Lettre n°43 - octobre 2015 - disponible sur omc.ceis.eu

"The ransomware is that good. To be honest, we often advise people just to pay the ransom.."
Déclaration de Joseph Bonavolonta, agent spécial adjoint chargé du programme CYBER et du contre-espionnage au FBI fin octobre 2015 au Cyber Security Summit 2015

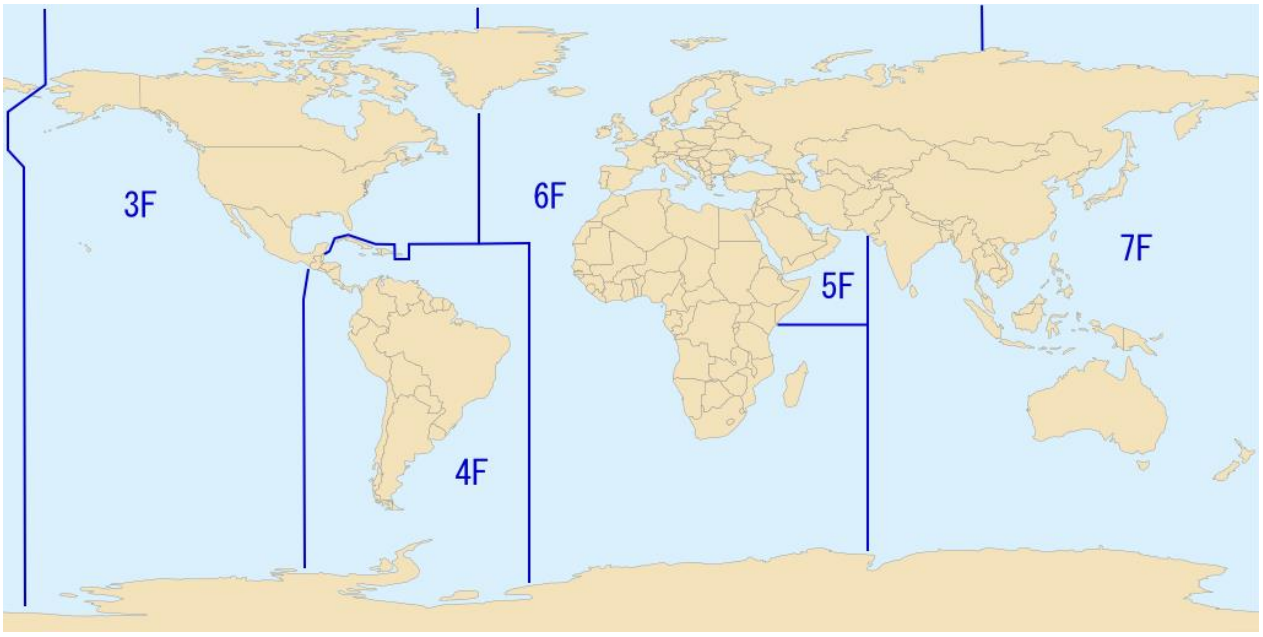
Table des matières

LA CYBERDEFENSE DANS L'US NAVY : ETAT DES LIEUX

Avec 326 046 miliaires actifs et 107 115 réservistes, l'*US Navy* est la force la plus importante du département de la Marine. Elle permet aux Etats Unis de projeter leur puissance militaire dans les domaines maritimes et aériens. En temps de paix, elle a aussi pour mission de sécuriser les voies maritimes et d'assurer la libre circulation des biens et des services.

Il y a actuellement 6 flottes actives au sein de l'*US Navy*, dont 5 sont en charge d'une zone géographique et la dernière du cyberespace :

- 3ème flotte : *U.S. Pacific Fleet's 3rd Fleet*
- 4ème flotte : *Naval Forces Southern Command's 4th Fleet*
- 5ème flotte : *Naval Forces Central Command's 5th Fleet*
- 6ème flotte : *Naval Forces Europe's 6th Fleet*
- 7ème flotte : *U.S. Pacific Fleet's 7th Fleet*
- 10ème flotte : *Fleet Cyber Command's 10th Fleet*



Source: Wikiversity

Le Fleet Cyber Command

Créé en 2010 pour gérer tous les aspects relatifs au cyberespace, le *Fleet Cyber Command*[1] (FCC) assure diverses missions[2] :

- Il constitue la composante maritime du *Cyber Command* américain ;
- Il est l'autorité de l'*US Navy* pour les opérations au sein du cyberespace ;
- Il dirige le service cryptologique de l'*US Navy* ;
- En étroite coordination avec tous les commandants de l'*US Navy*, il fournit les capacités pour les opérations d'information et les opérations dans le cyberespace et en assure le commandement opérationnel.

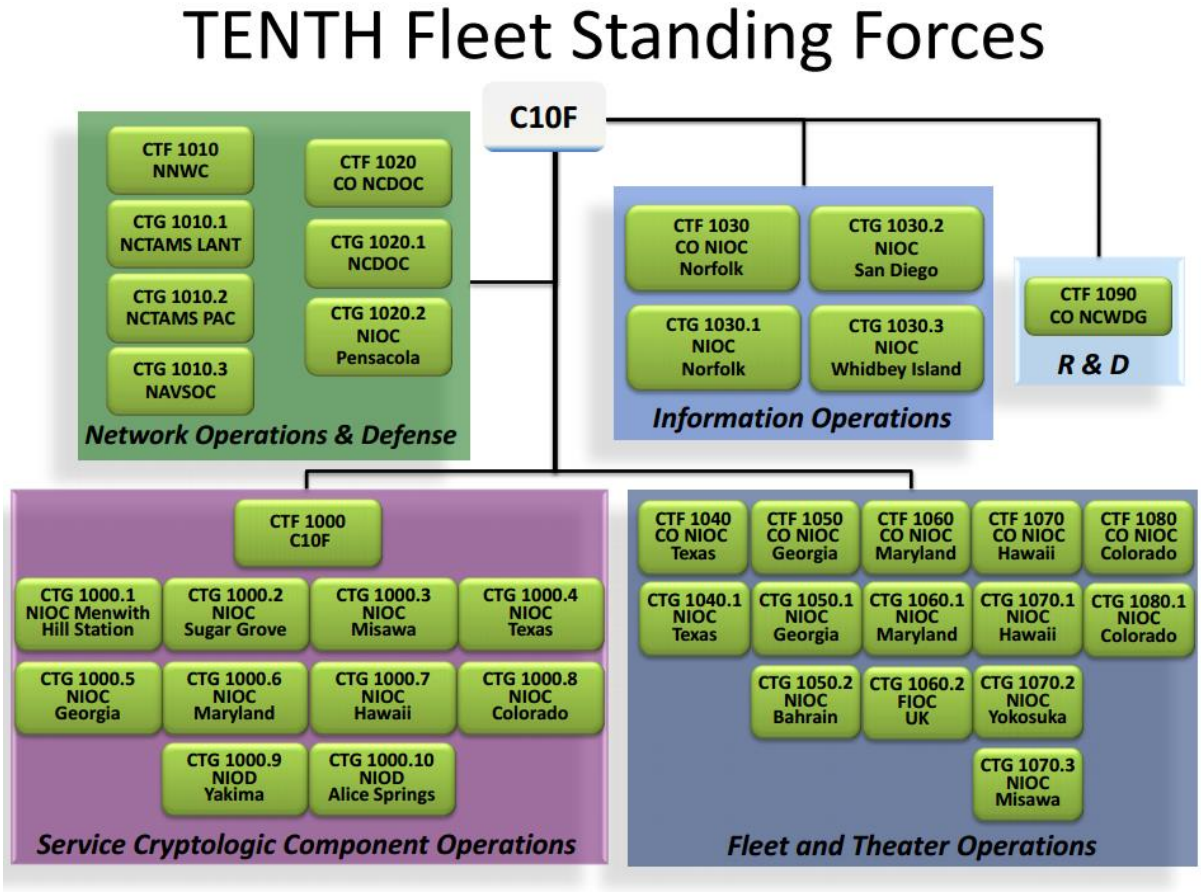
Sa mission est de « *de diriger les opérations dans le cyberespace de la Marine à l'échelle mondiale pour dissuader et vaincre l'agresseur et d'assurer la liberté d'action pour atteindre des objectifs militaires dans et à travers le cyberespace ; d'organiser et de diriger les opérations de cryptologie de la Marine à travers le monde et de soutenir les opérations d'information et de planification de l'espace et des opérations, comme indiqué ; de diriger, exploiter, entretenir, sécuriser et défendre la partie maritime du Global Information Grid (GID : réseau de transmission et de traitement de l'information maintenu par le département de la Défense des États-Unis) ; de livrer de la cyber intégrée, des opérations d'information, de cryptologie et de capacités spatiales ; et de fournir les besoins opérationnels de cyber commun, du réseau mondial de la Marine.* »[3]

L'organisation ci-dessous montre que le *Fleet Cyber Command* est composé de nombreuses unités (37 au total), classées en 5 différents domaines *: Network Operations & Defense* (exploitation des réseaux et cyberdéfense), *Information Operations* (guerre électronique, lutte informatique offensive, guerre de l'information), *R&D, Service Cryptologic Component Operations* (communications et chiffre) et *Fleet and Theater Operations* (commandements régionaux).

[1] http://www.public.navy.mil/fcc-c10f/Pages/home.aspx

[2] http://www.usna.edu/Cyber/_files/documents/idc/IDC_Overview.pdf

[3] *ibidem*

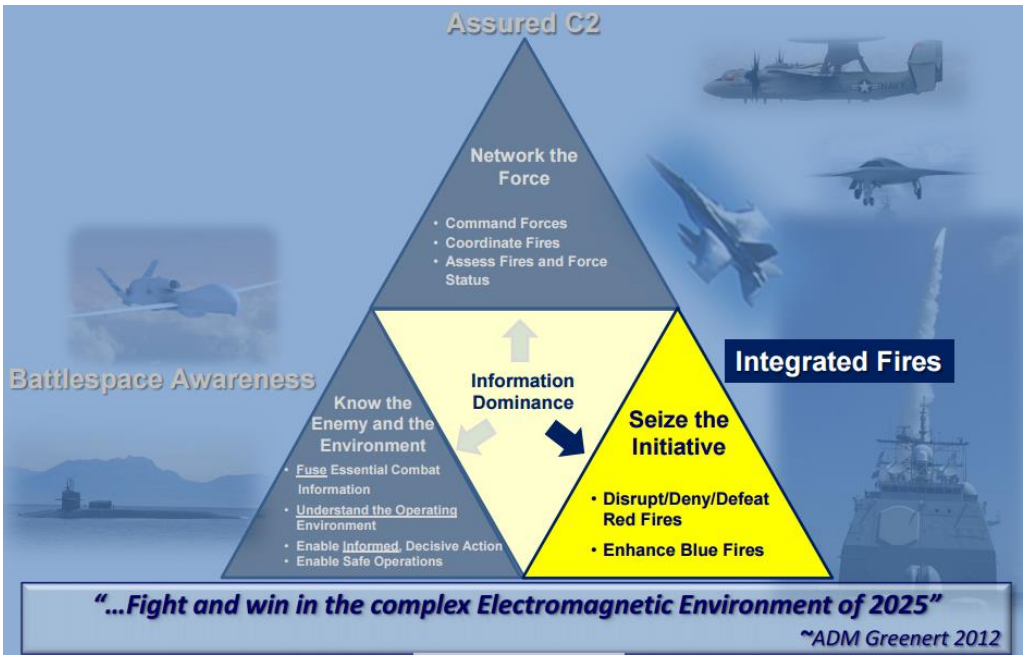


Source : http://www.public.navy.mil/fcc-c10f/Documents/C10F.ORG.pdf

L'US Navy Information Dominance Corps

Le *Fleet Cyber Command* est une composante opérationnelle de l'*U.S Navy Information Dominance Corps*. Créé en 2009, l'*Information Dominance Corps* (IDC) a pour objectif de former une communauté métier spécialisée dans le traitement au jour le jour de la menace cyber. C'est un corps de 45 000 personnes issues des différents domaines liés à l'information : renseignement, guerre de l'information, technologie de l'information, spatial, météorologie et océanographie. L'IDC a pour mission d'apporter à l'*US Navy* un avantage opérationnel en faisant de l'information l'une de ses capacités principales et en assurant la supériorité de la Navy en matière de renseignement, de cyber guerre et de gestion de l'information. La doctrine de l'*US Navy* définit trois piliers de la supériorité informationnelle (*Information Dominance*) : *Assured C2* (capacité de commandement et contrôle garantie), *Battlespace awareness* (perception totale de l'espace de combat), et *Integrated Fires* (intégration des diverses capacités d'action létales et non-létales)[4].

[4] http://mattcegelske.com/wp-content/uploads/2013/03/Information_Dominance_Roadmap_March_2013.pdf



Source : http://www.afcea.org/mission/intel/IntegratedFires.pdf

Une feuille de route 2013-2028 a été définie par l'*US Navy* pour l'*Information Dominance* en partant de l'analyse de l'environnement stratégique et opérationnel et de ses évolutions à moyen-long terme. Ce document doit notamment permettre à l'industrie de mieux comprendre les objectifs militaires en matière de cyberdéfense et d'accompagner le développement de la marine américaine dans le domaine.

La cyberstratégie au sein du département de la Marine

La cyberstratégie au sein du département de la Marine s'inscrit dans le cadre de la cyberstratégie militaire américaine, publiée en avril 2015 par le département de la Défense : la « *DoD Cyber Strategy*[5] » (évoquée dans la lettre mensuelle de l'OMC n°40).

Pour la Marine, le document « *U.S Fleet Cyber Command Strategic Plan 2015-2020* » a été publié cette année (voir paragraphe suivant).

L'*United States Coast Guard* (USCG) a de son côté publié en juin 2015 l'*United States Coast Guard Cyber Strategy*[6], qui fixe la stratégie opérationnelle des Garde-côtes américains dans le cyberespace à l'horizon 2025.

[5] http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[6] https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf

La cyberstratégie de l'USCG définit 3 grandes priorités :

1. Défendre le cyberespace de l'USCG *(Defending Cyberspace)* ;

Pour assurer le succès de ses missions aussi efficacement que possible, l'USCG doit protéger ses infrastructures informatiques et disposer d'un réseau résilient.

2. Apporter un appui aux opérations de l'USCG (*Enabling Operations*) ;
   Les opérations dans le cyberespace - à la fois dans et hors des systèmes d'information de l'USCG - sont essentielles dans ses diverses fonctions :

   - service armé;
   - organisme d'application des lois ;
   - organisme de régulation ;
   - membre de la communauté du renseignement.

3. Protéger les infrastructures maritimes critiques (*Protecting Infrastructure*).
   En liaison avec le DHS, les garde-côtes doivent renforcer la sécurité et la résilience des infrastructures critiques maritimes, notamment les navires, les infrastructures portuaires et tous les systèmes concourant au transport maritime.

On observe dans ce document de l'USCG une volonté de construire sur le long terme une protection complète des infrastructures critiques militaires et civiles.

La cyberstratégie au sein de la marine américaine

Le 6 mai 2015, l'*US Fleet Cyber Command* publie la cyberstratégie de l'*US Navy* de 2015 à 2020[7].

Cette stratégie se base sur deux constats : les océans n'isolent plus les Etats-Unis de leurs ennemis et la supériorité militaire américaine n'est pas acquise dans le cyberespace.

Le plan stratégique définit 5 objectifs à réaliser sur 5 ans. Des résultats intermédiaires sont par ailleurs attendus sous 18 mois afin que l'*US Navy* sache si elle se situe sur la bonne voie pour remplir ses objectifs.

1. Exploiter les réseaux de l'US Navy et considérer ceux-ci comme une plate-forme de combat (*Operate the Network as a Warfighting Platform*)

L'objectif est de garantir la disponibilité des systèmes de communication ainsi que des réseaux de l'*US Navy* pour répondre à des objectifs opérationnels.

Cet objectif se décline en plusieurs priorités :

- Garantir une capacité C2 à tout moment ;
- Réduire la surface de vulnérabilité aux attaques ;

[7] http://www.navy.mil/strategic/FCC-C10F%20Strategic%20Plan%202015-2020.pdf

- Améliorer la défense en profondeur des réseaux ;
- Réduire le délai de réponse aux intrusions en clarifiant l'organisation ;
- Renforcer la réactivité des processus d'acquisition capacitaire (*Planning Programming Budget and Execution*).

Résultats attendus sous 18 mois : ne subir aucune attaque réussie sur les réseaux de l'*US Navy*, tout en maintenant une disponibilité forte pour le réseau et les systèmes de communications.

2. Conduire des opérations de renseignement d'origine électromagnétique (SIGINT) (*Conduct Tailored Signals Intelligence*)

L'objectif est de s'adapter aux évolutions des besoins du commandement en matière de SIGINT, tout en partageant ses informations avec les autres agences gouvernementales, telle que la NSA et son *Central Security Service*.

Cet objectif se décline en plusieurs priorités :

- Institutionnaliser la collaboration entre organisations ;
- Etendre et améliorer les opérations SIGINT distribuées ;
- Maintenir une supériorité technique dans le domaine du SIGINT ;
- Intégrer des capacités SIGINT au niveau national.

Résultats attendus sous 18 mois : un retour positif du commandement sur la qualité des informations SIGINT de l'*US Fleet Cyber Command*, tout en continuant à fournir des forces sur le domaine du SIGINT à la NSA.

3. Produire des effets létaux et non létaux à travers le cyberespace (*Deliver Warfighting Effects Through Cyberspace*)

L'objectif est de développer des effets létaux et non létaux par les opérations dans le cyberespace, la guerre électronique et les opérations d'information.

Cet objectif se décline en plusieurs priorités :

- Amener tous les membres de l'*US Navy* à comprendre les effets et leur utilisation dans le cyberespace ;
- Institutionnaliser les capacités d'exécution du cyber.

Résultats attendus sous 18 mois : premiers résultats pour les projets prioritaires à partir d'un référentiel interne défini en 2014.

4. Etablir une situation intégrée partagée du cyberespace (*Create Shared Cyber Situational Awareness*)

L'objectif est de créer une image partagée et intégrée du cyberespace (*Cyber Common Operating Picture*) qui permette de surveiller et d'analyser en continu les systèmes d'information de l'*US Navy*, leur disponibilité et leurs vulnérabilités ainsi que de détecter toute activité malveillante sur ces systèmes. Le système devra être interopérable avec ceux du département de la Défense américain.

Cet objectif se décline en plusieurs priorités :

- Etablir un cloisonnement pour les opérations entre la LID (*Defensive Cyber Opérations*) et le réseau de la marine (*Departement of Defense Information Network-Navy)* ;
- Définir une stratégie de données unifiée et développer les capacités d'analyses de situation dans le cyberespace ;
- Définir les besoins d'outils de visualisation de situation dans le cyberespace.

Résultats attendus sous 18 mois : validation par l'*US Fleet Cyber Command* de la capacité de surveiller la situation opérationnelle, à la fois globale et locale, des réseaux et des communications et de détecter les activités suspectes ou malveillantes. La *Cyber Common Operating Picture* doit ainsi pouvoir être diffusée et adaptée à chacun des opérateurs concernés de l'*US Navy*. Les données doivent être interopérable (le format par exemple) pour permettre l'échange de ces données avec les agences du département de la Défense américain et idéalement l'ensemble du gouvernement.

5. Etablir et développer des équipes cyber projetables (*Establish and Mature Navy's Cyber Mission Forces*)

L'objectif est de participer à la mise en place des 133 équipes d'experts en cybersécurité, dénommées *Cyber Mission Forces* (CMF), prévues par la « *DoD Cyber Strategy »* du département de la Défense américain pour défendre les infrastructures nationales contre les cyberattaques (*National Mission Forces*), défendre et sécuriser le réseau du DoD (*Protection Forces*) et appuyer les commandants dans leur planification opérationnelle pour délivrer des effets à travers le cyberespace (*Combat Mission Forces*).

L'*US Fleet Cyber Command* a la responsabilité d'établir et de développer les 40 premières CMF.

Cet objectif se décline en plusieurs priorités :

- Développer des critères innovants de sélection et de recrutement des CMF ;
- Définir les besoins pour que les CMF disposent d'une avance technologique, tactique, technique et dans les procédures.
- Développer les capacités et les processus pour assurer un commandement et un contrôle efficaces des CMF.

Résultats attendus sous 18 mois : mettre en place des équipes initiales ayant atteint la pleine capacité opérationnelle (*Initial Operational Capability* à *Full Operational Capability*), ainsi qu'une stratégie durable de développement des CMF tout en ne sacrifiant aucune mission actuelle.

Avec ce plan stratégique, l'*US Fleet Cyber Command* montre son double engagement, sur le terrain défensif et offensif. Elle vise à intégrer pleinement la cyberdéfense de la Marine dans le dispositif du DoD et plus largement, du gouvernement, comme observé avec la *Cyber Mission Force* ou la stratégie de donnée unifiée. Le commandement est aussi pris en compte avec l'élaboration d'un guide à son intention. L'objectif

est clair : aider les décideurs à comprendre et prendre en compte au mieux l'outil cyber, une volonté forte observée dans d'autres projets militaires tels que le « Plan X »[8] de la DARPA.

Les programmes de recherche et d'armement de la marine américaine en cyberdéfense

En 2013, sur les 610 milliards de dollars du budget du département de la Défense américain, près de 10% (soit 63,3 milliards de dollars) sont consacrés à la recherche & développement. En France, ce même budget en 2014 est de 192 millions d'euros, soit 0.5% de notre budget de la défense (41,98 milliards d'euros) [9]. Les importants moyens financiers et humains de la marine américaine lui permettent d'investir fortement sur l'innovation et la R&D. Pour 2016, 559 millions de dollars sont ainsi dédiés au financement des nombreux programmes de recherche[10].

Ces programmes s'inscrivent dans les 7 priorités du département de la Défense américain pour la recherche : *Autonomy*, *Counter Weapons of Mass Destruction*, *Cyber Sciences*, *Data-to-Decisions*, *Electronic Warfare*, *Engineered Resilient Systems*, et *Human Systems*. On observe que le domaine cyber occupe une place de plus de plus en plus importante dans la recherche militaire américaine.

Pour la mise en œuvre de ces programmes, la marine américaine dispose de plusieurs centres de recherche en matière de sécurité des systèmes d'information et de cyberdéfense :

- L'*Office of Naval Research* (ONR) coordonne, exécute et promeut les programmes scientifiques et technologiques de l'*US Navy* et de l'*US Marine Corps* dans les écoles, les universités, les laboratoires de recherches gouvernementaux, ainsi que dans les entreprises et associations. Il fait aussi appel à près de 190 réservistes[11]. Les sujets cyber sont principalement traités par la Division 311[12] *Mathematics, Computers and Information Sciences* et la Division 312 *Electronics, Sensors and Networks Research*.

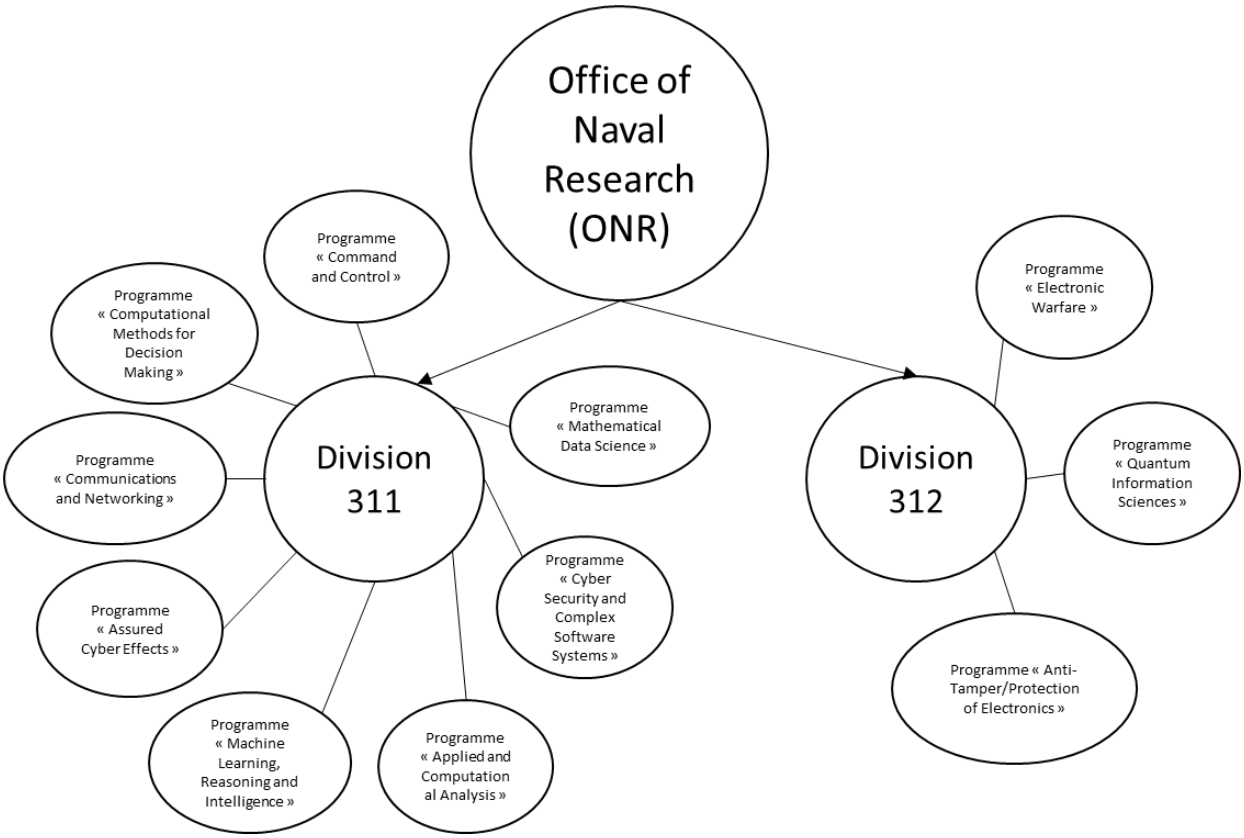
[8] http://www.darpa.mil/program/plan-x

[9] http://www.defense.gouv.fr/content/download/302625/4023676/file/Chiffres%20cl%C3%A9s%20de%20la%20D%C3%A9fense%20-%202014.pdf

[10] https://research.usc.edu/files/2011/05/Guide-to-FY2016-DOD-Basic-Research-Funding-.pdf

[11] http://www.onr.navy.mil/Media-Center/Press-Releases/2015/McAndrew-Navy-Reserve-Junior-Officer-Award.aspx

[12] http://www.onr.navy.mil/Science-Technology/Departments/Code-31/All-Programs/311-Mathematics-Computers-Research.aspx



Liste des programmes Cyber au sein de l'ONR - Source CEIS

En septembre 2015, un projet visant à développer un système de protection des infrastructures critiques des navires, nommé RHIMES (*Resilient Hull, Mechanical, and Electrical Security*)[13], a par exemple été officiellement lancé par l'ONR au sein du programme « *Cyber Security and Complex Software Systems Program* ».

- Le *Navy Cyber Warfare Development Group* (NCWDG) a en charge de rechercher et d'exploiter les vulnérabilités de l'adversaire ainsi que de fournir les tactiques et capacités cyber à l'*US Fleet Cyber Command* dont elle dépend[14]. Il n'existe aucune information publique sur les travaux de ce groupe de recherche.

- Le *Naval Sea Systems Command* (NAVSEA) conçoit, construit ou achète, et entretient les bâtiments de surface, les sous-marins et les systèmes de combat qui constitueront les futures capacités de l'*US Navy* et de l'*US Marine Corps*. Dans le cadre de ses 150 programmes d'armement (soit un quart du budget de la marine), la cybersécurité prend une place de plus en plus importante. La seconde édition de son *Strategic Business Plan 2013-2018*[15] intègre ce domaine comme l'une de ses 4 priorités, en concordance avec la doctrine de la supériorité informationnelle de l'*US Navy.* Trois objectifs sont définis : développer une culture de cybersécurité au sein du NAVSEA, intégrer

[13] http://www.navy.mil/submit/display.asp?story_id=91131

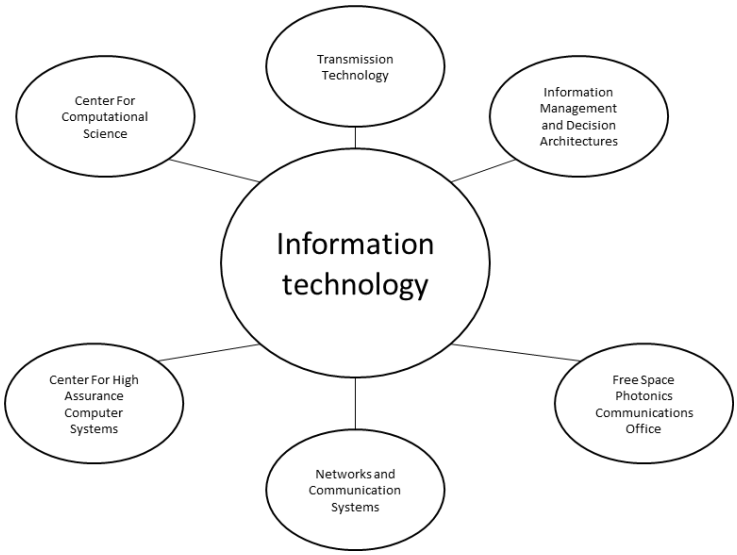
[14] http://navycaptain-therealnavy.blogspot.fr/2014/12/new-executive-officer-at-navy-cyber.html

[15] http://www.navsea.navy.mil/Portals/103/Documents/Strategic%20Documents/SBP13-14_Final-2ndEd.pdf

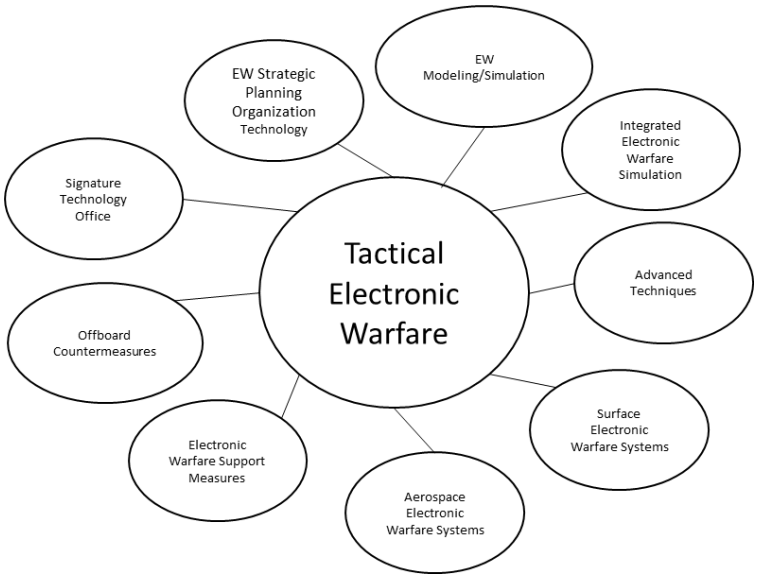
la composante cybersécurité dans les programmes d'armement conduits par le NAVSEA et mettre en place un processus de « certification, évaluation, autorisation ».

- Le *Naval Research Laboratory* (NRL) est le laboratoire de recherche de l'*US Navy* et de l'*US Marine Corps*. Il comprend 6 divisions: *Commanding Officer Business Operations, Systems, Materials Science & Component Technology, Ocean & Atmospheric Science & Technology* et *Naval Center for Space Technology*.

Au sein de *Systems*, deux sous-divisions travaillent directement et indirectement sur les problématiques de sécurité des systèmes d'information/cyberdéfense : *Information Technology* et *Tactical Electronic Warfare*.



Liste des programmes Cyber au sein de la branche Information Technology du NRL - Source CEIS



Liste des programmes Cyber au sein de la branche Tactical Electronic Warfare du NRL - Source CEIS

Hors de la marine américaine, la DARPA est l'agence du département de la Défense des États-Unis chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire. Elle conduit actuellement 22 programmes[16] sur le domaine de la cybersécurité, qui sont destinés à être utilisés par les différentes armées, dont l'*US Navy*.

[16] http://www.darpa.mil/tag-list?tt=15&type=Programs

INVALIDATION DU SAFE HARBOR : QUEL IMPACT ?

Mardi 6 octobre 2015, la Cour de justice de l'Union européenne (CJUE) invalidait l'accord Safe harbor, dit « Sphère de sécurité », qui encadrait - depuis le 26 juillet 2000 et la décision n°2000/520CE de la Commission européenne - les transferts de données personnelles de citoyens européens vers les Etats-Unis. Pourtant, malgré son annulation par la CJUE, le Département du commerce américain a indiqué qu'il continuerait de l'administrer et qu'il maintiendrait même l'enregistrement des dossiers des nouvelles sociétés souhaitant profiter de l'accord[17].

Les enjeux sont majeurs puisque ce texte permettait à environ 4 500 sociétés de transférer aux Etats-Unis les données personnelles de clients européens. C'est pourquoi le Département du Commerce indiquait son désir de voir un nouvel accord trouvé, position qui rejoint celle du G29 européen[18] qui a donné trois mois aux institutions européennes et aux gouvernements pour aboutir à un nouvel accord[19].

La décision de la CJUE intervient alors que les Etats-Unis et la Commission Européenne étaient en phase de négociations pour réformer et renforcer le Safe harbor[20] à la suite des révélations d'Edward Snowden. La clause du Safe harbor, qui permettait aux autorités américaines d'avoir accès, sous conditions, aux données personnelles transférées depuis l'UE[21], a en effet été interprétée par les autorités américaines de façon beaucoup extensive que ne l'imaginait la Commission européenne. Alors que cette clause stipulait que l'accès ne pouvait se faire que dans le cas d'une menace pour la sécurité nationale américaine, l'absence de définition de la notion de menace pour la sécurité nationale ne pouvait que favoriser les dérives…

Dans le cadre de la protection des citoyens et de la souveraineté nationale, cette invalidation, qui résulte de l'arrêt « *CJUE C-362/14 Maximillian Schrems/ Data Protection Commissionner* », témoigne de l'enjeu que représentent les compétences extraterritoriales de la législation américaine pour l'Union européenne. Par cet arrêt, l'Europe s'oppose directement à l'approche américaine en matière de données personnelles qui permet aujourd'hui au pays de « capter et mobiliser un grand nombre de données collectées et stockées par les grands opérateurs américains. »[22]

[17] http://www.export.gov/safeharbor/

[18] Le « G 29 » est le groupement européen des autorités de protection des données personnelles.

19 http://www.cnil.fr/linstitution/actualite/article/article/safe-harbor-le-g29-demande-aux-institutions-europeennes-et-aux-gouvernements-dagir-sous-3-mois/

[20] Ibidem.

[21] http://www.mediapart.fr/journal/international/061015/le-transfert-de-donnees-personnelles-vers-les-etats-unis-juge-illegal

[22] Etude « La balkanisation du web : chance ou risque pour l'Europe » réalisée par l'Institut Français de Géopolitique pour le compte de la Direction aux Affaires Stratégiques, Septembre 2014, p.96 : http://www.cyberstrategie.org/?q=fr/etude-prospective-strategique-balkanisation-du-web-chance-risque-europe

Un accord en sursis depuis les révélations Snowden

Le Safe harbor était en réalité menacé depuis les révélations d'Edward Snowden. Jan-Philip Albrecht, rapporteur du projet de règlement européen sur la protection des données, exigeait déjà aux lendemains de l'affaire la suspension de l'accord. Il avait même remporté une victoire symbolique lorsque le Parlement avait voté en 2014 une résolution allant dans le sens d'une suspension, sans pour autant que suite soit donnée par la Commission[23].

Selon Isabelle Falque-Pierrotin, présidente de la CNIL[24] et du G29, l'accord n'aurait d'ailleurs pas été suspendu à cause de son contenu, mais bel et bien à cause de la législation américaine, plus précisément « d'éléments du droit américain qui n'ont pas été pris en compte par la Commission et qui rendent le Safe harbor invalide »[25]. En d'autres termes : la surveillance massive effectuée en partie grâce aux transferts de données jusqu'ici autorisés par l'accord.

Cette invalidation a un impact direct sur l'économie numérique, puisque le Safe Harbor était le mécanisme le plus simple et le plus accessible d'un point de vue financier pour les entreprises concernées, américaines ou européennes. L'impact n'est cependant pas que financier. Le texte était également un gage de sécurité : à la façon d'un label, il consacrait le fait que les Etats-Unis assuraient la protection des données personnelles de façon satisfaisante. Sa suspension marque donc un nouveau signe de défiance à l'égard de l'écosystème numérique américain. Et malgré leur tranquillité affichée, les entreprises américaines ne s'y sont pas trompées. Facebook, qui certifiait que cette suspension n'avait que peu d'impact sur l'entreprise, a ainsi réclamé une renégociation rapide du Safe harbor, sous couvert d'une volonté de défense de l'écosystème des petites entreprises.[26]

Quelles conséquences ?

➡ Sur les entreprises

La première conséquence est que les entreprises américaines ne pourront plus s'auto-certifier comme respectant les normes européennes de protection des données personnelles. Ensuite, la décision de la CJUE, qui devrait théoriquement « imposer le maintien sur le territoire de l'UE des données personnelles des ressortissants européens »[27], suscite un flou juridique quant aux transferts de données opérés à l'heure actuelle par les entreprises, qui n'ont évidemment pas pu mettre fin du jour au lendemain à leurs activités. Si elle ne crée pas à proprement parler un vide juridique, l'invalidation du texte soulève désormais la

[23] http://www.lemonde.fr/pixels/article/2015/10/09/donnees-personnelles-la-seule-solution-est-que-les-etats-unis-acceptent-de-modifier-leur-legislation-nationale_4786529_4408996.html

[24] Commission nationale de l'informatique et des libertés.

[25] http://www.lemonde.fr/pixels/article/2015/10/10/isabelle-falque-pierrotin-la-justice-europeenne-a-pointe-le-systeme-de-surveillance-de-masse-des-etats-unis_4786781_4408996.html#I5RHb0CFYF2hySwt.99

[26] http://www.usine-digitale.fr/article/facebook-l-apres-safe-harbor-est-une-question-a-regler-de-gouvernement-a-gouvernement.N355895

[27] http://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Safe-harbor

question de la légalité de ces transferts. Une situation délicate pour les entreprises qui se voient donc contraintes de prendre un risque[28] puisqu'elles exploitent des données sans aucune base légale.

➡ Sur les internautes

A l'échelle de l'internaute, la suspension de l'accord donne aux citoyens la possibilité de demander aux autorités de protection des données de réexaminer les transferts de données. Cette possibilité reste néanmoins théorique puisque cela suppose que les internautes aient non seulement conscience des enjeux mais également la volonté d'agir. Comme le soulignait Isabelle Falque-Pierrotin[29], les internautes peuvent se retrouver dans une position ambivalente, puisqu'ils pourraient émettre une réaction positive quant à cette décision de la CJUE tout en craignant que les services dont ils bénéficiaient ne s'interrompent.[30]

➡ Sur les Autorités de protection des données

La décision de la CJUE renforce le pouvoir des autorités de protection des données des pays membres face aux entreprises américaines. Ces autorités peuvent maintenant « décider d'interdire la poursuite des flux de données si elles estiment que ceux-ci ne sont plus assez sécurisés pour les personnes concernées, comme le précise l'article 28.3 de la directive 95/46/CE ainsi que la loi 78-17 du 6 janvier 1978 »[31]. A l'échelle nationale, la CNIL aura ainsi un vrai rôle à jouer : elle devra contrôler le niveau de protection des transferts réalisés par les entreprises et les autoriser au cas par cas[32]. Une situation d'incertitude peu propice au climat des affaires et qui pourrait aussi avoir un impact sur la révision du règlement européen relatif à la protection des données[33].

Un impact a deux vitesses ?

Si les enjeux politiques et éthiques sont mis en avant, les enjeux économiques méritent que l'on s'y arrête. L'Europe entend en effet favoriser le développement du marché numérique européen et l'interdiction pour les TPE/PME américaines d'utiliser les données personnelles des citoyens européens peut marquer un coup d'arrêt pour certaines activités. Sans oublier la situation inverse, certes plus rare, selon laquelle des transferts de données personnelles de citoyens américains opérés vers l'Europe seraient compromis. C'est notamment le cas pour une entreprise comme Deezer, 3ème entreprise de streaming audio mondiale.

Pour autant, le Safe harbor n'est qu'un outil juridique parmi d'autres. Sa suspension aura un impact différent dépendamment du fait que les entreprises soient ou non en mesure de négocier des contrats particuliers qui permettent le transfert de données sur la base d'un cadre juridique légal. Il existe en effet d'autres outils

---

[28] http://www.lemonde.fr/pixels/article/2015/10/10/isabelle-falque-pierrotin-la-justice-europeenne-a-pointe-le-systeme-de-surveillance-de-masse-des-etats-unis_4786781_4408996.html#I5RHb0CFYF2hySwt.99

[29] http://www.lemonde.fr/pixels/article/2015/10/10/isabelle-falque-pierrotin-la-justice-europeenne-a-pointe-le-systeme-de-surveillance-de-masse-des-etats-unis_4786781_4408996.html#I5RHb0CFYF2hySwt.99

[30] Ibidem.

[31] https://www.laquadrature.net/fr/safe-harbor-lettre-cnil

[32] http://www.zdnet.fr/actualites/le-safe-harbor-invalide-qui-est-concerne-quels-effets-et-maintenant-39826048.htm

[33] http://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Safe-harbor

permettant le transfert de données, par le biais de Clauses contractuelles types ou via le système des Règles internes d'entreprises (*Binding Corporate Rules* ou BCR) qui sont définies par la CNIL comme « un contrat signé entre deux sociétés, un exportateur et un importateur de données qui s'engagent à assurer la sécurité et la confidentialité des données »[34]. Des règles, qui, sur la base de l'article 69 de la loi du 6 janvier 1978, peuvent prévoir des transferts de données en dehors du cadre du Safe harbor, et qui sont donc à l'heure actuelle les solutions de report vers lesquels l'écosystème de la donnée se tourne. D'autant plus que ces outils sont eux-mêmes considérés par la CJUE comme des « outils [qui] peuvent encore être utilisés par les entreprises » même si « les autorités de protection des données se réservent néanmoins la possibilité de contrôler certains transferts, notamment à la suite des plaintes qu'elles pourraient recevoir »[35].

L'invalidation de l'accord oblige ainsi les entreprises dont l'économie a pour carburant l'exploitation de données personnelles à se tourner vers d'autres solutions juridiques, en général plus coûteuses. In fine, cette politique pourrait donc « avoir un effet contre-productif par rapport aux objectifs de départ en accentuant le pouvoir des acteurs les plus importants »[36] de l'économie américaine comme Facebook, alors-même que cette dernière entreprise est à l'origine des revendications de Maximilian Schrems qui ont abouti à la suspension du Safe Harbor.

On constate en effet que les grosses entreprises américaines et européennes n'ont apparemment pas réagi à l'invalidation du Safe harbor, ce qui laisse à penser que ces entreprises considèrent que cette invalidation n'aura finalement qu'un impact limité sur leurs activités. Principalement pour deux raisons : d'une part, le fait que nombre de ces entreprises possèdent déjà des Datacenters sur le territoire européen (où qu'elles doivent prochainement en ouvrir à l'image de NetSuite[37]) et, d'autre part, l'existence des Règles internes d'entreprises. Car l'argument relatif à la localisation des données, qui présente l'implantation de datacenters sur le territoire européen comme la solution, ne suffit pas. Il est en effet nécessaire de comprendre, comme le souligne l'avocate Florence Chafiol du cabinet August & Debouzy, que « Les transferts ne sont pas forcément physiques. Ils peuvent être virtuels. Si une société américaine accède par exemple à des données personnelles stockées sur le territoire français, c'est un transfert. La consultation peut être considérée comme un transfert », ce qui démontre bien l'insuffisance de l'argument de localisation.

Et cette situation perturbe non seulement des entreprises américaines, mais aussi de nombreux acteurs européens. A l'instar du marché américain, les grosses entreprises françaises du B2B (Business to business) ne devraient pas ou peu en souffrir. La situation sera en revanche plus délicate pour les entreprises qui font du B2C (Business to consumer). Ces entreprises – dont les relations commerciales s'effectuent de l'entreprise vers le client final directement – n'ont en effet pas la possibilité de créer des contrats de type « règles internes d'entreprise » ou BCR avec un client final.

---

[34] http://www.zdnet.fr/actualites/le-safe-harbor-invalide-qui-est-concerne-quels-effets-et-maintenant-39826048.htm

[35] http://m.cnil.fr/linstitution/actualite/actualite/article/safe-harbor-le-g29-demande-aux-institutions-europeennes-et-aux-gouvernements-dagir-sous-3-mois/

[36] Etude « La balkanisation du web : chance ou risque pour l'Europe » réalisée avec le soutien de la Direction aux Affaires Stratégiques, Septembre 2014, p.99 : http://www.cyberstrategie.org/?q=fr/etude-prospective-strategique-balkanisation-du-web-chance-risque-europe

[37] http://diginomica.com/2015/10/02/its-time-for-the-us-cloud-industry-to-stand-up-to-europes-un-safe-harbor-bullies/#.Vio3TSsqh1Q

Ces derniers mécanismes reposent sur une relation d'entreprise à entreprise : elles s'appliquent par exemple dans le cas des transferts de données entre les entités d'une multinationale[38]. Mais des entreprises comme Facebook ou encore Google, dont les activités commerciales reposent sur une relation entreprise/client final, se trouvent confrontées au flou juridique qu'a créé la suspension du Safe harbor. Une entité européenne d'une multinationale américaine ne peut plus légalement assurer le transfert des données personnelles des citoyens européens vers les Etats-Unis[39]. Et elle ne peut opérer avec des Clauses contractuelles types ou des BCR pour passer outre l'interdiction de transfert de données vers les Etats-Unis. Dès lors, l'apparente sérénité des géants américains du web semble n'être qu'un jeu de façade.

A noter également que les banques et les assurances qui utilisent en quantité des données provenant d'usagers américains ne devraient pas être concernées par l'invalidation de l'accord. Le Safe harbor ne s'appliquait pas au secteur bancaire qui relève de l'accord SWIFT. Le secteur de l'assurance a par ailleurs d'ores et déjà recours au système des BCR, et ne devrait donc pas être gêné par son invalidation.

Outre les grands acteurs B2C, la suspension du texte devrait donc en réalité avoir surtout un impact sur les petites entreprises, comme l'indiquait le directeur général de Profusion, une société de conseil spécialisée dans la data science : les petites et moyennes entreprises, dont l'économie repose sur l'exploitation des données européennes vont se retrouver sous pression, et vont devoir revoir leurs ambitions européennes[40]. Nombres d'entre elles seront en effet dans l'incapacité de se doter de Clauses contractuelles type ou de BCR.

Cet impact affectera notamment les petites et moyennes entreprises européennes, par exemple celles qui utilisent des infrastructures américaines pour stocker et traiter les données de leurs clients[41]. « Cela rend potentiellement illégal l'hébergement de données personnelles chez un acteur dont le stockage ou le traitement des données a lieu sur le sol américain. De nombreux Cloud Providers sont malheureusement dans ce cas », explique par exemple la société Waycom sur son site[42]. Les entreprises devront alors endosser cette responsabilité et vérifier que les prestataires de Cloud garantissent bien une protection adéquate ou bien, dans le cas contraire, réformer leurs pratiques. Pour Yann Padova, ancien secrétaire général de la CNIL, les entreprises « doivent désormais modifier leurs architectures informatiques ou avoir recours à des prestataires de service de Cloud européens. Si elles veulent rester avec des prestataires américains, elles ont des solutions juridiques, mais aucune d'entre elles ne protège contre la surveillance de la NSA »[43].

---

[38] Ibidem.

[39] Ibidem.

[40] http://diginomica.com/2015/10/02/its-time-for-the-us-cloud-industry-to-stand-up-to-europes-un-safe-harbor-bullies/#.Vio3TSsqh1Q

[41] http://www.lemonde.fr/pixels/article/2015/09/25/pourquoi-l-accord-safe-harbor-sur-les-donnees-personnelles-cristallise-les-tensions_4771879_4408996.html

[42] http://www.waycom.net/retour-sur-la-mort-du-safe-harbor-et-ses-consequences-pour-les-entreprises-europeennes/

[43] http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/safe-harbor-la-cjue-affirme-que-la-protection-des-donnees-est-un-droit-fondamental-09-10-2015-1972222_56.php#xtor=CS3-194

Une opportunité politique à risque ?

Toute la question est en réalité de savoir si l'invalidation du Safe harbor constitue un risque ou une opportunité pour l'industrie numérique européenne. Politiquement, cet événement constitue à n'en pas douter une opportunité qui consacre la priorité accordée à la protection des données personnelles en Europe. Economiquement, il semble aussi que l'arrêt puisse contribuer à renforcer l'écosystème numérique européen et à insuffler une certaine dynamique entrepreneuriale. A l'image de la conférence franco-allemande sur le numérique le 27 octobre 2015, durant laquelle a été annoncé le lancement d'une plateforme visant à faciliter les co-investissements entre banques publiques, françaises et allemandes, dans les start-up. Avec notamment un premier co-investissement à hauteur de 75 millions d'euros dans Partech Growth, un fonds de capital-croissance destiné à apporter entre 10 et 30 millions d'euros aux entreprises en pleine croissance. La conférence fut aussi l'occasion pour Orange et Publicis d'annoncer le développement d'un fonds d'investissements en faveur des start-up européennes, l'Iris Growth, aussi à hauteur de 75 millions d'euros.[44] Ces nouveaux investissements émergent alors même que dès le début du mois d'octobre 2015, Axelle Lemaire, Secrétaire d'État chargée du Numérique, auprès du ministre de l'Économie, de l'Industrie et du Numérique, annonçait un appel à projets en faveur de trois domaines d'innovation : l'anonymisation des données personnelles, la protection de la vie privée dans les objets connectés et les architectures innovantes comme les architectures distribuées[45]. Trois domaines d'innovation qui se regroupent dans le secteur de la protection des données personnelles, à l'heure où le Safe harbor est en suspens. La volonté des européens de se forger une place sur le marché de la cybersécurité se fait là bien ressentir.

Mais l'invalidation du Safe harbor est aussi source de débat dans la sphère politique européenne : Günther Oettinger, commissaire européen à l'économie et à la société numérique, et Hans-Olaf Henkel, membre du Parlement européen, mettent en avant le risque d'un « effet domino »[46]. C'est l'idée que par effet rebond, la crise de confiance vis-à-vis des données exportées vers les Etats-Unis pourrait se propager en interne en Europe. Pour le général d'armée (2S) Marc Watin-Augouard, des crispations pourraient ainsi voir le jour en matière de transferts de données entre pays membres de l'UE, autour par exemple des lois françaises de programmation militaire du 18 décembre 2013 et relative au renseignement du 24 juillet 2015, qui pourraient être perçues comme des réminiscences des pratiques de surveillance massive contre lesquelles s'est opposée la CJUE.

Il est déjà possible de constater un effet domino, externe à l'UE, au regard de l'annonce du Préposé fédéral suisse à la protection des données et à la transparence (PFPDT) faite sur son site internet. En effet, ce dernier indique que « tant que la Suisse n'a pas renégocié un nouvel accord avec le gouvernement américain, l'accord « *U.S.-Swiss Safe Harbor Framework* » ne constitue plus une base légale suffisante pour une transmission de données personnelles aux États-Unis compatible avec la loi suisse sur la protection des données (LPD) »[47]. Cette annonce se base explicitement sur l'invalidation du Safe harbor

[44] http://www.journaldunet.com/ebusiness/le-net/1165285-le-couple-franco-allemand-veut-accelerer-la-construction-d-une-europe-du-numerique/

[45] http://www.journaldunet.com/ebusiness/le-net/1163202-axelle-lemaire-lance-un-appel-a-projets-pour-des-technos-de-protection-de-la-vie-privee/

[46] http://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Safe-harbor

[47] http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=fr

par la CJUE bien que la Suisse ne soit pas un pays membre. Cette initiative, pourrait-elle être la première d'une longue liste ?

Quelles perspectives ?

Pendant que les entreprises s'interrogent, les Etats-Unis et la Commission européenne poursuivent les négociations pour arriver à un nouvel accord sur le Safe harbor. Le texte n'a en effet pas été abrogé par l'arrêt de la CJUE mais bien suspendu de façon à préparer de nouvelles mesures prenant en compte la question des faiblesses juridiques américaines quant aux possibilités de surveillance de masse. L'invalidation de l'accord est donc en elle-même le meilleur moteur pour la négociation d'un Safe harbor II, lequel aurait déjà dû, selon le calendrier d'origine, aboutir depuis le 31 mai 2015.

Mais le dossier est épineux. Les Etats-Unis ne devraient pas lâcher si facilement alors que d'après le think-tank *Information Technology and Innovation Foundation*, le seul marché du cloud computing, pourrait perdre entre 21,5 et 35 milliards de dollars entre 2013 et 2016, du fait de la crise de confiance des acteurs européens envers le marché américain[48]. Côté européen, le travail de lobbying effectué sur la Commission européenne et les gouvernements européens avait déjà commencé bien avant la suspension de l'accord. La possibilité d'annulation du Safe harbor avait même été l'objet d'une étude de l'*European Centre for International Political Economy*, bien avant sa suspension. Cette étude concluait qu'elle « engendrerait une chute du PIB de l'UE entre -0,8 et -1,3%. En outre, les exportations de services européens aux Etats-Unis pourraient chuter jusqu'à 6,7% à cause de la perte de compétitivité engendrée ».

On retrouve là le traditionnel discours américain en faveur de « l'internet global » qui considère toutes les stratégies de puissance numérique non américaines comme autant de visées protectionnistes et liberticides susceptibles de conduire à une balkanisation irrémédiable d'internet. L'étude menée pour le compte de la Direction générale des relations internationales et de la stratégie (DGRIS) [49] par l'Institut Français de Géopolitique en 2014 soulignait d'ailleurs bien la volonté américaine de désigner les stratégies de protection des données personnelles des citoyens européens via des politiques de type *data localization* comme des stratégies à risque. Du point de vue de plusieurs études américaines, elles induiraient « un risque de fragmentation et une menace pour l'intégrité et l'unicité de l'Internet »[50].

Les négociations continuent cependant pour remettre à flot l'échange transatlantique de données. Que cela soit sur le plan politique, éthique ou économique, l'enjeu est en effet primordial non seulement pour l'Europe, mais également pour les Etats-Unis, qui ont tout à perdre d'une nouvelle crise de confiance des entreprises et citoyens européens. De fait, vingt jours seulement après l'invalidation de l'accord, la Commissaire européenne à la Justice, aux Consommateurs et à l'Égalité des genres, Věra Jourová, annonçait le 26 octobre 2015 que l'UE et les Etats-Unis avaient trouvé un accord de principe sur la signature d'un Safe harbor II. Soulignant les efforts américains en matière de protection des données personnelles depuis deux

[48] Etude « La balkanisation du web : chance ou risque pour l'Europe » réalisée avec le soutien de la Direction aux Affaires Stratégiques, Septembre 2014, p.99 : http://www.cyberstrategie.org/?q=fr/etude-prospective-strategique-balkanisation-du-web-chance-risque-europe

[49] Etude « La balkanisation du web : chance ou risque pour l'Europe » réalisée avec le soutien de la Direction aux Affaires Stratégiques, Septembre 2014, p.99-100 : http://www.cyberstrategie.org/?q=fr/etude-prospective-strategique-balkanisation-du-web-chance-risque-europe

[50] Ibidem, p.101.

ans, la Commissaire indiquait la mise en place d'une révision annuelle du cadre juridique de ce nouvel accord à venir[51].

[51] http://www.linformaticien.com/actualites/id/38321/vers-un-safe-harbor-ii.aspx

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** 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 **DGRIS** a confié à **CEIS** la réalisation de 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.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com