GLOBAL DEBATE & PUBLIC POLICY CHALLENGE

POLICY MEMORANDUM SAMPLES

I. Introduction

The following policy memorandum samples provide you with examples on the format of a policy memorandum. They display a variety and approaches and styles that you may find helpful when developing your own policy memorandum.

Please note that these examples do not necessarily correspond to the writing guidelines and evaluation criteria specifically established for the Global Debate and Public Policy Challenge (e.g. some memos do not provide sources). The samples are therefore by no means a template for your memo.

Please carefully follow the memo writing instructions provided separately to ensure that your submission meets the requirements established for the Global Debate and Public Policy Challenge.

II. List of sample policy memos

1. Harvard Kennedy School of Government (no date). *Re-organizing the Government to Combat the WMD Threat.* Retrieved from http://www.hks.harvard.edu/var/ezp_site/storage/fckeditor/file/pdfs/degree-programs/registrar/sample-policy-memo.pdf

2. LK11538 (2012). *Digital Freedoms and Canadian Economic Policy.* Submission to the Global Debate and Public Policy Challenge 2012-2013.

3. KG10240 (2012). *Sanctions of the 21st century.* Submission to the Global Debate and Public Policy Challenge 2012-2013.

MEMORANDUM

TO: President of the United States
FROM: [ ]
SUBJECT: **Re-organizing the Government to Combat the WMD Threat**
DATE: xx / xx / xxxx

The proliferation of nuclear, chemical, and biological weapons is the most serious threat to U.S. security today, and will remain so far into the future. Whereas combating proliferation is an inherently government-wide mission, the existing national security architecture has resulted in a series of agency-specific efforts that are often poorly coordinated and fail to take advantage of important synergies. Re-organizing the government to meet the WMD threat therefore requires reforms that strengthen White House management of nonproliferation programs, expand interagency counterproliferation capabilities, and improve WMD-related intelligence.

Strengthen White House Management of Nonproliferation Programs

The Departments of Energy (DOE), State, Defense (DOD), Commerce, and Homeland Security (DHS) all contribute to U.S. nonproliferation efforts, but receive insufficient top-level program guidance and coordination. For example, DOE did not learn of Libya's decision to abandon its nuclear program until it was revealed in the press. Moreover, DOE had no plan in place to dismantle Libya's nuclear assets despite its central role in performing such activities. Finally, proliferation detection R&D projects are currently managed by a community of end users that have overlapping needs but rarely communicate with each other.

To prevent future interagency breakdowns, the White House should designate a new senior-level Nonproliferation Policy and Program Director (NPD) to oversee all U.S. government nonproliferation programs. The NPD will chair a new National Security Council Policy Coordinating Committee on Nonproliferation (PCC) that will set overarching nonproliferation goals and priorities, develop an interagency strategic plan to achieve those goals and priorities, identify and assign missions and responsibilities to appropriate agencies, and coordinate program execution. To improve proliferation detection R&D, the NPD and PCC will also design an interagency technology development plan that will integrate and prioritize the needs of various technology end users across the government with the capabilities of the U.S. national laboratory system, private industry, and top universities. The Office of Management and Budget (OMB) will work with the new NPD and PCC to develop a multi-year interagency nonproliferation program budget, and will apply performance measures to monitor program management and implementation.

Although the NPD and the PCC will require little additional funding, past attempts at White House policy coordination – such as the Office of Homeland Security – have sunk into irrelevance because of agency resistance. To avoid suffering a similar fate, the NPD and PCC must possess clearly delineated authority and high level backing. In particular, the NPD should enjoy unambiguous control over nonproliferation policy and program budgets. The PCC should require agency participation at the Under Secretary level. Most important, the NPD and PCC must receive consistent, visible support from the President.

Expand Interagency Counterproliferation Capabilities

The U.S. military and homeland security communities must be able to rapidly respond to proliferation emergencies. To provide this capability, the United States should create and train "Proliferation Risk Mitigation Teams" – akin to the Department of Homeland Security's Nuclear Emergency Search Teams (NEST) – comprised of DOD special operations forces (SOF), CIA operatives, and DOE technical specialists. These teams will be capable of securing nuclear storage facilities and other sensitive infrastructure during combat operations or in response to the collapse of central authority in states that possess nuclear assets that are attractive to terrorists. They will also provide logistical and operational support to the Energy Department's "Global Cleanout" program that seeks to return stockpiles of weapons-usable highly enriched uranium to Russia and the United States. Finally, they will engage in extensive "red-teaming" simulations in order to foster better situation awareness and preparedness.

Operational control of Proliferation Risk Mitigation Teams will pose a major challenge. Congress may object to placing the teams under CIA control in light of the agency's past abuses. Moreover, DOD will be reluctant to assign SOF personnel to the teams if they will be placed under the command authority of a different agency. Given the types of operations in which the teams are likely to engage, DOD operational control would therefore seem most appropriate. The teams will cost approximately $500 million annually to train and equip. To provide the necessary funding, the United States should cancel the Missile Defense Agency's Airborne Laser program, which has been plagued by cost overruns and schedule delays.

Improve WMD Intelligence

The effectiveness of U.S. nonproliferation and counterproliferation efforts ultimately depends on the quality of WMD intelligence. Unfortunately, the U.S. intelligence community has a poor track record of detecting both state-level and sub-state WMD proliferation. It failed to anticipate India's nuclear test in 1998, produced flawed assessments of the threat from Saddam Hussein's Iraq, and only belatedly uncovered the nuclear black market smuggling ring of Pakistani scientist A.Q. Khan. In addition, the intelligence community remains unable to provide reliable information on the status of nuclear programs in North Korea and Iran.

To improve community-wide WMD intelligence collection and analysis, the United States should, per the recommendation of the recent WMD commission, create a new National Counter Proliferation Center (NCPC). The Center would report directly to the new Director for National Intelligence and set requirements for WMD-related human, imagery, and signals collection for the entire intelligence community. It would also house an analytical division that would provide high-quality, actionable intelligence assessments to customers across the U.S. government, including the new White House NPD.

The NCPC will require approximately $1 billion in annual funding. Given this price tag, Congress may resist creation of the NCPC until it can determine whether recent legislation will effectively address current intelligence community deficiencies. Moreover, CIA already operates an analytical unit devoted to WMD intelligence (WINPAC) that will fiercely resist encroachment upon its turf. The NCPC should therefore function as both a consumer and independent reviewer of WINPAC intelligence products while avoiding disruptive turf battles. Competition between WINPAC and the NCPC could result in higher-quality intelligence products from both.

ict consulting group

POLICY MEMO

TO: The Right Honourable Stephen Harper, Prime Minister of Canada

FROM: LK11538

DATE: November 30, 2012

RE: Digital Freedoms and Canadian Economic Policy

The Canadian Security Intelligence Service has obtained reliable intelligence confirming that the Canadian-based company, Saur-N, has entered into a contract to provide communications technology to China's authoritarian government. This technology will allow Chinese officials to track mobile telephone signals, break into email and social networking accounts, censor web searches, and block internet access and mobile phone signals. The Chinese regime is already notorious for such limitations on digital freedoms. Government departments regularly censor websites, monitor private emails, and regulate content of websites such as Google and Yahoo! (Human Rights Watch, 2006). However, while Saur-N's technology will further enable Chinese officials to monitor private communications and restrict freedom of expression via the internet, it will also improve the efficiency of China's private sector businesses and thereby develop the Chinese economy.

Historically, Canada has maintained a neutral relationship with China as there has been no history of Sino-Canadian conflict or competition. Canada's current, formal relationship with China allows bilateral access to each state's technological development activities if such access is for peaceful purposes (Agreement for Scientific and Technological Cooperation, 2008). Canada is also a signatory member of the Universal Declaration of Human Rights which declares that "everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers" (1948).

Tacit approval of the contract is the simplest policy available to the Government of Canada. It is said that the increased efficiency in Chinese private sector businesses will spur economic growth and reduce poverty (Wilson and Wilson, 2006). In turn, economic growth will shift Chinese values towards support for freedoms of expression and democracy (Inglehart and Welzel, 2009). This policy assumes that freedoms of expression inevitably result from economic

development. However, permitting the Saur-N contract would signal to the international community that Canada values economic growth over digital freedoms and human rights.

A second policy option limits the use of communications technology to private sector, Chinese businesses and, upon breach of this condition, allows Canada to block future sales. However, the international community will likely view this unfavourably as Canada should, based on public reports (Human Rights Watch, 2012), expect Chinese officials to inevitably utilize the technology to violate digital freedoms. Canada will then be forced to damage relations with the Chinese government by blocking future sales and economic development.

In reality, there is a policy option that allows Canada to maintain a favourable international reputation and strengthen relations with China. The Government of Canada must completely block the sale of Saur-N's technology. This policy will signal that Canada does not tolerate violations of basic digital rights by authoritarian regimes and that Canada will take a leading role in promoting freedoms of digital expression and online privacy rights. Canada must also promote economic cooperation through other means which will enhance relations with Chinese citizens.

Specifically, this policy requires the Department of Foreign Affairs and International Trade to issue private directives to Saur-N and make public statements requesting nullification of the sales contract. Secondly, the Canada Border Services Agency must implement a strict embargo on Saur-N's technology in the event that the company attempts to export its product despite discouragement from the government. Finally, Canada must establish the Canada-China Digital Entrepreneurship Consortium (CCDEC) as an initiative to promote economic development through private sector, digital businesses. After its creation, the Government of Canada should invest $20 million annually in the CCDEC for training conferences and seminars on the relationship between digital technology and business.

Firstly, public and private statements denouncing the sales contract send a strong message that the Government of Canada will not condone authoritarian practices by foreign regimes. A recent report indicates that Canadian multinational mining corporations have successfully implemented 18 of 27 recommendations of Canada's Corporate Social Responsibility Strategy including provision of tools to support human rights in local civil societies (Mining Association of Canada, 2012). In this instance, strong government action effectively pressured companies to develop international human rights through corporate practices. Therefore, public government statements promoting corporate social responsibility for digital rights are likely to convince Saur-N and other companies to refrain from business practices that assist Chinese officials in surveillance.

By also implementing an embargo on Saur-N's technology, Canada will demonstrate determination to prevent digital rights abuses. Historical evidence from the oil embargo of 1973 indicates that embargoes severely restrict an importing country's capability to execute policy. Arab oil exporting countries, seeking to punish the USA for supporting Israel in war, banned oil exports to Western countries, caused reductions of oil supply which varied from 7% to 35%, and

limited countries' ability to provide oil to citizens (Davis, 1976). If strictly applied, Canada's similar embargo will proactively restrict the Chinese regime's ability to further spy on private communications. Undertaking this leadership role will strengthen Canada's reputation internationally as a promoter of the rights declared in the Universal Declaration of Human Rights.

Lastly, the creation of and investment in the Canada-China Digital Entrepreneurship Consortium will achieve Canadian, Chinese and international objectives by developing digital freedoms while stimulating international economic growth. The CCDEC shows potential based on evidence from the Digital Freedom Initiative (DFI) launched in 2003 by the USA. The DFI was a public-private initiative that successfully achieved similar objectives. Partnerships were created between the USA and Senegal to train Senegalese citizens how to use email and the Internet to research and create international economic relationships through The Cyber Luoma marketplace (United States Agency for International Development, 2005). This success indicates that the CCDEC can expand digital freedoms by allowing Chinese citizens to access unrestricted digital content through Canadian-sponsored training seminars. The Chinese can then apply their digital training, as the Senegalese did, to international entrepreneurial activities that stimulate international trade and economic growth.

The policy suggested here is superior to the alternatives because it advances digital freedoms as its primary objective while allowing for subsequent economic growth. Therefore, it will satisfy most stakeholders. It will achieve international support as it affirms international treaty obligations, domestic support as it strengthens Canada's economy, and support from Chinese citizens as it provides them with basic digital freedoms.

Saur-N is willing to fulfill their contractual obligations to the Chinese. Should it obtain the company's communications technology, the Chinese regime’s capabilities to monitor private communications between citizens will be greatly expanded and digital freedoms will be egregiously violated. While the technology will improve the efficiency of Chinese businesses, Canada cannot support policies that condone unethical business practices and policies that place economic growth before the promotion of digital freedom. It is recommended that the Government of Canada block the business deal outright. This will require public and private condemnation of the contract along with a strict embargo of Saur-N's technology. It is critical that the government simultaneously develop the Canada-China Digital Entrepreneurship Consortium to strengthen economic ties. By implementing the policy suggested here, the Government of Canada will not only satisfy Chinese and Canadian citizens but also uphold international treaty obligations by promoting global digital freedoms.

Works Cited

Agreement for Scientific and Technological Cooperation between the Government of Canada and the Government of the People's Republic of China, Canada-People's Republic of China, 17 July 2008, Canada Treaty Series 2008 No 6. Retrieved October 21, 2012, from http://www.treaty-accord.gc.ca/text-texte.aspx?id=105085

Davis, Jerome. (1976). The Arab Use of Oil: October 1973-July 1974. *Cooperation and Conflict, 11*(1), 57-67.

Human Rights Watch. (2006). *Race to the Bottom: Corporate Complicity in Chinese Internet Censorship* (Human Rights Watch Report Volume 18, No. 8(C)). Human Rights Watch. Retrieved October 21, 2012, from www.hrw.org/sites/default/files/reports/china0806webwcover.pdf

Human Rights Watch. (2012). *World Report 2012*. New York, NY: Seven Stories Press. Retrieved November 7, 2012, from www.hrw.org

Inglehart, Ronald, and Christian Welzel. (2009). How Development Leads to Democracy: What We Know About Modernization. *Foreign Affairs, 88*(2). Retrieved November 5, 2012, from http://www.foreignaffairs.com/

Mining Association of Canada. (2012). *Recommendations of the National Roundtables on Corporate Social Responsibility and the Extractive Industry in Developing Countries: Current Actions, Stakeholder Opinions and Emerging Issues*. Ottawa, ON: Mining Association of Canada. Retrieved November 7, 2012, from http://www.mining.ca/site/index.php/en/news-a-media/publications.html

UN General Assembly. (1948). *Universal Declaration of Human Rights*. Resolution 217 A (III). Retrieved November 7, 2012, from http://www.unhcr.org/cgi-bin/texis/vtx/refworld/rwmain?docid=3ae6b3712c&page=search

United States Agency for International Development. (2005). *The Digital Freedom Initiative Annual Report: March 2004-March 2005*. Washington, D.C.: United States Agency for International Development. Retrieved November 8 2012, from https://dec.usaid.gov/dec/home/Default.aspx

Wilson, Craig, and Peter Wilson. (2006). *Make Poverty Business: Increase Profits and Reduce Risks by Engaging with the Poor*. Sheffield, UK: Greenleaf Publishing Limited.

SANCTIONS OF THE 21ST CENTURY

From: KG10240
To: DEPARTMENT OF STATE, U.S.
Re: SCENARIO D
Date: NOVEMBER 30, 2012

1. INTRODUCTION

In October 2011 the Wall Street Journal published an article describing how the oppressive Syrian government bought censorship systems of US-based company Blue Coat Systems Inc. (2011) We now face another company, Saur-N, trying to sell its surveillance mechanisms to a well-known authoritative regime (henceforth referred to as "WKAR").

The problem of reselling censorship systems affects everyone: both liberal and illiberal governments, people thereof and international organizations – in the Arab Spring we saw them all get involved. (See Figure 1.1) Since declaration on the Internet can now lead to serious harm or possibly death of many, as it has in the case of Abdul Ghani Al Khanjar, this is an issue of utmost importance. (Silver & Elgin, 2011)

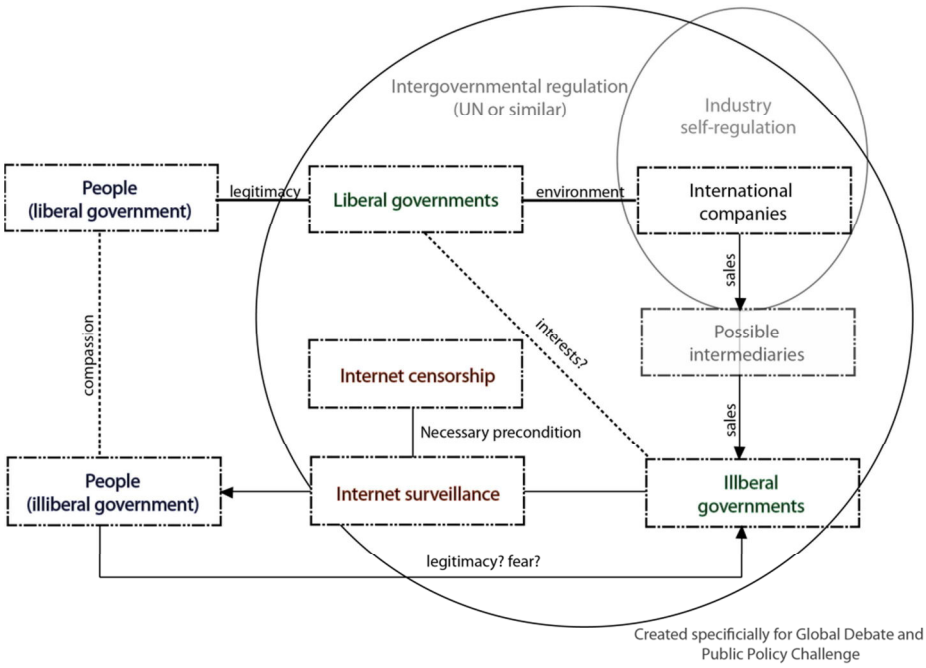

Figure 1.1 Structure of relationships

2. GENERAL DISCUSSION

Impact of internet censorship is hard to estimate, but an analogy with the defense industry seems to be appropriate, as one Member of the European Parliament said: "We have to acknowledge that certain software products now are actually as effective as weapons." (RWB, 2012, p. 1) Size-wise, US arms exports industry, amounted to $85.3 billion in 2011, while the whole project of China's censorship cost $800 million until 2002—which we can use a rough guide to the size of the censorship industry—making it clear that censorship is economically less important than the arms industry. (Shanker, 2012) (Yang, 2003) **The relatively smaller, equally important, censorship industry**

should be regulated in some fashion, as the bigger already is – in 2007 alone, the US government investigated 37 defense deals, many including expensive equipment like jet-fighters. (Department of Justice, 2007)

However, there is a number of European companies—e.g. French Télécom—that export censorship technology to Asia and Africa and thus we must weight possible disadvantage to the American industry & Saur-N, if we block this sale. (Wagner, 2012)

Any policy should ideally:

- Limit trade as little as possible
- Do as little damage to mutual relations
- Protect Human Rights like the right to assembly and freedom of speech

US foreign policy stresses human rights and *jus cogens*—norms that are legally binding and cannot be changed by treaties—as embodied by many documents, *inter alia* the Universal Declaration of Human Rights. (Department of State, 2012) (Trindade, 2008) We do not have any legally binding obligation to prevent the sale of "dual use" products—products that can be used for both civilian and military/oppressive purposes. (Brown & Korff, 2012) **Nevertheless, letting the trade go through without any restrictions is too great of a risk to human rights, to our binding obligations to them, image of the United States and the current administration.** So far, this problem has been rather peripheral, due to low public awareness; however issues pertaining to surveillance can irritate the public, as reaction to ACTA testifies. (Arthur, 2012)

Some transactions are done via intermediaries, which is the only reason why the Blue Coat sale to Syria was not a direct violation of the 2004 US export ban. (Carbone, 2012) Thus we need policy to allow us to prevent such trade. For instance, the aforementioned Blue Coat sale to Syria, had a proportion going to Burma, which was legal even though, at that time, there were many other trade restrictions placed on Burma. (Department of State, 2012) (Carbone, 2012) The sale to Syria *was illegal*, just because this specific ban is defined negatively, by listing trade articles which are non-restricted—food and medicine. (US Embassy, 2012) **To be effective, any proposal must therefore cover possible re-sale of censorship systems via intermediaries** to states more oppressive than WKAR.

3. POLICY OPTIONS

BLOCK	
+ No possibility of loopholes	- Worsened bilateral relations
+ Positive image of US – selfless act	- Significantly harms Saur-N and the whole US industry
+ Simple future regulation	- Saur-N might simply be replaced by a competitor company
+ Quick implementation	- Does not set up future guidelines

This policy is bold and is not yet matched by Europe, which only passed a non-binding resolution on April 18, 2012 against any oppressive regime trying to purchase censorship systems. (Brown & Korff, 2012) The impact on bilateral relations is hard to estimate, as we cannot know how important this trade is for WKAR. Allegedly, WKAR will be able to conduct its business more efficiently; however, given the nature of the regime and what other countries have done with censorship systems, there are some serious reasons to doubt this. (Wagner, 2012) (OpenNet Initative, 2012) US already restricted

software manufacturers' exports in the past and this sale could potentially enable much more significant abuses. (Ogonowski, 1997)

ALLOW TRADE WITH RESTRICTIONS	
+ The trade can still go through	- Need to deal with intermediaries
+ If we justify the restrictions well, bilateral relations will be preserved	- Can still worsen bilateral relationships, if not justified properly
+ Might establish a sustainable long-term policy	- Some harm to US industry
+ If the deal still goes through, there is no harm to Saur-N and will not be replaced by a European or Chinese competitor. (Rohde, 2011)	- Negative image of US – we allow censorship (some people might misconstrue this as even supporting censorship abroad)

There is a variety of possible restrictions; (Chiang, 2010) however the following seem to be most beneficial:

(1) Companies exporting censorship systems should be obligated to integrate remote kill mechanisms that would allow these companies, if asked by a relevant body, to cease all the systems' censoring
(2) There should be limits on the level of sophistication of censorship systems, as was common with ICT in the past with for instance Content Scrambling System (Seltzer, 2000)
(3) Facilitate information pooling between censorship vendors as to assess the demander's credibility as a final buyer. (Brown & Korff, 2012) Moreover require vendors to track whether the system ends up where it was sold.
(4) Further inspiration in existing US bills (Smith, 2012)

To specify (1): remote termination of censorship will only be carried out if US imposes an arms export ban on the government as well, since that shows that a government is a threat to international security. US can also demand (1) if systems gets re-sold to a different state to which there are export bans; **this effectively solves the intermediary issue.**

4. POLICY RECOMMENDATIONS

In either scenario, there will be indirect costs to US – the industry is still implicitly weakened and Saur-N is required to take on some additional costs. Nevertheless, since we cannot rule out of possibility of WKAR buying censorship only for its business, banning it outright seems excessive as many democratic nations use censorship. (Google, 2012) On the other extreme, trade without any regulation is unacceptable as the political risks are too great.

US should allow this trade with restriction, as the cost-benefit ratio appears to be the best possible. Restriction (1) should not bother WKAR, since it is a problem only if the government is severely violating human rights. As for (2), there is already some precedent and hence this procedure is standard. **Therefore such proposal should remain acceptable to WKAR and is acceptable to the US.**

Bibliography

Arthur, C. (2012, January 27). *Acta protests break out as EU states sign up to treaty*. Retrieved from The Guardian: http://www.guardian.co.uk/technology/2012/jan/27/acta-protests-eu-states-sign-treaty

Brown, I., & Korff, D. (2012). *Digital Freedoms in International Law.* Global Network Initiative.

Carbone, M. (2012, March 17). *Exporting Censorship – US Technology Companies in Repressive Countries*. Retrieved from Future Challenges: http://futurechallenges.org/local/exporting-censorship-us-technology-companies-in-repressive-countries/

Chiang, M. (2010). *A Taxonomy of Internet Censorship and Anti-Censorship.* Princeton.

Department of Justice. (2007, October 11). *Fact Sheet: Major U.S. Export Enforcement Actions in the Past Year*. Retrieved from US Department of Justice: http://www.justice.gov/opa/pr/2007/October/07_nsd_807.html

Department of State. (2012). *Human Rights*. Retrieved from US Department of State: http://www.state.gov/j/drl/hr/index.htm

Department of State. (2012, August 1). *U.S. Relations With Burma*. Retrieved from U.S. Department of State: http://www.state.gov/r/pa/ei/bgn/35910.htm

Google. (2012, November 23). *Government Removal Requests - Google Transparency Report*. Retrieved from Google Inc.: http://www.google.com/transparencyreport/removals/government/

Moskvitch, K. (2012, June 15). *Ethiopia clamps down on Skype and other internet use on Tor*. Retrieved from BBC News: http://www.bbc.co.uk/news/technology-18461292

Ogonowski, M. (1997, August/September). *U.S. Export Policy and the International Distribution of Computer Encryption Technology: The Conflict Between National Security and International Trade.* Retrieved from College of Behavioral and Social Sciences - University of Maryland: http://www.bsos.umd.edu/pgsd/people/staffpubs/Matthew%20Encryption.pdf

OpenNet Initative. (2012). *Internet Filtering (Political)*. Retrieved from OpenNet Initiative: http://map.opennet.net/filtering-pol.html

Poetranto , I. (2012, November 1). *Update on information controls in Ethiopia*. Retrieved from Open Net Initiative: http://opennet.net/blog/2012/11/update-information-controls-ethiopia#8

Rohde, D. (2011, November 17). *China's newest export: Internet censorship*. Retrieved from Reuters: http://blogs.reuters.com/david-rohde/2011/11/17/chinas-newest-export-internet-censorship/

RWB. (2012). *Position paper of Reporters without Borders on the export of European surveillance technology.* Berlin: German section of Reporters without Borders.

Seltzer, W. e. (2000, May 03). *The Openlaw DVD/DeCSS Forum Frequently Asked Questions (FAQ) List*. Retrieved from Berkman Center for Internet & Society at Harvard University: http://cyber.law.harvard.edu/openlaw/DVD/dvd-discuss-faq.html

Shanker, T. (2012, August 26). *U.S. Arms Sales Make Up Most of Global Market*. Retrieved from New York Times: http://www.nytimes.com/2012/08/27/world/middleeast/us-foreign-arms-sales-reach-66-3-billion-in-2011.html

Silver, V., & Elgin, B. (2011, August 22). *Torture in Bahrain Becomes Routine With Help From Nokia Siemens*. Retrieved from Bloomberg News: http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

Smith, C. [.-N. (2012, March 27). *H.R. 3605: Global Online Freedom Act of 2011*. Retrieved from GovTrack.Us : http://www.govtrack.us/congress/bills/112/hr3605

Trindade, A. C. (2008). *Universal Declaration of Human Rights - Main Page*. Retrieved from United Nations: http://untreaty.un.org/cod/avl/ha/udhr/udhr.html

UN. (2012). *Subsidiary Bodies of the United Nations Security Council*. Retrieved from United Nations: http://www.un.org/en/sc/subsidiary/

US Embassy. (2012). *Syria Accountability Act - FAQ | Embassy of the United States Damascus, Syria*. Retrieved from Embassy of the United States Damascus, Syria: http://damascus.usembassy.gov/saa-faq.html

Valentino-Derives, J., Sonne, P., & Malas, N. (2011, October 2011). *U.S. Firm Acknowledges Syria Uses Its Gear to Block Web*. Retrieved from Wall Street Journal: http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

Wagner, B. (2012). *Exporting Censorship and Surveillance Technology.* The Hague: Humanist Institute for Co-operation with Developing Countries (Hivos).

Yang, X. (2003, October 22). *金盾工程前期耗8亿美元 建全国性监视系统*. Retrieved from EpochTimes.Com: http://www.epochtimes.com/gb/3/10/22/n397830p.htm