IRAN HUMAN RIGHTS PROJECT

FOUNDATION FOR DEFENSE OF DEMOCRACIES

Iranian Tools of Oppression and the Companies that Provide Them

July 2011

THE WALL STREET JOURNAL.
WSJ.com

June 22, 2009

Iran's Web Spying Aided by Western Technology

European Gear Used in Vast Effort to Monitor Communications

IRAN HUMAN RIGHTS PROJECT

FOUNDATION FOR DEFENSE OF DEMOCRACIES

Iranian Tools of Oppression and the Companies that Provide Them

Since the fraudulent June 2009 elections, the human rights situation in Iran has continued to deteriorate. Attempting to keep power, the Iranian regime has systematically violated both international law and protections granted by the Iranian constitution. These include:

- Use of public executions
- Rape and sexual violence as a means of coercion
- Religious persecution
- Unlawful arrests and violence towards peaceful protestors
- Censorship of the press
- Communications limits

The Iranian regime utilizes equipment and technology manufactured by international companies. The range of products include riot gear, weapons and communication monitoring technology

While the Iranian regime may be using the equipment and technology for purposes unintended by the manufacturer, it is important for these companies to understand the larger implications of their activities. It is critical that firms perform the necessary due diligence when conducting business deals to insure their products will not be used to violate the rights of innocent civilians and that they are not doing business with the Iranian regime.

The following products and manufacturers provide a glance at the larger international market of equipment and technology that the Iranian regime has accessed or continues to use to violate their citizens' human rights. The information is based on publicly available information.

We invite the companies listed below to share any updated information they have about the use of their products in Iran.

Product: DES-516B Anti-Riot Water Cannon Vehicle
Company: Dalian Eagle Sky
Country: China
Program/Deal:

- Dalian Eagle Sky delivered on undisclosed number of high-tech armored anti-riot vehicles to Iran in later 2009.[1]
- The vehicles, allegedly priced at $650,000 per unit, can be used to douse people with water, tear gas or paint; with a plow, they can demolish barriers or be used more violently to push protestors out of the way.[2]
- It is unclear when Dalian agreed to deliver the equipment to Iran.

Year: Vehicles delivered in 2009
Value of deal: Unknown

Source: Dalian Eagle Sky

Source: Los Angeles Times

Product: STEYR HS .50 Caliber Sniper Rifles
Company: Steyr Mannlicher
Country: Austria
Program/Deal:

- In 2004, the Austrian government approved the sale of Steyr Mannlicher HS .50 caliber rifles to the National Iranian Police Force.[3]
- In 2005, Steyr Mannlicher sold 800 of the rifles for the Iranian police forces to use in anti-drug operations.[4]
- In December 2005, Steyr Mannlicher was sanctioned by the United States under the Iran Nonproliferation Act of 2000. The two-year long sanctions bar American companies from doing business with the sanctioned company.[5]
- Since the rifles were sold to the Iranian National Police force, there is no way to ensure that they will not be used against civilians.

---

[1] "IRAN: Chinese-Made Armored Anti-Riot Trucks, Equipped With Plows, May Arrive in Tehran," *Los Angeles Times*, January 1, 2010. (http://latimesblogs.latimes.com/babylonbeyond/2010/01/iran-protesters-truck-anti-riot-killing-video-runover-ashura-khamenei.html)
[2] "IRAN: Chinese-Made Armored Anti-Riot Trucks, Equipped With Plows, May Arrive in Tehran," *Los Angeles Times*, January 1, 2010. (http://latimesblogs.latimes.com/babylonbeyond/2010/01/iran-protesters-truck-anti-riot-killing-video-runover-ashura-khamenei.html)
[3] John J, Tkacik Jr., "The Arsenal of the Iraq Insurgency: It's Made in China," *The Weekly Standard,* August 13, 2007. (http://www.weeklystandard.com/Content/Public/Articles/000/000/013/956wspet.asp)
[4] Emanuele Ottolenghi, "Iran's Deceptive Commercial Practices," *Begin-Sadat Center for Strategic Studies,* April 15, 2008. (http://www.biu.ac.il/Besa/perspectives41.html)
[5] "Iran Non Proliferation Act of 2000," *United States Department of State,* February 7, 2008. (http://www.state.gov/t/isn/c15234.htm)

Year: 2005
Value of Deal: £8,000,000 EST.[6]

Source: Wikimedia Commons

Product: Motorcycles
Company: KTM Sportmotorcycle AG
Country: Austria
Program/Deal:

- Motorcycles routinely ridden by the Islamic Revolutionary Guard Corps (IRGC) are manufactured by Austrian firm KTM.[7]

Year: Unknown
Value of Deal: Unknown

Source: Fars News Agency

[6] Thomas Harding, "Iraqi Insurgents Using Austrian Rifles from Iran," *Telegraph UK*, February 13, 2007. (http://www.telegraph.co.uk/news/worldnews/1542559/Iraqi-insurgents-using-Austrian-rifles-from-Iran.html)
[7] Emanuele Ottolenghi, "Iran's Deceptive Commercial Practices," *Begin-Sadat Center for Strategic Studies,* April 15, 2008. (http://www.biu.ac.il/Besa/perspectives41.html)

Product: Motorcycles
Company: Honda Motor Company
Country: Japan
Program/Deal:

- Motorcycles routinely ridden by the IRGC are manufactured by Honda.[8]
- Tehran's police force has also been photographed by Iran's Fars News Agency using Honda motorcycle as part of their fleet.[9]
- Honda worked in Iran between 1974 and 2008; the company is completing work on contracts but has no plans to make any future investments in Iran. It has partnered with an Iranian firm, Tizro, to manufacture motorcycles and deliver other equipment to the Islamic Republic but ended the agreement in 2008. While the company continues to the active in Iran, it is not engaging in any new business.[10]

Year: Unknown
Value of Deal: Unknown


Source: Cryptome

Source: Cryptome

[8] Emanuele Ottolenghi, "Iran's Deceptive Commercial Practices," *Begin-Sadat Center for Strategic Studies,* April 15, 2008. (http://www.biu.ac.il/Besa/perspectives41.html)
[9] "Tehran Police Review – Pictorial," *Uskowi on Iran,* March 22, 2011. (http://www.uskowioniran.com/2011/03/tehran-police-review-pictorial.html)
[10] "Profiting from Iran, and the U.S.," *The New York Times,* March 12, 2010. (http://www.nytimes.com/interactive/2010/03/06/world/iran-sanctions.html)

Product: Toyota Land Cruiser
Company: Toyota Motor Corporation
Country: Japan
Program/Deal:

- The IRGC frequently uses Toyota Land Cruisers in their operations, mounting machine guns to the cars. [11]
- Toyota vehicle sales were managed by an independent Iranian company.[12] However, as a result of international pressure, the company announced in August 2010 that it was suspending its automotive exports to Iran.[13]
- Toyota Land Cruisers have been used as police 'Special Unit' transportation.[14]

Year: Unknown
Value of Deal: Unknown

Source: IranMilitaryForum.net

[11] Emanuele Ottolenghi, "Iran's Deceptive Commercial Practices," *Begin-Sadat Center for Strategic Studies,* April 15, 2008. (http://www.biu.ac.il/Besa/perspectives41.html)
[12] "Profiting from Iran, and the U.S.," *The New York Times,* March 22, 2011. (http://www.nytimes.com/interactive/2010/03/06/world/iran-sanctions.html)
[13] Kazahiro Shimamura, "Sanctions Lead Toyota to Halt Iran Exports," *The Wall Street Journal*, August 12, 2010. (http://online.wsj.com/article/SB10001424052748704901104575422601786781766.html)
[14] *Mehr News Iran,* accessed May 2, 2011. (http://www.mehrnews.com/mehr_media/image/2005/10/151882_orig.jpg)

Product: Toyota Hilux
Company: Toyota Motor Corporation
Country: Japan
Program/Deal:

- Published photos show that the IRGC and Basij use Toyota Hilux pick-up trucks, sometimes mounting machine guns to the truck beds.
- Toyota vehicle sales were managed by an independent Iranian company.[15] However, as a result of international pressure, the company announced in August 2010 that it was suspending its automotive exports to Iran.[16]

Year: Unknown
Value of Deal: Unknown

Source: IranMilitaryForum.Net


Source: IranMilitaryForum.Net

[15] "Profiting from Iran, and the U.S.," *The New York Times,* March 22, 2011. (http://www.nytimes.com/interactive/2010/03/06/world/iran-sanctions.html)
[16] Kazahiro Shimamura, "Sanctions Lead Toyota to Halt Iran Exports," *The Wall Street Journal*, August 12, 2010. (http://online.wsj.com/article/SB10001424052748704901104575422601786781766.html)

Cranes

- Numerous publicly available photos provide evidence that cranes, including those made by the manufacturers listed below, have been used for public executions in Iran.
- While it is unclear how Iranian authorities acquired the cranes, companies whose cranes have been used for executions must conduct due diligence to ensure their products are not used for illicit purposes.

Company: Tadano Ltd.
Country: Japan
Program/Deal:

- According to open source photographs, Iran has been using Tadano cranes to perform state-sanctioned executions.[17]
- Tadano uses IER-Iran as its service representative in Iran.[18]
- Tadano Ltd. has an American subsidiary Tadano Mantis Corporation that was acquired in December 2008, according to the company's 2010 Annual Report.[19]
- According to USASpending.gov, Tadano Ltd. has received over $6 million in U.S. federal government grants since 2000.[20]

Year: Unknown
Value of Deal: Unknown

Source: OpenSalon.com

Source: Mardomank.org

[17] "Tadano," *United Against a Nuclear Iran*, accessed May 9, 2011. (http://www.unitedagainstnucleariran.com/cranes#2)
[18] "Worldwide Network," *Tadano Website*, accessed May 9, 2011. (http://www.tadano.co.jp/ihq/service/world/html)
[19] Tadano, "Annual Report 2010," p.2. (http://www.tadano.co.jp/ihq/company/finance/pdf/annual2010.pdf)
[20] "Tadano Ltd.," *USASpending.gov*, accessed May 9, 2011. (http://www.usaspending.gov)

Company: Furukawa UNIC Corporation (UNIC)
Country: Japan
Program/Deal:

- According to its website, Furukawa UNIC Corporation manufacturers truck mounted and mini-crawler cranes. [21]
- According to photographs available on the internet, the Iranian regime has used cranes manufactured by UNIC to perform state-sanctioned executions.[22]

Year: Unknown
Value of Deal: Unknown

Source: Kamangir.net

Source: IranNaz.com

[21] "UNIC Machinery," *Furukawa UNIC Corporation Website*, accessed May 9, 2011. (http://www.furukawakk.co.jp/e/business/unic/)
[22] "UNIC," *United Against a Nuclear Iran*, accessed May 9, 2011. (http://www.unitedagainstnucleariran.com/cranes#3)

Product: Communications Monitoring Equipment
Company: Nokia Siemens Networks (NSN)
Country: Finland
Program/Deal:

- In the aftermath of the fraudulent June 2009 elections, it was clear that the Iranian regime used technology to block communications, monitor and gather information about individuals. The technology used had been sold to Iran by Nokia Siemens Networks in 2008, as part of a larger contract which, included a "monitoring center" that was put into the government's telecom monopoly.[23]
- The technology provided by Nokia Siemens can be used to identify individual cell phone users.[24]
- According to a Nokia Siemens statement made shortly after the elections, "Nokia Siemens Networks has provided Lawful Intercept capability sole for the monitoring of local voice calls in Iran. Nokia Siemens Networks has not provided any deep packet inspection, web censorship or Internet filtering capability to Iran."[25]
- The equipment's provision was confirmed by a Nokia Siemens executive on June 2, 2010, who regretted its use against dissidents. "We delivered mobile networks for MCI and Irancell, the two leading mobile network operators in Iran, over the course of several years… As part of these networks we provided a Lawful Interception capability to both operators, as well as a related monitoring center to MCI."[26]
- In a statement before the European Parliament, an official from Nokia Siemens Networks stated: "Monitoring centers are, in our view, more problematic and have a risk of raising issues related to human rights that we are not adequately suited to address. Our core competency is not working with law enforcement agencies, who are not our typical customers. Those agencies could have an interest in expanding the capability of monitoring centers beyond the standards-based approach of Lawful Interception. Such expansion could include more intrusive practices such as broad network scanning to detect new subjects based on the content of their communications, or filtering of content to block open debate and discussion. While tools to do just that are ready available from multiple sources, we have not and will not provide technology intended for such purposes. As a result, soon after our formation as a company, we made a decision to exit from the monitoring center business, and closed a transaction to divest our remaining assets in March 2009, well before the disputed election in June."[27]
- While NSN says it stopped selling this technology, it had reportedly continued to sell passive interception capabilities, which need instructions – usually accompanied by a police warrant – as to what to intercept and where to send the data.[28]

Year: 2008
Value of deal: Unknown

---

[23] Christopher Rhoads and Loretta Chao, "Iran's Web Spying Aided by Western Technology," *The Wall Street Journal,* June 22, 2009. (http://online.wsj.com/article/SB124562668777335653.html#mod)
[24] Valentina Pop, "Nokia-Siemens Rues Iran Crackdown Role," *Bloomberg,* June 3, 2010. (http://www.businessweek.com/globalbiz/content/jun2010/gb2010063_509207.htm)
[25] Nokia Siemens Networks, Press Statement, "Provision of Lawful Intercept Capability in Iran," June 22, 2009. (http://www.nokiasiemensnetworks.com/news-events/press-room/press-releases/provision-of-lawful-intercept-capability-in-iran)
[26] Barry French, "Hearing on New Information Technologies and Human Rights," European Parliament, Subcommittee on Human Rights, June 2, 2010. (http://www.nokiasiemensnetworks.com/news-events/press-room/statement-to-the-public-hearing-on-new-information-technologies-and-human-rights)
[27] Barry French, "Hearing on New Information Technologies and Human Rights," European Parliament, Subcommittee on Human Rights, June 2, 2010. (http://www.nokiasiemensnetworks.com/news-events/press-room/statement-to-the-public-hearing-on-new-information-technologies-and-human-rights)
[28] Valentina Pop, "Nokia-Siemens Rues Iran Crackdown Role," *Bloomberg,* June 3, 2010. (http://www.businessweek.com/globalbiz/content/jun2010/gb2010063_509207.htm)

SOURCE DOCUMENT

Iraqi Insurgents Using Austrian Rifles from Iran
Thomas Harding
The Telegraph (U.K.)
February 13, 2007
http://www.telegraph.co.uk/news/worldnews/1542559/Iraqi-insurgents-using-Austrian-rifles-from-Iran.html

Austrian sniper rifles that were exported to Iran have been discovered in the hands of Iraqi terrorists, The Daily Telegraph has learned.

More than 100 of the.50 calibre weapons, capable of penetrating body armour, have been discovered by American troops during raids.

The guns were part of a shipment of 800 rifles that the Austrian company, Steyr-Mannlicher, exported legally to Iran last year.

The sale was condemned in Washington and London because officials were worried that the weapons would be used by insurgents against British and American troops.

Within 45 days of the first HS50 Steyr Mannlicher rifles arriving in Iran, an American officer in an armoured vehicle was shot dead by an Iraqi insurgent using the weapon.

Over the last six months American forces have found small caches of the £10,000 rifles but in the last 24 hours a raid in Baghdad brought the total to more than 100, US defence sources reported.

The find is the latest in a series of discoveries that indicate that Teheran is providing support to Iraq's Shia insurgents.

Mahmoud Ahmadinejad, the Iranian president, yesterday denied that Iran had supplied weapons to Iraqi insurgents. But on Sunday US officials in Baghdad displayed a range of weapons they claimed had originated in Iran.

They said 170 American and British soldiers had been killed by such weapons.

The discovery of the sniper rifles will further encourage those in Washington who want to see Iran's uranium-enriching facilities destroyed before a nuclear weapon is produced.

The Foreign Office expressed "serious concerns" over the sale of the rifles last year and Britain protested to the Austrian government.

A Foreign Office spokesman said last night: "Although we did make our worries known the sale unfortunately went ahead and now the potential that these weapons could fall into the wrong hands appears to have happened."

The rifle can pierce all body armour from up to a mile and penetrate armoured Humvee troop carriers.

It is highly accurate and fires a round called an armour piercing incendiary, a bullet that the Iranians manufacture.

The National Iranian Police Organisation bought the rifles allegedly to use them against drug smugglers in an £8 million order placed with Steyr in 2005.

The company was given permission to export them by the Austrian government, which is not a Nato member.

The Arsenal of the Iraq Insurgency: It's Made in China
John J. Tkacik Jr.
The Weekly Standard
August 13, 2007
http://www.weeklystandard.com/print/Content/Public/Articles/000/000/013/956wspet.asp?nopager=1

This year, many truckloads of small arms and explosives direct from Chinese government-owned factories to the Iranian Revolutionary Guards have been transshipped to Iraq and Afghanistan, where they are used against American soldiers and Marines and NATO forces. Since April, according to a knowledgeable Bush administration official, "vast amounts" of Chinese-made large caliber sniper rifles, "millions of rounds" of ammunition, rocket-propelled grenades (RPGs), and "IED [improvised explosive device] components" have been convoyed from Iran into Iraq and to the Taliban in Afghanistan.

Secretary of Defense Robert Gates insists there is "no evidence as yet" that Tehran government officials are involved in shipping weapons to Iraq for use against U.S. forces, a judgment that seems to hinge on the view that the Revolutionary Guards are not part of the "government." But the administration source cautioned, "these are Revolutionary Guards trucks, and although we can't see the mullahs at the wheel, you can bet this is [Tehran] government-sanctioned."

In addition, in early June the Washington Times reported from Kabul that the Pentagon had evidence of new shipments of Chinese shoulder-fired HN-5 antiaircraft missiles reaching Taliban units in Afghanistan's Kandahar province. This shouldn't be surprising. The Pentagon has known since last August that the Iranian Revolutionary Guards had supplied Chinese-made C-802 antiship missiles with advanced antijamming countermeasures to Hezbollah in Lebanon. One slammed into the Israeli destroyer Hanit killing four sailors on July 14, 2006, during the Lebanon war.

The amount of raw intelligence on these Chinese arms shipments to Iran is growing, according to the official, who has seen it. Some items show Iran has made "urgent" requests for "vast amounts" of Chinese-made sniper rifles, apparently exact copies of the Austrian-made Steyr-Mannlicher HS50 which the Vienna government approved for sale to Iran's National Iranian Police Organization in 2004 (ostensibly to help customs officers police Iran's long and sparsely populated mountainous borders). At the time, the United States and Great Britain glowered at the Austrian government and slapped a two-year sales ban on Steyr-Mannlicher. Then in February, as if to confirm the worst suspicions, U.S. troops in Iraq uncovered caches of about 100 of the sniper weapons that looked like the Austrian rifles, the Daily Telegraph reported.

U.S. officials in Baghdad told reporters that at least 170 U.S. and British soldiers had been killed by well-trained and heavily armed snipers. On June 22, for example, an Army specialist was struck by a sniper as he climbed out of his Abrams tank during Operation Bull Run in Al Duraiya. Earlier that morning, the same sniper shot out the tank's thermal sights. He was "probably the most skilled sniper we've seen down here," the soldier's platoon leader told National Public Radio.

But were the Iraqi snipers indeed using Austrian-made armor-piercing .50 caliber weapons?

Perhaps not. There was little official American reaction to the discovery of the sniper rifle cache in February. In March, Steyr-Mannlicher claimed that U.S. authorities had yet to ask it for help in tracing the weapons, a simple matter of checking serial numbers, or even letting Austrian technicians examine the rifles. The Americans never approached the Austrian firearms firm. On March 29, Vienna's Wiener Zeitung quoted U.S. Central Command spokesman Scott Miller as admitting, "No Austrian weapons have been found in Iraq."

Upon hearing this, Steyr-Mannlicher owner Franz Holzschuh noted that the patents on the HS .50 expired "years ago," and they were being counterfeited all over the world. A quick Google search for "sniper rifles" confirms that China South Industries' AMR-2 12.7mm antimateriel rifle is a good replica of the HS .50.

In fact, Iran's Revolutionary Guards had placed large orders for Chinese sniper rifles, among other things. According to the administration official, U.S. intelligence picked up urgent messages from Iranian customers to Chinese arms factories pleading that the shipments were needed "quickly" and specifying that the "serial numbers are to be removed." The Chinese vendors, according to the intelligence, were only too happy to comply. The Chinese also suggested helpfully that the shipments be made directly from China to Iran by cargo aircraft "to minimize the possibility that the shipments will be interdicted."

According to sources who have seen the intel reports, the evidence of China-Iran arms deliveries is overwhelming. This is not a case of ambiguous intelligence. The intelligence points to Chinese government complicity in the Iranian shipments of Chinese small arms to Iraqi insurgents.

Yet top State Department and National Security Council officials prefer to believe that the relationship between Chinese government-owned and operated arms exporters and Iranian terrorists is "unofficial." Therefore, they ought not make too much out of it, lest the Chinese government be unhelpful with the North Koreans. This is the "China exception" at work; it pervades both the intelligence and national security bureaucracies. Moreover, there is a belief in some circles in the administration and on Capitol Hill that Iran's government can be "negotiated" with and therefore the activities of Tehran's Revolutionary Guards must not be seen as reflecting Iranian government policy.

Of course, it is inconceivable that the Iranian Revolutionary Guards send convoys of newly minted Chinese weapons into Iraq and Afghanistan without the clear intention of killing U.S. troops there. And it is equally inconceivable that the Chinese People's Liberation Army facilitates these shipments from its own factories and via its own air bases without the same outcome in mind. If, however, the shipments are occurring against the wishes of Beijing--if the Chinese central government cannot control the behavior of its own army--then the situation is dire indeed: How can anyone expect Beijing to restrain shipments of even more destructive weapons (missiles, submarines, torpedoes, nuclear weapons components) to rogue states? It is a prospect that U.S. officials simply cannot handle.

After leaks of this alarming intelligence surfaced in Bill Gertz's "Inside the Ring" column in the Washington Times, top Pentagon officials began to acknowledge the troubling truth behind them. On July 22, Agence France-Presse quoted the top U.S. military spokesman in Baghdad, Rear Admiral Mark I. Fox, as acknowledging: "There are missiles that are actually manufactured in China that we assess come through Iran" in order to arm groups fighting U.S.-led forces.

Deputy Undersecretary of Defense Richard Lawless told the Financial Times on July 7 that the United States has "become increasingly alarmed that Chinese armor-piercing ammunition has been used by the Taliban in Afghanistan and insurgents in Iraq." The FT quoted one unnamed U.S. official as saying that the United States would like China to "do a better job of policing these sales," as if China actually wanted to "police" its arms exports.

Lawless, revered in the Pentagon as a steely-eyed China skeptic, evinced less agnosticism to the FT, explaining that the country of origin was less important than who was facilitating the transfer. One might wonder why Beijing, as a matter of policy, would sell weapons to Iran for the clear purpose of killing American soldiers. "There is a great shortfall in our understanding of China's intentions," said Lawless of China's overall military policies, and "when you don't know why they are doing it, it is pretty damn threatening. . . . They leave us no choice but to assume the worst."

Why China is "doing it" need not be a mystery. In 2004, Beijing's top America analyst, Wang Jisi, noted, "The facts have proven that it is beneficial for our international environment to have the United States militarily and diplomatically deeply sunk in the Mideast to the extent that it can hardly extricate itself." It is sobering to consider that China's small-arms proliferation behavior since then suggests that this principle is indeed guiding Chinese foreign policy.

Beijing's strategists learned much from their collaboration with Washington during the 1980s, when the two powers prosecuted a successful decade-long campaign to drive the Soviet Union out of Afghanistan. The trick is to avoid a head-to-head confrontation with your adversary while getting insurgents to keep him tied down and taking advantage of his distraction to pursue your interests elsewhere. The cynical difference is that in the Afghan war of the 1980s, the U.S.-supported mujahedeen killed tens of thousands of Soviet troops, while in the early 21st century, Iranian (and Chinese)-supported insurgents in Afghanistan and Iraq are mostly killing Afghans and Iraqis.

The "China exception" notwithstanding, the ease with which Chinese state-owned munitions industries export vast quantities of small arms to violence-prone and war-ravaged areas--from Iraq and Afghanistan to Darfur--leaves no room to doubt that the Chinese government pursues this behavior as a matter of state policy. A regime with $1.3 trillion in foreign exchange reserves cannot claim that it "needs the money" and so turns a blind eye to dangerous exports by its own military. But until the scales fall from the eyes of Washington's diplomats and geopoliticians and they see China's cynical global strategy for what it is, few of the globe's current crises are likely to be resolved in America's--or democracy's--favor.
In particular, U.S. soldiers and Iraqi and Afghan civilians will continue to be killed by Chinese weapons.

John J. Tkacik Jr., a senior fellow at the Heritage Foundation in Washington, D.C., served in Beijing, Guangzhou, Hong Kong, and Taipei in the U.S. Foreign Service.

Iran's Deceptive Commercial Practices
Emanuele Ottolenghi
Begin-Sadat Center for Strategic Studies
April 15, 2008
http://www.biu.ac.il/SOC/besa/perspectives41.html

Executive Summary: Sanctions against Iran focus on nuclear and ballistic missile technology, drawing a distinction between legitimate and illegitimate trade. But a closer look at Iran's commercial practices proves that Iran is systematically abusing its access to Western technology. Technology it is acquiring for civilian projects or for legitimate policing activities is being diverted in order to bolster Iran's Revolutionary Guard Corps and its overwhelming economic role in Iran; and also for the development of Iran's clandestine nuclear activities. In short, Western technology sold to Iran is being utilized in ways that Iran's Western suppliers have never dreamed of, even in their worst nightmares. The current reality is that for a healthy profit and without moral compunctions, Western companies are legally selling Iran tools to repress its own citizens, to bully its neighbors, and to destabilize the entire region.

Iran's Human Rights Violations

In the seven weeks since the UN called for an international moratorium of executions, in late December 2007, Iran hung more than 60 people, frequently in public. Recent pictures, which the Iranian regime has now ordered off the internet to avoid international embarrassment, show convicts hanging from cranes made by such Japanese companies as TADANO, KATO, and UNIC. Many European companies sell similar equipment to Iran. Nor do they necessarily sell these products knowing Iran will turn construction equipment into death machines. Accusing them of complicity is like accusing, say, Volkswagen, of complicity with bank robbers if they happen to drive a VW Golf while escaping the scene of the crime.

Of course, there is nothing illegal about selling cranes and thousands of other products to Iran. But when it comes to Iran, Western companies should know better: they are dealing with masters of deception. Iran has been executing tens of thousands of people, since its 1979 Islamic Revolution, by using cranes. Deal with Tehran and sooner or later your company's logo will experience an embarrassing moment of exposure.

Iran's Systematic Diversion of Technology

Even if deals do not violate either UN sanctions or export controls over dual use technology, Iran is sure to divert perfectly legitimate products for sinister purposes. Legally, there is no complicity with Iran's behavior. But the legality of such transactions only highlights the inefficacy of the current sanctions' regime against Iran and the consequent lightness of the moral burden affecting western companies and their economic self-interest.

Examples abound. Wirth – a German producer of tunnel boring machinery – proudly boasts on its website that "When Barcelona receives a new metro system, a bridge is built over the Orinoco in Venezuela or a new water supply system is created in the Iranian mountains of Isfahan, Wirth machines are used." Indeed they are. The problem is that one of Wirth's project clients in Iran is Sahel Consulting Engineers – a company owned by the Iranian Revolutionary Guard Corps (IRGC). Wirth has so far declined to comment on the matter. BAFA, the German export controls' agency, has confirmed that the machines sold to Sahel are not subject to embargo – a perfectly transparent deal, with all the seals of approval, to be used in a harmless civilian project.

Seli – an Italian company in the same line of business – also provided machinery and technicians for the previous phase of the same tunnel project – which was done through a consortium of which Wirth was a partner. The deal, worth 8.5 million Euro, was completed in 2005. The client was Ghaem, another IRGC subsidiary. The deal was similarly not subject to any restrictions or embargoes. Seli is involved in other important projects in Iran.

Another, much bigger contract is the Kerman Water Tunnel Project, a five-year deal worth 134.6 million Euro signed in 2004 with the active involvement, again, of Sahel Consulting Engineers. Italian and German tunneling equipment was thus sold to the IRGC and made available, once the water tunnel was completed, for other projects the IRGC may wish to undertake. Intelligence reports have repeatedly suggested that much of Iran's clandestine nuclear program is being built deep underground, in bunkers that are accessible through tunnels – tunnels which only technology such as the one provided by Wirth and Seli can build. What guarantee did Western governments have that Wirth and Seli's IRGC clients would not later use their machinery to advance Iran's military ambitions?

Legitimate Business Projects – Illegitimate Business Partners

In other cases, European companies sell advanced technology to IRGC companies for huge infrastructure projects in a no-bid context: Austrian Andritz VA Tech Hydro, Finnish Po?r?, and German KTI-Plersch are all involved in different technical aspects of dam building in Iran – and all list IRGC companies as

their clients. Not all deals involve dual use technology – but by dealing with the IRGC, European companies help them flourish economically. Such examples are not confined to the civilian sector. IRGC units carrying RPG launchers for hit-and-run action routinely ride Japanese Honda and Austrian KTM motorbikes; Iran's military employs Italian-made IVECO trucks as missile launchers; the IRGC uses Mercedes trucks for its transports and mounts machine guns on Toyota Land Cruisers. Not the best flattery, for Western products.

Selling Weapons to Iran – At Our Own Peril

Even when military equipment is supplied to Iran under tight controls, things go wrong. In 2003, Great Britain and Italy supplied night-imaging equipment to Iran's anti-drug units to fight drug smugglers in Iran's eastern provinces, under a United Nations Drug Control Office approved scheme. Israeli troops later found similar equipment inside Hizballah's headquarters in south Lebanon.

In 2005, Austria's arms manufacturer, Steyr-Mannlicher sold Iran 800 .50 caliber sniper rifles to be used by Iran's police drug fighting units in their war against drug smugglers. At the time, the US protested the deal and put sanctions on Steyr-Mannlicher – but the Austrian Minister of Defense called the deal "unimpeachable" and confirmed it. When 108 such guns were found in insurgents' safe houses in Baghdad by American troops, a small media storm ensued, but the Austrians – both company and diplomats – successfully challenged the initial media reports demanding evidence that those were the same weapons.

What eventually transpired was that the media were wrong – the weapons were perfect copies, made in Iran and China. Soon after the delivery, Iran's defense industries engaged in reverse engineering for the sniper rifles and quickly managed to produce its own version – which the IRGC is now busy distributing to insurgents across the Middle East. Once more, Western technology, sold under license and for ostensibly legitimate purposes, abetted Iran's sinister activities, given Iran's systematically fraudulent behavior.

"I Sold Boats, Not Weapons!"

The same happened with the IRGC speedboats involved in the recent naval incident in the Straits of Hormuz – according to diplomatic sources the boats are made in Iran, but frame and design come from Italy's FB Design, a famous producer of racing boats that sold Iran its patrol boat "Levriero" along with frames and blueprints under a now revoked government license. The owner recently protested his innocence in an interview: "I sold boats, not weapons!"

With Iran, unfortunately, there is no such distinction. European and other Western companies sell Iran a variety of sophisticated technological tools which apparently fulfill harmless but profitable deals outside the purview of the UN sanctions' regime. Soon after the merchandise reaches Iran, the regime systematically diverts it from legitimate activities to illegitimate ones. A recent Financial Action Task Force statement encourages its financial institutions to apply "enhanced due diligence" in dealing with Iran, due to its deceptive financial practices. This is because Western credit lines, which may well finance apparently legitimate operations, in fact involve money laundering and the financing of terrorism and Iran's ballistic and nuclear programs.

What the above examples prove is that the principle of enhanced due diligence must now be expanded by Europeans to apply to all trade with Iran. This is true even when Iranian interlocutors appear innocuous and well intentioned, and even when legally speaking there are no impediments to exporting certain products to Iran. The current reality is that for a healthy profit and without moral compunctions, Western

companies are legally selling Iran tools to repress its own citizens, to bully its neighbors, and to destabilize the entire region.

Dr. Emanuele Ottolenghi is the Director of the Transatlantic Institute, a Brussels-based think tank (www.transatlanticinstitute.org). This article is based on Dr. Ottolenghi's lecture at BESA as part of the Annual Leonard Wolinsky Lecture series.

Iran's Web Spying Aided By Western Technology
Christopher Rhoads and Loretta Chao
The Wall Street Journal
June 22, 2009
http://online.wsj.com/article/SB124562668777335653.html#ixzz1IZO7u0j1

The Iranian regime has developed, with the assistance of European telecommunications companies, one of the world's most sophisticated mechanisms for controlling and censoring the Internet, allowing it to examine the content of individual online communications on a massive scale.

Interviews with technology experts in Iran and outside the country say Iranian efforts at monitoring Internet information go well beyond blocking access to Web sites or severing Internet connections.

Warning: This YouTube video contains graphic images. It purports to show a woman dying after being shot in an Iran street protest. The Wall Street Journal has not independently verified its contents.

Instead, in confronting the political turmoil that has consumed the country this past week, the Iranian government appears to be engaging in a practice often called deep packet inspection, which enables authorities to not only block communication but to monitor it to gather information about individuals, as well as alter it for disinformation purposes, according to these experts.

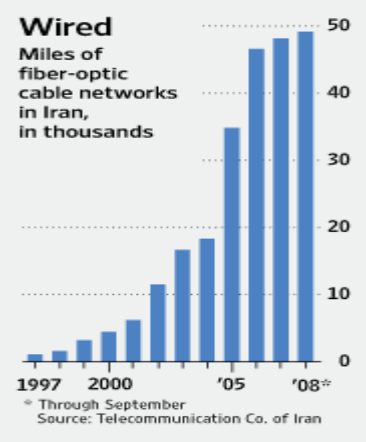
The monitoring capability was provided, at least in part, by a joint venture of Siemens AG, the German conglomerate, and Nokia Corp., the Finnish cellphone company, in the second half of 2008, Ben Roome, a spokesman for the joint venture, confirmed.

The "monitoring center," installed within the government's telecom monopoly, was part of a larger contract with Iran that included mobile-phone networking technology, Mr. Roome said.
"If you sell networks, you also, intrinsically, sell the capability to intercept any communication that runs over them," said Mr. Roome.

The sale of the equipment to Iran by the joint venture, called Nokia Siemens Networks, was previously reported last year by the editor of an Austrian information-technology Web site called Futurezone.

The Iranian government had experimented with the equipment for brief periods in recent months, but it had not been used extensively, and therefore its capabilities weren't fully displayed -- until during the recent unrest, the Internet experts interviewed said.

"We didn't know they could do this much," said a network engineer in Tehran. "Now we know they have powerful things that allow them to do very complex tracking on the network."



Deep packet inspection involves inserting equipment into a flow of online data, from emails and Internet phone calls to images and messages on social-networking sites such as Facebook and Twitter. Every digitized packet of online data is deconstructed, examined for keywords and reconstructed within milliseconds. In Iran's case, this is done for the entire country at a single choke point, according to networking engineers familiar with the country's system. It couldn't be determined whether the equipment from Nokia Siemens Networks is used specifically for deep packet inspection.

All eyes have been on the Internet amid the crisis in Iran, and government attempts to crack down on information. The infiltration of Iranian online traffic could explain why the government has allowed the Internet to continue to function -- and also why it has been running at such slow speeds in the days since the results of the presidential vote spurred unrest.

Users in the country report the Internet having slowed to less than a tenth of normal speeds. Deep packet inspection delays the transmission of online data unless it is offset by a huge increase in processing power, according to Internet experts.

Iran is "now drilling into what the population is trying to say," said Bradley Anstis, director of technical strategy with Marshal8e6 Inc., an Internet security company in Orange, Calif. He and other experts interviewed have examined Internet traffic flows in and out of Iran that show characteristics of content inspection, among other measures. "This looks like a step beyond what any other country is doing, including China."

China's vaunted "Great Firewall," which is widely considered the most advanced and extensive Internet censoring in the world, is believed also to involve deep packet inspection. But China appears to be developing this capability in a more decentralized manner, at the level of its Internet service providers rather than through a single hub, according to experts. That suggests its implementation might not be as uniform as that in Iran, they said, as the arrangement depends on the cooperation of all the service providers.

Checks and Balances

Iran's government is a combination of democracy and Islamic theocracy. Take a look at the power structure.

The difference, at least in part, has to do with scale: China has about 300 million Internet users, the most of any country. Iran, which has an estimated 23 million users, can track all online communication through a single location called the Telecommunication Infrastructure Co., part of the government's telecom monopoly. All of the country's international links run through the company.

Separately, officials from the U.S. embassy in Beijing on Friday met with Chinese officials to express concerns about a new requirement that all PCs sold in the China starting July 1 be installed with Web-filtering software.

If a government wants to control the flow of information across its borders it's no longer enough to block access to Web sites hosted elsewhere. Now, as sharing online images and messages through social-networking sites has become easy and popular, repressive regimes are turning to technologies that allow them to scan such content from their own citizens, message by message.

Human-rights groups have criticized the selling of such equipment to Iran and other regimes considered repressive, because it can be used to crack down on dissent, as evidenced in the Iran crisis. Asked about

selling such equipment to a government like Iran's, Mr. Roome of Nokia Siemens Networks said the company "does have a choice about whether to do business in any country. We believe providing people, wherever they are, with the ability to communicate is preferable to leaving them without the choice to be heard."

Countries with repressive governments aren't the only ones interested in such technology. Britain has a list of blocked sites, and the German government is considering similar measures. In the U.S., the National Security Agency has such capability, which was employed as part of the Bush administration's "Terrorist Surveillance Program." A White House official wouldn't comment on if or how this is being used under the Obama administration.

The Australian government is experimenting with Web-site filtering to protect its youth from online pornography, an undertaking that has triggered criticism that it amounts to government-backed censorship.

Content inspection and filtering technology are already common among corporations, schools and other institutions, as part of efforts to block spam and viruses, as well as to ensure that employees and students comply with computer-use guidelines. Families use filtering on their home computers to protect their children from undesirable sites, such as pornography and gambling.

Internet censoring in Iran was developed with the initial justification of blocking online pornography, among other material considered offensive by the regime, according to those who have studied the country's censoring.

Iran has been grappling with controlling the Internet since its use moved beyond universities and government agencies in the late 1990s. At times, the government has tried to limit the country's vibrant blogosphere -- for instance, requiring bloggers to obtain licenses from the government, a directive that has proved difficult to enforce, according to the OpenNet Initiative, a partnership of universities that study Internet filtering and surveillance. (The partners are Harvard University, the University of Toronto, the University of Cambridge and the University of Oxford.)

Beginning in 2001, the government required Internet service providers to install filtering systems, and also that all international connections link to a single gateway controlled by the country's telecom monopoly, according to an OpenNet study.

Iran has since blocked Internet users in the country from more than five million sites in recent years, according to estimates from the press-freedom group Reporters Without Borders.

In the 2005 presidential election, the government shut down the Internet for hours, blaming it on a cyberattack from abroad, a claim that proved false, according to several Tehran engineers.

Several years ago, research by OpenNet discovered the government using filtering equipment from a U.S. company, Secure Computing Corp. Due to the U.S. trade embargo on Iran, in place since the 1979 Islamic revolution overthrew the U.S.-backed shah, that was illegal. Secure Computing, now owned by McAfee Inc., at the time denied any knowledge of the use of its products in Iran. McAfee said due diligence before the acquisition revealed no contract or support being provided in Iran.

Building online-content inspection on a national scale and coordinated at a single location requires hefty resources, including manpower, processing power and technical expertise, Internet experts said.

Nokia Siemens Networks provided equipment to Iran last year under the internationally recognized concept of "lawful intercept," said Mr. Roome. That relates to intercepting data for the purposes of

combating terrorism, child pornography, drug trafficking and other criminal activities carried out online, a capability that most if not all telecom companies have, he said.

The monitoring center that Nokia Siemens Networks sold to Iran was described in a company brochure as allowing "the monitoring and interception of all types of voice and data communication on all networks." The joint venture exited the business that included the monitoring equipment, what it called "intelligence solutions," at the end of March, by selling it to Perusa Partners Fund 1 LP, a Munich-based investment firm, Mr. Roome said. He said the company determined it was no longer part of its core business.

IRAN: Chinese-Made Armored Anti-Riot Trucks, Equipped with Plows, May Arrive in Tehran
The Los Angeles Times
January 1, 2010
http://latimesblogs.latimes.com/babylonbeyond/2010/01/iran-protesters-truck-anti-riot-killing-video-runover-ashura-khamenei.html

An opposition news website is reporting that Iran has imported high-tech armored anti-riot vehicles equipped with water cannons that can douse people with boiling water or teargas.

The U.S.-based Persian-language news website Rahesabz, or Green Path, posted a photograph of what it described as a photograph of two of the trucks arriving at the Iranian port city of Bandar Abbas in the south.

The website said the vehicles were a rush order from their manufacturers in China, Dalian Eagle-Sky, according to the blogger Sohrebestan.(See a translation of his post in English at the blog Persian2English.)

With an alleged price of $650,000 a unit, the 25-ton trucks each hold 2,640 gallons of water, which can shoot hot or cold water at a distance of up 220 feet.

They can also shoot tear gas, burning chemicals or paint stored in three 26-gallon containers.
It includes a plow, which can presumably demolish makeshift barriers placed on streets by protesters, or even the demonstrators themselves.

Iranian protesters torched police vehicles and motorcycles during anti-government riots last weekend, when police trucks allegedly ran over at least one demonstrator, as shown in the video below.

Iranian officials say the video footage was fake, doctored by the West to make Iran look bad.

Just hours after the cellphone camera photo was posted today, Iranian protest movement supporters began discussing what to do about them if they are employed on city streets.

"I would suggest luring them into narrow streets or between obstacles that are too narrow for them to turn around in, and then trapping them there from the front and behind with cars or barriers of some sort," wrote one commentator who goes by the pseudonym Coyote. "Then come at them from the areas where the cannons cannot point, preferably after the crews have abandoned them, and set them on fire from the inside. Burn their guts."

Another commentator, Dragoon, noted that Shah Mohammad Reza Pahlavi also employed anti-riot vehicles to put down protesters during the months leading up to the 1979 revolution.

Top photo: An amateur picture purportedly shows new anti-riot vehicles arriving in Iran. Credit: Rahesabz. Bottom photo: The 25-ton truck as promoted on the website of its Chinese manufacturer. Video: Police vehicles ram protesters on the streets of Tehran. Credit: YouTube

Fed Contractor, Cell Phone Maker Sold Spy System to Iran
Eli Lake
The Washington Times
April 13, 2010
http://www.washingtontimes.com/news/2009/apr/13/europe39s-telecoms-aid-with-spy-tech/?page=all#pagebreak

Two European companies — a major contractor to the U.S. government and a top cell-phone equipment maker — last year installed an electronic surveillance system for Iran that human rights advocates and intelligence experts say can help Iran target dissidents.

Nokia Siemens Networks (NSN), a joint venture between the Finnish cell-phone giant Nokia and German powerhouse Siemens, delivered what is known as a monitoring center to Irantelecom, Iran's state-owned telephone company.

A spokesman for NSN said the servers were sold for “lawful intercept functionality,” a technical term used by the cell-phone industry to refer to law enforcement's ability to tap phones, read e-mails and surveil electronic data on communications networks.

In Iran, a country that frequently jails dissidents and where regime opponents rely heavily on Web-based communication with the outside world, a monitoring center that can archive these intercepts could

provide a valuable tool to intensify repression.

Lily Mazaheri, a human rights and immigration lawyer who represents high-profile Iranian dissidents, said she had suspected that the government had increased its capability to monitor its perceived enemies.

Recently, one of her clients was arrested because of instant messaging he had participated in with Ms. Mazaheri, she said. “He told me he had received a call from the Ministry of Intelligence, and this guy when he went to the interrogation, they put in front of him printed copies of his chats with me. He said he was dumbfounded, and he was sent to prison.”

The sale also highlights a rift between the government of Germany, which has endorsed diplomatic and economic pressure on Iran to curb its nuclear program, and German corporations that continue to export sensitive technology to Iran. On March 31, NSN sold the portion of its business that services the monitoring center to a private German holding company called Perusa Partners Fund LLP.

Since 2005, Siemens had done more than $900 million worth of business with the U.S. government and employs about 70,000 people in the United States. Nokia is one of the leading mobile handset providers in the United States.

A spokeswoman for Siemens AG, Elizabeth Cho, said that Siemens “retains only a non-controlling financial interest in NSN, with the day-to-day operations residing with Nokia.” She added that Siemens has been “exiting out of the telecom business” throughout the last five years.
Promotional literature says the monitoring center's “modular architecture allows the monitoring and interception of all types of voice and data communication in all networks, i.e. fixed, mobile, Next Generation Network (NGN) and the Internet. The MC's [monitoring center's] unified view-concept greatly facilitates investigative work and opens completely new and efficient ways to pursue leads.”

Ben Roome, a spokesman for NSN, said, “We provide these systems to be used under the applicable laws in their countries and make sure we are abiding by U.N. and [European Union] export regulations and code of conduct. We provided the monitoring center to Irantelecom. We are not going to comment on the use of it. It is there to record lawful intercepts.”

But William Daly, a former CIA signal-intelligence officer for the agency's Office of Science and Technology who retired in 2000, said the monitoring center in Iran will be used to “monitor dissidents and those ayatollahs who oppose the Supreme Leader [Ayatollah Ali Khamenei].”

Mr. Daly, who provided technical assistance on surveillance missions for the CIA, said that lawful intercept as a concept was created by the cell-phone industry to provide law enforcement agencies the ability to track criminals and terrorists.

Indeed, the telecommunications industry's own international standards require that data networks allow law enforcement to intercept phone calls, e-mails and other electronic data.

“This functionality is offered by all major mobile and fixed network system vendors,” Mr. Roome said. “Such functionality can provide the proper authorities with an important tool for the investigation of serious criminal activities, such as terrorism, child pornography or drug trafficking. The use of such surveillance is based on local legislation and typically overseen by high-level independent government bodies, such as courts.”

Mr. Daly said, however, that the technical switches telecommunications companies embed in their systems can easily be abused.

“The concept of 'lawful intercept' came about with the development of cellular phones,” he said. “They had no way of monitoring them if it did not go through a landline switch. With [Global System for Mobile communications, or GSM], it is possible to communicate in the cell without going to the switch. This was part of the basic argument for why they developed it. But the real answer is that governments want to know what their people are doing.”

Tom Malinowski, Washington advocacy director for Human Rights Watch, said the monitoring center NSN sold to Iran last year should be regulated as though it were “dual-use technology” - items that can have military as well as civilian applications.

“There are a lot of export controls in place in Western countries on technology that might have a dual military purpose,” he said. “But there are virtually no restrictions on the export of high-tech equipment that can be used to monitor or control free expression.” When Cisco Systems Inc., an American company, sold China technology to facilitate the state's ability to monitor the Web searches of its citizens, the Commerce Department had to review the export license to make sure Beijing was not obtaining technology it could use to repress Chinese citizens - a requirement for all U.S. exports to China following the 1989 crackdown at Tiananmen Square.

Mr. Roome said he did not consider the Iranian monitoring center to be dual-use technology. Indeed, NSN also provides telecommunications equipment to support the wireless telephone network used by Iranian citizens inside the country, he said.

“We believe that the connectivity we provide brings important benefits to societies through enabling the open sharing of information and enhancing economic prosperity,” he said. “We are concerned about human rights and the well-being of people across the globe and have therefore created very detailed ethical guidelines and code of conduct for our operations. These guidelines apply to our own operations and those of our business partners.

“We also recognize the legitimate authority of political decision makers in the global community to determine whether it is appropriate or not to do business in any particular country. We are strongly committed to the highest standards of ethical conduct, and operate in full compliance with all applicable national and international laws.”

The Iranian mission to the United Nations did not reply to requests for comment on the issue.
Iranian dissidents reacted with anger to the news about the sale.

Mohsen Sazegara, a founder of Iran's Revolutionary Guards who became a democracy advocate and was arrested in 2003 for his opposition to the Islamic republic, said there were rumors in Iranian opposition circles that the Germans had sold the state powerful new technology that would make their monitoring efforts more effective.

“My first reaction is, 'Wow! Why do they do this?' Don't they know that this will be used against the people of Iran?” said Mr. Sazegara, who now lives in the United States.

“They facilitate a regime which easily violates human rights in Iran and the privacy of the people of Iran. They have facilitated the regime with a high technology that allows them to monitor every student activist, every women's rights activist, every labor activist and every ordinary person.”

Hadi Ghaemi, spokesman for the International Campaign for Human Rights in Iran, said 12 women´s rights activists were arrested late last month at a private meeting to celebrate the Persian New Year. He said the raid suggested the state had access to private communications.

"This is an absolute threat to the privacy of all Iranian activists. It puts them in danger of being constantly monitored by the intelligence services, something that we know is already happening," Mr. Ghaemi said.

Hearing on New Information Technologies and Human Rights
Barry French
European Parliament, Subcommittee on Human Rights
June 2, 2010
http://www.nokiasiemensnetworks.com/news-events/press-room/statement-to-the-public-hearing-on-new-information-technologies-and-human-rights

Introduction

Thank you for inviting me here today. My name is Barry French, and I am a member of the Executive Board at Nokia Siemens Networks, responsible for corporate affairs.

I was asked to talk today about the experience of Nokia Siemens Networks related to Iran and the reported use of telecommunications technology in that country to suppress human rights.

I will do that, but will also try to make some broader points about the underlying issues and lessons related to our experience. I would also note that that we have provided a longer statement to be included in the written record, as these are complex issues difficult to fully address in short remarks.

Iran Background

First, let me start with our experience related to Iran.

In 2009, media reports drew attention to the delivery of "surveillance technology" by Nokia Siemens Networks to Iran. The facts are that we delivered mobile networks for MCI and Irancell, the two leading mobile network operators in Iran, over the course of several years.

Our deliveries contributed roughly one third of the deployed capacity of those operators, with other vendors providing the remaining two thirds. We provided GSM voice network technology to MCI, and GSM voice and GPRS mobile data network technology to Irancell. As part of these networks we provided a Lawful Interception capability to both operators, as well as a related monitoring center to MCI.

LI and Monitoring Centers

Let me provide some background on each of these systems.

Lawful Interception – or LI – is the name given to an internationally agreed approach for law enforcement authorities to intercept communications running over networks within their jurisdiction. It is a principle noted in the constitution of the International Telecommunications Union; addressed in several resolutions of the Council of the European Union; and firmly embedded in transparent technical standards, including those set out by the European Telecommunications Standards Institute (ETSI) and the 3GPP (3rd Generation Partnership Project).

Today, governments in almost all nations require operators to deploy Lawful Interception as a condition of their license to operate. As a result, LI is present in almost every telecommunications network in the world, including those that are being used by probably everyone in this room today. And, for good

reason: to support law enforcement in combating things like child pornography, drug trafficking and terrorism.

Lawful Interception capability is passive in the sense that it needs to receive instructions on what to intercept and where to send intercepted information. A system typically known as a monitoring center is the active tool that provides those instructions and then receives, records and orders the intercepted communications. For all practical purposes, for the lawful interception capability in a network to be useful, it must have some form of monitoring center.

Nokia Siemens Networks Perspective

Despite the fact that both the passive and active components of LI are needed to implement a right expressly acknowledged by the International Telecommunications Union – the right of member states of the United Nations, including Iran, to intercept communication in enforcement of their national laws—our company views those two components very differently. These different perspectives are based on our core competency and focus as a company; on the existence of well-defined and understood standards; and on our view of the potential risk to human rights related to each.

Our core competency is working with telecommunication operators, and providing network-focused products and services. The passive element of Lawful Interception is closely linked to the network; is a legal requirement for our customers to deploy; and is based on clear standards and a transparent foundation in law and practice.

This standards-based approach provides some safeguards over bespoke mechanisms, such as the ability to only intercept communications from pre-determined targets. LI follows a strict sequence that first requires identification of a subject, presumably based on appropriate legal procedures, and then restricts the interception of communication only to these individuals, but not from others.

Monitoring centers are, in our view, more problematic and have a risk of raising issues related to human rights that we are not adequately suited to address. Our core competency is not working with law enforcement agencies, who are not our typical customers. Those agencies could have an interest in expanding the capability of monitoring centers beyond the standards-based approach of Lawful Interception.

Such expansion could include more intrusive practices such as broad network scanning to detect new subjects based on the content of their communications, or filtering of content to block open debate and discussion. While tools to do just that are readily available from multiple sources, we have not and will not provide technology intended for such purposes.

As a result, soon after our formation as a company, we made a decision to exit from the monitoring center business, and closed a transaction to divest our remaining assets in March 2009, well before the disputed election in June. The monitoring center was provided to Iran in 2008 while the divestiture process was underway. While we do not intend to enter this business again, we will continue to provide standard Lawful Interception capability within the networks we build.

While we halted all work related to monitoring centers in Iran in 2009, including service and support, we believe that we should have understood the issues in Iran better in advance and addressed them more proactively. There have been credible reports from Iran that telecommunications monitoring has been used as a tool to suppress dissent and freedom of speech. We deplore such use of a technology that can bring so many positive benefits to society – and that, in fact, we believe has brought so many positive benefits to Iran.

While we cannot reinvent history, we can ensure we do better in the future. To help do this, we are in the process of assessing our policies and processes, as well as engaging with important stakeholders such as the people in this room today for input and feedback. Our target is to have our core policies in this area reviewed and approved by our full Executive Board by the end of July.

While it is premature to share those policies in any depth today, they will be shaped by some fundamental beliefs, including:

1. A belief in the principles and values of The Universal Declaration of Human Rights, including freedom of speech and assembly. These are embedded in our Code of Conduct and in our thinking as a company.
2. A belief that communication networks support human rights through enabling free expression, access to information, exchange of ideas and economic development.
3. A belief that Nokia Siemens Networks has a responsibility to help ensure that the communications technologies we provide are used to support, and not infringe, human rights.
4. A belief that the misuse of communication technologies to infringe human rights is wrong and, ultimately, that those who do so must be accountable for their actions.
5. A belief that given the pace of technical innovation and widespread availability of communication technology, addressing the issues being raised in this forum requires a political and industry consensus, and not just a technical solution.

Inherent Tensions

As we work to go from these beliefs to specific policies, it is clear that there are inherent tensions related to the issues being addressed here that will not be easy to resolve.

Consider the fact that the systems that we provided to Iran were designed to implement a right that the ITU has explicitly said is held by member states, and are required by law in the vast majority of those member states. Yet, when we help to meet those requirements, we are subject to considerable criticism, including in the European Parliament resolution on Iran of 10 February 2010.

Of course, there are other underlying conflicts as well, several of which I believe are appropriate to raise here.

The first is the conflict between appropriate and inappropriate content filtering. Content filtering is not directly related to lawful interception, but is an area of our business where we believe there is some risk of abuse.

While it is easy to say that there should be no filtering of any kind, we do not believe that would be a wise policy. The fact is that filtering technology is deployed in many, many countries, by many, many operators, for very legitimate purposes, such as the removal of spam text messages and pornography of various kinds, and the identification of software viruses and malware.

On the other hand, there is filtering that we believe is inappropriate and would be inconsistent with widely accepted human rights. While this is not something that has ever been requested from us as a company, and not a capability we would agree to provide, it is not inconceivable that filtering could be used for purposes such as blocking messages designed to coordinate the assembly of people in order to engage in legitimate political discourse.

The second conflict is between local law and human rights such as those defined by the Universal Declaration of Human Rights, including freedom of speech and assembly. Again, it is certainly not inconceivable that local law could be inconsistent with those rights, and it is not always easy to bridge this gap. We believe that there is a broad consensus that telecommunications technology and the sharing of ideas and information that it enables, is a tool for social good. Thus, we do not believe that an "absolutist" policy entailing steps such as a full market exit in the face of evidence of human rights infringements would be a wise approach.

Our belief is that each circumstance needs to be looked at in a way that on balance provides the best outcome for human rights. That requires a nuanced view of each situation; an ability to assess what technology is best sold to what customers in what countries; and the flexibility to find creative ways to mitigate the risk of harm. Our draft policies, and indeed the processes we have in place already, seek to avoid black and white declarations, focus on intent, and give room for management review, debate and discussion.

There is an additional conflict rooted in the fact that the human rights environment that exists in any particular country can change dramatically during the lifespan of the networks we provide. We are always at risk of finding that we have deployed technology that seemed appropriate for use by one government only to find it misused by the next.

Conclusion

I hope I have been able to provide a greater understanding of the role we played in Iran, as well as some sense of the complexity of the issues at stake here. Ultimately, we believe that we have a responsibility to assess what technology is sold where and, on balance, make decisions that are in the best interests of human rights.

At the same time, we believe that there should be no doubt where ultimate accountability rests.

We provide technology that is intended to be used in ways that support human rights. When that technology is misused, the accountability must sit with those who misuse it.

We also need your help to address some of the underlying conflicts that give rise to a situation where we are criticized for providing technology that is designed to meet requirements specified by organizations such as the European Union.

I am optimistic that we can work together in good faith to make real progress on these difficult issues.

Thank you very much.

Nokia-Siemens Rues Iran Crackdown Role
Valentina Pop
Bloomberg
June 3, 2010
http://www.businessweek.com/globalbiz/content/jun2010/gb2010063_509207.htm

Nokia-Siemens Networks on Wednesday (2 June) admitted its share of the blame for Iran's brutal crackdown on anti-government demonstrators last year after selling mobile phone surveillance to the authoritarian regime.

"We absolutely do find ourselves in a tricky situation and need the help of people in this room to help us navigate in these challenging times," Barry French, head of marketing and corporate affairs with Nokia-Siemens Networks, a joint venture of Nokia (NOK) and Siemens (SI), told MEPs during a hearing on human rights and new information technologies.

The Finnish-German telecoms joint venture was at the centre of an ethics controversy last year when it emerged that it had supplied surveillance technology to two Iranian mobile phone operators. The technology was used to track down dissidents amid the mass protests following the contested re-election of President Mahmoud Ahmadinejad in June 2009.

Apart from the crackdown on demonstrators, which saw 36 confirmed deaths, Iranian authorities blocked websites such as Twitter and Facebook, jammed and tracked cell phone calls and text messages. They used the so-called monitoring centre acquired from Nokia-Siemens in 2008 to carry out the work.

Mr. French maintained that the surveillance technology was part of the legal requirements imposed by governments all over the world, including in the EU and US for mobile phone operators to get a licence.

"We deplore the use of this technology against dissidents," he said, adding that his company has learned its "lesson" and has meanwhile pulled out of the "monitoring centre business."
Nokia-Siemens Networks is however still selling "passive" interception capabilities, which need "instructions" – usually accompanied by a police warrant – as to what to intercept and where to send the data.

Mr. French said that this technology helps police and prosecutors track down criminals and terrorists around the world and that there are international standards requiring such capabilities.

But he agreed to the need for establishing codes of conduct for European companies when dealing with repressive regimes.

Reporters Without Borders, an international organisation advocating freedom of speech, stressed the role of the EU in preventing human rights infringements facilitated by European companies.

"The EU needs to encourage European companies to sit down and carve out a voluntary code of conduct when dealing with repressive regimes," the group's Lucie Morillon said during the parliamentary hearing.

She pointed to the US, where Congress has recently passed the "Global Freedom Act," preventing companies from collaborating with regimes engaging in censorship and human rights violations.
If the EU adopted something similar, it would also make it easier for European companies to resist pressure from hostile regimes to engage in such practices, she argued.

"EU diplomats should also press more to eliminate Internet censorship, they should visit jailed 'netizens' and bilateral agreements should not only look at human rights in general, but also at internet rights," she added.

Rolf Timans, head of the human rights and democratisation unit in the European Commission, rejected the idea of legal restrictions for EU companies.

But he welcomed the idea of "corporate voluntary agreements" and common guidelines for European companies when dealing with these "tricky issues."

Sanctions Lead Toyota to Halt Iran Exports
Kazuhiro Shimamura
The Wall Street Journal
August 12, 2010
http://online.wsj.com/article/SB10001424052748704901104575422601786781766.html

TOKYO—Bowing to growing international pressure over Iran's nuclear-development program, Toyota Motor Corp. said Wednesday that it suspended car exports to the Middle Eastern nation.

"In light of the current situation" exports have been halted, a spokeswoman for the Japanese auto maker said. Toyota shipped about 220 cars to Iran so far this year until the suspension took effect in June.

Toyota's exports to Iran are few when compared with the 7.38 million vehicles that the company aims to sell world-wide during the current fiscal year.

Still, the move could help the world's largest car maker sidestep tarnishing its image even further in the U.S., which has been putting pressure on Japan to limit its business transactions with Iran. The U.S. continues to be Toyota's biggest market even after a massive vehicle recall earlier this year seriously dented the company's sales.

Toyota has exported its cars to Iran for years, mainly sport-utility vehicles for general consumers, through the affiliated trading firm Toyota Tsusho Corp. It shipped about 250 vehicles in 2009 and 4,000 vehicles in 2008.

In June, the United Nations Security Council imposed a fourth round of sanctions against Iran, with the U.S. and the European Union implementing their own sanctions to sever corporate ties in the financial and resources sectors.

U.S. sanctions penalize foreign companies exporting banned materials and technologies to Iran by limiting their financial transactions and business activities in the U.S.

Other Japanese manufacturers have also become cautious about exporting their products to Iran. Nippon Steel Corp., Japan's largest steelmaker by output, said it consults Japanese government officials first to make sure that their products won't raise security concerns.

The steelmaker's shipments to Iran may decline in the future, a company official said. Nippon Steel doesn't disclose the amount it ships to the country.

U.S. researchers have named oil-and-gas producer Inpex Corp. and units of Japan's three largest banks—Mitsubishi UFJ Financial Group Inc., Sumitomo Mitsui Financial Group Inc. and Mizuho Financial Group Inc.—as engaging in business that could possibly run afoul of the U.S. sanctions.

Inpex initially owned a 75% stake in the Azadegan oil field in southwestern Iran and was set to be the operator of the field, but the National Iranian Oil Co. took over the bulk of the project's shareholding and operations in 2006 as the U.S. stepped up pressure on its allies to curb business ties with Iran.

While some other manufacturers could be forced into shrinking their remaining businesses with Iran, trading and resources companies say they currently don't have plans to change their operations.

Japan supported the U.N. sanctions, but Japan and Iran, one of the Asian nation's major oil suppliers, maintain relatively friendly ties.