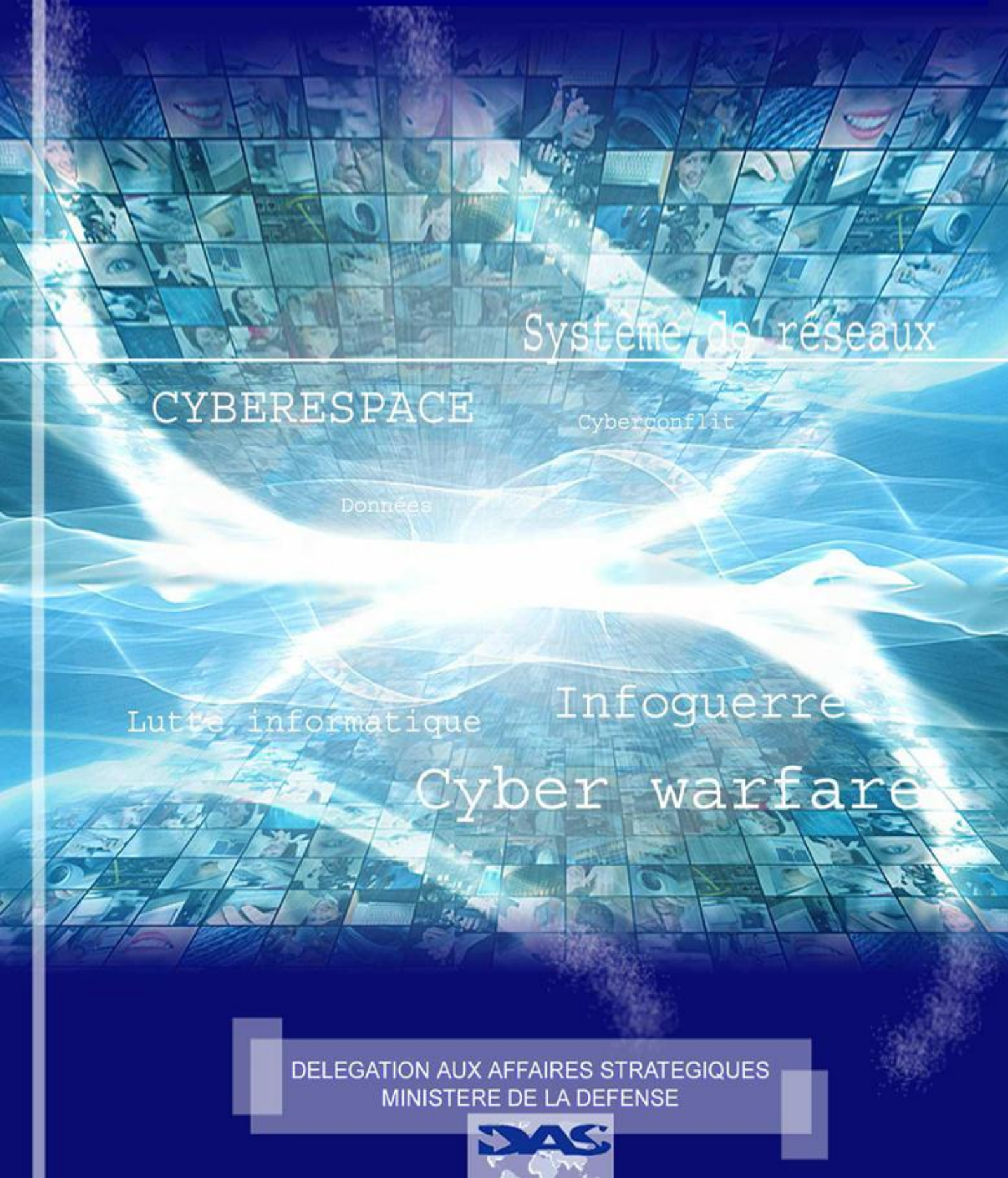
Observatoire du Monde Cybernétique
Trimestriel

Décembre
2012



DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Sommaire

1 Analyse de la stratégie de R&D américaine en matière de cybersécurité

1.1 Introduction : la dynamique du marché ne suffit pas

Depuis quelques années, un constat s'est imposé aux Etats-Unis : la dynamique du marché ne suffit pas à créer les technologies nécessaires en matière de cybersécurité et de cyberdéfense. Il subsiste donc des gaps capacitaires, tant dans le domaine civil que militaire, que le marché ne peut combler, faute de retour sur investissement à court terme ou tout simplement de conscience du besoin. Plus grave encore, la concentration de la R&D sur des problématiques de court terme, son morcellement, sa dimension purement incrémentale ne permettrait pas, selon certains analystes, de créer les conditions d'un nouveau rebond technologique lié à la convergence croissance de l'informatique, des nanotechnologies et des biotechnologies, « *l'alliance du bit, de l'atome et du gène* » pour reprendre les propos de Michel Riguidel[1].

Les Etats-Unis ont donc choisi d'adopter une politique industrielle très volontariste. L'importance des moyens financiers et humains consentis, ainsi que la concentration des énergies sur ce thème, laissent même penser à une sorte de nouvelle initiative de défense stratégique « cyber » lancée par le Président Obama, dont on se souvient qu'il déclarait en mai 2009 : « *la prospérité des Etats-unis au 21ème siècle dépend de la cybersécurité* ». Les menaces, mêmes réelles, ainsi que la réponse cybersécuritaire qui leur est apportée, ne sont finalement qu'un prétexte. L'objectif est plus vaste : il s'agit d'engager une offensive politique, diplomatique, technologique, industrielle et militaire permettant aux Etats-Unis de maintenir et d'accentuer le gap qui les sépare encore de leurs compétiteurs dans le cyberespace.

La stratégie américaine dans le cyberespace repose sur cinq piliers :

- Un pilier politique constitué par la stratégie internationale pour le cyberespace, publiée en mai 2011, qui défend une approche universelle et libératrice d'internet[2] ;
- Un pilier militaire avec la stratégie du DoD pour les opérations dans le cyberespace, publiée en juillet 2011[3]. Ce document reconnait le cyberespace comme un espace de bataille, évoque la nécessité de la coopération internationale et insiste sur le besoin d'innovations technologiques rapides dans le domaine ;

[1] http://www.economie.gouv.fr/files/files/import/2011_france_numerique_consultation/2011_france_numerique_michel_riguidel.pdf
[2] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[3] http://www.defense.gov/news/d20110714cyber.pdf

- Un pilier sécuritaire constitué de la stratégie de cybersécurité du Department of Homeland Security intitulée « Blueprint for a secure cyber future » et publiée en novembre 2011[4] ;

- Un pilier sectoriel comprenant des stratégies en matière d'éducation, de services financiers, de transport, d'énergie et de santé ainsi qu'une stratégie nationale en matière d'identité électronique édictée par la Maison blanche en avril 2011 intitulée « National strategy for trusted identities in cyberspace »[5] dont l'objectif est de bâtir un écosystème d'identité interopérable pour accéder aux services en ligne ;

- Un pilier technologique comprenant la stratégie fédérale édictée par la Maison Blanche en décembre 2011 ainsi que l'agenda technologique du DHS de novembre 2009.

Quelles sont les caractéristiques ce dernier pilier ? Quelles sont les priorités technologiques qui ont été identifiées ? Quels sont les principaux programmes ? Quels sont les résultats de cette politique industrielle ? Telles sont les questions qui seront abordées dans la suite de cette note.

1.2 Des « roadmaps » technologiques structurées

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 »[6] ;

- L'agenda technologique du DHS publié en novembre 2009 intitulé « a roadmap for cybersecurity research »[7].

1.2.1 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 4 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

[4] http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf
[5] http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
[6] http://www.cyber.st.dhs.gov/wp-content/uploads/2011/12/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf
[7] http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

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 métriques 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.

1.2.1.1 Designed-in security

L'objectif est de parvenir à une meilleure intégration de la sécurité dans les phases d'ingénierie et de développement logiciel. Plusieurs exemples de programmes de R&D gouvernementaux dans le domaine :

- Survivable Systems Engineering [OSD/SEI CERT] ;
- Trusted Computing [DARPA, NSA, OSD, NIST] ;
- Software Development Environment for Secure System Software & Applications [ONR] ;
- META (flows, tools, and processes for correct-by-construction system design) [DARPA] ;
- Software Assurance Metrics And Tool Evaluation (SAMATE) [DHS, NIST].

1.2.1.2 Tailored trustworthy spaces

L'objectif est de pouvoir 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. Plusieurs exemples de programmes lancés dans ce domaine :

- Trusted foundation for cyberspace operations [OSD and Service Labs] ;
- High assurance security architectures [NSA, ONR, AFRL,NIST] ;
- Content and Context Aware Trusted Router (C2TR) [AFRL] ;
- Information Security Automation Program [NIST, NSA,DHS] ;
- Security Content Automation Protocol (SCAP) ;
- Access Control Policy Machine [NIST] ;
- Military Networking Protocol (MNP) program [DARPA] ;
- High-Level Language Support for Trustworthy Networks [NSF].

1.2.1.3 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. Quelques exemples de programmes dans ce domaine, essentiellement gérés par les agences du Département de la défense :

- Polymorphic Enclaves and Polymorphic Machines [AFRL]
- Self Regenerative, Incorruptible Enterprise that Dynamically Recovers with Immunity [AFRL]
- Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) [DARPA]
- Cyber Camouflage, Concealment, and Deception [DARPA]
- Morphing Network Assets to Restrict Adversarial Reconnaissance (Morphinator) [Army]
- Defensive Enhancements for Information Assurance Technologies (DEFIANT) [Army]
- Robust Autonomic Computing Systems [ONR]

1.2.1.4 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 métriques permettant de dire si un système est sûr ou non, s'il peut l'être et à quel coût supplémentaire. L'objectif est donc de développer une base scientifique pour l'analyse de risques et du retour sur investissement. Un exemple de programme : le « Secure And Trustworthy Cyberspace » (SaTV program) de la NSF.

1.2.2 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 »[8] organisé autour de 14 axes de recherche (« Technical Topic Area ou TTA). Chacun de 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 et plus de 200 offreurs ont été sollicités. Des présentations détaillées de certains de ces projets ont été faites lors d'une réunion qui s'est tenue en octobre 2012[9]. Plus de 1 000 contributions ont également été reçues par le DHS dans le cadre de cette consultation. On note enfin que 4 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.

[8] http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf
[9] http://www.cyber.st.dhs.gov/oct2012pi-presentations/

Liste des organisations sélectionnées

- Applied Visions, Inc, Northport, NY
- Carnegie-Mellon University, Pittsburgh, PA
- Columbia University, New York, NY
- Def-Logix, Provo, UT
- George Mason University, Fairfax, VA
- Georgia Tech Research Corp., Atlanta, GA[10].
- HRL Laboratories, LLC, Malibu, CA
- IBM Research, Yorktown Heights, NY
- International Computer Science Institute, Berkeley, CA
- ITT Advanced Engineering & Sciences Division, Rome, NY
- Kestrel Technology, LLC, Palo Alto, CA
- Merit Network Inc, Ann Arbor, MI
- Morgridge Institute for Research, Madison, WI
- Naval Postgraduate School, Monterey, CA
- Northrop Grumman Information Systems, McLean, VA
- Oak Ridge National Laboratory, Oak Ridge, TN
- Pacific NW National Laboratory, Richland, WA
- Purdue University, West Lafayette, IN
- Raytheon BBN Technologies, Cambridge, MA
- Rutgers University - New Brunswick Campus, New Brunswick, NJ
- The Trustees of Princeton University, Princeton, NJ
- The University of Alabama at Birmingham, Birmingham, AL
- The University of North Carolina at Chapel Hill, Chapel Hill, NC
- Trustees of Dartmouth College, Hanover, NH
- Trustees of Indiana University, Bloomington, IN
- University of California, San Diego, San Diego, CA

[10] L'importance du Georgia Institute of Technology (Georgia Tech) en matière de R&D cybersécurité mérite d'être soulignée. Le Georgia Tech Research Institute (GTRI) a ainsi été désigné en 2011 pour conduire le programme HOST (Homeland Open Security Technology). A noter également que le Georgia Tech possède une antenne à Metz.

- University of Illinois at Urbana-Champaign, Champaign, IL
- University of Maryland, College Park, MD
- University of Southern California Information Sciences Institute, Marina del Rey, CA

Pour chaque axe, un exemple de l'un des projets lancés est sommairement présenté ci-dessous à titre d'illustration.

1.2.2.1 Axe 1 : l'assurance qualité logiciel.

Parmi les projets :

- le « Software Assurance Market Place » ou SWAMP. Chaque développeur est incité à transmettre son code et peut ainsi améliorer la qualité de son logiciel (voir axe spécifique n°14).
- Le « Protected Repository For the Defense of Infrastructure Against Cyber Threats » ou PREDICT[11]. 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 simulation

Différents programmes 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[12].
- 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[13]. Lockheed Martin, le principal contractant, a remporté un contrat de 80 millions de dollars sur 5 ans pour fournir le support logiciel et hardware[14].

[11] http://www.cyber.st.dhs.gov/predict et http://www.predict.org/
[12] http://www.cyber.st.dhs.gov/deter/ et http://www.deter-project.org/
[13] Source : http://www.gsnmagazine.com/node/27823
[14] Source : http://defensesystems.com/articles/2012/11/13/lockheed-national-cyber-range-contract.aspx?m=2

- Le Information Assurance Range de la DISA. C'est la société Breaking Point Systems[15] qui travaille sur ce projet (ainsi que pour l'EUCOM).
- Le Joint Information operations (IO) range du Joint Staff.

1.2.2.2 Axe 2 : les métriques de sécurité

Ces métriques doivent être basées sur des standards et permettre une visualisation interactive. Exemples de métriques : vulnérabilités, exploitabilité, probabilité d'une attaque etc.

1.2.2.3 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.

1.2.2.4 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.

1.2.2.5 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.

1.2.2.6 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.

[15] Source : http://www.breakingpointsystems.com/default/assets/File/white%20papers/WP-Cyber-Range-40200-01-1.pdf

1.2.2.7 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.

1.2.2.8 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.

1.2.2.9 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.

1.2.2.10 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).

1.2.2.11 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[16].

1.2.2.12 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[17].

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

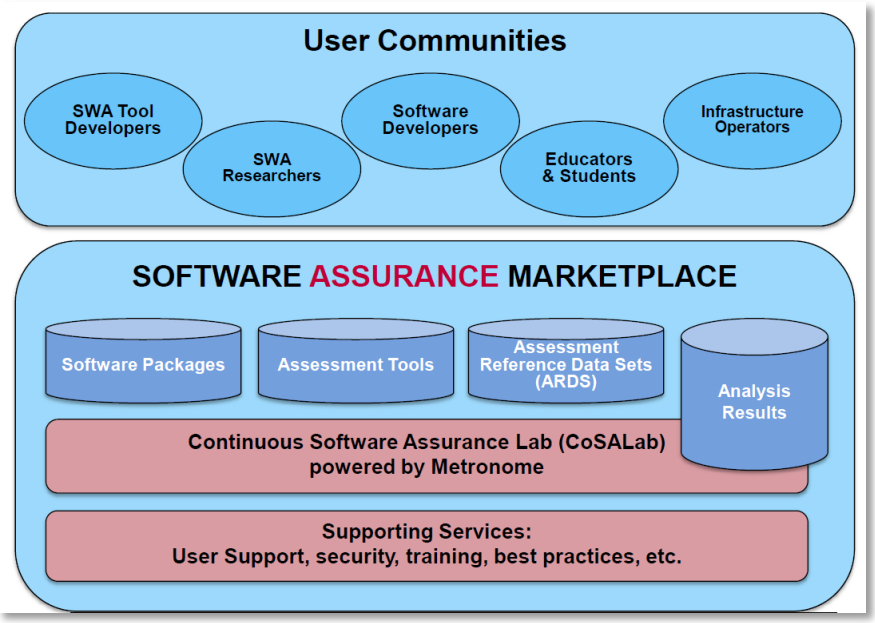
1.2.2.13 Axe 13 : une hygiène numérique inspirée par la nature (« Nature inspired cyber health »)

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.

1.2.2.14 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.

Composition du SWAMP[18]



1.3 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 le Office of Naval Research, le Army Research Laboratory ou le Air Force Research Laboratory qui ont tous des programme en matière de cybersécurité. A noter par exemple le projet CHAMP (Counter-electronics

[18] http://www.cyber.st.dhs.gov/wp-content/uploads/2012/10/Day-3.02-TTA14-SWAMP-Livny.pdf

High-powered Microwave Advanced Missile Project) développé par le 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 informatiques[19].

1.3.1 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[20]. L'importance de ces budgets montre s'il en était besoin 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 fabriqué 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).

1.3.2 Exemple d'un 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 »[21]. Le meilleur exemple de cette recherche de l'innovation de rupture est sans doute le projet Plan X annoncé en mai 2012[22] pour un budget de 110 millions de dollars.

1.3.2.1 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.

---

[19] http://securityaffairs.co/wordpress/10783/cyber-warfare-2/new-weapons-for-cyber-warfare-the-champ-project.html
[20] Source http://www.darpa.mil/NewsEvents/Releases/2012/03/12c.aspx
[21] 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
[22] Communiqué de presse officiel : http://www.darpa.mil/NewsEvents/Releases/2012/10/17.aspx

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.[23] »

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.

1.3.2.2 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.

[23] Source : broad agency announcement, foundational Cyberwarfare (Plan X), 20 novembre 2012, https://www.fbo.gov/utils/view?id=49be462164f948384d455587f00abf19

- 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 permet 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.

1.3.2.3 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.

1.3.2.4 Au plan technique

Au plan technique, l'objectif de Plan X est de construire une plateforme de bout en bout basé 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.

- TA1 (architecture système) : 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.

- TA2 (analyse de l'espace de bataille cyber). 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.

- TA3 (construction de mission). 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 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.

- TA4 (exécution de mission) : 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…).

- TA5 (interfaces intuitives). 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.

1.4 Quels résultats ?

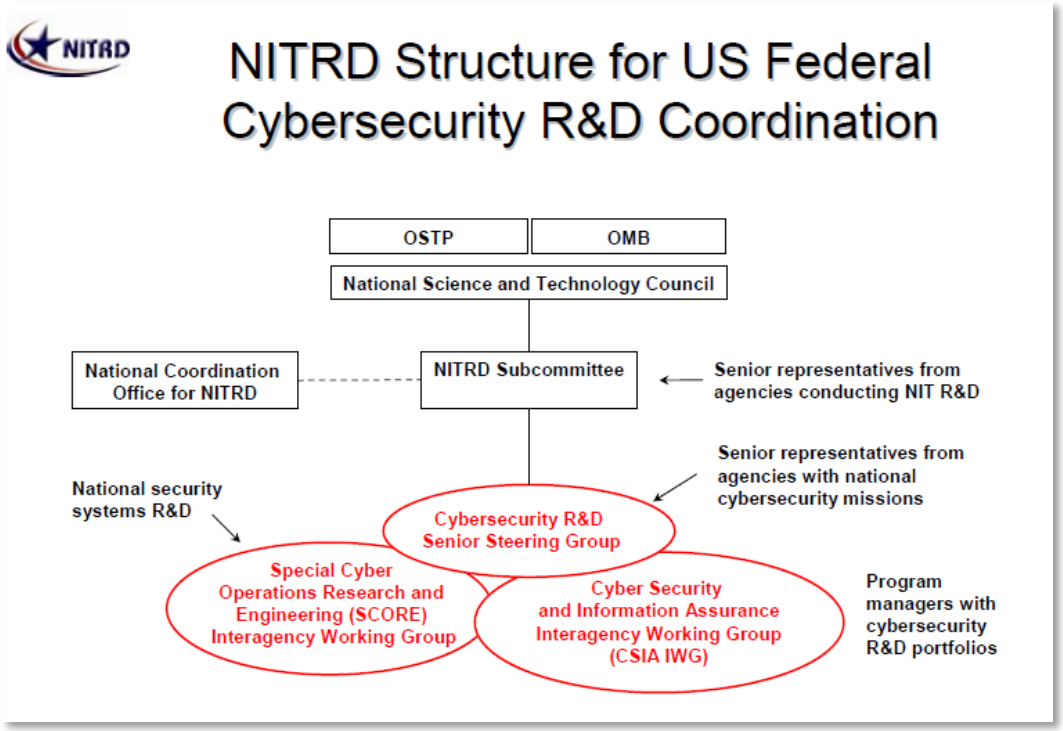
Peu après l'élection d'Obama, la Commission sur la cybersécurité pour la 44ème présidence mise en place par le Center for Strategic International Studies (CSIS) estimait que seulement 300 millions sur les 143 milliards de R&D investis en 2009 par le gouvernement fédéral était affecté à la cybersécurité. 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.

1.4.1 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 :

- Le SSG, le Senior Steering Group for Cybersecurity, qui comprend des représentants des deux groupes de travail suivants ;
- Le CSIA, Cyber Security and Information Assurance Working Group, groupe de travail interagences sur la cybercriminalité.
- Le SCORE, Special Cyber Operations Research and Engineering : établi en 2008 et travaille 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[24]



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) ;

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

- 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).

1.4.2 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[25], 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 %.

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

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

	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

1.4.3 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 et aborde des disciplines scientifiques variées.
- 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[26].

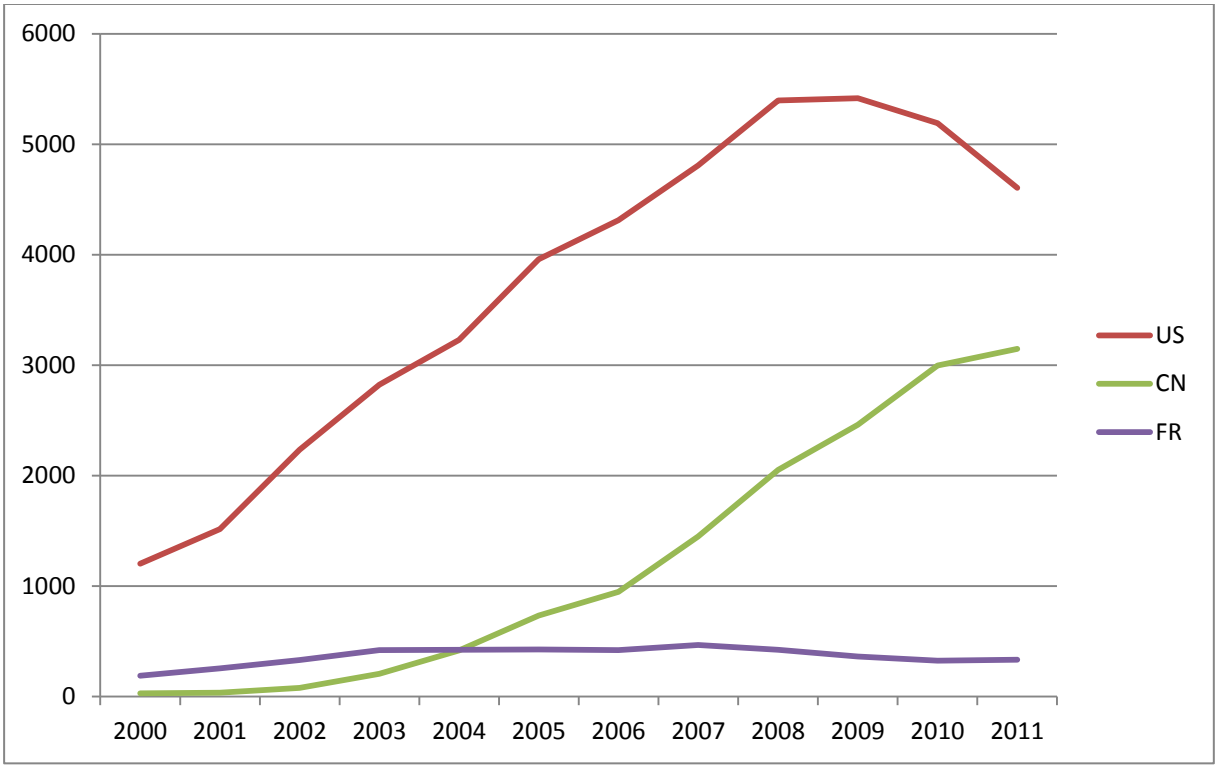
1.4.4 Analyse des brevets en matière de sécurité

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 qui pourraient faire l'objet d'une valorisation dans le domaine considéré.

1.4.4.1 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[27] ont été publiés avec pour pays d'application prioritaire les Etats-Unis[28]. 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



[26] http://www.cybersecurityresearch.org/news_and_events/press_releases/pr_20121023.html
[27] 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).
[28] Source : base de données Thomson Innovation.

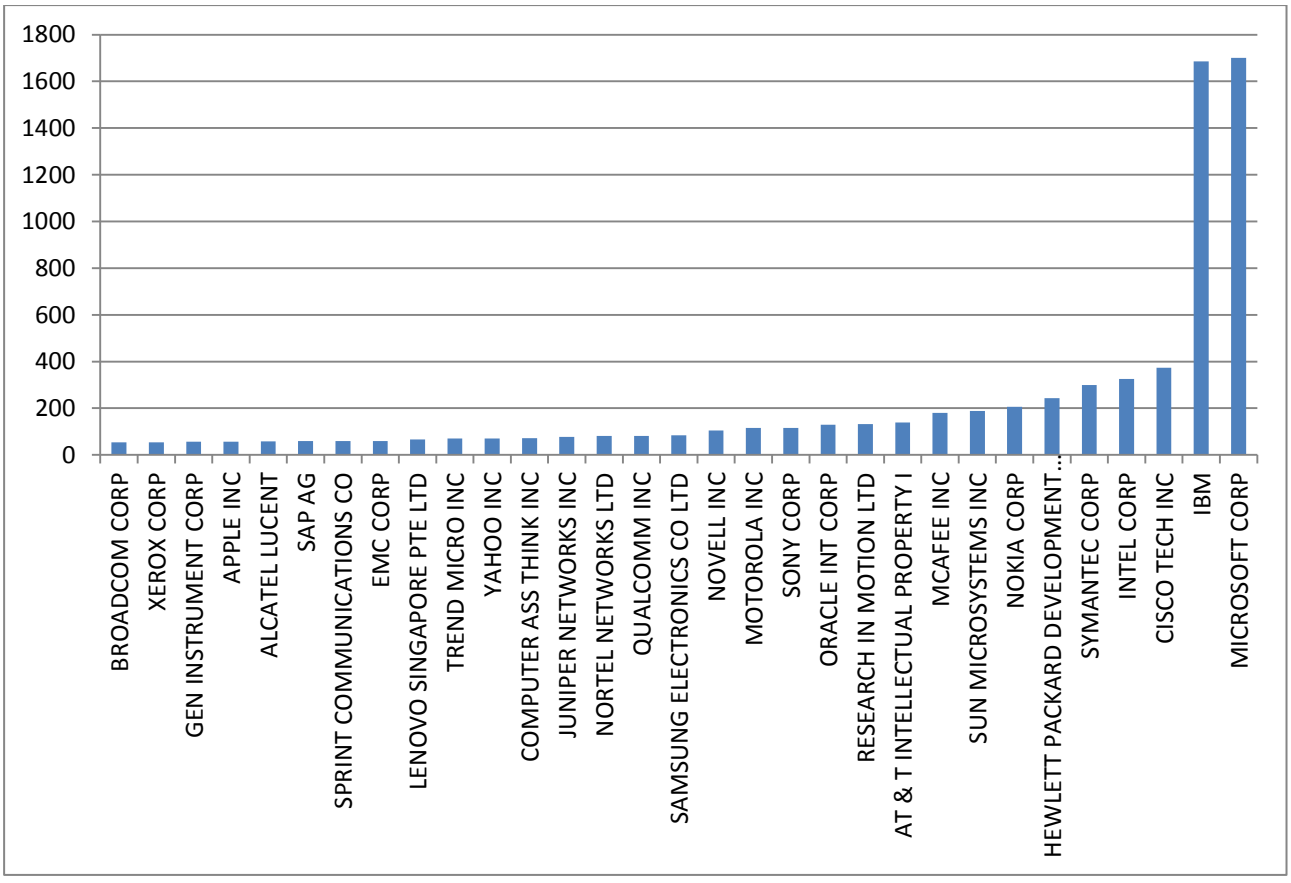
En termes de comparaison, les Etats-Unis restent donc très largement en tête en termes de brevets sécurité, même si l'on observe une montée en puissance continue de la Chine sur la période, résultat de la stratégie de propriété intellectuelle du gouvernement chinois, relayée dans la plupart des entreprises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

1.4.4.2 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.

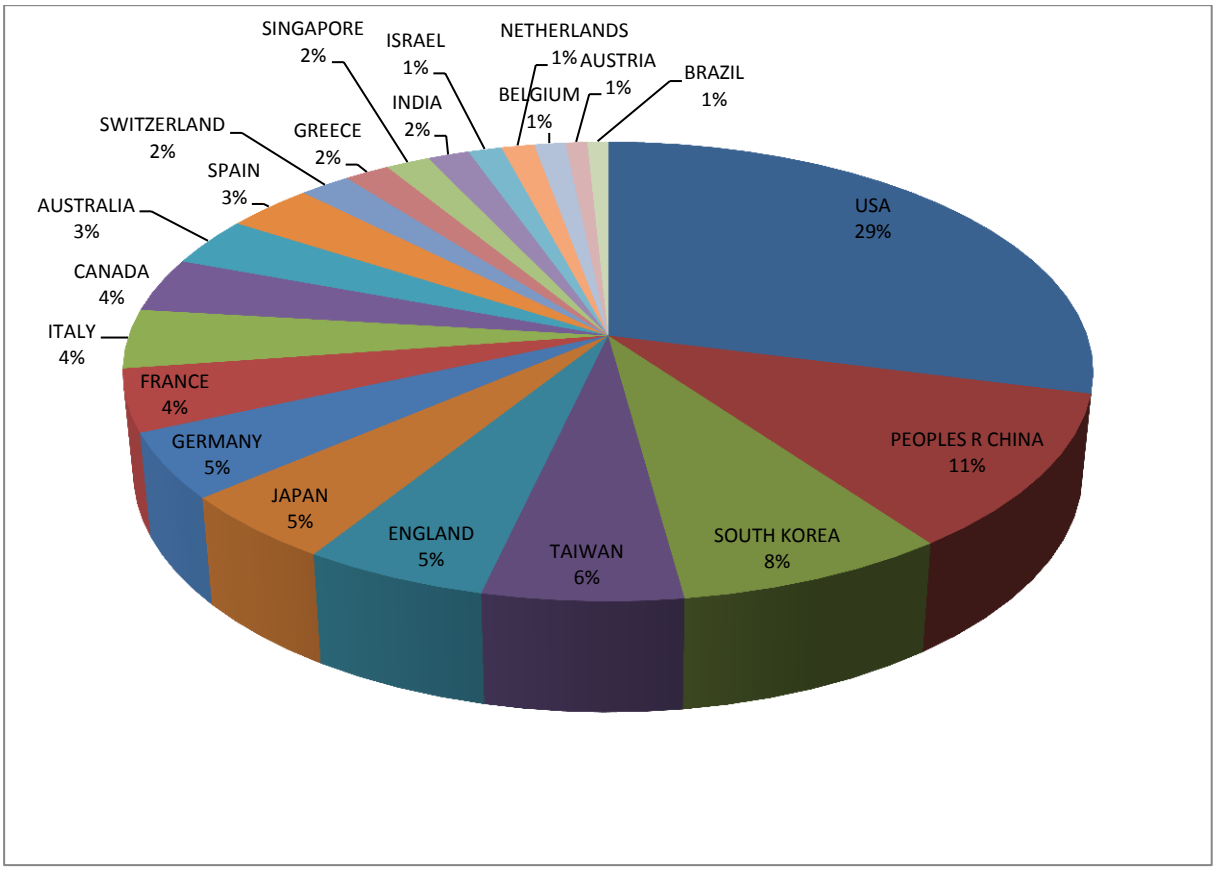
Principales sociétés déposantes



1.4.5.1 Analyse comparée des publications scientifiques

L'analyse des publications scientifiques en matière de sécurité informatique de 2000 à 2011[29] 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



1.4.6 Une stratégie soutenue par une approche de plus en plus décomplexée

La politique de R&D américaine est soutenue par une approche de plus en plus décomplexée du cyberespace. Les révélations sur l'origine de Stuxnet dans le livre écrit par David E. Sanger[30], le lancement du projet « plan X » de la DARPA : tout ceci témoigne de la volonté du pays de marquer de son empreinte le débat sur la cybersécurité et de pousser progressivement l'ensemble des opinions publiques à accepter l'éventualité de conflits militaires dans le cyberespace. On passe d'une zone de secret à une zone de semi-secret où il n'est plus question de nier même s'il ne s'agit pas de tout dire.

[29] Source : base de données Thomson Innovation
[30] Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power, juin 2012.

James A. Lewis, du Center for Strategic and International Studies[31] explique ainsi qu'il voit le plan X comme un tournant dans le débat sur le « cyber warfare ». On assume désormais la possibilité d'utiliser le cyberespace comme un champ de bataille et donc de développer des armes offensives. Une leçon tirée des expériences récentes : Matthew Waxman, un professeur de l'université Columbia et ancien du DoD constate aussi 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* ».

[31] 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

2 Le cadre juridique français de l'action répressive des autorités sur Internet

Le Patriot Act américain a fait l'actualité 2012[32]. Véritable « ingérence », accomplissement de la « prédiction d'Orwell »… Les qualificatifs sont nombreux pour ce texte donnant aux autorités américaines la main sur une quantité incroyable de données circulant sur Internet. Cependant, la France n'est pas en reste.

Qu'il s'agisse du blocage et du filtrage, de l'observation et interception de données, ou des mesures de conservation et de perquisition de données, les autorités françaises disposent d'un arsenal, certes éparpillé, mais vaste, d'outils leur permettant d'agir et de faire respecter l'ordre sur Internet.

Quel est aujourd'hui le cadre juridique français de l'action répressive des autorités sur Internet ? Quels sont les outils à leur disposition ?

La Convention européenne des droits de l'homme stipule en son article 1er que *« toute personne a droit à la liberté d'expression »*, et pose une exception reprise par la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique : *« L'exercice de cette liberté ne peut être limité que dans la mesure requise, […] par la sauvegarde de l'ordre public […] ».* C'est, entre autres, sur ce fondement que de nombreuses mesures viennent restreindre certains droits et libertés fondamentaux.

2.1 Les mesures de blocage et de filtrage

Les acteurs militant pour une meilleure lutte contre la cybercriminalité « poussent au développement du blocage pour empêcher l'accès aux contenus « illicites » »[33].

Les débats sur le blocage et le filtrage ont été initiés en 2008 en France, avec le lancement des discussions autour de la LOPPSI 2[34]. Dans un discours de la même année, Michèle Alliot-Marie

[32] Adopté le 25 octobre 2001, le « Uniting and Strengthening America by Providing Appropriate Tools Required to intercept and Obstruct Terrorism Act » créé à l'attention des sociétés américaines et leurs filiales, ainsi qu'aux sociétés non américaines dont les serveurs ou les plateformes se trouvent aux Etats-Unis, des obligations[32] de laisser accéder les services d'enquête aux données stockées dans leur serveur notamment sur leur plateforme Cloud, y compris les données stockées en Europe par des sociétés américaines, à l'insu des titulaires des données sans qu'ils en soient immédiatement informés[32]. La loi a notamment confirmé l'autorisation accordée au FBI d'installer un logiciel de surveillance, nommé Carnivore (DS 1000), chez certains FAI, afin d'épier la circulation des messages électroniques et de conserver les traces de la navigation sur le Web de toute personne suspectée de contact avec une puissance étrangère. Et pour ce faire, seul l'aval d'une juridiction spéciale, dont les activités sont confidentielles, est nécessaire. Le texte de la loi allonge également la liste des informations que les enquêteurs peuvent exiger des FAI sans l'aval d'un juge. Il autorise ces derniers à remettre aux autorités, de leur propre initiative, des informations qui ne sont pas relatives au contenu, telle la navigation sur le Web. En contrepartie, le prestataire n'a aucune obligation d'avertir le propriétaire des données. Selon l'Electronic Frontier Foundation, Google répondrait à des milliers d'injonction de ce type.

[33] http://www.assemblee-nationale.fr/13/rap-info/i3336.asp

expliquait en effet sa détermination à bloquer les contenus pédopornographiques. Si le texte n'a pas été adopté à l'époque, la possibilité de bloquer des sites Internet a bien été intégrée dans le droit français, mais dans d'autres contextes : **dans le cadre de la protection de la propriété intellectuelle et dans le cadre de la lutte contre les opérateurs illégaux de jeux en ligne**.

C'est dans son article 4, venant modifier l'article 6 de la loi n° 2004–575 du 21 juin 2004 pour la confiance dans l'économie numérique, que le nouveau texte de la LOPPSI 2 a prévu à son tour le **blocage de sites pédopornographiques**.

La procédure décrite est entièrement administrative : les hébergeurs sont contactés par une autorité administrative (avec le concours de l'OCLCTIC) afin de procéder au blocage de tel ou tel site. Site ayant préalablement été mentionné sur la fameuse « liste noire ».

2.1.1 Les critiques

Les critiques émises font référence aux conséquences de cette mesure de blocage[35]. La conséquence directe est la restriction de la liberté d'expression et de communication. La conséquence indirecte est le risque de sur-blocage, d'accroissement de l'utilisation des techniques d'anonymisation et de détournement et tout simplement d'inefficacité.

2.1.1.1 L'absence de juge face à la restriction de la liberté d'expression et de communication.

Toute restriction à un droit ou une liberté fondamentale doit être accompagnée d'une procédure garantissant les principes du droit au procès équitable (article 6 de la Convention européenne des droits de l'homme). Comme indiqué par le Conseil constitutionnel dans sa décision Hadopi[36], seul le juge peut mettre en œuvre des mesures qui, si elles sont mal évaluées, pourraient mettre en cause *« l'exercice du droit de libre communication et de la liberté de parler, écrire et imprimer ».* Mais cette jurisprudence n'a pas été retenue lors de l'analyse, par ce même Conseil constitutionnel, du texte de la LOPPSI 2, notamment de son article 4.

Le texte a été définitivement adopté comme tel, avec un système de liste noire validé par les autorités administratives. Les promesses de réforme du gouvernement de Jean-Marc Ayrault en faveur de l'intervention d'un juge dans le processus de l'article 4 sont, quant à elles, loin d'être acquises. L'objectif était en effet de ne pas publier de décret d'application de cet article, écartant ainsi sa mise en œuvre. Mais en octobre dernier, le ministère de l'Intérieur annonçait[37] que le décret manquant, relatif à *« la compensation des surcoûts résultant des obligations mises à la charge des opérateurs dans le cadre de la lutte contre la diffusion des images ou des représentations de mineurs à caractère pornographique »* était toujours sur les rails, et serait en pleine consultation auprès des fournisseurs d'accès à Internet.

---

[34] LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieur

[35] http://www.assemblee-nationale.fr/13/rap-info/i3336.asp

[36] Décision n° 2009-580 DC du 10 juin 2009 relative à loi favorisant la diffusion et la protection de la création sur internet. Considérant 12.

[37] http://questions.assemblee-nationale.fr/q14/14-2747QE.htm

Notons toutefois que le recours au juge ne suffirait pas, à lui seul, à garantir un Internet libre et neutre, selon certains observateurs. La Quadrature du net[38] rappelle en ce sens que *« même dans les cas où il est ordonné par l'autorité judiciaire, le filtrage du Net porte atteinte aux libertés fondamentales, ainsi qu'à l'architecture de l'Internet libre et ouvert en conduisant à la « balkanisation » du réseau. Il mène à la censure généralisée et au contrôle d'Internet à mesure de son extension à de nouveaux domaines, par exemple pour sanctionner des propos diffamatoires ou des atteintes au droit d'auteur. »*[39]

2.1.1.2 La neutralité du net

La neutralité du net se définit comme *« l'absence de discrimination dans l'acheminement des flux »*[40] ; ou le fait de *« traiter tous les contenus, sites et plateformes de manière égale »*[41]. Ce principe fondateur d'internet *« garantit que les opérateurs télécoms ne discriminent pas les communications de leurs utilisateurs, mais demeurent de simples transmetteurs d'information. »*[42]

Pour l'ASIC[43], les mesures de blocage et de filtrage présentent le risque de porter atteinte au principe essentiel de neutralité vis-à-vis des contenus et des correspondances privées transportées sur les réseaux.[44] Si le débat sur la neutralité du net est avant tout économique et technique, il présente également des aspects sociétaux et éthiques. En vertu de la neutralité du net, l'internaute a la possibilité d'accéder à toute sorte de contenus, sans discrimination.

Cette neutralité trouve un écho dans les textes, les opérateurs devant en effet respecter un principe de neutralité à l'égard des contenus qu'ils acheminent (art. L. 33-1 et D. 98-5 du Code des Postes et télécommunications électroniques) et le secret des correspondances (art. L. 32-3 du même code). Mais ces dispositions ne portent que sur le contenu des informations transportées. Rien ne les empêchant de faire varier les *« caractéristiques de l'acheminement »*[45].

Les objectifs fixés aux autorités réglementaires à l'article L. 32-1 CPCE leur permettent de promouvoir certaines dimensions de la neutralité (notamment à travers l'objectif de veiller à *« l'absence de discrimination, dans des circonstances analogues, dans les relations entre opérateurs et fournisseurs de services de communications au public en ligne pour l'acheminement du trafic et l'accès à ces services* », ainsi qu'au *« respect par les opérateurs de communications électroniques du secret des correspondances et du principe de neutralité au regard du contenu des messages transmis »)»*. Mais cette vision reste restrictive. C'est pourquoi la députée Laure de la Raudière, dans

---

[38] Organisation de défense des droits et libertés des citoyens sur Internet

[39] http://www.laquadrature.net/fr/filtrage-du-net

[40] http://www.assemblee-nationale.fr/13/rap-info/i3336.asp

[41] « *Network Neutrality, Broadband Discrimination »,* Journal of Telecommunications and High Technology Law, *2003 - juriste américain Tim Wu*

[42] http://www.laquadrature.net/fr/neutralite_du_Net

[43] L'Association des services internet communautaires (ASIC), créée en 2007, est la première organisation française qui regroupe les acteurs du web 2.0.

[44] http://www.pcinpact.com/news/51491-hadopi-loppsi-asic-usurpation-blocage.htm

[45] http://www.assemblee-nationale.fr/13/rap-info/i3336.asp

un rapport[46] présenté le 13 avril 2011, propose de donner valeur juridique à une conception plus ferme de la neutralité du net.

2.1.1.3 La boîte de Pandore

Selon la Quadrature du net, l'argument de la lutte contre la pédopornographie ne serait qu'un cheval de Troie, *« un faux prétexte visant à légitimer le filtrage administratif d'Internet et à déployer une infrastructure technique de censure ».* L'association relève que le système de liste noire mis en place remet en cause tout espoir de contestation et de contrôle du contenu de cette liste. Il s'agirait, dès lors, d'une *« violation disproportionnée de la liberté d'expression et de communication, notamment dans le cas d'inévitables censures collatérales »*[47].

2.1.1.4 Analyse juridique[48]

C'est l'article 10 de la Convention européenne des droits de l'homme qui protège la liberté de communication. *« Toute personne a droit à la liberté d'expression. […] L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique […] ».* Et comme le sous-entend cet extrait, toute atteinte à cette liberté doit être « *légitime* » et *« nécessaire dans une société démocratique ».*

En somme, l'article 4 de la LOPPSI devrait être efficace et proportionnel. Or, ce sont justement les deux critiques principales formulées contre les mesures de blocage et de filtrage de contenus en ligne : elles seraient totalement disproportionnées au regard de leur inefficacité concrète. Le blocage et le filtrage ne seraient donc pas *« nécessaires dans une société démocratique »*.[49]

2.1.1.4.1 Inefficacité

Beaucoup d'observateurs jugent le dispositif de l'article 4 inefficace, voire contreproductif.

Concrètement, il s'agit de mettre en œuvre une technique de filtrage dite *« hybride »* permettant le blocage au niveau de l'URL, c'est-à-dire au niveau de la page elle-même et non du serveur entier. Cette solution, relativement chère, limite considérablement les risques de blocage abusif. Pour autant, elle est particulièrement complexe à mettre en œuvre sur le réseau français compte tenu de ses caractéristiques spécifiques (réseau ouvert) et pourrait nécessiter des aménagements importants des infrastructures de certains opérateurs Internet[50].

---

[46] http://www.assemblee-nationale.fr/13/rap-info/i3336.asp

[47] Félix Tréguer, chargé des affaires institutionnelles et juridiques à La Quadrature du Net - http://www.laquadrature.net/fr/loppsi-definitivement-adoptee-internet-sous-controle

[48] Etude juridique relative aux mesures de filtrage publiée en 2009 par une équipe de juristes européens - Cormac Callanan, Marco Gercke, Estelle De Marco et Hein Dries-Ziekenheiner, 2009, Internet Blocking: Balancing Cybercrime Responses in Democratic Societies, Aconite Internet Solutions : http://www.aconite.com/blocking/study

[49] http://www.laquadrature.net/fr/le-filtrage-dinternet-viole-letat-de-droit

[50] Les enfants du Net III - Forum des droits sur l'Internet - http://www.forumInternet.org/IMG/pdf/reco-enfantsIII_finale.pdf

Cette méthode a été très critiquée car, comme a pu l'expliquer Carole Gay, responsable affaires juridiques et règlementaires de l'AFA, l'association des fournisseurs d'accès et de services Internet, *« lorsqu'un contenu est bloqué, il reste en ligne, et n'est que temporairement inaccessible puisque la mesure de blocage est facilement contournable. L'auteur du contenu bloqué peut en effet en quelques minutes faire héberger son site sous un autre nom de domaine ou une autre URL, selon la technique de blocage utilisée ».*

De son coté, *« l'internaute souhaitant accéder au site qui fait l'objet du blocage dispose de plusieurs outils de contournement ; il peut notamment demander l'accès au site de façon anonyme, par l'intermédiaire d'un "anonymiseur", qui lui permettra d'utiliser un DNS non sujet à restrictions. L'internaute peut encore utiliser le DNS d'un FAI étranger, en modifiant l'un des paramètres de sa connexion Internet »*[51].

Une des solutions pouvant être envisagée, est le retrait des contenus à la source, et non leur blocage ou filtrage. Toutefois, aucune méthode de blocage n'est sûre à 100% et les dommages collatéraux seront toujours présents quel que soit le type de filtrage utilisé[52]. Cependant, s'adresser à l'hébergeur du contenu afin qu'il le retire à la source permet de laisser le nom de domaine accessible et d'éviter le blocage d'une adresse IP ou de tout un nom de domaine.

L'association des industriels allemands de l'Internet, l'ECO, avait notamment démontré en 2008 que la suppression des contenus pédopornographiques à la source était bien plus efficace que le blocage au niveau des FAI ou la saisie de noms de domaine. Une position retenue par les autorités allemandes qui, en 2010, se sont positionnées contre une mesure similaire à l'article 4. Suite à une expérience[53], le gouvernement allemand a décidé d'abandonner définitivement le filtrage du net et indiqué qu'il soumettrait plutôt loi relative à la suppression des contenus. Cette dernière technique étant d'une efficacité supérieure.

2.1.1.4.2 Proportionnalité

La mesure de blocage prévue par l'article 4 de la LOPPSI 2 doit être proportionnée au but poursuivi. Afin d'évaluer ce point, la Cour européenne vérifie si l'objectif final *« peut être atteint de manière satisfaisante par d'autres moyens, moins restrictifs de droits »*[54].

Les mesures de blocage et de filtrage sont difficilement considérées comme proportionnelles en raison du fort risque de sur-blocage. Déjà, en 2008, lorsque l'Internet Watch Foundation (IWF) a souhaité bloquer la page de Wikipédia consacrée à l'album Virgin Killer du groupe Scorpion à cause de la pochette d'album soupçonnée d'être pédopornographique, c'est tout une partie du site Internet Wikipédia qui a été rendue inaccessible.

---

[51] Communiqué de l'AFA : « LOPPSI 2 et blocage de la pédopornographie : une solution d'ultime recours pour l'AFA » http://www.afafrance.com/p_loppsi2_AFA.html

[52] Voir étude réalisée par Christophe Espern – « Principe, intérêts, limites et risques du filtrage hybride à des fins de blocage de ressources pédopornographiques hébergées sur des serveurs étrangers » - http://www.laquadrature.net/files/note-quadrature-filtrage-hybride.pdf

[53] http://www.laquadrature.net/fr/supprimer-au-lieu-de-bloquer-ca-marche

[54] CEDH, 27 mars 1996, Goodwin contre Royaume-Uni

Autre cas d'espèce : dans le cadre de l'opération « Protect Our Children » menée conjointement par le Department of Homeland Security (DHS) et le Department of Justice (DOJ), les Services des douanes américaines disposant d'un mandat de saisie à cet effet, ont fait procéder au blocage de 10 noms de domaines au contenu jugé pédopornographique. Mais suite à une erreur, ce sont 84 000 sites légitimes qui ont été bloqués. Ont ainsi été faussement accusés des pages personnelles (greyghost.mooo.com par exemple), des blogs, des sites de commerce électronique et même des sites ayant servi de miroirs dédiés à Wikileaks (newworld.mooo.com) ; tous étant redirigés par le serveur DNS vers l'adresse IP http://74.81.170.110/ hébergeant la page d'avertissement des autorités américaines. Le nom de domaine mooo.com, l'un des noms de domaines les plus utilisés du fournisseur de domaines gratuits FreeDNS, aurait été saisi par erreur par les autorités américaines, entraînant ainsi le blocage et la redirection abusifs de 84 000 sous-domaines lui étant associés. Cette erreur a été rendue possible par la méthode de filtrage choisie par les autorités américaines : le blocage par saisie de nom de domaine.

Cette méthode, si elle permet d'empêcher efficacement l'accès à un site, comporte un risque de sur-blocage élevé. En effet, puisqu'elle consiste à filtrer l'ensemble du domaine Internet qui héberge le site litigieux, le blocage peut conduire à fermer l'accès à l'ensemble du site concerné et non aux seules pages illicites. Cette méthode entraîne également le blocage de tous les services proposés sur le domaine blacklisté : pages Web (sous-domaines : par exemple « exemple.mooo.com »), courriels, messagerie instantanée, etc. Le blocage peut aussi s'étendre à d'autres sites Internet, qui eux sont licites, mais partagent le même nom de domaine. Techniquement, plusieurs milliers de sites peuvent ainsi relever d'un unique serveur DNS. C'est notamment le cas pour des services d'hébergement mutualisé ou les pages dites personnelles[55]. Et c'est ce qui s'est produit lorsque le nom de domaine mooo.com a été saisi : 84 000 de ses sous-domaines ont été, eux aussi, interdits d'accès.

Il faut souligner enfin que le sur-blocage ou blocage abusif de sites peut, lorsqu'il touche des sites de commerce en ligne ou lorsqu'il porte atteinte à l'honneur et la considération du titulaire de la page Internet, donner lieu à une action en justice. Dans son communiqué, FreeDNS a précisé qu'il avait fallu environ trois jours avant que les serveurs DNS se mettent à jour et que le blocage et la redirection soient supprimés ; trois jours durant lesquels les visiteurs des sites visés ont été systématiquement redirigés vers le message du DHS et du DOJ accusant à tort le titulaire du site d'un crime fédéral. L'utilisation d'un système à haut risque de « sur-blocage » pose donc d'évidentes difficultés et s'avère potentiellement contraire à la liberté d'expression et de communication ainsi qu'à la liberté du commerce et de l'industrie. De ce fait, il présenterait un risque d'engagement de la responsabilité de l'État et des fournisseurs d'accès ayant procédé au blocage[56].

[55] Les enfants du Net III - Forum des droits sur l'Internet - http://www.forumInternet.org/IMG/pdf/reco-enfantsIII_finale.pdf
[56] Les enfants du Net III - Forum des droits sur l'Internet - http://www.forumInternet.org/IMG/pdf/reco-enfantsIII_finale.pdf

Il en ressort donc que, *« en raison de ces inévitables effets collatéraux, le filtrage est une mesure bien trop dangereuse par rapport à son objet. Le risque de sur-blocage remet donc fortement en question le caractère proportionné des mesures de filtrage. »*[57]

Cela a été rappelé récemment dans l'affaire dite Scarlet / SABAM, en Belgique. En l'espèce, une juridiction nationale avait ordonné à Scarlet, fournisseur d'accès à Internet, de mettre en place un système de filtrage général visant à rendre impossibles les échanges de fichiers par peer-to-peer reprenant une œuvre du répertoire de la société d'auteurs SABAM. Dans un l'arrêt du 24 novembre 2011, la CJUE a souligné que le droit de l'Union s'opposait à une telle injonction, dès lors notamment que cette mesure ne respectait pas l'exigence d'assurer un juste équilibre entre les droits et libertés en cause.[58]

2.1.2 Récapitulatif des mesures

Texte	Fondement/contexte
Loi relative à la confiance dans l'économie numérique, article 6, I.7. : « Lorsque les nécessités de **la lutte contre la diffusion des images ou des représentations de mineurs** relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 du présent I [les fournisseurs d'accès à internet] les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai. »	Lutte contre la pédopornographie
Loi relative à la confiance dans l'économie numérique, article 6, I.8. : « L'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 [les hébergeurs] ou, à défaut, à toute personne mentionnée au 1 [les fournisseurs d'accès à internet], toutes mesures propres à **prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne**. »	Faire cesser tout type d'atteinte constituée par un contenu ou service en ligne
Code de la propriété intellectuelle, article L. 336-1 : « En présence d'une **atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne**, le tribunal de grande	Atteinte au droit d'auteur ou à un droit voisin

[57] http://www.laquadrature.net/fr/le-filtrage-dinternet-viole-letat-de-droit#footnote7_w229ywj
[58] http://www.arcep.fr/uploads/tx_gspublication/rapport-parlement-net-neutralite-sept2012.pdf

instance, statuant le cas échéant en la forme des **référés**, peut ordonner à la demande des titulaires de droits sur les œuvres et objets protégés, de leurs ayants droit, des sociétés de perception et de répartition des droits visées à l'article L. 321-1 ou des organismes de défense professionnelle visés à l'article L. 331-1, **toutes mesures propres à prévenir ou à faire cesser une telle atteinte** à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier.	
Loi relative aux jeux en ligne, article 61 : « À l'issue de ce délai, en cas d'inexécution par l'opérateur intéressé de l'injonction de cesser son activité d'offre de paris ou de jeux d'argent et de hasard, le président de l'Autorité de régulation des jeux en ligne peut saisir le président du tribunal de grande instance de Paris aux fins d'ordonner, en la forme des référés, **l'arrêt de l'accès à ce service** aux personnes mentionnées au 2 du I [les hébergeurs] et, le cas échéant, au 1 du I [les fournisseurs d'accès à internet] de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. »	Lutte contre les opérateurs illégaux de jeux en ligne

2.2 Les mesures de cybersurveillance relatives à la procédure pénale

Face au caractère volatile de la cybercriminalité, de nombreux textes sont venus renforcer les moyens à disposition des enquêteurs judiciaires. Deux catégories de mesures peuvent être évoquées : d'une part, on retrouve les outils classiques qui sont exploités dans le cadre des investigations cybercriminelles (perquisition, infiltration…) ; d'autre part, le législateur a mis au point des outils spécifiques à l'avènement d'internet. L'une des mesures les plus polémiques est sans nul doute celle de captation des données informatiques introduite par la LOPPSI 2.

2.2.1 Focus sur la captation des données informatiques

2.2.1.1 Contexte

La possibilité, pour l'officier de police judiciaire, de procéder à l'interception de communications sur Internet existait depuis quelques temps déjà. Ce procédé, visant les correspondances privées, est décrit aux articles 100 et suivants du code de procédure pénale. Au moyen d'une dérivation sur la ligne de l'internaute suspecté ou avec le concours de l'opérateur Internet ou de téléphonie mobile, l'enquêteur *« interposera »* un procédé d'enregistrement des conversations (un sniffer par exemple).

Mais cette disposition était largement insuffisante face aux nouveaux usages de la criminalité en bande organisée. Désormais se côtoient chiffrement, transmission des informations hors ligne par clé USB ou CD-ROM, utilisation du mode brouillon de la boîte aux lettres, utilisation de poste informatique non-surveillé par les procédés classiques de l'article 100 du CPC, etc. Autant de techniques qui mettent en échec le dispositif du sniffer décrit ci-dessus.

C'est pourquoi la LOPPSI 2 est venue insérer dans le code de procédure pénale un nouvel article 706-102-1 permettant la capture de données informatiques à distance. Un décret du 3 novembre 2011[59] a précisé la liste des personnes susceptibles de mettre en œuvre ce *« mouchard »*[60] :

- la direction centrale de la police judiciaire et ses directions interrégionales et régionales ;
- la direction centrale du renseignement intérieur ;
- les offices centraux de police judiciaire ;
- l'unité de recherche, assistance, intervention et dissuasion ;
- les groupes d'intervention de la police nationale ;
- la sous-direction de la police judiciaire de la gendarmerie nationale ;
- les sections de recherches de la gendarmerie nationale ;
- les sections d'appui judiciaire de la gendarmerie nationale ;
- le groupe d'intervention de la gendarmerie nationale.

Ces entités peuvent *« sans le consentement des intéressés »,* accéder aux données informatiques *« telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères »*.

L'outil visé par ce texte est un logiciel de type keylogger. Il permettra aux autorités policières de prendre connaissance des données en temps réel.

Deux modes opératoires pourront être employés :

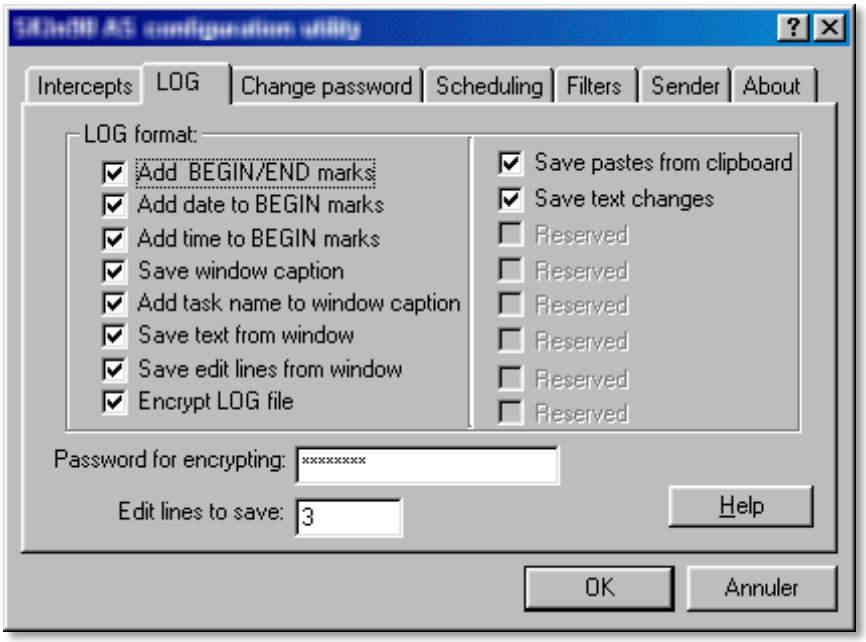
- L'installation physique sur l'ordinateur ou le terminal de l'intéressé d'un appareil d'interception ;

[59] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024752774

[60] ttp://www.numerama.com/magazine/20460-loppsi-les-personnes-habilitees-a-utiliser-le-mouchard-devoilees.html

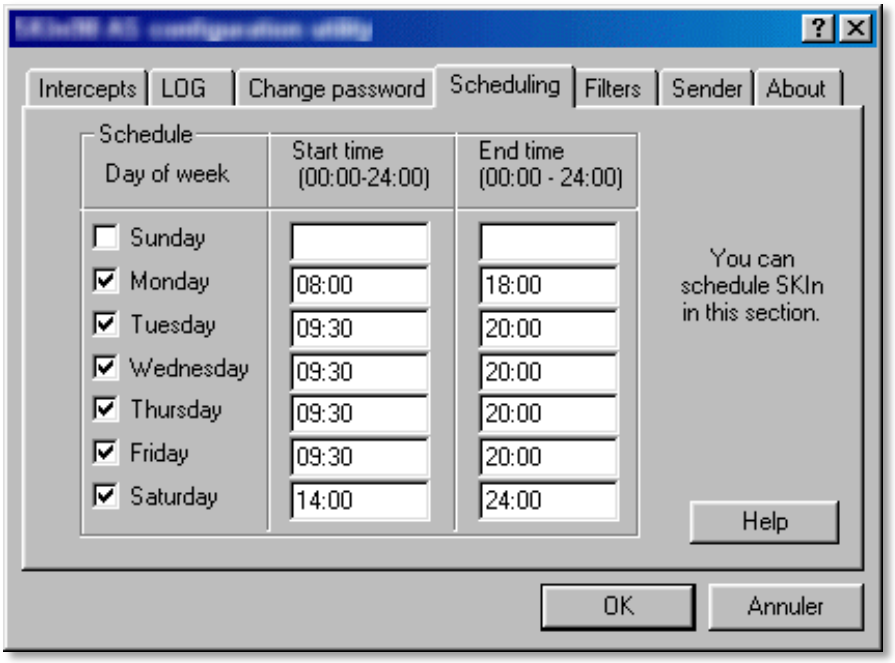
Exemple d'un enregistreur de frappe matériel.

Source : http://www.weboctopus.nl/webshop/img/p/59-430-large.jpg

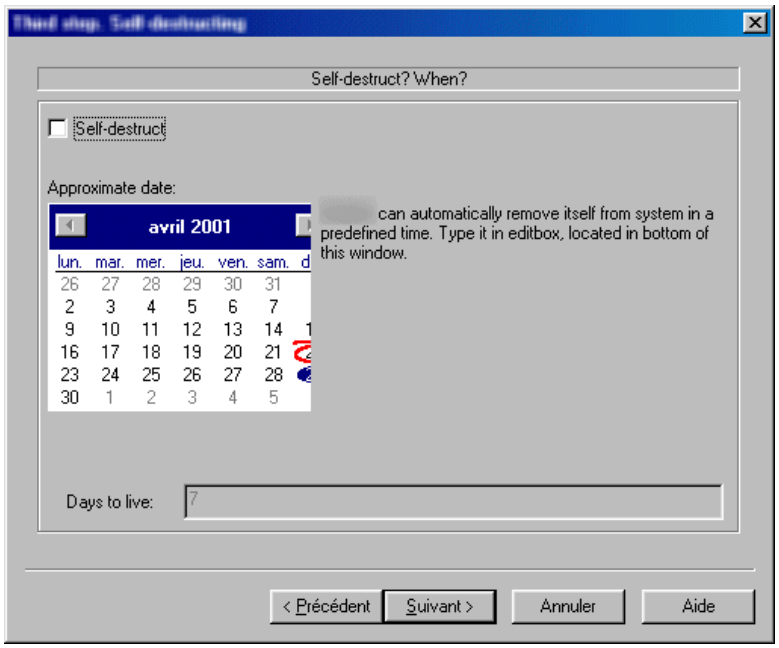


Captures d’écran de la console d’administration d’un keylogger

(Possibilité de prendre des captures d’écran)



(Possibilité de programmer dans le temps l'enregistrement des frappes)



(Possibilité de programmer une autodestruction du logiciel)

Source : http://www.securiteinfo.com/attaques/divers/keylogger.shtml

- Le juge d'instruction pourra également autoriser *« la transmission par un réseau de communications électroniques »* d'un logiciel.

2.2.1.2 Les critiques

Censé permettre la simple adaptation du principe des écoutes téléphoniques à l'ère informatique[61], ces dispositions sont toutefois à l'origine d'importantes polémiques.

2.2.1.2.1 Dérives et détournement possible

Dès octobre 2011 ont été publiés les résultats d'une étude menée par les hackers du Chaos Computer Club, plus grand rassemblement de hackers en Europe. Ils ont démontré que le logiciel utilisé par les services de police allemand, **Quellen-TKÜ**, disposant de fonctionnalités similaires à celui envisagé par la LOPPSI 2 pour les forces de police et de gendarmerie françaises, était très peu sécurisé. Ce dernier peut être utilisé pour y envoyer des données, et peut être contrôlé à distance par des tiers[62]. Il serait même possible d'y installer des modules à distance, d'envoyer de fausses preuves sur l'ordinateur du suspect, voire d'en supprimer. Ce qui poserait un grave problème de *« sincérité de l'enquête »,* selon les hackers. De plus, quid de la réutilisation de tels dispositifs à des fins cybercriminelles ?

2.2.1.2.2 Vers un détournement de la finalité de la perquisition informatique ?

Dans un avis datant du 16 avril 2009, la CNIL a émis quelques critiques à l'égard d'une version du projet de loi LOPPSI 2, notamment à l'égard des dispositions prévoyant le fameux *« mouchard ».* La Commission précise que ces interceptions ne doivent concerner que ce qui est *« utile à la manifestation de la vérité »*, afin d'éviter que les données liées à la vie privée soient enregistrées et stockées inutilement. Ce dispositif prévoit en effet d'aller bien plus loin que la perquisition informatique (en procédant à une capture en continu et à l'insu de l'intéressé), et que la captation de correspondance plus classique (en interceptant bien plus que de simples correspondances, et en agissant également hors ligne).

2.2.1.2.3 Des mesures participant à l'alimentation d'un système de surveillance généralisée ?

Ces dispositions de la LOPPSI 2, couplées à celles prévues par le même texte sur le blocage des sites par une autorité administrative, ont valu à la France d'être qualifiée de pays à surveiller par Reporters Sans Frontières.

Le cas du honeypot

Véritable leurres, les honeypots sont des ordinateurs, serveurs, ou programmes laissés volontairement vulnérables afin d'attirer et de piéger les hackers. Ils permettent ainsi d'observer le mode opératoire du cybercriminel et, par la même, de récupérer des données permettant de l'identifier.

La légalité de l'utilisation de ce procédé par l'enquêteur judiciaire est cependant encore source de controverses. En vertu du principe de loyauté de la preuve pénale, le policier ne peut provoquer la

[61] http://www.numerama.com/magazine/20460-loppsi-les-personnes-habilitees-a-utiliser-le-mouchard-devoilees.html
[62] http://www.numerama.com/magazine/20112-des-failles-sur-le-mouchard-informatique-de-la-police-allemande.html

commission d'une infraction. Tout élément de preuve obtenu de cette façon sera irrecevable. Ce principe a été rappelé par la Chambre criminelle de Cour de cassation dans un arrêt du 4 juin 2008 (Bulletin criminel 2008, n°141). En l'espèce, un ressortissant français avait été identifié suite à sa connexion à un site contenant des images pédopornographiques. Or ce site avait été monté de toutes pièces par l'unité de criminalité informatique de la police de New York dans le but d'attirer les pédophiles. Dans cette affaire, la Cour a déclaré irrégulières et donc irrecevables ces preuves, considérant qu'elles avaient été obtenues par provocation policière. Ce raisonnement peut trouver à s'appliquer dans le cas du honeypot.

Il faut rappeler que seul l'officier de police judiciaire est soumis au principe de légalité de la preuve. La partie privée bénéficie quant à elle d'une jurisprudence clémente. Dans un arrêt du 27 janvier 2010 (pourvoi n°09-83.395), la Cour de cassation a rappelé qu'*« aucune disposition légale ne permet aux juges répressifs d'écarter des moyens de preuve remis par un particulier aux services d'enquête, au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale ».*

2.2.2 Récapitulatif des mesures

Texte	Fondement/contexte
De la **captation des données informatiques** : Article 706-102-1 du Code de Procédure Pénale : « Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 (criminalité et à la délinquance organisées) l'exigent, le juge d'instruction peut […]mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères. » Le texte a été adopté sur le modèle de celui des sonorisations effectuées dans le cadre d'une information judiciaire. Cette mesure ne peut être mise en œuvre que pour une durée de 4 mois renouvelable une seule fois (article 706-102-3 CPP).	Renforcement de la lutte contre la criminalité et de l'efficacité des moyens de répression
Décret n° 2011-1431 du 3 novembre 2011 « portant modification du code de procédure pénale pris pour l'application de l'article 706-102-6 de ce code relatif à la captation des données informatiques ».	

Précise la liste des entités autorisées à procéder à la captation de données informatiques.	
Circulaire du 4 août 2011[63] portant sur la présentation des dispositions de la loi n° 2011-267 du 14 mars 2011 dite « LOPPSI II » relatives à la criminalité organisée et autres contentieux spécialisés Précise le contexte et l'utilité du texte LOPPSI 2.	
L'interception de communications : articles 100 et suivants du code de procédure pénale. Procédé décrit ci-dessus.	Interception réalisée dans le contexte plus classique des correspondances privées
Le gel de données informatiques situées hors du territoire national. Article 29, Convention sur la cybercriminalité de Budapest de 2001. Cet article dispose en qu'« une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition […], de la saisie […], ou de la divulgation desdites données ».	Améliorer la coopération internationale et l'efficacité des enquêtes transfrontalières
Loi pour la confiance dans l'économie numérique, article 6, II Ce texte impose aux prestataires techniques d'identifier leurs clients et ainsi de **conserver les données techniques** pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.	Conservation des données techniques pour les besoins de l'enquête pénale Transpose les dispositions de la directive européenne 2000/31/CE
Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne	Précise les données à conserver par les FAI et les

[63] http://asset.rue89.com/files/JUSD1121937C.pdf

ayant contribué à la création d'un contenu mis en ligne[64].	hébergeurs
L.34-1 du Code des postes et des communications électroniques (CPCE) impose une obligation de conservation des données aux opérateurs de communication électronique.	
Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques. Précisait à l'époque les données que doivent conserver les opérateurs.	Transposition de la directive européenne, adoptée en 2006 pour lutter contre le terrorisme et la criminalité organisée : Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE
Encadrement du chiffrement : Article 434-15-2 du Code pénal : « Est puni de trois ans d'emprisonnement et de 45 000 euros d'amende [*taux*] le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de **refuser de remettre ladite convention aux autorités judiciaires** ».	Volonté d'encadrer l'usage du chiffrement par la Loi pour la confiance dans l'économie numérique

64 http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000023646013&dateTexte=&oldAction=rechJO&categorieLien=id

Article Article 132-79 du Code pénal : L'utilisation d'un **moyen chiffrement dans le but de commettre un délit** peut engendrer une peine aggravante.	
Perquisition informatique : L'article 56 al. 5 du code de procédure pénale permet la perquisition de données informatiques. L'enquêteur procédera *« à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous-main de la justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition ».* L'enquêteur peut également procéder à une perquisition en ligne (article 57-1 CPP pour l'enquête de flagrance, 76-3 pour l'enquête préliminaire, 97-1 sous-commission rogatoire). Et ce droit de perquisitionner connaît une limite importante : l'accès à des données stockées sur des serveurs situés hors du territoire national. Si les données accessibles en ligne sont stockées en France, aucun problème ne se posera. La perquisition s'effectuera selon la procédure ordinaire définie à l'article 56 al. 2 du code de procédure pénale. Si les données sont localisées à l'étranger, l'article 57-1 du code indique qu' « elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur ».	Adaptation du droit de perquisitionner aux évolutions de l'ère informatique. Permet d'envisager les situations impliquant le cloud computing
L'infiltration numérique Article 706-81 du code de procédure pénale. Des enquêteurs spécialement habilités peuvent « surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs ». Ce procédé ne peut être utilisé que pour les enquêtes concernant les infractions listées par l'article 706-73 du même code.	Infiltration numérique dans le cadre des besoins de l'enquête

2.3 Conclusion

Si les débats internationaux actuels laissent entrevoir une séparation nette entre les Etats pratiquant la censure et ceux prônant la liberté sur Internet, la distinction est plus floue en réalité. En témoigne le classement de RSF plaçant la France comme Etat à surveiller. En cause : l'existence de nombreux fondement justifiant le blocage et le filtrage selon les intérêts d'ayant-droits ; l'utilisation de méthodes controversées de blocage et de filtrage ; une remise en cause non-proportionnée des droits et libertés fondamentaux. Et ce constat est celui qui prévaut au sein de la société civile et des défenseurs d'un Internet libre et neutre, même s'il s'agit parfois de donner aux forces de police les moyens de rivaliser avec des cybercriminels inventifs et novateurs.

L'un des éléments clés de cette perception négative reste l'usage dual de certaines technologies. Le « mouchard » proposé par la LOPPSI 2 ne serait rien d'autre qu'un malware exploité à des fins policières. Le filtrage (ou le blocage), ici utilisé a priori uniquement à des fins légitime de protection des mineurs ou de protection contre les jeux illicites d'argent en ligne, a pour conséquence concrète d'introduire dans le régime français la possibilité de filtrer. Le risque étant que ce filtrage soit au fil de l'eau étendu à toute sorte de site « gênant » quel qu'en soit le motif. Un risque prospectif d'autant plus important puisque les technologies exploitées dans certains Etats contre leurs dissidents lors du Printemps arabe pour filtrer leurs réseaux sont les mêmes.

Le cas de la LOPPSI est encore plus évocateur puisqu'il consacre le filtrage administratif, excluant l'autorité judiciaire du processus de prise de décision. Les risques de dérive sont en effet très présents à l'encontre des contenus légitimes sur Internet. Les risques de détournement aussi.

En somme, en se donnant les moyens d'agir sur Internet, l'Etat, qui tente de reprendre une part de sa souveraineté d'action, bouscule la vision libre et neutre du réseau qu'on certains de ses défenseurs.

Le challenge est donc de trouver le juste milieu, le juste placement du curseur afin de ne pas susciter le refus catégorique de la société civile. Le recours au juge ? Le retrait à la source ? Si des solutions semblent envisageables quant aux problématiques de blocage et de filtrage, l'issue semble moins évidente lorsqu'il s'agit d'étendre les moyens d'action des cyberenquêteurs. La lutte contre la cybercriminalité se heurte en effet généralement à des contraintes d'ordre éthique et juridique. Comment concilier les impératifs du respect de la vie privée des citoyens et de leurs droits fondamentaux aux besoins de marge de manœuvre essentielle à une démarche efficace de lutte contre les cybermenaces ?