Exercice de guerre de l'information

STRATÉGIE DE CONTRE-OFFENSIVE DE SIEMENS SUITE À LA CRISE POLITIQUE IRANIENNE DE JUIN 2009

Travail de recherche réalisé dans le cadre du cours de la guerre de l'information

Auteurs:

Claude Lepère

Fabien Droz

Franck Langlet

Jean-Christophe Marcoux

Philipp Bauer

Sous la direction de:

Christian Harbulot

SOMMAIRE

EXECUTIVE SUMMARY

The present document aims at presenting the diverse aspects of a complex informational war, which took place from March to July 2009, aimed at destabilizing one European telecommunication infrastructure provider, namely Nokia Siemens Networks (NSN). This joint-venture between the infrastructure division of Siemens and Nokia ranks among the world leaders, mastering key technologies for both fixed and wireless networks. In this time, in the frame of the Iranian general elections and the ferocious repressions seen in the country against political opponents and the youth, NSN and its stakeholders were heavily attacked in the Western media as being, by the sale of their sophisticated network provision and monitoring technology, objective allies of the Mullah regime. Despite NSN has effectively sold these technologies to the Mullah regime, the attacks are nevertheless to be seen in a much larger scope. In particular, the heavy commercial battles for the supremacy on the leadership on telecommunication infrastructure. In this global struggle, dominated by American companies, Europeans have come close to the US level. Therefore, this sector is particularly sensitive to political pressures, since the struggle for global leaders and flagship companies is particularly violent. Therefore, the actions observed against Nokia, albeit resulting of an objective weakness, has been largely exploited and amplified by US instances.

In this study, all stakeholder types of this informational war have been identified, and the ties between them highlighted. Since Nokia and Siemens both have been severely impacted by these actions, this document also presents potential actions which could have been taken for:

- Diversion of the attacks, by provision either of other subjects, or targets of higher value

- Striking back, in order to obtain a more balanced situation. This shall be done by attacking the Computer & Communication Industry Association, and transforming the moral weakness in a common regulation frame for all actors. This would in turn protect European industry from unfair American attacks on similar subjects in the future.

Facts

The present document aims at presenting the multiple implications

- ❖ A major information crisis with strong potential impact on Siemens' business occurred mid-June 2009, further to the political crisis caused by the controversial result of the presidential election that took place in Iran

Results of our analysis

- ❖ Evidence of the orchestration of the attack against Siemens, through different ways, and at different levels:
  - Medias: Murdoch group (Wall Street Journal, etc.)
  - Social networks (Twitter, Facebook, Youtube, etc.)
  - Politics (U.S. Congress, lobbyists)

- Identified potential impacts of the crisis on Siemens' business:
  - Serious economic and financial consequences
  - Brand image integrity risk
  - Union protests' risks
- Identification of targets and channels for the counterattack

Our objective

- To divert the attack towards:
  - other issues
  - other targets

Our action plan

- Main target:
  - The Computer & Communications Industry Association (CCIA)
- Other targets:
  - Individual activists and/or groups of activists
  - World public opinion
  - Murdoch group

Our methodology to hit the main target

- To attack the American Telco lobby (CCIA), by forcing it to adopt a clear position on the latest legislation concerning IT monitoring systems sold to governments worldwide, considering the recent legislation voted by the US Congress about freedom on Internet

Expected results

- To put an end to the discrimination towards E.U. actors in Telcos (e.g. Siemens), in order:
  - to obtain a more balanced situation, and the same rules and regulations with other foreign firms, included American major players in Telcos
  - to protect EU firms in Telco towards non democratic governments demands, especially in sensitive security monitoring systems.
- Neutralizing the individual activists, particularly "cyber- liberties defenders and libertarian cyber-activists" who regularly launch campaign against Siemens by web2.0,

The consequence being a stop in the flaw of informational attacks against Siemens in the short, medium and long term.

SIEMENS EN ÉTAT DE "GUERRE DE L'INFORMATION": CONTEXTE ET RAPPEL DES FAITS

Siemens a subit les effets d'une attaque informationnelle majeure et orchestrée, qui s'est appuyée sur un contexte historique et une conjoncture (crise Iranienne) très favorable pour les agresseurs. Cette orchestration est principalement le résultat du franchissement d'un seuil de tolérance, provenant de la capacité de Siemens à altérer durablement les intérêts américains dans les domaines économique, géopolitique et géostratégique.

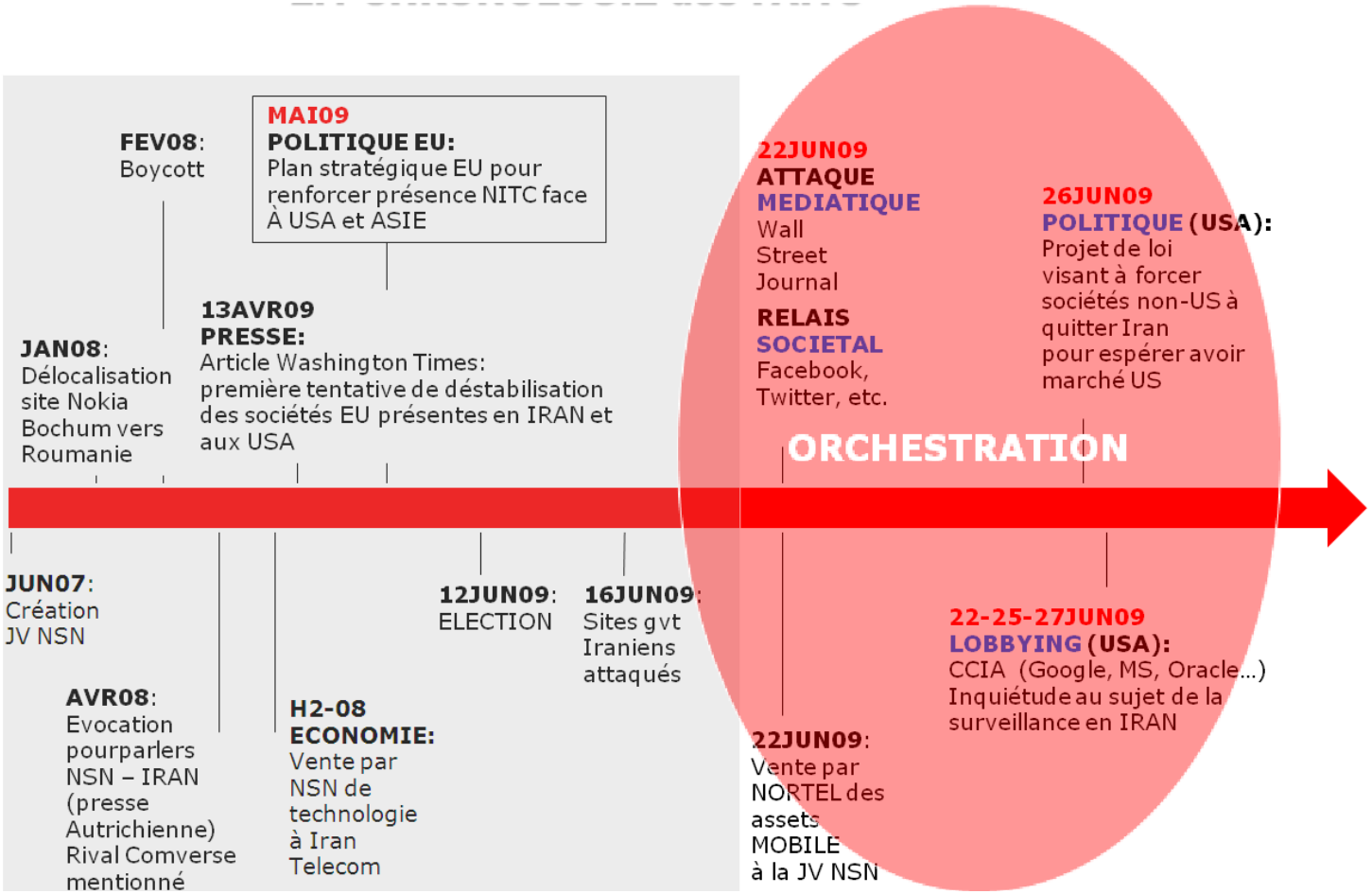
Cette campagne a été portée par la convergence des actions de différents lobbies, américains ou non, épaulant peu ou prou les intérêts économiques américains mais dans tous les cas servant efficacement la stratégie globale américaine.

Ce sont certains organismes associatifs, des activistes ou groupes d'activistes et/ou des opposants iraniens en exil qui ont été les vecteurs de l'opération, même si pour ces derniers on peut les associer plus directement à l'action des autorités américaines dans le cadre de la lutte directe contre le régime des Mollah.

Développement de Siemens sur le marché international

- Stratégie de Siemens : une « globalisation réussie »
- Montée en puissance de Siemens
- Technologie très avancée à l'égal des US mais :
  - Une image sociale dégradée pour NSN et pour Siemens
  - Rivalités économiques exacerbées dans des technologies sensibles
- Siemens est donc devenue ces dernières années un acteur majeur, gênant pour les intérêts américains y compris dans son pré carré Nord américain. Implantation aux US, velléité de NSN, rachat de la globalité de Nortel Networks et succès commerciaux. Partenaire de Microsoft (70000 emplois aux US)
  - Atteinte à la sécurité des US
- La crise iranienne: position de Siemens via NSN. prétexte et catalyseur pour les attaques

CHRONOLOGIE DES FAITS



ACTEURS ET PARTIES PRENANTES DE CETTE GUERRE DE L'INFORMATION

Acteur/Partie prenante	Définition	Rôle et action
Nokia Siemens Networks	**Nokia Siemens Networks**, compagnie détenue par Siemens et Nokia, regroupe les différentes activités de fabrication de matériel d'infrastructure réseau et de services associés. Cette entité est actuellement 2ème et 3ème sur les marchés d'infrastructures de téléphonie fixe et de téléphonie mobile	1. A vendu en Mars 2007 un réseau à larges bandes à l'Iran, ainsi que des stations d'écoute et de décryptage du contenu. 2. A vendu un système centralisé d'interception et de surveillance des communications téléphoniques, Internet, SMS, et autres canaux dernier cri, permettant à qui le contrôle de surveiller avec une précision redoutable tout le trafic de communication entrant et sortant du pays, ainsi qu'au sein du pays même. Cette vente, signée en 2007, est la vulnérabilité qui sera exploitée lors des attaques informationnelles *A noter : Comme cette vente portait sur des technologies de souveraineté, elles ont dû être autorisées (ou du moins tolérées) par des autorités de contrôle des exportations allemandes et finlandaises. Cette transaction porte sur un montant important mais non communiqué.*
Telecommunications Infrastructures Co.	Opérateur iranien national monopoliste	Exploitation du système livré par NSN

Acteur/Partie prenante	Définition	Rôle et action
Open Net Initiative	Groupement de chercheurs des universités de Harvard, Oxford, Cambridge et Toronto	1. Mise en évidence en 2005 que le réseau Internet développé en Iran est surveillé. Cette surveillance s'exercerait par le biais de solutions techniques construites par les sociétés Cisco Systems et Secure Solutions Corp. (rachetée entre-temps par McAfee). 2. Ces technologies auraient été implantées en Iran au cours des années 2004/5. Sensibles, elles auraient nécessité la fourniture d'une autorisation d'exportation. Hors, depuis 1979, l'exportation de technologies duales sensibles est soumise à un embargo, et une telle exportation aurait été légalement impossible. Les compagnies en question avaient démenti à l'époque. Néanmoins, cette activité jette le doute sur la main active (ou du moins la laxiste tolérance) des services américains *A noter : CS-CSC n'a pas été retenu pour la deuxième version du système de surveillance* 3. ONI édite un rapport au printemps 2009 annonçant que le système de Nokia Siemens Networks est maintenant pleinement opérationnel en Iran 4. ONI annonce que le logiciel Green Dam Youth Escort que le MIT (Ministère chinois de l'Industrie et de la Technologie) oblige à installer sur tous les ordinateurs « *a une influence qui s'étend bien au-delà de la protection de la jeunesse; les options de filtrage incluent la possibilité de bloquer du contenu politique et religieux* ».

Acteur/Partie prenante	Définition	Rôle et action
European and libertarian cyberactivists	• **Erich Möchel,** Journaliste spécialisé en nouvelles technologies au sein de la rédaction technique du journal numérique de l'Östereichischem Rundfunk (ORF) • **ONG Privacy International,** bénéficie de l'aide de grands fonds internationaux (German Marshall Fund, Carnegie Mellon Foundation, Soros Foundation) • Association autrichienne **quintessenz.org**	1. 22 juin 2009 : Erich Möchel, fait le lien avec le Washington Post et pointe sur son site *quintessenz.org*, où la documentation de Siemens est largement accessible. Il édite des articles incriminant nommément Siemens, ces articles sont cités par la presse traditionnelle américaine, tous les journaux se citant de façon circulaire 2. 7 au 8 avril 2008 sont déposées sur le site *quintessenz.org* les différentes présentations institutionnelles des versions successives du Monitoring Center (la solution technique de contrôle des communications vendue par Siemens à l'Iran).
Jerusalem Post		8 avril 2008 : article intitulé *« German firm helps Iran monitor Israel »*, dans lequel un journaliste décrie Siemens et Nokia Siemens Network comme ayant vendu lesdites technologies d'interception à l'Iran. Erich Möchel est repris et cité nommément, et affirme qu'il était « sûr à 99% » que ces technologies ont été livrées à l'Iran
Opposants iraniens exilés	• **Adi Ghaemi** • ***Mohsen Sazegara*** • ***Lily Mahazeri*** • ***Et beaucoup d'autres***	Site appelant au boycott des produits de Nokia et de Siemens et relayant les articles.

Acteur/Partie prenante	Définition	Rôle et action
Washington Times	Journal américain	Article du 13 avril 2009, dénonce pour la première fois le fait que le régime iranien pourrait traquer les opposants au régime en utilisant de l'appareillage sophistiqué vendu par Nokia Siemens Networks. La mise en cause de NSN intervient un an exactement après les premières révélations sur les contacts entre la joint-venture et Iran Telecom au sujet de la vente d'un système de télécommunication en Iran. L'article quotidien américain déplore qu'une entreprise bénéficiant de nombreux contrats avec le gouvernement américain et employant plus de 70'000 employés aux Etats-Unis collabore également avec des régimes répressifs permettant d'espionner leurs citoyens et de les envoyer en prison. Le *Washington Times* met en perspective les déclarations du porte-parole de Siemens avec un ancien membre des services de renseignements américains, un militant des droits de l'homme et des dissidents iraniens qui déplorent que les gouvernements européens n'aient pas de contrôle strict en ce qui concerne l'exportation de matériel technologique à double usage civil et militaire. Cette première salve à l'encontre du géant des télécommunications européen reste toutefois isolée et n'est pas répercutée au sein du microcosme médiatique américain malgré le contexte préélectoral en Iran.
Wall Street Journal	Groupe *News Corporation* de Rupert Murdoch	1. 22 juin 2009 : article accusateur sur NSN et l'Iran, (le jour du rachat des activités sans fil de Nortel, l'équipementier d'origine canadienne, est annoncé par l'équipementier européen) 2. 26 juin 2009 **:** Le *Wall Street Journal* publie un deuxième article sur l'implication de NSN dans la répression du régime iranien contre les manifestants en soulignant notamment l'étude d'un projet de loi au Congrès visant à empêcher les entreprises étrangères qui fournissent des technologies de surveillance à l'Iran de faire des affaires avec le gouvernement américain

Acteur/Partie prenante	Définition	Rôle et action
Facebook Twitter Youtube	Réseaux sociaux web 2.0	Relais des articles du WSJ et mots d'ordre des activistes
Austin Heap	Geek de San Francisco	Attaque des sites gouvernementaux iraniens grâce à l'utilisation de serveurs proxy fourni par un Américain et qui permettent de franchir les firewalls iraniens
Trovicor	Société allemande appartenant au fond d'investissements Perusa Partners	Il s'agit de l'ancienne division de Solutions de sécurité de Siemens, qui a développé le Siemens Monitoring Centre
Perusa Partners Fund	Fond d'investissements allemand qui s'est spécialisé dans le partenariat à long terme avec des sociétés externalisées	Avant les élections iraniennes, Siemens et NSN ont externalisé la division "Solutions Sécurisées" et l'ont vendu à Perusa Partners Fund NB : puisque les associés impliqués dans le fonds ne sont pas divulgués, il est possible que cette externalisation ait été exécutée seulement pour permettre de diminuer l'attention médiatique.
Comverse (à travers sa filiale ***Verint***)	Principal concurrent de NSN sur le marché de la surveillance du web.	Eprouve des difficultés à vendre son produit au Moyen-Orient du fait de sa proximité avec les intérêts israéliens
Nortel	Opérateur canadien	Opérateur canadien démantelé et dont une partie des activités a été racheté par NSN
Viviane Reding	Commissaire européenne en charge de la société de l'information et des médias	En mai 2009, l'Union européenne met en place une stratégie propre à renforcer son poids sur l'échiquier mondial des technologies de l'information face à l'Amérique du Nord et à l'Asie. V. Reding multiplie les initiatives sur le front des télécoms et des logiciels. Elle a également adoptée des décisions relativement fermes par rapport aux Etats-Unis.

Acteur/Partie prenante	Définition	Rôle et action
Charles E. Schumer **Lindsey Graham**	Deux députés (D-NY) et (R-SC) du Sénat américain	Charles E. Schumer et Lindsey Graham proposent 2 jours après l'article du WSJ un projet de loi dénonçant le commerce des entreprises occidentales avec l'Iran dans le domaine de la surveillance des télécommunications. Le texte va encore plus loin puisqu'il vise à empêcher les entreprises faisant du commerce avec l'Iran d'obtenir ou de renouveler des contrats existants avec le gouvernement américain Il est intéressant de dresser un parallèle entre d'une part, la dénonciation de la surveillance des citoyens par le gouvernement iranien, et d'autre part les mesures adoptées par l'ancien procureur général Alberto Gonzales lors du Patriot Act voté sous la présidence de George Bush et cautionnées par Graham.
CCIA	*Computer & Communications Industry Association* est une organisation internationale sans but lucratif basée aux Etats-Unis. Elle représente une grande partie des industriels dans le domaine des communications et de l'informatique. Elle compte parmi ses rangs des poids lourds comme Google, Microsoft, Oracle Corporation, Yahoo ou encore Sun Microsystems. Elle a pour but de préserver le libre-marché, une compétition juste et pleine ainsi que la liberté de circulation sur internet. La CCIA est également très active au Congrès où elle fait du lobbying intensif pour promouvoir ses objectifs.	**22, 25 et 27 juin 2009 :** Le 22 juin 2009, la CCIA réagit à l'article du *Wall Street Journal* en dénonçant l'utilisation par l'Iran de systèmes d'interception du trafic sur internet, ce qui porte atteinte à la liberté de communiquer sur internet. La CCIA veut ainsi démontrer pourquoi l'utilisation de certaines technologies comme le « *deep packet inspection* » devrait être restreinte dans le monde. Adepte de la libre circulation de l'information sur internet, la CCIA demande au Département d'Etat américain d'inclure la liberté de circulation sur internet dans son contrôle des droits humains dans le monde. 25 et 27 juin : La CCIA, s'inquiète ouvertement sur le fait que les autorités iraniennes disposent de technologies fournies par des entreprises occidentales (dont Siemens) puis la CCIA condamne…

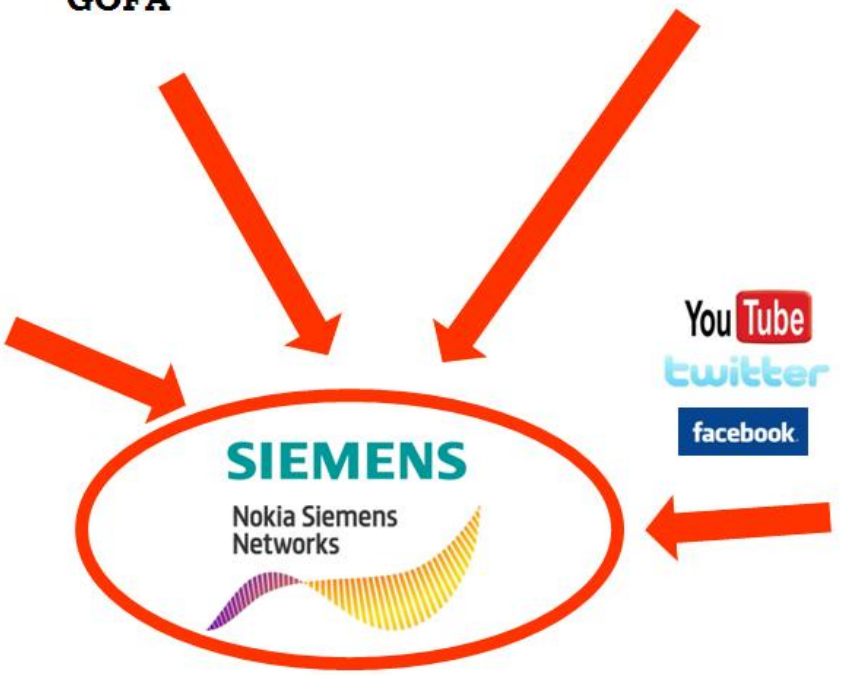
Acteur/Partie prenante	Définition	Rôle et action
Microsoft	Entreprise américaine de software	1. Seule l'entreprise américaine Microsoft s'est inquiétée des effets sur la libre circulation de l'information de l'installation du logiciel Green Dam Youth Escort que le MIT (Ministère chinois de l'Industrie et de la Technologie) oblige à installer sur tous les ordinateurs 2. Microsoft**,** qui fait partie du CCIA, est lié économiquement à Siemens aux Etats-Unis.
Reporters sans Frontières	ONG française pour la liberté de la presse	Article de Reporters sans Frontières **23/06/2009:** RSF insiste sur la nécessité d'adopter une législation permettant aux entreprises Internet américaines et européennes implantées dans des pays répressifs d'échapper aux mesures qui leur sont imposées par les gouvernements locaux. Parallèle entre l'Iran, (le gouvernement utilise les systèmes occidentaux de technologies, notamment Nokia et Siemens, pour filtrer le Web et intercepter les échanges de messages) et la Chine, (le ministère de l'Industrie et de la Technologie de l'information (MIIT) vient de confirmer que tous les fabricants d'ordinateurs devront proposer un logiciel de filtrage pour lutter contre la pornographie à leurs clients à partir du 1er juillet pour tout achat d'un ordinateur individuel). L'Iran et la Chine peuvent aujourd'hui bloquer l'accès à l'information grâce à des technologies occidentales. Il est grand temps que les Etats-Unis et l'Union européenne protègent leurs entreprises…

Acteur/Partie prenante	Définition	Rôle et action
Christopher Smith, (GOFA)	Le Global Online Freedom Act (GOFA) est une proposition de loi étudiée aux Etats-Unis et au sein de l'Union européenne dans une version différente. S'inspirant du Foreign Corrupt Practices Act, elle vise à « empêcher les entreprises américaines de collaborer avec des pays répressifs qui cherchent à transformer Internet en un outil de censure et de surveillance, à assurer le rôle du gouvernement américain de promotion de la liberté d'expression sur Internet et à restaurer la confiance du public en l'intégrité des entreprises américaines ».	A l'initiative du sénateur républicain Christopher Smith, elle a été introduite à la Chambre américaine des représentants dans sa nouvelle version le 6 mai 2009.
Jules Maaten (ALDE).	Député hollandais au Parlement Européen	La version européenne du GOFA a été présentée, le 17 juillet 2008, au Parlement européen par l'eurodéputé hollandais Jules Maaten (ALDE). Inspirée du modèle américain, cette proposition de directive demande aux entreprises de « *prendre leurs responsabilités au regard des principes de la Déclaration universelle des droits de l'homme* » et les incite notamment à héberger leurs serveurs à l'extérieur des pays répressifs.

PHASE D'ATTAQUE CONTRE SIEMENS

GOFA

Washington Times
Wall Street Journal
MURDOCH



Erich
Möchel

OBJECTIF: CHANGEMENT D'ÉCHIQUIER

- Développer une problématique globale à l'échelle mondiale (sortir du problème particulier Siemens – Iran) sur la régulation de la vente par les entreprises (occidentales ou non) de systèmes sensibles vers des pays non démocratiques (non seulement télécom mais aussi internet, en y associant tous les major US du secteur des NTIC).

- Se positionner en alliée et non en rival des US : défense des intérêts communs avec la promotion d'une réglementation commune limitant la « prolifération des outils de censure des NTIC » tout particulièrement pour les états non démocratiques et/ou ne respectant pas les libertés individuelles

- Neutraliser les vecteurs « satellitaires »: (hors institutionnel US) milieux cyber libertaires, opposants récurrents à Siemens.

Leviers:

- Contre-attaquer sur les contradictions de la CCIA – *(vecteurs indirects)* :

  Partialité de son action. La contraindre à respecter, quels que soient les acteurs, les valeurs que cette association est censée défendre

  - 1er exemple: Chine – " On May 19, 2009, the Ministry of Industry and Information Technology (MIIT) in China sent a notification to computer manufacturers of its intention to require all new PCs sold in China after July 1 to have filtering software pre-installed"

  - 2e exemple: *L'Open Net Initiative (groupement de chercheurs des universités de Harvard, Oxford, Cambridge et Toronto), mettent en évidence en 2005 que le réseau Internet développé en Iran est surveillé. Cette surveillance s'exercerait par le biais de solutions techniques construites par les sociétés Cisco Systems et Secure Solutions Corp.*

    Position de la CCIA dans cette affaire: pas de réaction

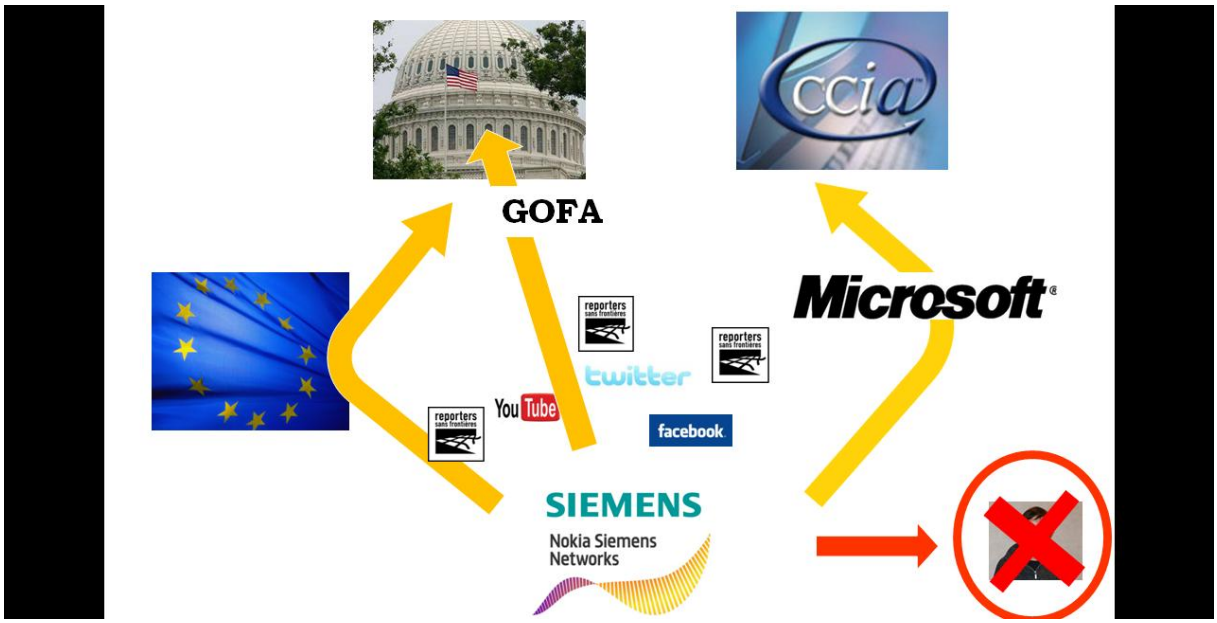
- Soutenir le Projet de Loi Gofa : - *(Lobbying, vecteurs indirect et direct)* porter par certain sénateurs US et députés en Europe et relayer par certaines organisations telles RSF.

- Promouvoir la nécessité de protection des entreprises occidentales (et donc démocratiques) contre l'obligation (implicite mais réelle) de livrer des technologies de surveillance avancées aux régimes non démocratiques → fixer un cadre légal à l'échelle mondiale

- Développer les intérêts communs entre toutes les entreprises occidentales et américaines. Exercer des pressions vers les pays extérieurs qui ne joueraient pas le jeu, les obliger à adhérer à la réglementation, suite à la mise en place d'une règlementation internationale et d'une autorité de régulation et des libertés (ONU, OMC…)

- S'appuyer sur la position de Siemens aux États-Unis *(Lobbying, vecteurs indirect et direct):*
    - lien avec Microsoft
    - 70000 emplois

CONTRE ATTAQUE DE SIEMENS



Vecteurs/Caisses de résonance:

- Elus sénateurs américains instigateurs et/ou favorables à la loi GOFA
- Elus européens favorables à la loi GOFA
- Commissaire européen en charge de la société de l'information et des medias
- Gouvernements européens
- Microsoft → CCIA et élus américains
- Reporters sans Frontières, mouvements associés et blogosphere
- Médias traditionnels et spécialisés

SITUATION FINALE