Droits et Démocratie
Rights & Democracy

Centre international des droits de la personne et du développement démocratique
International Centre for Human Rights and Democratic Development

Human Rights at Risk on the Cyber-battlefield:
The Sale of Security & Surveillance Technology to China

"The cyber-battlefield is real. It`s a place where computers are used instead of guns, data packets instead of bullets, and firewalls are used instead of barbed wire." [1]

In collaboration with the Chinese Ministry for Public Security, Canada`s National Research Council (NRC) and the Canadian Police Research Centre sponsored a recent trade mission to China to explore China's growing demand for advanced surveillance technology and identify business opportunities related to security needs in the lead up to the Beijing Olympics to take place in the summer of 2008[2].

The trade mission was just one part of a wider initiative to promote Canadian security and surveillance technology in the People's Republic of China. The Canadian Advanced Technology Alliance (CATA) recently announced the signing of a memorandum of understanding in collaboration with the NRC, the Canadian Police Research Centre and the Chinese Ministry of Public Security outlining a range of strategies to promote business partnerships in the hi-tech sector including the identification of opportunities to supply Canadian advanced technology and services to China`s Golden Shield Project.

China's Golden Shield project, described by CATA as "modernizing public safety and justice networks in China"[3] is an all-encompassing surveillance network – a gigantic online database - incorporating speech and face recognition, closed-circuit television, smart cards, credit records and Internet surveillance. It has been described by the Government of China as a means of strengthening central police control and improving efficiency and it was the subject of a major study by Rights & Democracy in 2001.[4]

Other initiatives announced by CATA included corporate participation within the Canadian Pavillion of the China Hi-Tech Fair held in Shenzhen earlier this month and organization of the Canadian Pavillion within the PT Expo Comm 2004 Trade Show in Beijing from October 26-30, 2004. All of these initiatives have been undertaken with the participation of the Canadian Embassy and its trade promotion offices in China.

What is Surveillance Technology?

---

[1] Richard Tracy, *Cybercrime… Cyberterrorism… Cyberwarfare…Averting an Electronic Waterloo,* November 1998, Center for Strategic and International Studies. As quoted on the Canadian Security and Intelligence Service (CSIS) website, http://www.csis.gc.ca/eng/operat/io2_e.html

[2] Canadian Embassy news release, September 17, 2004, http://www.beijing.gc.ca/beijing/en/1376.htm

[3] CATA press release : August 18, 2004, http://www.cata.ca

[4] See *China's Golden Shield : Corporations and the Development of Surveillance Technology in the People's Republic of China*, Greg Walton, Rights & Democracy, 2001, http://publications.gc.ca/collections/Collection/E84-7-2001E.pdf

Protecting athletes and fans during an event such as the Olympic games has become a daunting and expensive affair – especially since the terrorist attacks on the World Trade Center in 2001. In ensuring that national security is protected during such high-profile events, governments are turning increasingly towards security and surveillance technologies that are often derived from hi-tech military research programs originally designed to track the movements of troops on the battlefield. These surveillance and "C4I" technologies (command, control, communication, computers and intelligence) cover a wide range of components, sub-systems, products and software. They are used by military, law enforcement, emergency services, commercial and private organizations. While the term C4I generally refers to military and police systems, civilian systems are more commonly referred to as ICT (Information & Communication Technologies). However, most civilian communications have surveillance and control facilities that mirror and are derived from military applications.

Surveillance systems can range from closed circuit television surveillance, to local, regional or national traffic control and to global systems for the monitoring of telephone, internet and fax communication. Such systems have legitimate military, police and civilian uses but they also have inherent capabilities that facilitate human rights violations when unfettered by the checks and balances taken for granted in most democratic states. In the new millennium, it is this state of the art technology and communications equipment that enables the security apparatus of a single-party state to identify and arrest human rights defenders, pro-democracy campaigners, trade union organizers and political dissidents.

Digital Alchemy – the Art of Systems Integration

Modern military, security and police organizations rely upon sensors to yield intelligence, surveillance and reconnaissance (ISR) and they use networks to integrate and share the information that is gathered. Once the sensors and networks are integrated, they collectively comprise what William Owens, CEO of Nortel, has called a "System of Systems".[5] The technology transfer that the Government of China is most actively seeking from Canada is precisely this - sensors, networks and the ability to integrate them.

Sensors and networks are the key components for both modern day security systems and modern day warfare. While they are not in and of themselves "weapons", integrated sensors and networks combined with real time operational intelligence are. Herein lies their dual-use nature. They are the key to military, security and police modernisation in

[5] see *The Emerging U.S. System-of-Systems*, Admiral William A. Owens, Vice Chairman, Joint Chiefs of Staff, conclusion: http://www.ndu.edu/inss/strforum/SF_63/forum63.html

China today and exactly the type of technology being offered by Canadian companies participating in the recent trade mission and series of trade fairs mentioned above.

Of course, being able to buy the components that make up such a "system of systems" is not the same as being able to put them together. North American capabilities in the field of systems integration are unmatched, but developing countries such as China and India have huge pools of technical talent and technically trained workers fully able to meet the challenge. With the transfer of technology through trade or technical assistance programs and through reverse engineering initiatives, soon anyone with enough patience will be able to master the skills required to transform neutral technology into a system that hears, sees and thinks for the government that controls it.

Even without existing technical expertise, any country with enough money could simply purchase a surveillance network as Greece did for the Athens Olympics. It obtained a $300 million fully-integrated security system managed entirely by the US-based Science Applications International Corporation's (SAIC) with its unrivalled experience with integration of military technologies. The 633 member Chinese delegation that was in Athens included a contingent from the Ministry of Public Security to assess the performance of SAIC's C4I system.

Bidding for security and surveillance contracts at the Beijing Olympics will pit US, European and Canadian hi-tech sectors against each other. The leading contenders are a SAIC-led consortium and an EADS-led consortium,[6] including Canada's Nortel Networks for all C4I telecommunications. Canadian companies may, in fact, have a significant edge. In the MOU it signed with CATA and the NRC, the Government of China has "agreed to give CATA advance information on all procurements related to the modernization of the 2008 Beijing Olympic Games."[7]

The Government of China is clearly aware of the opportunity provided by the Olympic games to concurrently position itself as a central player in the military, security and police industry. Between 2001 and 2004, the Ministry of Science and Technology allocated $2.4 billion in grants to promote research related to commercial products with military, security and police applications. This was twice the total amount provided during the previous 15 years. The research being funded is reportedly directed towards

---

[6] SAIC is reportedly the largest recipient of contracts from the National Security Agency (NSA) and one of the top five contractors to the Central Intelligence Agency (CIA).
Source: http://www.corpwatch.org/article.php?id=9508 .
EADS (European Aeronautic Defence & Space Company) is the largest aerospace company in Europe and is active in the area of surveillance technology. EADS C4I systems are based around Nortel Networks IP switching and optical transmission products. Source: http://www.eads-telecom.com/france/1058/1994/2042/2058/6669.asp

[7] CATA press release, September 9, 2004. http://www.cata-china.org

cutting-edge fields, with priority areas being wireless networks, semiconductor design and new materials.[8]

Safeguards and the issue of complicity

"Those who cause 'especially serious harm' by providing 'state secrets' to overseas organizations and individuals over the Internet may be sentenced to death."[9]

Surveillance technologies and software have developed at such a rapid pace that they have outpaced developments in export controls. In many cases politicians, policy makers and human rights organizations lack the technical expertise to adequately assess the impact that such technology could have when it is exported to repressive regimes that have little regard for the rule of law or the protection of human rights. In fact, multilateral trade and investment liberalization has itself reduced the interest and capacity of states to distinguish between recipient countries when exporting dual-use technology.

The Canadian Security and Intelligence Service (CSIS) has acknowledged that ICT is a double-edged sword. As an example, it refers to a group of tech-savvie activists in Canada who made use of highly sophisticated information technology systems to actually shut down a Chinese communications satellite.[10] In addition, CSIS points out that communications technology has been used by foreign governments for espionage purposes here in Canada (particularly economic espionage). However, there is no acknowledgement that technology developed in Canada and promoted internationally by the Government of Canada might be misused by to violate the human rights in the importing country.

For its part, CATA vows to promote privacy protection especially in relation to the biometric industry. It states on its website that "In addition to promoting solutions that emphasize physical safety, CATA Biometrics Group is also focused on tackling policy and guidelines to ensure protection of privacy and the integrity of personal data".[11] How CATA will accomplish this objective in a country such as China is unclear. What is clear is that the right to privacy is binding on those states, such as Canada, that have ratified the *International Covenant on Civil and Political Rights* (ICCPR*)* and it is government regulation that is required to ensure those basic human rights standards are protected.[12]

While the actual legal nature of extraterritorial human rights obligations is still a debate within UN circles, many would argue that in promoting the sale of dual-use technology to

---

[8] Charles Hutzler, Wall Street Journal, (Eastern edition), N.Y, Jul 16, 2004. pg. A.1
[9] China Supreme People's Court ruling, January 21, 2001
[10] CSIS briefing note *Information Operations (the cyber threat)*. http://www.csis-scrs.gc.ca
[11] CATA Biometrics Group mandate as quoted from its website, http://www1.cata.ca/biometrics
[12] China has signed, but not ratified, the ICCPR. As a signatory it is required not to undermine the spirit or intent of the treaty.

non-democratic states, both the Government of Canada and the corporations that will profit directly from the eventual sales, have at least a moral obligation to develop official safeguard policies or human rights screening mechanisms. While human rights impact assessments are already a topic of serious study among European governments, there has been little interest in Canada and existing mechanisms, already weak, have not kept pace with innovations in security technology.

Currently, Foreign Affairs Canada (FAC) maintains a Military and Technology Export Control List that includes what it terms "dual-use" categories such as electronics, telecommunications, information security, sensors and lasers. However, within these categories, there are interesting exceptions. For example, systems and modules or integrated circuits for information security are exempted from the dual-use category. Moreover, government controls do not extend to personalized "smart cards" for which use is restricted to the exempted categories. If personalized smart cards have multiple functions then the control status of each function is assessed individually.[13] Under such rules, Canada could find itself meeting the requirements of its Export Control List, but still be at risk of undermining human rights principles when it sells state-of-the-art surveillance and security technology in China or in other authoritarian states.

To address some of these concerns, Canada could look towards the Wassenaar Arrangement for Export Controls for Conventional Arms and Dual Use Weapons and Technologies of which it is a member.[14] The Arrangement sets out a "community regime for the control of exports of dual-use items and technology" but more importantly it provides a forum for states that develop and export dual-use technology. That forum meets regularly to update its guidelines in accordance with recent innovations.

Efforts within the European Union might also provide ideas for a more effective Canadian safeguard procedure. The EU adopted a Code of Conduct for Arms Exports in 1998 which makes special reference to human rights concerns. According to Criterion 2 of the Code, States will,

> "exercise special caution and vigilance in issuing licences, on a case-by-case basis and taking account of the nature of the equipment, to countries where serious violations of human rights have been established by the competent bodies of the UN, the Council of Europe or by the EU... For these purposes, equipment which might be used for internal repression will include, inter alia, equipment where there is evidence of the use of this or similar equipment for internal repression by the proposed end-user, or where there is reason to believe that the equipment will be diverted from its stated end-use or end-user and used for internal repression… the

[13] See http://www.dfait-maeci.gc.ca/trade/eicb/military/gr1150-en.asp?#category1150
[14] Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom & United States.

> nature of the equipment will be considered carefully, particularly if it is intended for internal security purposes."[15]

The EU Code goes on to define internal repression making specific reference to international human rights instruments including the Universal Declaration on Human Rights and the ICCPR.

The Organisation for Security and Co-operation in Europe's Document on Small Arms and Light Weapons also makes reference to human rights and requires states to consider proposed exports of small arms in light of the respect for human rights and fundamental freedoms in the recipient country. It also calls upon member states to avoid issuing export licenses where there is a risk they will be used to violate or suppress human rights.[16] While surveillance and security technology may not be considered as "small arms" in the conventional sense, their military applications are clear and therefore relevant when designing export control regulations.

Conclusion and Recommendations

"Efforts to achieve secure networks and information systems must ensure that human rights and civil liberties, such as privacy and legal protection are appropriately and adequately guaranteed."[17]

Rights & Democracy believes that there is a credible and reasonable expectation that security and surveillance technology sold to the People's Republic of China will be used to repress free speech and violate a series of related human rights. There have been numerous reports and studies by reputable organizations documenting such abuse.[18]

The United Nations Commission on Human Rights is currently developing norms aimed at clarifying the responsibility of private actors with regards to human rights.[19]

---

[15] Council of the European Union, Code of Conduct on Arms Exports, http://ue.eu.int/cms3_fo/showPage.asp?lang=en&id=408&mode=g&name=#exp3

[16] See http://www.osce.org/docs/english/fsc/2000/decisions/fscew231.htm

[17] Government of Canada in its final submission to the World Summit on Information Society, Geneva, 2003, www.itu.int/dms_pub/itu-s/md/03/wsispc3/c/S03-wsispc3-C-0068!!MSW-E.doc

[18] For example, see: *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*, Shanthi Kalathil and Taylor Boas; *Big Mama is Watching You: Internet Control and the Chinese Government*, Lokman Tsui; *China's Internet: A Technology of Freedom?* Matthew McMahon; *Free Expression on the Internet*, Human Rights Watch; *Wired China: Whose Hand is on the Switch?* Congressional - Executive Commission on China; *How China Censors the Net by Domain Name Hijacking*, Bill Xia; *"Purifying" the Net, China-style,* Digital Freedom Network; *State Control of the Internet in China*, Amnesty International; You've *Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies*, RAND, *In Custody: People imprisoned in connection with Journalism or the Internet* (list), Human Rights in China (China Rights Forum No.3, 2003)

[19] see http://www1.umn.edu/humanrts/links/norms-Aug2003.html

Nevertheless, the responsibility of governments that actively involve themselves in the transfer of sensitive technology under the guise of trade promotion is clear and they risk being accused of complicity in any human rights violations that may result. While there may not be any actual intent by such governments or corporations to facilitate human rights violations, their failure to conduct due diligence in the face of a reasonable expectation of human rights abuse, is cause for serious concern and must be addressed.

Rights & Democracy therefore makes the following recommendations:

1. The Government of Canada should impose a temporary ban of the sale of security and surveillance technology to China until sufficient safeguard procedures can be put into place. Such safeguard procedures should be undertaken within a multi-stakeholder process that includes civil society organizations.

2. The Government of Canada should undertake to develop a multilateral consensus on the issue of trade in dual-use technology. Such a process might be based upon the successful campaign to ban land-mines in which Canada initiated an informal "Ottawa process" built upon the strength of civil society movements and smaller governments from the Commonwealth and Francophonie.

3. The Government of Canada should ensure that the issue of terrorism, surveillance and human rights becomes a standing discussion topic within the Canada-China Bilateral Human Rights Dialogue, including active Canadian involvement in ensuring the release of human rights defenders and democracy activists currently imprisoned as a result of electronic surveillance.

4. The Government of Canada should adopt an over-arching and coherent strategy to assess the impact of its trade and investment policies and promotion activities on human rights in the countries with which it does business.

October 2004