



Informational warfare exercise

COUNTERSTRIKE PROPOSITION FOR SIEMENS

Auteurs:

Claude Lepère

Fabien Droz

Franck Langlet

Jean-Christophe Marcoux

Philipp Bauer

Under supervision of:

Christian Harbulot

Avertissement et Copyright

Ce document d'analyse, d'opinion, d'étude et/ou de recherche a été réalisé par un (ou des) membre(s) de l'Association de l'École de Guerre Économique. Préalablement à leurs publications et/ou diffusions, elles ont été soumises au Conseil scientifique de l'Association. L'analyse, l'opinion et/ou la recherche reposent sur l'utilisation de sources éthiquement fiables mais l'exhaustivité et l'exactitude ne peuvent être garanties. Sauf mention contraire, les projections ou autres informations ne sont valables qu'à la date de la publication du document, et sont dès lors sujettes à évolution ou amendement dans le temps. Le contenu de ces documents et/ou études n'a, en aucune manière, vocation à indiquer ou garantir des évolutions futures.

Le contenu de cet article n'engage la responsabilité que de ses auteurs, il ne reflète pas nécessairement les opinions du(des) employeur(s), la politique ou l'opinion d'un organisme quelconque, y compris celui de gouvernements, d'administrations ou de ministères pouvant être concernés par ces informations. Et, les erreurs éventuelles relèvent de l'entière responsabilité des seuls auteurs.

Les droits patrimoniaux de ce document et/ou étude appartiennent à l'Association, voire un organisme auquel les sources auraient pu être empruntées. Toute utilisation, diffusion, citation ou reproduction, en totalité ou en partie, de ce document et/ou étude ne peut se faire sans la permission expresse du(es) rédacteur(s) et du propriétaire des droits patrimoniaux.

SOMMAIRE

EXECUTIVE SUMMARY	3
Nokia Siemens Networks within economic war: Background and context.....	5
A detailed chronology	6
Stakeholder analysis and informational checkers.....	7
Siemens under attack.....	17
Objectives: Perception from a larger scale	18
Siemens's counter attack	19
In the end	20

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 struggling 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 have both been severely impacted by these actions, this document presents also potential actions which could have been taken for:

- Diversion of the attacks, by provision either of other subjects, or targets of higher value, such as, for example
- 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 counter attack

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

The 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 flow of informational attacks against Siemens in the short, medium and long term.

Siemens is the target of the information war due to the sale of the deep packet inspection to Iranian authorities. Beside the riots of opponents related to the reelection of the President in Iran, everybody notice the information war which rose around this « political » phenomenon. In this hostile context for people in favor or dealing with the former and reelected President, actors that had interests in seeing NSN declining took advantage of this situation.

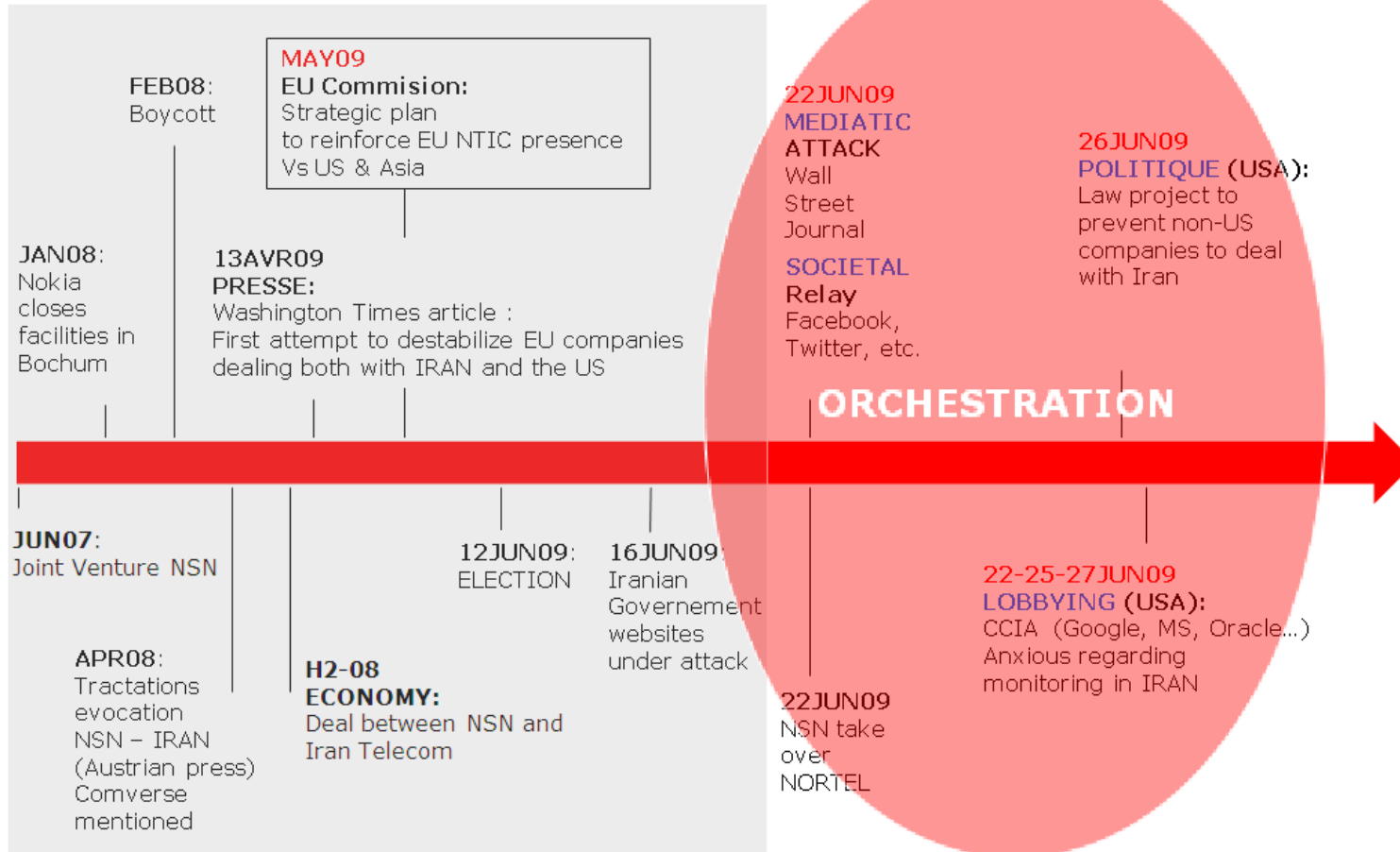
The reason for this attack has its roots in the fact that Siemens has increasingly and sustainably showed its capacity to challenge the American in areas where they used to be alone, more precisely in key-sectors such as information technology.

Such a campaign is not only a success due to the context in which people are interacting but because there is a combination of various actions at different levels focusing Siemens. No doubt on the fact that the goal of those actions is to reinforce the American position. Even some nonprofit organization, activists or Iranian opponents, from outside their country, enhanced the effect, even if they were not aware of the whole orchestration behind.

Development of Siemens on the international market

- Siemens strategy: a " successful globalization "
- Increasing role of Siemens worldwide
- Advanced technology just like US competitors but:
 - o degraded social image for NSN and Siemens
 - o keen competition, more obviously regarding sensible technologies
- Recently Siemens became a major actor even in markets where the American were dominant, i.e. NSN took over Nortel Networks. On the other side Siemens is a strong partner for Microsoft, employing 70000 people in the US)
- Finally; the Iranian crisis: exposition of Siemens via NSN: pretext for current attacks

A DETAILED CHRONOLOGY



STAKEHOLDER ANALYSIS AND INFORMATIONAL CHECKERS

The table provided hereafter aims at briefly presenting the different identified stakeholders of this informational fight, as well as their position and interests followed.

Actor / Stakeholder	Definition	Role & taken actions
Nokia Siemens Networks	Joint-venture between Siemens and Nokia, holds the different production sites for communication infrastructure design and production sites. This joint compagny is currently the 2 nd largest compagny in the world for manufacture of communication infrastructure for fix phonelines, and 3 rd largest manufacturer for wireless network infrastructures.	<ul style="list-style-type: none"> • Has sold in March 2007 a wide-band network to Iran, with related interception and decryption stations. These stations allow free and unlimited access to the communications. • Has sold a centralized interception and decryption infrastructure (named <i>Monitoring Center</i>), able to simultaneously monitor phone calls, Internet content, SMS and other communication means:. Since this infrastructure is posted on the central node connecting Iran to the rest of the world, this allows simultaneous tracking of contents in all Iranian networks, as well as surveillance of the communications between Iran and the rest of the World. This transaction is the weak point on which NSN is attacked during the observed informational battles. <p><i>NB: as this sale engages critical technologies, they must have been authorized by the German and Finish state department. The value of this sale is important but undisclosed yet.</i></p>
Telecommunications Infrastructures Co.	Iranian national telecommunication company,	Operation of the delivered interception system sold by NSN, in close contact with the Iranian Revolution Guards

Actor / Stakeholder	Definition	Role & taken actions
	state-owned, sole operator of Iranian Network	
Open Net Initiative	Researcher network, involving the Universities of Harvard, Oxford, Cambridge and Toronto	<ul style="list-style-type: none"> • Discovered in 2005 evidences that the Iranian Internet is being monitored. This control is made by an infrastructure involving technologies sold by Cisco Systems and Secure Solution Corporation (which has been bought in the meantime by McAfee). The export of these technologies has taken place in 2004 or 2005, and should have been approved by US state department. But, since 1979, Iran is black-listed for this kind of exportation, therefore, this sale should not take place. Contacted by the ONI, the companies issued a firm dementi. But, this puts the doubt on the active hand (or at least on the knowing neglect) of the American state department. <i>NB: these two companies have not been retained for delivery of the second version of this infrastructure.</i> • ONI releases a study in spring 2007, in which the NSN system is found to be fully operational in Iran. • ONI announces that the <i>Green Dam Youth Escort</i> software of the Chinese Ministry of Industry and Technology imposes on each Chinese computer has “a larger role than solely protection of the youth, since the filtering capabilities allow blocking of religious and political content”.

Actor / Stakeholder	Definition	Role & taken actions
<p>(H)activists in Europe and America</p>	<ul style="list-style-type: none"> • Erich Möchel, author specialized in new and emerging technologies for the online edition of the news of the <i>Östereicher Rundfunk (ÖRF)</i> (Austrian state-owned broadcast service) • Privacy International, NGO funded by major international funds, such as the German Marshall Fund, the Carnegie Mellon Foundation and the Soros Fundation • quintessenz.org, Austrian alternative activist organisation specialized in digital freedom. 	<ul style="list-style-type: none"> • On the 22th of June 2007, Erich Möchel links on his post on the Austrian broadcast service website an article of the Washington Post to the <i>quintessenz.org</i> website, on which the sale documentation of the NSN surveillance platform is largely accessible. • On 7th and 8th of April 2008, other documentation of the different versions of the NSN monitoring center are put on the <i>quintessenz.org</i> website.

Actor / Stakeholder	Definition	Role & taken actions
Jerusalem Post	Israeli newspaper	Publishes on the 8 th of April 2008 an article entitled <i>“Germany helps Iran monitor Israel”</i> , in which the columnist presents the deal between Siemens and NSN and the Iranian state for the delivery of the Monitoring System. Erich Möchel is namely cited, stating <i>“being sure to 99 percent”</i> that these sensitive technologies have been provided to Iran.
Iranian Contras in exile	<ul style="list-style-type: none"> • Adi Ghaemi, • Mohsen Sazegara, • Lily Mahazeri • ... and many more 	Active relay of NSN and Siemens-bashing articles and information, active relay of the Boycott of Siemens and Nokia products.
Washington Times,	US newspaper	<p>Publishes on the 13th of April 2009 an article in which for the first time it is revealed that the Iranian regime is able to track opponents by using the NSN-provided technology. The implication of NSN comes exactly one year after the revelation of contacts between NSN and the Iranian state-owned phone company. The newspaper furthermore regrets that the company, as having strong ties to the US government and markets, and employing more than 70.000 people in the US, actively enables this repressive regime in Iran, and exports sensitive dual-use technology.</p> <p>This first attack of European interests remains isolated, and is not</p>

Actor / Stakeholder	Definition	Role & taken actions
		relayed in the American mediasphere, despite the fact that the Iran is in front of general elections.
Wall Street Journal	US Newspaper, part of the News Corporation , owned by Rupert Murdoch	Two facts, both on the 22th of June, 2009 <ul style="list-style-type: none"> • Publication of the first article involving NSN and the Iran. The same day, NSN announces the take-over of the Canadian Nortel Networks company, also specialized in information network technologies. • The newspaper publishes a second article, in which implication of the NSN company in the repression of the Iranian opponents. It also relates the proposal of a Congress law aiming at preventing foreign companies which are selling technologies to Iran of dealing with the US government.
Social Networks	<ul style="list-style-type: none"> • Facebook • Twitter • Youtube • ... among others 	Active relay of the Wall Street Journal article
Austin Heap	American technologist, who as put on Internet technical instructions on how to set-up IP	Attacks the Iranian governmental websites, by using proxy-servers provided by American activists allowing bypassing the Iranian

Actor / Stakeholder	Definition	Role & taken actions
	proxies allowing activists to pass the governmental firewalls.	firewalls.
Trovicor,	German company owned by the investment fund Perusa Partners	Is the former Security Solutions divisions from Siemens, which has developed the Siemens Monitoring Center.
Perusa Partners Fund,	German investment fund specialized in the long-term partnership with externalized companies	Before the Iranian elections, Siemens and NSN externalized the "Secure Solutions" division, and sold it to Perusa Partners Fund. <i>NB: since the partners involved in the fund are not disclosed, it is possible that this externalization was performed only for allowing the mediatic attention to decrease.</i>
Comverse (via its subsidiary Verint)	Main competitor of NSN on the Internet monitoring sector.	Is unable to sell its solutions in the Middle Orient due to its proximity with Israeli interests
Nortel	American company, which has been dismantled and of which one division was sold to NSN	

Actor / Stakeholder	Definition	Role & taken actions
Viviane Reding	European Commissar in charge of the Information Society, the media and Information	In May 2009, the European Union sets up a proper strategy allowing to reinforce its weight on the world market of information technologies, and countering in particular American interests. Viviane Redding multiplies initiatives backed by the European Commission on communications and software, and has also adopted strong position against American interests.
Charles E. Schumer Lindsey Graham	US Senators (democrat from New-York and Republican from South Carolina)	Two days after the the article of the Wall Street Journal, both issues jointly a law draft aimed at forbidding commercial ties between occidental companies and the Iran on the field of communications and surveillance technologies. This law would forbid to companies involved in such deals of concluding or renewing contracts with the American government. <i>NB: Senator Graham was already in favour of the Patriot Act. During the Bush legislature, he was already in favour of prosecuting « fifth column » movements, for which no mandate should be needed. This was strongly supported by the President Bush then.</i>
Computer and Communication Industry Association (CCIA)	International US-based industrial association; which represents the interests of professionals in the field of	Following actions were taken during June 2009: <ul style="list-style-type: none"> • 22th of June 2009: CCIA reacts to the Wall Street Journal article by firmly denouncing the use by the Iran of

Actor / Stakeholder	Definition	Role & taken actions
	<p>computer and communication technologies. Main members are, among others, Microsoft, Google, Oracle, Yahoo and Sun Microsystems.</p> <p>This grouping aims at protecting the free market and fair competition on the market, as well as freedom on the Internet.</p> <p>CCIA is involved in lobbying towards Congress and Senate for promotion of its goals.</p>	<p>sophisticated interception means, which attains to freedom on Internet. In particular, “<i>deep packet inspect</i>” technology¹, which allows this kind of in-depth control, should be restricted to certain areas in the world. The CCIA therefore asks the State Department to include the freedom on Internet in its monitored Human Rights indicators.</p> <ul style="list-style-type: none"> • 25th and 27th of June 200: the CCIA is publicly concerned by the fact that Iranian officials employs technologies provided by occidental companies including Siemens, and condemns again the use of these technologies for repression.
Microsoft	US Software company	<ul style="list-style-type: none"> • Microsoft was the noly company concerned by the effects of free circulation on Internet of the Chinese software Green Dam Youth Escort, which has to be installed on each computer in China. • Microsoft is also part of the CCIA, and linked to Siemens in the US.

¹ The Monitoring Center of NSN is mainly based on this technology.

Actor / Stakeholder	Definition	Role & taken actions
Reporters sans Frontières/Reporters without Borders	French NGO battling for Freedom of Information	<ul style="list-style-type: none"> • Published on the 23th of June 2009 an article, in which the NGO insists on the need for the US Internet companies making business with repressive regimes of not being subject to local rules imposed by these governments. • In parallel, this NGO confirmed the obligation for each computer being used in China of installing the Great Firewall, which allows extensive filtering capabilities of the Internet content. • This makes the parallel between China and Iran, both being able to actively monitor the use of Internet of their citizens by using western technologies.
Christopher Smith, initiator of the Global Online Freedom Act (GOFA)	The GOFA is a law draft currently under consideration by the US and European chambers (in slightly different versions). Based on the Foreign Corrupt Practices Act, this proposition aims at “preventing American companies of collaborating with repressive states which seek for censoring Internet, and which brings the US government to actively	<ul style="list-style-type: none"> • Led by the initiative of the Republican Senator Christopher Smith, this law proposal has been brought to debate within the US congress in its new version on the 6th of May 2009.

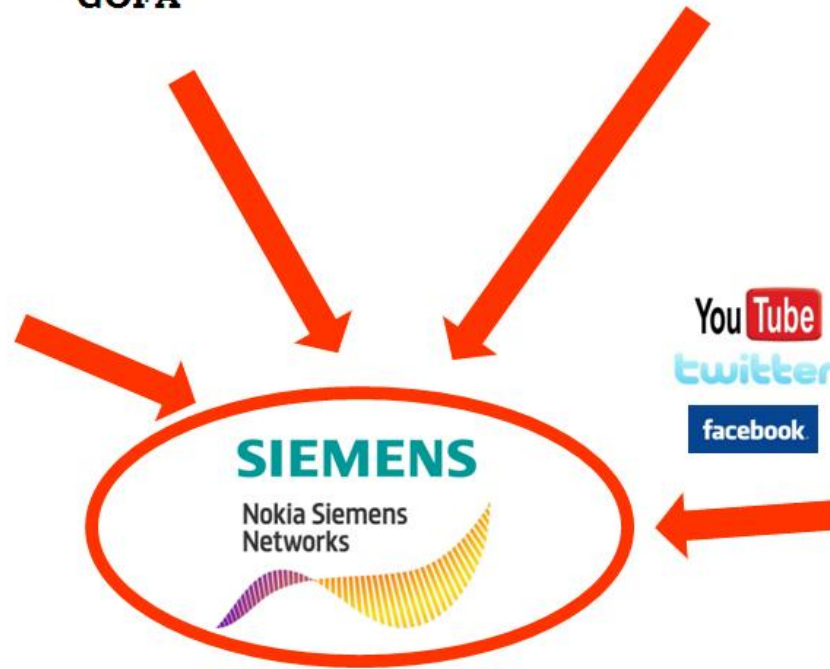
<i>Actor / Stakeholder</i>	<i>Definition</i>	<i>Role & taken actions</i>
	defend the freedom of information worldwide and in restoring the confidence of the American people in the integrity of their companies”.	
Jules Maaten, MEP, Alliance of the Liberal Democrats in Europe (ALDE)	Dutch Member of the European Parliament	<ul style="list-style-type: none"> The European version of the GOFA has been presented on the 17th of July 2008 to the European Parliament by the MEP Jules Maaten. Largely inspired by the US model, this directive proposal asks the companies to “take their responsibilities with regard to the principles of the Human Rights” and force them, among other points, of hosting their servers in repressive countries.



GOFA



Washington Times
Wall Street Journal
MURDOCH



OBJECTIVES: PERCEPTION FROM A LARGER SCALE

- ❖ Developing a global problematic that concerns other actors in the world (escaping from the particular Siemens problem related to Iran) on the sales regulations for companies (western or not) developing sensible applications used by non democratic government (for Telecom and internet, and associating major US NTIC companies).
- ❖ Taking position of US allies instead of being rivals: finding points of compromise on which common positions may come arise and together support regulation limiting the use of Internet systems which censor information and spy on citizens using it
- ❖ Neutralize "satellite" vectors: (except institutional US) circles recurring opponents on the web of Siemens.

Leverages

- ❖ Counter-attack on CCIA contradictions - (indirect vectors)

Giving evidence that this nonprofit organization is partial in its speech and this demonstration should lead to get it back on the position which respect neutrality regardless the actors that are concerned

1st example: China – “ 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”

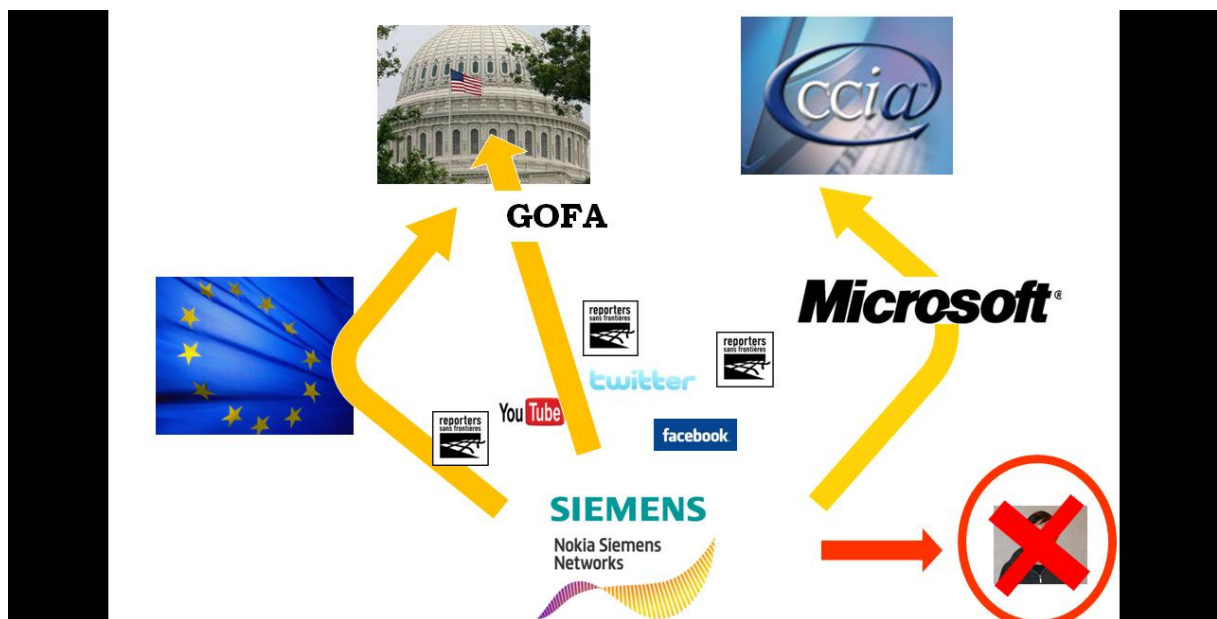
2nd example: In 2005, the Open Net Initiative (Group of researchers at Harvard University, Oxford, Cambridge and Toronto) is giving evidence of the monitoring on the Internet network developed in Iran. This is possible thanks to material developed by Cisco Systems and Secure Solutions Corp.

➔ CCIA and US Companies position on this matter, no reaction on Microsoft side (Siemens partner in the US)

- ❖ Sustain the GOFA law draft: (by lobbying, using direct and indirect vectors) The aim of this action is to be defended by US and European congressmen, and to be relayed by other organizations, such as, for example, RSF
- ❖ Propagate the need of protection of western companies (which shall then be seen as democratic) against the (implicit but strong) need to transfer advanced monitor and security technologies to non-democratic regimes. This shall fix a worldwide regulation frame

- ❖ Develop common interests between all European and American companies. Here, pressure has to be put on countries exterior to the western regulation sphere that would form a band apart, in order to force them to adhere to the regulation. This could be obtained by implementation of this regulation within an international representative organization, such as, for example, UN or the WTO
- ❖ Taking advantage of Siemens position in the U S: (lobbying, indirect and direct vectors)
 - link with Microsoft
 - 70000 jobs(uses)

SIEMENS'S COUNTER ATTACK



Sound box / vectors

- ❖ Elected American senators instigators and/or favorable to the law GOFA
- ❖ Elected European favorable to the law GOFA
- ❖ European Commission in charge of the information society and the media
- ❖ European Governments
- ❖ Microsoft → CCIA and American elected representatives
- ❖ Reporters without Borders, associated movements and blogosphere
- ❖ Traditional and specialized Media

IN THE END



 **Computer & Communications Industry Association** OPEN MARKETS. OPEN SYSTEMS. OPEN NETWORKS
FULL, FAIR, AND OPEN COMPETITION

 **ORACLE**  **NORTEL NETWORKS** **Microsoft**
  

SIEMENS