus loin), la diffusion publique d'offres d'emploi pour des postes d'analystes spécialisés en « Computer Network Attack » (CNA) ou « Computer Network Exploitation » (CNE) : tout témoigne de la volonté des Etats-Unis d'imprimer leur marque dans le débat sur le cyberespace afin de préparer les opinions publiques à ce type d'affrontement et d'amener progressivement les compétiteurs sur ce terrain où ils sont à leur avantage.

James A. Lewis, du Center for Strategic and International Studies[5] explique ainsi qu'il voit le projet « plan X » comme un tournant dans le débat sur le « cyber warfare ». Les autorités assument désormais l'utilisation du cyberespace comme un champ de bataille et donc le développement de capacités offensives. Une leçon tirée des expériences récentes : Matthew Waxman, un professeur de l'université Columbia et ancien du DoD constate que les administrations Bush et Obama ont été lentes à parler publiquement de l'utilisation des drones armés et que cela a conduit à céder du terrain sur le plan de l'acceptabilité de cette pratique. « C'est parce que les Etats-Unis occupent une position avantageuse sur les capacités cyber offensives, que le pays doit saisir l'opportunité de pousser un certain nombre de règles pour lui-même et pour les autres ».

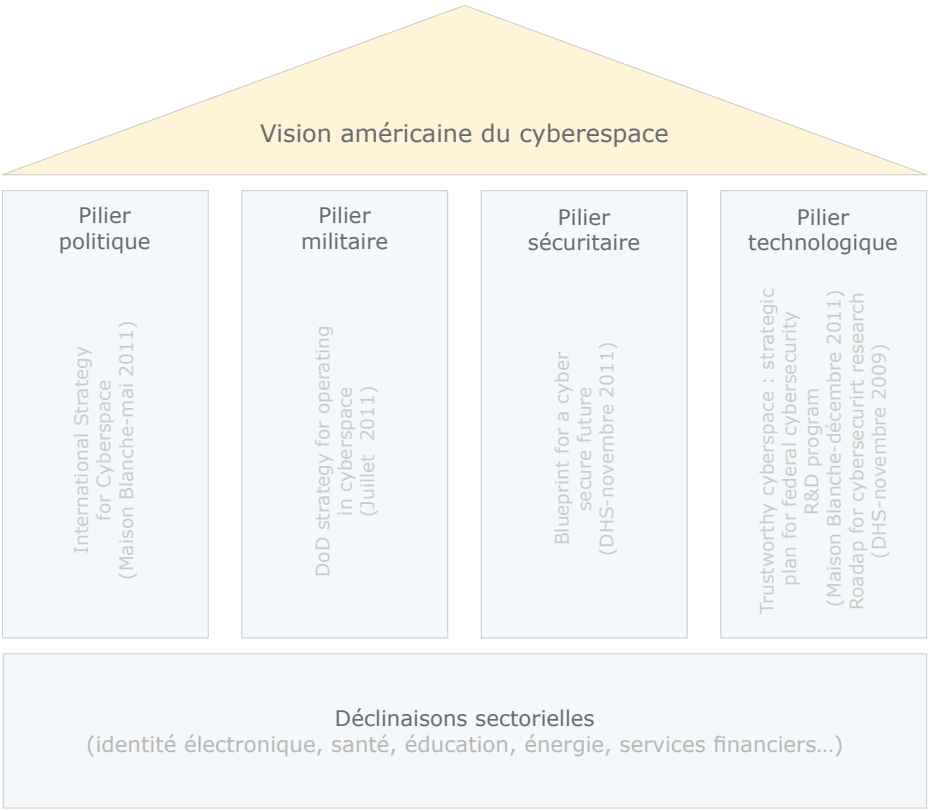
---

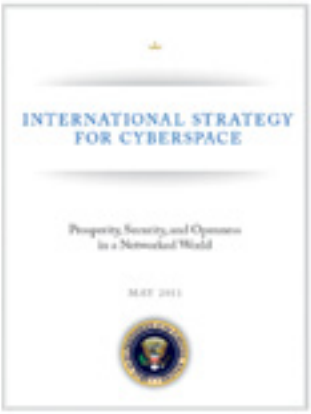
[3]Lire à ce sujet une étude intitulée « Cyber 2020, asserting global leadership in the Cyber Domain » publiée par la société Booz Allen Hamilton. Cette étude présente quatre scénarios d'évolution du cyberespace en 2020 : un internet fragmenté, un internet « stagnant », un internet chinois et un internet universel et global.
[4]Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power, juin 2012.
[5]Source : Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials, Scott Chane, 26 septembre 2012, New York Times, http://cryptome.org/2012/09/darpa-plan-x.pdf

Les 4 piliers de la stratégie « cyber » américaine

L'offensive américaine dans le cyberespace repose sur quatre piliers : politique, militaire, sécuritaire et technologique.

Les 4 piliers de la stratégie américaine dans le cyberespace



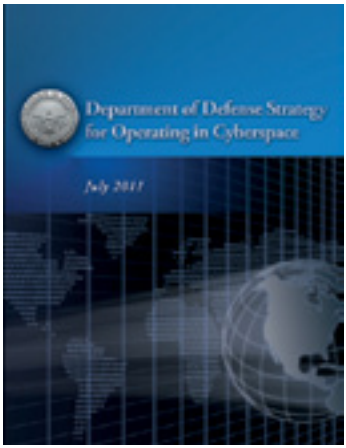


Le pilier politique

Le pilier politique est constitué de la stratégie internationale pour le cyberespace, publiée en mai 2011, qui défend une approche universelle et libératrice d'internet[6]. Cette stratégie de « soft power » est notamment mise en œuvre par le Département d'Etat à travers des programmes de « diplomatie numérique » visant à former au numérique les élites de certains pays d'Afrique et du Moyen-Orient (programme TechWomen) ou à développer des solutions techniques anti-censure (programme Commotion Wireless destiné à développer une solution technique permettant de se connecter à Internet depuis un pays coupé du monde). Au total, ce sont quelques 150 millions de $ qui auraient été consacrés à ces initiatives de diplomatie numérique depuis leur création.

Le pilier militaire

Le pilier militaire s'appuie sur la stratégie du Département de la défense (DoD) pour les opérations dans le cyberespace, publiée en juillet 2011[7]. Ce document définit cinq actions stratégiques :
Appréhender le cyberespace comme un domaine opérationnel en termes d'action militaire ;
Employer des nouveaux concepts opérationnels pour protéger les réseaux et systèmes du DoD ;
Développer les partenariats avec les autres agences fédérales et avec le secteur privé ;
Bâtir des relations fortes avec les pays alliés et construire un système de cybersécurité collectif ;
Développer l'innovation technologique et les expertises en matière de cybersécurité.



Le pilier sécuritaire

Le pilier sécuritaire est constitué de la stratégie de cybersécurité du Department of Homeland Security (DHS) intitulée « Blueprint for a secure cyber future » et publiée en novembre 2011[8]. Objectif : construire un cyberespace sûr, résilient, favorisant l'innovation, protégeant la santé publique et la sûreté, promouvant la compétitivité économique et la défense nationale.
Deux priorités : la protection des infrastructures sensibles, en développant notamment une « vision partagée de la situation », ainsi que le renforcement de l'écosystème « cyber ».

[6] *http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf*
[7] *http://www.defense.gov/news/d20110714cyber.pdf*
[8] *http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf*

Le pilier technologique

Le pilier technologique de la stratégie américaine dans le cyberespace comprend deux documents principaux :
La stratégie fédérale édictée par la Maison Blanche en décembre 2011 intitulée « Trustworthy cyberspace : strategic plan for federal cybersecurity research and development program »[9] ;
L'agenda technologique du DHS publié en novembre 2009 intitulé « a roadmap for cybersecurity research »[10].

Les déclinaisons sectorielles

Ces grandes orientations sont ensuite déclinées à travers des politiques sectorielles en matière d'éducation, de services financiers, de transport, d'énergie et de santé. Elles s'appuient également sur une stratégie nationale en matière d'identité électronique édictée par la Maison blanche en avril 2011 et intitulée « National strategy for trusted identities in cyberspace »[11]. Objectif : bâtir un écosystème d'identité interopérable pour accéder aux services en ligne.

[9] *http://www.cyber.st.dhs.gov/wp-content/uploads/2011/12/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf*
[10] *http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf*
[11] *http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf*

Des agendas technologiques structurés

La vision stratégique américaine s'appuie sur une feuille de route technologique principalement composée de l'agenda fédéral de R&D en matière de sécurité et de la « roadmap » du Department of Homeland Security (DHS).

L'agenda fédéral de R&D en matière de cybersécurité

En décembre 2011, l'Office of Science and Technology Policy (OSTP) publie un document intitulé « Trustworthy cyberspace : strategic plan for federal cybersecurity research and development program ». Un appel à contribution était d'ailleurs ouvert jusqu'à fin décembre 2012 pour la mise à jour de ce plan.

Ce document cadre fixe quatre objectifs clés : induire le changement et canaliser les efforts, accélérer la transition de la théorie à la pratique, développer les bases scientifiques et maximiser l'impact de la recherche. Les constats sont en effet sans appel : les défenses ne progressent que lorsque les systèmes ont été attaqués avec succès et les bases scientifiques de la cybersécurité sont encore balbutiantes, tant au plan technologique qu'au plan politique, réglementaire, juridique, économique et humain. Il faut donc développer une approche plus scientifique et plus rigoureuse du sujet à travers par exemple la mise en place d'expérimentations et de critères d'évaluation appropriées. Autres points clés : fournir des jeux de données complets aux chercheurs pour leur permettre de tester leurs technologies « in vivo » et développer une meilleure collaboration entre public et privé, encourager les chercheurs à publier leurs travaux, établir un lien entre recherche amont et la recherche & développement (« valley of death ») à travers différents canaux de transition.

En termes de technologies, le document fixe 4 priorités thématiques.

- « Designed-in security ». L'objectif est de parvenir à une meilleure intégration de la sécurité dans les phases d'ingénierie et de développement logiciel ;
- « Tailored trustworthy spaces ». Il s'agit de créer des espaces de confiance et des contextes de sécurité spécifiques pour que les utilisateurs puissent sélectionner des environnements avec des niveaux de confidentialité, d'anonymat, d'intégrité, de disponibilité et de traçabilité adaptés aux usages ;
- « Moving targets ». Les « cibles mobiles » doivent permettre d'augmenter l'incertitude et la complexité pour les attaquants et de réduire leurs fenêtres d'opportunité. Plusieurs technologies clés : le « data chunking », la décentralisation des données, la création de leurres, la détection des fuites d'information etc. Les programmes engagés en vertu de cet objectif sont principalement gérés par les agences du Département de la défense.
- « Cyber economic incentives ». Le constat est que les solutions techniques existent souvent mais que les utilisateurs ne sont pas incités à les utiliser. Il faut donc être en mesure de développer des critères d'évaluation (metrics) permettant de dire si un système est sûr ou non, s'il peut l'être et à quel coût supplémentaire. L'objectif est de développer une base scientifique pour l'analyse de risques et du retour sur investissement.

Principaux programmes
et agences responsables

Source : CEIS

L'agenda technologique du DHS

Près de deux ans avant la stratégie fédérale, en novembre 2009, le DHS avait publié un agenda technologique intitulé « a roadmap for cybersecurity research »[12] organisé autour de 14 axes de recherche (« Technical Topic Area ou TTA). Ces axes ont l'objet d'un appel à projet lancé en janvier 2011. Au total, 34 contrats de R&D ont pour le moment été attribués dans le cadre de ce programme à 29 organisations publiques et privés.
Des présentations détaillées de certains de ces projets ont été faites lors d'une réunion qui s'est tenue en octobre 2012[13]. Plus de 1 000 contributions ont également été reçues par le DHS dans le cadre de cette consultation. On note enfin que quatre de ces contrats incluent du cofinancement de partenaires internationaux : deux originaires de Grande-Bretagne et deux d'Australie. Des négociations seraient en cours avec d'autres partenaires potentiels au Canada, en Suède et en Hollande.
Pour chaque axe, un exemple de l'un des projets lancés est sommairement présenté ci-dessous à titre d'illustration.

Axe 1 : l'assurance qualité logiciel.

Parmi les projets :

- le « Software Assurance Market Place » ou SWAMP (voir axe spécifique n°14).
- Le « Protected Repository For the Defense of Infrastructure Against Cyber Threats » ou PREDICT[14]. L'objectif est de fournir aux développeurs des jeux de données opérationnelles relatives à des attaques, qu'il s'agisse de données fournies par des IDS, des firewalls etc.

Les différents programmes de banc d'essai en cybersécurité
Différents programmes de banc d'essai et de simulation ont été lancés par les agences fédérales américaines, civiles ou militaires :
Du côté du DHS : Le DHS possède aussi depuis plusieurs années son propre environnement de test et de simulation baptisé DETER[15];
Du côté du DoD :

- Le National Cyber Range (NCR) de la DARPA. Initié en 2008, le programme a été conçu comme un prototype devant évoluer vers un Cyber Range Environment (CRE), Le prototype a été achevé à la mi-2012. Il a été transféré au Cyber Command en octobre 2012[16]. Lockheed Martin, le principal contractant, a remporté un contrat de 80 millions de dollars sur 5 ans pour fournir le support logiciel et hardware[17],
- Le Information Assurance Range de la DISA. C'est notamment la société Breaking Point Systems[18] qui travaille sur ce projet (ainsi que pour l'EUCOM),
- Le Joint Information Operations (IO) range du Joint Staff.

[12] *http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf*
[13] *http://www.cyber.st.dhs.gov/oct2012pi-presentations/*
[14] *http://www.cyber.st.dhs.gov/predict et http://www.predict.org/*
[15] *http://www.cyber.st.dhs.gov/deter/ et http://www.deter-project.org/*
[16] *Source : http://www.gsnmagazine.com/node/27823*
[17] *Source : http://defensesystems.com/articles/2012/11/13/lockheed-national-cyber-range-contract.aspx?m=2*
[18] *Source : http://www.breakingpointsystems.com/default/assets/File/white%20papers/WP-Cyber-Range-40200-01-1.pdf*

Axe 2 : les critères de sécurité

Ces critères d'évaluation doivent être basées sur des standards et permettre une visualisation interactive. Exemples de ces « metrics » : vulnérabilités, exploitabilité, probabilité d'une attaque etc.

Axe 3 : sécurité intuitive (« usable security »).

L'objectif est de construire des systèmes de sécurité plus intuitifs basés notamment sur l'analyse du contexte pour guider les utilisateurs. On note dans ce domaine la présence d'une PME baptisée Applied Vision qui travaille sur le sujet du facteur humain dans la sécurité.

Axe 4 : les menaces internes (« insider threat »).

Exemple : le projet Detecting Threatening Insiders with Lightweight Media Forensics qui vise à détecter les "insiders" hostiles en comparant les « profils » de stockage des utilisateurs internes. D'une durée de 3 ans, le projet est géré par le Naval Postgraduate School.

Axe 5 : systèmes et réseaux résilients.

Certains systèmes sont en permanence attaqués. On reconnait donc la spécificité de ces systèmes et leurs besoins spécifiques en termes de résilience. Exemple : le projet Real-Time Protocol Shepherd (RePS). D'une durée de 14 mois, ce projet géré par Raytheon BBN Technologies a pour but de développer un dispositif permettant de gérer en temps réel des interfaces externes en renforçant les capacités de détection d'intrusion (IPS) et de réponse.

Axe 6 : la modélisation des attaques internet.

Premier exemple de projet : le développement d'un système d'analyse de malware fédéral (Federal Malware Analysis System ou FMAS). Autre projet : STUCCO (Situation & Threat Understanding by Correlating Contextual Observations) a pour objectif de développer des méthodes pour intégrer et visualiser l'ensemble des données relatives aux menaces cybernétiques, qu'elles que soient les sources d'origine (presse, médias sociaux…) pour pouvoir les représenter avec les données de cyber sécurité d'origine « technique ». D'une durée de trois ans, le programme est mené par le Oak Ridge National Laboratory, le Pacific Northwest National Laboratory, la Stanford University et le REN-ISAC.

Axe 7 : la cartographie réseau et l'évaluation

L'objectif de l'un des projets lancés est notamment de renforcer l'outil Netalyzr pour lui permettre par exemple de détecter l'utilisation de DNSSEC chez un client, de détecter les manipulations de DNS ou de TLS. Le projet a une durée de 24 mois. Il est géré par l'Université de Berkeley.

Axe 8 : la création d'une communauté de réponse aux incidents

A partir de l'identification des processus-type des CSIRT, l'un des projets cherche à définir des modèles de processus favorisant la coopération entre les équipes internes et externes susceptibles d'être impliquées dans une réponse à incident. Ce projet de 3 ans a été lancé en octobre 2012 et est géré par la George Mason University avec le concours de l'Université de Dartmourth et de la société HP

Axe 9 : les incitations économiques en matière de cybersécurité (« cyber economics »)

L'objectif est notamment de mieux comprendre les défis liés aux investissements en cybersécurité dans le secteur privé. Il s'agit notamment d'encourager les vendeurs à intégrer la sécurité et à promouvoir des environnements où les utilisateurs sont systématiquement informés des risques qu'ils prennent et des retours sur investissement potentiels en matière de sécurité.

Axe 10 : la « provenance digitale »

L'objectif de l'un des projets acceptés est de fournir un système permettant de suivre et de tracer la donnée dans des environnements virtualisés. Une interface graphique permet ensuite de gérer et d'exploiter les données collectées. Ce projet d'une durée de deux ans est mené par l'Université de Caroline du Nord en liaison avec RENCI (Renaissance Computing Institute).

Axe 11: Hardware de confiance (« Hardware enabled trust »)

Le hardware est le « sanctuaire » des données et la base de la confiance dans l'environnement informatique. Or les technologies actuelles sous-utilisent les capacités hardware en matière de sécurité système. Le projet, d'une durée d'un an et demi, est mené par la société Def Logix[19].

Axe 12 : la défense mobile (« Moving target defense »)

Les systèmes IT sont construits pour opérer de façon relativement statique. Les adresses, les noms, les piles logicielles, les réseaux restent statiques. Cela permettait d'avoir des systèmes simples quand les vulnérabilités n'étaient pas exploitées. L'objectif est de développer l'incertitude et la complexité et de réduire les fenêtres d'opportunité des attaquants. Le projet, d'une durée de deux ans, est géré par l'Université de Princeton avec l'aide de la société Analog Bits[20].

Axe 13 : une hygiène numérique inspirée par la nature (« Nature inspired cyber health »)

L'axe 13 a pour objectif de transposer au plan informatique certains mécanismes du corps humain comme les défenses immunitaires, voire d'imaginer des attaques permettant d'immuniser des systèmes vulnérables. Il s'agirait aussi de développer un système d'alerte et de partage de l'information basé sur le modèle du Center for Disease Control.

Axe 14 : Software assurance marketplace (SWAMP)

L'objectif est de créer une sorte de boîte à outils commune pour que les développeurs puissent tester leurs outils et identifier d'éventuelles vulnérabilités. Lancé en octobre 2012, le programme devrait s'achever en 2017. Il devrait fournir les ressources nécessaires pour analyser 275 millions de lignes de code par jour. Le projet se basera sur les outils déjà développés et l'expérience du « Build and Test Facility (BaTLab) de l'Université de Wisconsin-Madison.

[19] *http://www.cyber.st.dhs.gov/wp-content/uploads/2012/10/Day-3.09-TTA11-Def-Logix-Rivera.pdf*
[20] *http://www.cyber.st.dhs.gov/wp-content/uploads/2012/10/Day-2.13-TTA12-Princeton-Lee.pdf*

Focus sur le Département de la défense

La R&D du département de la défense est éclatée entre plusieurs agences sous la coordination de l'Office of the Director. Il y a tout d'abord les organisations de recherche comme l'Office of Naval Research, l'Army Research Laboratory ou l'Air Force Research Laboratory qui ont tous des programme en matière de cybersécurité. A noter par exemple le projet CHAMP (Counter-electronics High-powered Microwave Advanced Missile Project) développé par l'Air Force Research Laboratory et conduit par Boeing avec l'aide de la société Ktech achetée par Raytheon en 2011, qui explore la possibilité d'une arme à énergie dirigée capable de détruire les systèmes informatiques21.

La DARPA, principal instrument de R&D du DoD

Mais les investissements les plus importants concernent la DARPA, qui est l'instrument principal de la R&D du Département de la défense, et la NSA (via son National Information Assurance Research Group). Le budget de la DARPA (247 millions de dollars en matière de R&D de cybersécurité en 2013) devrait ainsi continuer à progresser de 2013 à 2017 de 8 à 12 % par an et s'élever au total à 1,54 milliards de dollars[22]. L'importance de ces budgets montre à l'envi que les besoins spécifiques du DoD dans le domaine ont été totalement intégrés.

Les activités de la DARPA en matière de R&D cybersécurité sont principalement conduites par le Strategic Technology Office et l'Information Assurance and Survavibility Project. Ce projet inclut de nombreux programmes comme le IAMANET (Intrinsically Assured Mobile Ad hoc Network) concernant le développement de réseaux sans fil tactiques sécurisés. Autre projet : le Trustworthy Systems Program qui a pour objectif de fournir des ordinateurs de confiance pour les systèmes de défense. La DARPA examine aussi les vulnérabilités potentielles dans la chaîne d'approvisionnement informatique dans le cadre du TRusted Uncompromised Semiconductor Technology program (Trust) dont l'objectif est de développer des méthodes et outils pour déterminer si une puce fabriquée dans le cadre d'un processus non contrôlé peut être certifiée pour exécuter une opération donnée ou non. La DARPA a enfin développé le National Cyber Range (NCR) dont l'objectif est de fournir un environnement de test (voir plus haut l'encadré sur les programmes de simulation).

[21] http://securityaffairs.co/wordpress/10783/cyber-warfare-2/new-weapons-for-cyber-warfare-the-champ-project.html

[22] Source http://www.darpa.mil/NewsEvents/Releases/2012/03/12c.aspx

Un exemple de programme de rupture : le Projet Plan X

La DARPA se concentre essentiellement sur de la R&D de long terme. Martin Libicki de la Rand Corporation explique à son propos : « même si 90 % de leurs idées ne débouchent pas, les 10 % qui sont valables font plus que payer la différence »23. Le meilleur exemple de cette recherche de l'innovation de rupture est sans doute le projet Plan X annoncé en mai 201224 pour un budget de 110 millions de dollars.

Objectifs

L'objectif de Plan X est clairement affiché : « Parce que l'origine des cyberattaques a été la communauté du renseignement, on a tendance à considérer qu'en faisant simplement plus que ce que nous faisons aujourd'hui, on nous donnera ce dont nous avons besoin, explique Kaigham J. Gabriel, directeur de la DARPA. Ce n'est pas comme cela que nous voyons les choses : il y a une échelle, une vitesse et des capacités différentes dont nous avons besoin ». Il s'agit donc d'explorer des « territoires non connus », de créer des « technologies révolutionnaires pour comprendre, planifier et gérer le combat cyber en temps réel, à grande échelle et dans des environnements dynamiques ». Principaux défis : mesurer, quantifier et comprendre le cyberespace pour développer le « situational awareness » avec toutes les interactions que cela peut avoir dans les autres domaines. L'objectif est en fait de passer d'une approche manuelle, artisanale à une approche technologique permettant une automatisation plus ou moins totale pour parvenir au niveau requis de complexité opérationnelle et compresser les phases de reconnaissance, planification, exécution et évaluation. On se situe dans l'affrontement machine contre machine avec l'impérieuse nécessité d'agir en quelques microsecondes. La DARPA indique : « dans un environnement où les microsecondes comptent et où les opérateurs utilisent un clavier pour diriger les opérations, l'avantage va à l'opposant qui peut penser et taper plus vite. Dans le cas de la machine contre la machine, l'avantage va au hardware et au logiciel qui s'exécute plus vite. Cependant si l'opérateur est technologiquement assisté pour être meilleur en planification opérationnelle et en exécution en temps réel, il aura l'avantage.[25]»

Il importe donc changer de paradigme et ne pas se limiter à une simple amélioration du processus manuel. L'un des points clés à améliorer est par ailleurs la mesure des effets, tant dans la phase de planification que dans celle d'exécution. Cette préoccupation répond en fait à de nombreuses considérations politiques et juridiques. Le journaliste du NYT David E. Sanger rapporte ainsi dans son ouvrage « Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power » publié en juin 2012 les confessions de l'un des concepteurs du virus Stuxnet qui aurait déclaré avoir consacré une partie non négligeable de son temps à s'assurer que Stuxnet ne violait pas le droit des conflits armés. Nombreuses sont d'ailleurs les opérations (Irak en 2003 par exemple) où certaines informations font état a posteriori d'opérations informatiques planifiées mais non exécutées en raison de difficultés d'évaluation des effets de l'attaque.

[23]Source : http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story_1.html
[24]Communiqué de presse officiel : http://www.darpa.mil/NewsEvents/Releases/2012/10/17.aspx
[25]Source : broad agency announcement, foundational Cyberwarfare (Plan X), 20 novembre 2012, https://www.fbo.gov/utils/view?id=49be462164f948384d455587f00abf19

Au plan conceptuel

Sur un plan conceptuel, l'espace de bataille cyber tel que le conçoit le projet se définit avec 3 concepts principaux : la carte réseau, les unités opérationnelles et les « sets » de capacités.

La carte réseau est constituée d'un ensemble de nœuds et de liens. Elle possède deux couches : l'une est la topologie logique, l'autre est constituée par les meta-data, c'est-à-dire des différents attributs des liens (latence, bande passante…) ou des nœuds (nombre de liens, système d'exploitation, protocole, ports…). Cette carte est par définition dynamique, voire très volatile. Plus cette carte est fidèle, plus les planificateurs et opérateurs seront susceptibles de manœuvrer efficacement.

Les unités opérationnelles peuvent être les nœuds d'entrée ou les plateformes support. Les nœuds d'entrée sont les accès physiques au réseau. Les plans doivent ainsi inclure plusieurs nœuds d'entrée pour multiplier les chances de succès. Les plateformes sont quant à elles déployées pour contrôler les différentes facettes de l'opération : déploiement de capacités, mesure des effets, assurer la communication entre les nœuds et les plateformes support…

Les « sets » de capacités sont constituées d'un ensemble de technologies classées en trois catégories : l'accès, le fonctionnel et la communication. Les technologies d'accès permettent d'exécuter des instructions sur un ordinateur. C'est en réalité un exploit qui est utilisé pour lancer des programmes et des charges utiles. Les technologies fonctionnelles représentent les technologies susceptibles d'affecter les ordinateurs et les réseaux : rootkits, scanners réseaux… Les technologies de communication représentent enfin les technologies fournissant les chemins de communication pour les nœuds d'entrée, les plateformes support et les capacités. Exemples : les commandes de malware, le peer to peer, les connexions SSL etc.

Au plan pratique

Au plan pratique, le projet plan X qui est conduit par le DARPA Cyberwar Laboratory a fait l'objet d'une réunion de deux jours en octobre 2012 afin de présenter le projet aux organisations susceptibles de candidater à l'appel à projet, qui est clos le 25 janvier 2013, et de stimuler les partenariats entre organisations intéressées. 350 personnes auraient participé à ce séminaire. Les sociétés et organisations qui répondront seront organisées en « startup technologique virtuelle », c'est-à-dire qu'elles conduiront leur R&D depuis leurs propres installations autour d'un « Collaborative Research Space » localisé à Arlington en Virginie où les technologies seront intégrées, revues et testées.

D'une durée de 4 ans, le programme s'articule autour de 4 phases d'un an, chacune constituées de 4 spirales de développement incluant 6 périodes de deux semaines de développement, lesquelles s'achèvent par une phase de vérification d'une semaine. Chacune de ces 4 phases d'un an comprend par ailleurs 4 échéances dont une majeure qui se traduit par le lancement du produit et donne lieu à un événement gouvernement-industrie de deux jours.

Au plan technique

Au plan technique, l'objectif de Plan X est de construire une plateforme de bout en bout basée sur une architecture ouverte afin de pouvoir intégrer de nombreuses technologies d'origine gouvernementale ou privée. Cinq domaines techniques (Technical Areas ou TAs) ont été définis.

Architecture Système (TA1) :

Conception et développement des APIs, spécification des formats de données. Cette tâche intègre également le hardware et la maintenance de toute l'infrastructure. A noter que le dispositif devra permette des connexions extérieures pour les partenaires selon les conditions de sécurité de la directive ICD 503. Premier objectif de ce domaine technique : la conception et l'implémentation d'un moteur graphique pour représenter l'espace de bataille cyber. Ce moteur constitue véritablement le cœur du système car son rôle est de recevoir, de récupérer, de modéliser et d'envoyer des instructions sur l'espace de bataille aux autres composants du système. La topologie logique est construite à partir de multiples informations : traceroute, niveaux de latence, routes BGP, headers IP TTL, tables de routage… A cette cartographie viennent ensuite s'accrocher des données de planification (nœuds d'entrée, placement des plateformes de soutien, chemins de communication, cibles…) ou d'exécution (statut en temps réel des différents objets, évaluation des effets…). L'opérateur peut ainsi facilement passer d'une vision conceptuelle du terrain à une vision réelle. Second objectif : concevoir et construire l'infrastructure du système qui doit pouvoir opérer depuis les niveaux non classifiés jusqu'à secret. Les organisations qui postuleront sont ainsi invitées à analyser les architectures temps réel sur étagère ainsi que les moteurs utilisés dans le monde du jeu en ligne.

Analyse de l'espace de bataille cyber (TA2) :

L'objectif est de développer des technologies d'analyse automatique pour faciliter la compréhension que l'humain peut avoir de l'espace de bataille cyber, l'aider à développer des stratégies de « cyber warfare », évaluer et modéliser les effets. Premier focus : développer des technologies permettant aux planificateurs de concevoir des opérations dans le cyberespace. Deux champs de recherche distincts : le développement de techniques automatiques pour générer des plans de bataille, le développement d'applications de simulation pour modéliser les mouvements et contre-mouvements des adversaires. Une large partie de ce domaine technique vise en fait à comprendre et quantifier les effets, tant au niveau micro qu'au niveau macro. Quelques exemples de problématiques qui pourront être abordées : l'assistance dans la sélection des nœuds (nœuds d'entrée, nœuds cibles, nœuds à éviter…) ; la réduction topologique, c'est-à-dire la capacité à visualiser une cartographie réduite en fonction d'un plan donné ou de différents critères (chemin le plus court pour atteindre une cible par exemple) ; le placement optimal des plateformes de soutien (via par exemple un calcul du ratio coût / bénéfice) ; la sélection des chemins de communication (routes primaires, routes alternatives). Second focus : le développement de technologies de simulation pour analyser les dynamiques potentielles de l'adversaire.

Construction de mission (TA3) :

Ce domaine technique vise à développer des technologies permettant de construire des plans de missions et de les synthétiser sous la forme de scripts automatiquement exécutables. L'idée est aussi de pouvoir vérifier formellement ces plans et quantifier les effets attendus. Ce domaine technique est basé sur le développement de langages de programmation spécifiques. Ces langages doivent non seulement permettre d'exécuter les missions en transmettant, nœud après nœud, les instructions mais aussi de vérifier les opérations (création de points de vérification permettant éventuellement à l'opérateur d'opter pour une variante, de fournir une information additionnelle…), de résister aux pannes (prise de contrôle en mode manuel par l'opérateur), de passer en mode totalement automatique au cas par exemple où les liaisons de données sont suspendues, de procéder à une analyse formelle permettant de détecter les erreurs, les bugs et les incohérences, d'appliquer les règles d'engagement (de façon native, les plans sont construits pour limiter les options et la marge de manœuvre des opérateurs), de rejouer une opération pour faciliter une future planification grâce à un « package mission » comprenant le script de mission, les règles d'engagement, les spécifications de capacités etc.

Exécution de mission (TA4) :

Ce domaine porte sur l'environnement d'exécution des scripts mission. La R&D se focalisera sur la construction de systèmes d'exploitation et de machines virtuelles conçues pour opérer dans des environnements réseaux dynamiques et hostiles. Les plateformes support seront conçues pour fonctionner sur tout type d'architectures informatiques. Première thématique de recherche : l'environnement d'exécution et la construction d'un framework permettant d'assembler les capacités pour chaque mission. Les organisations qui candidateront sont ainsi appelés à challenger certains outils publics comme Metasploit, Immunity Cancas et d'autres toolkits standard. Second sujet de recherche : le développement de systèmes d'exploitation et de machines virtuelles permettant d'exécuter les missions, ce qui inclut le développement de plateformes supportant des fonctions opérationnelles, d'évaluation des effets, de relai de communication, de « défense adaptable » (filtrage de paquets…).

Interfaces intuitives (TA5) :

Ce segment a pour objet de fournir une interface la plus intégrée et intuitive possible pour les utilisateurs afin de minimiser le niveau d'expertise technique requis. Il s'agit notamment de développer plusieurs workflows pour contrôler les différentes fonctions du système : une vision temps réel du champ de bataille cyber (« heat map ») avec la possibilité de zoomer rapidement et de voir une opération spécifique ou de « désencombrer » la carte pour disposer d'une vision de synthèse, la vision du processus de planification qui est considérée comme la plus complexe car pouvant résulter d'une approche très hiérarchisée ou au contraire d'une approche « crowdsource », la vision des capacités construites, la vision « opérateur » avec la possibilité d'interagir avec le script de mission mais aussi d'interagir avec l'opération sans script de mission et sans créer un plan spécifique, pour réagir en temps réel et mener une opération « en conduite » avec un feedback direct. Point important : les interfaces graphiques développées doivent être conçues pour fonctionner sur une très large gamme d'équipements (tablettes tactiles, systèmes de réalité augmentée…) et avec des « imputs » utilisateurs très variés. Il est précisé que les interactions traditionnelles clavier / souris sont possibles mais doivent être minimisées.

Quels résultats au plan industriel ?

Peu après l'élection d'Obama, la Commission sur la cybersécurité pour la 44ème présidence mise en place par le Center for Strategic International Studies (CSIS) estimait que seulement 300 millions sur les 143 milliards de R&D investis en 2009 par le gouvernement fédéral était affectés à la cybersécurité. Jugeant cet investissement insuffisant, les différents rapports de la commission militaient pour une augmentation des budgets de R&D et une meilleure coordination et priorisation des fonds alloués à la R&D en cybersécurité.

Une stratégie de R&D coordonnée sous l'égide du NITRD

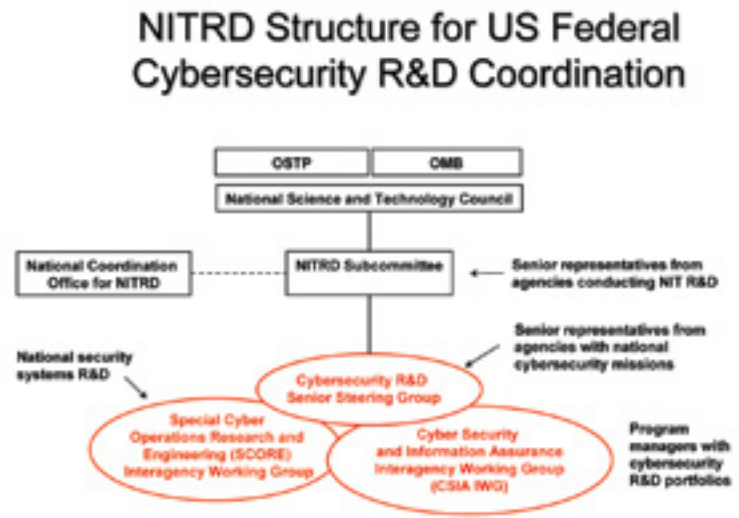
Le programme Networking and Information Technology Research and Development (NITRD), chargé de coordonner l'effort de R&D dans le domaine, a donc vu son rôle renforcé. Ce programme, qui rassemble 14 agences fédérales, est géré par trois groupes de travail :

1 - Le SSG, le Senior Steering Group for Cybersecurity, qui comprend des représentants des deux groupes de travail suivants ;

2 -Le CSIA, Cyber Security and Information Assurance Working Group, groupe de travail interagences sur la cybercriminalité.

3 - Le SCORE, Special Cyber Operations Research and Engineering : établi en 2008, iltravaille en parallèle du CSIA pour coordonner la recherche classifiée en cybersécurité. Il est géré par l'Office of Science and Technology Policy (OSTP) de la Maison Blanche et le Director of National Intelligence (DNI).

Structure du NITRD[26]



[26]*Source : http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb2_federal-cybersecurity-rd-program_bnewhouse.pdf*

Le NITRD est enfin organisé autour de 7 projets distincts :

- Cyber Security and Information Assurance (CSIA) ;
- Human Computer Interaction and Information Management (HCI&IM) ;
- High Confidence Software and Systems (HCSS) ;
- High End Computing (HEC) ;
- Large Scale Networking (LSN) ;
- Software Design and Productivity (SDP) ;
- Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW).

Des budgets en nette progression

Le NITRD gère environ 4 milliards de dollars au total. Pour 2013, la demande budgétaire globale sur la R&D consacrée aux technologies de l'information a ainsi été de 3,8 milliards[27], en très légère progression de 1,8 % par rapport à l'année précédente.

Répartition et évolution de la R&D en matière de technologies de l'information (en millions de $)

	2011	2012	2013
NSF	1.189,4	1.138,3	1.207,2
DoD	749,9	694,1	654
NIH	551	553	551
DOE	489,2	542,5	568,5
DARPA	436	489	462
NIST	78,3	100,2	116,7
NASA	94,3	102,6	100,4
DHS	47	47	64
AHRQ	27,6	25,6	25,6
NOAA	26,3	22	25,6
DOE/NNSA	30	18	25
EPA	6	6	6
NARA	2	1	1
DOT	0	0	1
TOTAL	3.72	3.73	3.8

Les budgets alloués au programme Cyber Security and Information Assurance (CSIA) apparaissent en revanche en très nette augmentation puisqu'ils devraient passer de 445,1 millions de dollars à 667,4 en 2013, soit une augmentation de plus de 30 %.

[27]Au total, 140,8 milliards de dollars ont été demandés pour la R&D par le gouvernement pour l'année fiscal 2013.

Répartition et évolution de la R&D en matière de cybersécurité (en millions de $)

	2011	2012	2013
NSF	76,5	98,5	114,1
DoD	141,4	114,6	156,6
NIH			
DOE	33,5	33,5	33,5
DARPA	127	223	247
NIST	25,7	47,2	55,2
NASA			
DHS	41	43	61
AHRQ			
NOAA			
DOE/NNSA			
EPA			
NARA			
DOT			
TOTAL	445,1	559,8	667,4

Une approche équilibrée

La stratégie de R&D américaine apparait relativement équilibrée, et ce à différents niveaux :

- Elle est à la fois civile et militaire, classifiée et non classifiée, ce qui permet d'enclencher un cercle vertueux ;
- Elle comprend différents horizons temporels :
  - *Court terme : 1 à 3 ans,*
  - *Moyen terme : 3 à 5 ans,*
  - *Long terme : 5 ans et plus,*
- Elle est interdisciplinaire;
- Elle est basée sur un renforcement des partenariats publics-privés. On observe d'ailleurs que des relais se sont mis en place du côté des industriels. L'initiative la plus notable en la matière est la création en octobre 2012 de la Cyber Security Research Alliance (CSRA) autour de Lockheed Martin, AMD, Intel Corporation, Honeywell et RSA (division de EMC). Cette organisation prévoit, en liaison avec le NIST, un symposium sur la R&D dans le domaine début 2013[28].

[28] *http://www.cybersecurityresearch.org/news_and_events/press_releases/pr_20121023.html*

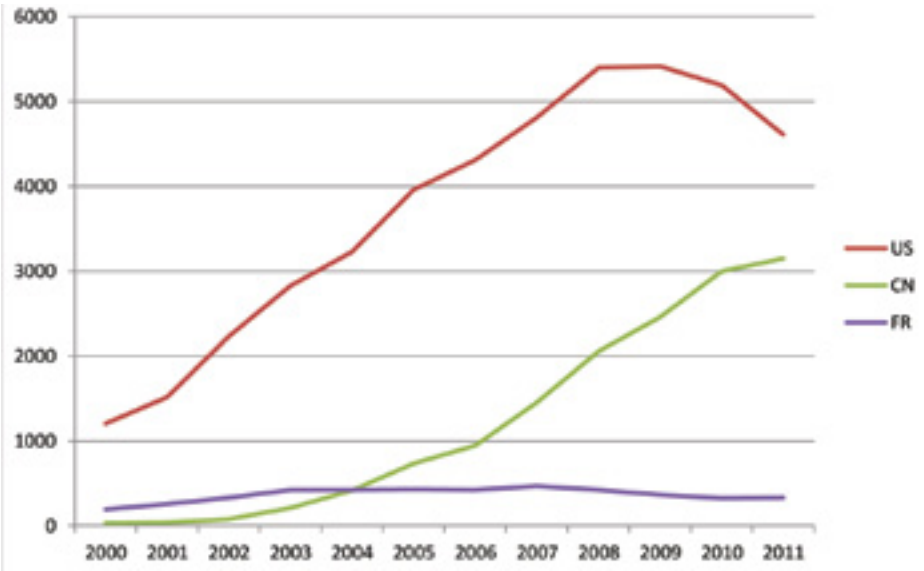
Analyse des brevets en matière de sécurité

Les brevets constituent un bon indicateur de la R&D même s'il ne s'agit pas du seul indicateur valable. Par ailleurs, les recherches par mot-clé ou sur des classes ont toujours un effet déformant puisque l'on ne prend par définition en compte que les innovations qui ont été spécifiquement conçues pour l'application recherchée, et non les innovations issues d'autres domaines scientifiques et technologiques qui pourraient être exploitées dans le domaine considéré.

Evolution du nombre de brevets sécurité aux Etats-Unis

Sur la période 2000-2011, 44 689 brevets en matière de sécurité informatique ou de sécurité des télécommunications[29] ont été publiés avec pour pays d'application prioritaire les Etats-Unis[30]. On observe une forte augmentation d'année en année, de 1 200 environ en 2000 à près de 5 000 en 2009 avant d'enregistrer un tassement en 2010 et 2011.

Evolution du nombre de brevets sécurité aux Etats-Unis



En termes de comparaison, les Etats-Unis restent donc très largement en tête en termes de brevets sécurité, même si l'on observe une montée en puissance continue de la Chine sur la période, résultat de la stratégie de propriété intellectuelle du gouvernement chinois, relayée dans la plupart des entreprises publiques ou privées (les salariés de Huawei sont par exemple financièrement encouragés à déposer).

[29] *Ces analyses portent sur 3 sous-classes selon la nomenclature internationale : H04W 12 (Security arrangements, e.g. access security or fraud detection; Authentication, e.g. verifying user identity or authorisation; Protecting privacy or anonymity), G6F 21 (Security arrangements for protecting computers or computer systems against unauthorised activity), H04L9 (arrangements for secret or secure communication).*

[30] *Source : base de données Thomson Innovation.*

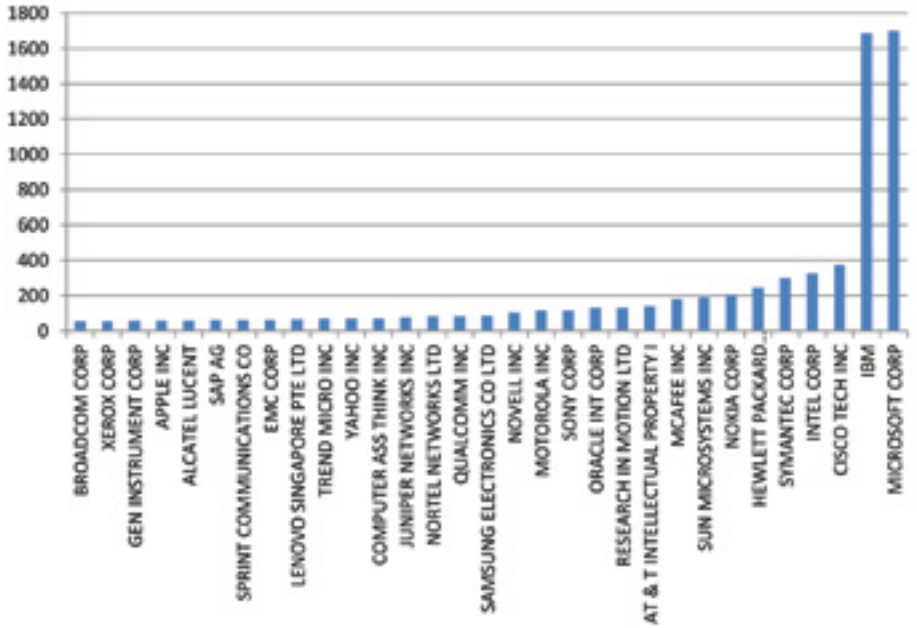
En 2011, on compte ainsi 3 147 brevets publiés ayant pour pays d'application principale la Chine. Cette vision purement quantitative doit cependant être relativisée par une approche plus qualitative : les brevets chinois ne sont que rarement des brevets d'innovation.

Toujours à titre de comparaison, la France apparait nettement en retrait en termes de brevets sécurité avec un total de 4 385 brevets publiés de 2000 à 2011 ayant pour pays d'application prioritaire la France.

Principales sociétés représentées aux Etats-Unis

Ce sont les sociétés Microsoft et IBM qui ont publié le plus de brevets sécurité sur la période avec respectivement 1 701 et 1 686 brevets.

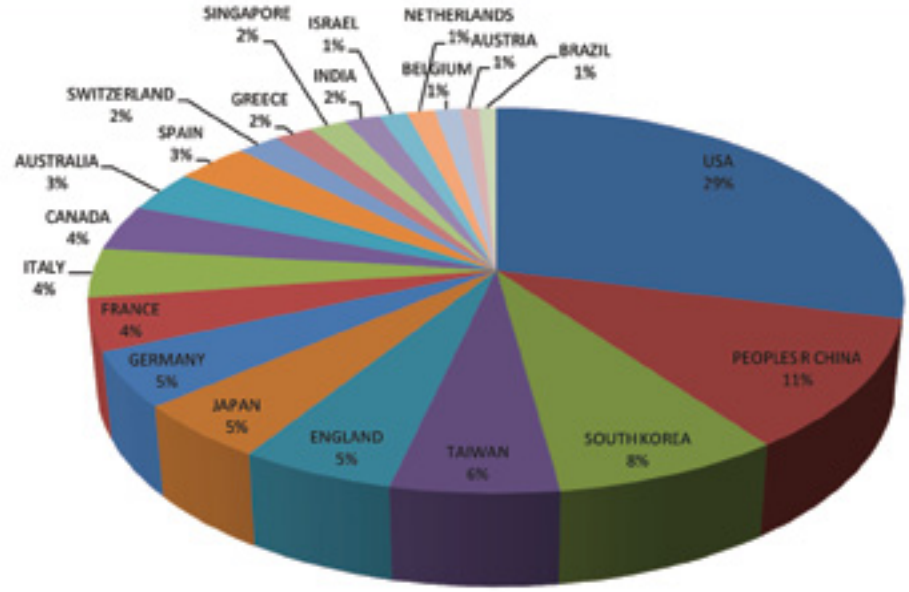
Principales sociétés déposantes



Analyse comparée des publications scientifiques

L'analyse des publications scientifiques en matière de sécurité informatique de 2000 à 2011[31] montre une nette domination américaine avec 29 % des publications, suivie par la Chine (11%), la Corée du Sud (8 %), Taïwan (6%). La France arrive en 8ème position à 4 % derrière l'Allemagne, la Grande-Bretagne et le Japon ex-aequo à 5 %.

Répartition des publications scientifiques par pays



[31] *Source : base de données Thomson Innovation*

Conclusion

Si la vision très techno-centrée des Etats-Unis en matière d'affrontements cybernétiques n'est pas exempte de critiques, la nouvelle initiative de défense stratégique américaine dans le cyberespace a le mérite d'utiliser la cybersécurité comme un véritable catalyseur technologique et industriel pour mobiliser les énergies autour d'une vision stratégique du cyberespace, considéré comme un enjeu de puissance majeur. Quels enseignements peut-on en tirer ?

Une triple opportunité

La cybersécurité ne doit pas être considérée uniquement comme une réponse face à une menace. L'enjeu est nettement plus vaste. La cybersécurité et la confiance numérique sont aussi et surtout une réponse à une triple opportunité sociétale, technologique et économique.

Une opportunité sociétale

Le numérique et les « smart technologies » permettent d'inventer chaque jour de nouveaux usages : e-administration, e-commerce, e-santé, e-éducation, télétravail… Les technologies de l'information et de la communication sont également susceptibles de jouer un rôle clé en matière de développement durable, notamment avec le développement des réseaux électriques intelligents (« smart grids »). Or sans sécurité, sans fiabilité, sans confiance de la part du citoyen ou du consommateur, le développement de ces services est tout simplement impossible.

Une opportunité technologique

L'imbrication croissante du réel et du virtuel marque l'émergence d'une nouvelle révolution technologique qui génère un besoin particulièrement important de sécurité et de fiabilité. Comme le souligne Michel Riguidel[32], « les technologies numériques ont maintenant atteint un stade de maturité qui fait que les avancées et les perspectives dans les applications viendront essentiellement de la synergie de cette discipline avec d'autres domaines scientifiques et technologiques comme les nouveaux matériaux, la biologie et les sciences de la vie. Les progrès dans la maitrise de la complexité pour le logiciel, l'informatique et les réseaux, dans la maitrise de l'infiniment petit pour les matériaux et les technologies du vivant vont se cristalliser pour amorcer une nouvelle convergence pleine de promesses en termes d'applications et créer une rupture décisive dans le domaine des sciences par l'émergence d'une médiation entre l'intangible, le matériel et le vivant, par la réalisation d'une liaison plus étroite et plus riche entre les bits et les quanta d'information, les atomes et les gènes. Dans la prochaine décennie, la fertilisation croisée entre les disciplines du numérique, du quantique, des nanotechnologies et des bio-géno-technologies va s'intensifier et il est crucial pour la France de maitriser cette "nouvelle convergence" et d'être un acteur majeur dans cette domestication de l'alliance entre le bit, l'atome et le gène. »

Une opportunité économique

Près de 80 % des français ont déjà acheté ou consultent leur compte bancaire en ligne. Près de 100 000 sites marchands étaient actifs en France en 2011. Mais surtout, au-delà de l'industrie numérique stricto sensu, les technologies de l'information irriguent l'ensemble de l'économie.

[32]Source : Michel Riguidel, consultation pour le plan France numérique 2020, http://www.economie.gouv.fr/files/files/import/2011_france_numerique_consultation/2011_france_numerique_michel_riguidel.pdf

L'impact du numérique sur l'économie est en effet beaucoup plus important que le chiffre souvent évoqué de 4,1 % en moyenne dans les pays du G20. Il est un facteur de compétitivité majeur et un moteur d'évolution et de croissance durable.

La cybersécurité est enfin, en tant que telle, une opportunité économique car le marché est en forte progression. Evalué à environ 60 milliards de dollars en 2011, dont 15,9 milliards de dollars pour le seul secteur militaire[33], il devrait croître de 8 à 10 % par an pour atteindre selon les analyses entre 80 et 90 milliards en 2017. Ce serait même l'un des segments IT qui devrait le plus progresser. Principal moteur de cette croissance : la convergence entre le domaine traditionnel des technologies de l'Information et de la communication, les équipements de télécommunication et les systèmes industriels.

La dynamique du marché ne suffit pas

La forte progression du marché de la cybersécurité cache pourtant des réalités très disparates. Certaines régions apparaissent particulièrement en pointe comme l'Amérique du Nord (près de 40 % du C.A. global en 2011), suivie par le Japon et par le Royaume-Uni. Par ailleurs, le marché américain ou britannique est très nettement soutenu par le volontarisme politique et l'importance de la commande publique qui représente dans ces deux pays environ la moitié du chiffre d'affaires du secteur contre moins de 20 % en France.
La dynamique du marché ne peut donc à elle seule suffire à concevoir et développer les technologies de cybersécurité permettant :

- D'une part, de concevoir et développer les technologies de cybersécurité et de cyberdéfense nécessaires pour faire face aux menaces actuelles. D'où l'existence de « gaps » capacitaires, tant dans le domaine civil que militaire, que le marché ne peut combler, faute de retour sur investissements à court terme ou tout simplement de conscience du besoin ;

- D'autre part, de créer les conditions d'un nouveau rebond technologique lié à la convergence croissante de l'informatique, des nanotechnologies et des biotechnologies. En cause : la concentration naturelle de la R&D privée sur des problématiques de court terme, son morcellement, sa dimension purement incrémentale.

Pour toucher les dividendes du numérique, une politique industrielle structurée et de long terme en matière de cybersécurité est donc indispensable. La feuille de route du Department of Homeland Security américain le dit clairement[34] : « l'approche incrémentale et les efforts isolés et individuels ne sont pas suffisants pour répondre aux menaces actuelles et futures. Il faut un effort de R&D coordonné. (…) Dans ce contexte, le gouvernement fédéral a un rôle et une responsabilité unique : il doit conduire ce changement fondamental en investissant dans la recherche fondamentale pour améliorer la sécurité et la sûreté cyber pour les personnes, les systèmes informatiques et les réseaux, l'information et les infrastructures critiques. L'investissement du gouvernement dans la recherche fondamentale est essentiel quand notre industrie n'a pas l'intérêt économique ou d'horizon suffisant en termes de retour sur investissements pour faire de tels investissements ».

[33]Source : Cyber Security M&A, decoding deals in the global cyber security industry, PwC, http://www.pwc.com/en_GX/gx/aerospace-defence/pdf/cyber-security-mergers-acquisitions.pdf
[34]Source : Trustworthy cyberspace : strategic plan for the federal cyber security research and development plan, DHS, 2011, http://www.cyber.st.dhs.gov/wp-content/uploads/2011/12/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

Quelle politique industrielle en matière de cybersécurité ?

La politique industrielle française en matière de cybersécurité doit tout d'abord s'appuyer sur une vision pragmatique des intérêts français dans le cyberespace. Au moment où les États-Unis et la Chine affirment sans complexe leurs ambitions « dans » et « par » le cyberespace, celui-ci doit désormais être considéré comme un nouvel enjeu de puissance et de souveraineté. Alors que les délocalisations industrielles sont au cœur du débat public, la question de la délocalisation des données, de leurs traitements, et des emplois qui vont avec, mérite par exemple d'être posée sans tabou. Faute de disposer d'acteurs majeurs du web, est-on prêt à observer nos opérateurs de télécommunication, voire demain nos opérateurs énergétiques, devenir de simples gestionnaires de tuyaux progressivement amputés de la relation clientèle, c'est-à-dire d'un élément essentiel de la chaîne de la valeur ? En matière de gestion des identités, pourrait-on enfin accepter de s'en remettre à des systèmes non totalement maîtrisés alors qu'il s'agit là de la « colonne vertébrale »[35] de l'économie numérique ?

Cette nouvelle politique industrielle devra en particulier identifier quelques thèmes prioritaires pour guider la R&D. Un exercice de prospective qui doit permettre, grâce à une feuille de route technologique, d'anticiper les grandes tendances technologiques et culturelles ainsi que les menaces émergentes, et de cibler quelques technologies clés en fonction du tissu existant. Objectifs : éviter le saupoudrage budgétaire, refuser un modèle purement « suiviste » et adopter une stratégie de « spécialisation intelligente » ciblant des technologies transverses, duales et couvrant les différentes couches du modèle OSI.

La France dispose dans le domaine de nombreux atouts, comme des expertises de premier plan en matière de carte à puce, d'identité numérique, de monétique ou de biométrie. Selon une étude de l'Alliance pour la Confiance Numérique[36], l'industrie de la sécurité numérique au sens large est constituée de 700 à 800 acteurs en France et représente de 50 à 56 000 emplois. Au total, ce sont ainsi 100 éditeurs, 600 sociétés de service et une centaine d'équipementiers et d'industriels qui génèreraient un chiffre d'affaires de 10 milliards d'euros, dont 5 milliards d'euros en France (3 milliards pour les services, 1,2 milliards pour les solutions logicielles, 800 millions pour les solutions matérielles).

Quelques exemples de thématiques apparaissent d'ores et déjà prioritaires : la maîtrise des composants matériels (avec en particulier la question de l'après-transistor et le remplacement du silicium), les équipements hardware (notamment les routeurs « cœur de réseau » ou les super calculateurs), les systèmes d'exploitation, les moteurs d'indexation (prise en compte du phénomène de croissance et de massification des données, appelé « big data »), la cryptographie (notamment quantique), la cartographie d'Internet ou bien encore la géo-localisation contextualisée. L'arrivée en service prochaine de Galileo jouera à cet égard un rôle clé. Il faut souligner que la plupart de ces besoins sont à la fois civils et militaires, même si certains besoins spécifiques existent côté militaire.

Il s'agit ensuite d'accélérer la transformation de ces technologies en produits et services. Cela signifie à la fois disposer d'un modèle d'incubation dynamique et encourager l'adoption précoce des technologies par des acteurs étatiques ou privés.

Les cursus de formation spécialisés doivent être également développés. Le secteur des technologies de l'information doit disposer d'une offre de formation variée permettant de former des architectes, des développeurs, des administrateurs mais aussi des techniciens, etc. Cette offre diversifiée est la condition sine qua non du développement de la R&D nationale et de l'attractivité du pays pour l'installation de centres de R&D d'entreprises étrangères.

---

[35]Guy de Felcourt, responsable de l'atelier identité numérique de Forum ATENA, newsletter n° 52, septembre 2012, http://www.forumatena.org/?q=node/391
[36]Source : les données chiffrées de la confiance numérique, société Pierre Audoin Consultants http://www.group-sts.com/documents/ACN-les_donnees_chiffrees_de_la_confiance_numerique.pdf

CEIS

LES NOTES STRATÉGIQUES

Déjà parus :

Nouvelles guerres de l'information : le cas de la Syrie. Novembre 2012

La sauvegarde de la BITD italienne : quel rôle pour les districts aérospatiaux ? Mai 2012

Enjeux caucasiens : quelles recompositions d'alliances ? Juin 2012

Puissance aérienne française et format de l'armée de l'air
Le cas de l'aviation de combat. Juin 2012

L'assistance militaire à des armées étrangères, l'avenir de l'action indirecte. Juillet 2012 – english version available

Le F35/JSF : ambition américaine, mirage européen. Juillet 2012

Ariane et l'avenir des lancements spatiaux européens. Août 2012

Compagnie Européenne d'Intelligence Stratégique (CEIS)

Société Anonyme au capital de 150 510 € - SIRET : 414 881 821 00022 - APE : 741 G

280 boulevard Saint Germain – 75007 Paris
Tél. : 01 45 55 00 20 – Fax : 01 45 55 00 60