
**RESEARCH PAPER**
**No. 113**

**SEPTEMBER**
**2007**

# SECURING A NETWORK SOCIETY
# CYBER-TERRORISM, INTERNATIONAL COOPERATION AND TRANSNATIONAL SURVEILLANCE

***ELIOT CHE***
**(Researcher, Carleton University, Canada)**

**RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)**

**# 1, Kalavryton Street, Ano-Kalamaki, Athens, 17456, Greece**
**RIEAS URL:http://www.rieas.gr**

## RIEAS MISSION STATEMENT

**Objective**

The objective of the Research Institute for European and American Studies (RIEAS) is to promote the understanding of international affairs. Special attention is devoted to transatlantic relations, intelligence studies and terrorism, European integration, international security, Balkan and Mediterranean studies, Russian foreign policy as well as policy making on national and international markets.

**Activities**

The Research Institute for European and American Studies seeks to achieve this objective through research, by publishing its research papers on international politics and intelligence studies, organizing seminars, as well as providing analyses via its web site. The Institute maintains a library and documentation center. RIEAS is an institute with an international focus. Young analysts, journalists, military personnel as well as academicians are frequently invited to give lectures and to take part in seminars. RIEAS maintains regular contact with other major research institutes throughout Europe and the United States and, together with similar institutes in Western Europe, Middle East, Russia and Southeast Asia.

**Status**

The Research Institute for European and American Studies is a non-profit research institute established under Greek law. RIEAS's budget is generated by membership subscriptions, donations from individuals and foundations, as well as from various research projects. The Institute is autonomous organization. Its activities and views are independent of any public or private bodies, and the Institute is not allied to any political party, denominational group or ideological movement.

**Dr. John M. Nomikos**
**Director**

## RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)

**Postal Address:**

# 1, Kalavryton Street
Ano-Kalamaki
Athens, 17456
Greece

Tel/Fax: + 30 210 9911214

E-mail: rieas@otenet.gr



## Administrative Board

**Dr. John M. Nomikos,** Director
**Mr. Charles Rault,** Senior Advisor
**Dr. Darko Trifunovic,** Senior Advisor
**Dr. Andrei Korobkov,** Senior Advisor

## Research Team

**Andrew Liaropoulos,** Senior Analyst
**Maria Alvanou,** Senior Analyst
**Panos Kostakos,** Senior Analyst
**Ioannis Michaletos,** Junior Analyst
**Aya Burweila,** Junior Analyst

## International Advisors

**Mr. Richard R. Valcourt**, Editor-in-Chief, International Journal of Intelligence and Counterintelligence
**Dr. Shlomo Shpiro**, Bar Illan University
**Prof. Siegfried Beer**, Director, Austrian Centre for Intelligence, Propaganda and Security Studies
**Dr. Ioannis D. Galatas** (MD), CBRN Officer and Planner
**Mr. James Bilotto**, CBRN Chief Operating Officer
**Dr. Yannis A. Stivachtis**, Virginia Polytechnic Institute and State University
**Dr. Evangelos Venetis**, University of Leiden
**Dr. Konstantinos Filis**, Center for Eurasia Studies
**Mr. Chris Kuehl, Armada** Corporate Intelligence Review
**Prof. Vasilis Botopoulos,** Chancellor, University of Indianapolis (Athens Campus)
**Prof. Marco Lombardi**, Director, Italian Team for Security and Managing Emergencies, Catholic University
**Dr. Zweiri Mahjoob**, Centre for Strategic Studies, Jordan University
**Mr. Makis Kalpogiannakis**, Business Development Manager, Intracom
**Mr. Dimitris Lidarikiotis**, Spacephone SA

## Research Associates

**Mr. Ioannis Moutsos**, Independent Investigative Journalist
**Mr. Hamilton Bean**, Intelligence Studies
**Mr. Konstantopoulos Ioannis**, Intelligence Studies
**Dr. Despina Moissidou**, Former Crime Scene Investigator
**Mr. Nadim Hasbani**, Lebanon-Syria and North Africa Studies
**Mr. Nikos Lalazisis**, European Intelligence Cooperation
**Mr. Naveed Ahmad**, South & Central Asia and Muslim world

**RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES**

**(RIEAS)**

**RESEARCH PAPER**
**No. 113**

**SEPTEMBER**
**2007**

# SECURING A NETWORK SOCIETY
# CYBER-TERRORISM, INTERNATIONAL COOPERATION AND TRANSNATIONAL SURVEILLANCE

**ELIOT CHE**
**(Researcher, Carleton University, Canada)**

## Abstract:

The advent of the Information Age, coupled with the resurgence of terrorism on the international landscape brings forth questions on the nature of security and the mechanisms for confronting new asymmetric threats. While globalization and advances in computer technology have led to increased opportunities in numerous fields, they have also resulted in new dangers. In the global post-9/11 environment, new transnational threats are emerging. This paper examines the role of information technology in a period some have identified as the "Age of Terrorism." First, cyberterrorism becomes an increasing concern as society's dependence on information technology intensifies. However, cyberterrorism can and must be distinguished from both legal and illegal forms of computer-driven activism and dissent, as this distinction is necessary for the maintenance of civil liberties. Second, prospects for addressing the cyberterrorist and global terrorist threat include numerous forms of military and political cooperation, from the regional and national to the international. Current and potential mechanisms of surveillance and defence cooperation are diverse, from satellite technology to analyses of both computer-system vulnerabilities and the structure of social networks. Third, a legal approach illustrates concerns over the balance between rights and security and the restrictions on each when contemplating the role of information technology. This paper explores the many faces of terrorism and security in the Information Age, addressing questions on the nature of the threat, prospects for defence, and the protection of civil rights.

**Keywords:** Counter-terrorism, information technology, privacy, surveillance, terrorism.

**Note: Paper presented at the Seventh Annual CISS Millennium Conference as "Security Today", June 14 – 16, 2007, Buçaco, Portugal**

Advances in computer technology have remapped the world, to the point that distances from Ottawa to Toronto and from New York to London are virtually identical. While globalization and the Information Age have led to increased opportunities in numerous fields, they have also resulted in new dangers. In the post-9/11 international environment, new transnational threats to Canada are emerging. The coinciding of amplified adoption and implementation of computer and information technologies with the re-emergence of terrorism on a transnational scale brings forth several questions. What contribution will technological innovations make to terrorism and counter-terrorism efforts? What are the legal justifications for and social consequences of increased technological intervention into domestic and foreign societies? What might some of the remedies be for upholding privacy rights in the "new normal" of the Age of Terrorism?

As such, this paper makes two arguments. First, information and communications technologies enable new modes of terrorism, the threat of which intensifies as society becomes increasingly dependent upon computer networks. Technology-driven terrorism is discrete from virtual forms of activism or dissent, and such a distinction is necessary for the preservation of civil liberties. Second, information and communication technologies also make possible new modes of counter-terrorism. Central to this argument are questions regarding what techniques have been facilitated through more recent technological innovations. While transnational approaches to addressing terrorism are particularly significant in a network society, can technology-driven methods of intervention and intelligence-gathering be less intrusive than more traditional techniques in the violation of privacy rights? In light of the recent debates over the balancing of rights and security, this paper argues that a particular configuration of legal and technological mechanisms may enable not only the capacity to maintain security, but also the potential for preserving the essence of the right to privacy. While current forms of technology-driven surveillance are not legally justified in the Canadian context, technological and

legal remedies can bring them into the boundaries of Canadian law. In exploring these hypotheses, this paper is presented in four parts: (1) an examination of various forms of politically-driven technological action; (2) a scalar comparison of possibilities for addressing terrorism in the Information Age; (3) a description of the current classifications of technology-driven surveillance and intelligence-gathering; and (4) an analysis of the legal and social implications of technological intervention and intrusion during an Age of Terrorism.

## Technology-driven Terrorism: The Nature of the Cyberterrorist Threat

In the 1983 movie WarGames, Matthew Broderick's character breached the Pentagon computer system and almost started World War III. Since then, much of the Western world has been both captivated and mystified by the idea of computer conflict, hacking and, more recently, cyberterrorism. The concept of cyberterrorism is rooted in two fields of study: information technology and asymmetric conflict. First, the modern technological revolution, originating in the 1980s, has led authors such as Alvin and Heidi Toffler to argue that information technologies are transforming industrial (second-wave) societies into information-based (third-wave) societies. Occurring primarily in developed, industrialized regions, there exists an increasing reliance upon complex networks and modern technologies for the proper functioning of society. This post-industrial period has been coined the "Information Age" (Toffler, 1980). Manuel Castells argues that the most recent period of the Information Age is one dominated by networks. As a new socio-political and economic configuration, "network society" consists of a "space of flows" where various transactions and encounters take place (Castells, 1996).

Second, asymmetric threats, specifically in the form of terrorism, have existed since the dawn of warfare. Defined by the U.S. Joint Chiefs of staff as attempts to circumvent or undermine a superior military power's strengths while exploiting its weaknesses, using methods that differ from the superior military power's expected mode of operations (United States Joint Staff, 1999), the recent escalation in asymmetric threats is commonly considered a result of the demonstration of U.S. military might in the first Gulf War (Sloan, 2002: 110). Not limited solely to cyberterrorism, those seeking to challenge U.S. power have recognized that conflict on the traditional battlefield using conventional military weaponry is no longer

feasible. As such, the threat of cyberterrorism comes from both states and non-state actors and, though negative, is perhaps an inevitable consequence of the transition to an information-based society.

***Defining the Boundaries Cyberterrorism***

Attempts to define cyberterrorism suffer from the same dilemmas as definitions of terrorism. Generally, cyberterrorism is a result of the convergence of technology and terrorism, and consists of two mutually dependent elements. First, it refers to attacks and threats of attacks against computers, networks and the information stored within them, for the purpose of intimidating or influencing a government or society to further political or social objectives. Second, the attack results in violence against persons or property, or at least causes enough harm to generate fear. The definition is a reinterpretation of mainstream characterizations of terrorism infused with technological terminology. While it should be noted that terrorism is still somewhat of a contested term, section 83.01 of the *Anti-Terrorism Act* provides an in-depth classification within the Canadian context.

A cyberterrorist differs from a terrorist who uses technology. Cyberterrorism consists of an attack on a technological factor using another technological factor. This is distinct from a terrorist utilizing technology to commit a traditional act of terrorism, and is also distinct from a terrorist using non-technological means to commit an act of terrorism against a network of computer system. For example, an act of cyberterrorism occurs when an individual or organization uses a computer network to overload and destroy a national power-management system. Cyberterrorism does not occur when a suicide bomber destroys an electrical grid – nor does cyberterrorism occur if a terrorist uses the World Wide Web to acquire information on building a chemical weapon.

Distinctions must also be made between cyberterrorism and hacktivism, the latter being a term coined by scholars to describe the marriage of hacking with political activism (Denning, 1999: 241). While politically motivated, hacktivism differs from cyberterrorism in that the former seeks to protest and disrupt, not to kill, physically injure, or terrify. As such, serious attacks against critical infrastructure, depending on their impact, could be acts of terrorism; whereas attacks that disrupt nonessential services would most likely not. This distinction between cyberterrorism and cyberdissent is of significance as it addresses, to a limited extent specifically in

the field of computer technology, historical critiques on the inability of legal institutions in recognizing legitimate and/or illegitimate dissent (Mandel, 1982: 14-17; Richard, 1990: 31-83). In the context of terrorism contrasted with dissent, self-branded civil libertarian, Irwin Cotler, makes a persuasive argument on the differentiation by outlining some of the key principles that underpin Canada's *Anti-Terrorism Act*, while also addressing some of the concerns. He argues that the inclusion of section 83.01(1)(b)(ii)(E) seeks to ensure that "any advocacy, protest, dissent or work stoppage activity, even if unlawful, even if attended by violence, even if it causes disruption to a public or private essential service or facility, would not be considered a terrorist activity" (2002: 37). However, it remains to be seen whether this policy will withstand public and governmental pressure once a test case is presented to the courts.

***Why Use Cyberterrorism?***

As a result of globalization, computerization and the emergence of a network society, numerous authors have argued that cyberterrorism is becoming increasingly attractive to terrorists for several reasons (Weissman, 2005). First, cyberterrorism is generally perceived to be more cost-effective than traditional terrorist methods. Typical computers and phone or broadband internet connections are generally much cheaper and easier to acquire than traditional types of weaponry, such as explosives and military-grade vehicles. Cyberterrorist attacks also do not result in the attacker's death, as is the case with suicide bombers, and as is potentially the case in traditional acts of terrorism. Second, cyberterrorism possesses a certain amount of anonymity not found in more traditional forms of terrorism. The global extension of computer technologies in post-industrial societies has facilitated terrorist mobility and deployability. As such, it has become increasingly difficult for security agencies to determine the real identities of the terrorists. This complex obstacle is further enhanced by the lack of customs, borders or checkpoints within cyberspace. While the fact remains that all Internet traffic passes through at least one of thirteen central servers that act as the foundation of the World Wide Web, the sheer amount of information transferred creates considerable challenges for data analysis and effective intelligence collection.

Third, the quantity and quality of targets increases as society moves towards further dependence on information technologies (Weissman, 2005). The multiplicity

of potential targets is already enormous, ranging from government military systems to civilian economic and scientific networks. Fourth, cyberterrorism removes or reduces the requirement for geographical proximity to the target. This virtually eliminates the traditional requirements for physical and psychological training to avoid capture, and risk of mortality. The ability to conduct cyberterrorism remotely is a key factor in the transnational nature of committing terrorist acts and in recruiting new members. Fifth, cyberterrorism can potentially have a direct affect on a larger number of people than traditional terrorist methods, thereby generating widespread effects and increasing awareness of particular causes (for example, through greater media coverage). While a suicide bomber may destroy a building, killing the tens or hundreds of individuals inside, a cyberterrorist attack on a waste-management or energy system has the potential to kill or injure thousands, if not millions of people.

***Is There a Real Threat?***

It should be emphasized that no single cyberterrorist attack has been recorded – that is, categorized as such. This begs the question of whether cyberterrorism is a real threat. Current discussions revolve around military systems, intelligence networks, government systems and critical infrastructure. First, suggestions have been put forth that cyberterrorists could compromise military systems, such as a nuclear missile launch facility, and either launch a missile or disable the entire system. Currently, the cyberterrorism threat of this type is non-existent. Government statements indicate that major military systems, such as the Canadian Department of National Defence, the Pentagon, and nuclear launch facilities, are “air-gapped” (Libicki, 1996; Green, 2002; Mitchell, 2005). That is, they are not physically connected to external networks such as the Internet. The implied conclusion is that computer network attacks would be ineffective against these types of military networks. However, during a U.S. military exercise conducted by the National Security Agency (NSA), attackers using tools available on the Internet were able to gain access to several key U.S. systems. While the details remain classified, the report on the exercise concluded that military infrastructure could be disrupted and troop deployments could be hindered (Denning, 1999).

Most security and intelligence systems are also protected in the same way as military infrastructure. The Canadian Security and Intelligence Service (CSIS), the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) all

utilize stand-alone networks (Government of Canada, 1999; Green, 2002). Martin Libicki, a defence analyst at the National Defence University (1996) and RAND Corporation, indicates that this is partially rooted in the general paranoia that exists within intelligence agencies, and that such paranoia is a sound governing principle when considering cybersecurity. Like most military systems, security and intelligence systems in their current form are shielded from computer attack. More general government systems, in both the United States and in Canada, are further protected by the development of proprietary systems, unique to each branch of government. While this has often led to difficulties in cooperation between agencies, it has also provided protection in that only a select few individuals understand the systems well enough to violate them. In an ironic twist, inefficiency breeds security. While government systems may be connected to external networks, such as the Internet, the proprietary nature of current computer applications in combination with screening processes for new employees ensures a relatively high level of security from the cyberterrorist threat.

Critical infrastructure consists of less-protected secondary targets, such as power grids, oil pipelines, water-treatment and waste-management systems. Particularly in the United States, most of these systems are privatized and are not currently as of much a concern as military or government systems. As such, critical infrastructure systems are less secure than military, intelligence or government systems. Concerns over the susceptibility of U.S. critical infrastructure are significant to Canadians due to the numerous connections between Canadian and U.S. systems (as evidenced by the August 2003 Canada-U.S. blackout). Additionally, 85% of Canada's critical infrastructure is owned by stake holders other than the federal government (Canadian Office of Critical Infrastructure Protection and Emergency Preparedness, 2005). However, while critical infrastructure is possibly more vulnerable to cyberterrorism, it is still quite secure. These systems are under constant threat from natural disasters such as hurricanes, floods or tornados, and company employees are trained to act in emergency scenarios. Nonetheless, as a consequence of openness to external networks and lower security thresholds, a cyberterrorist threat to critical infrastructure does exist. Cyberattacks differ from traditional emergencies and natural disasters in that they can be directed and concentrated at specific weak points in a computer network. During the NSA exercise mentioned above, attackers

were also able to gain access to power grid and emergency 9-1-1 systems, resulting in service disruptions.

Currently, it seems as though the greatest threat to the aforementioned systems comes not from cyberterrorism, but from two other factors: insider action and deregulation. Insiders possess specialized knowledge that is difficult, if not impossible, for outsiders to acquire. Disgruntled staff or vengeance-seeking former employees may possess both the resolve and the means to wreak havoc on internal computer and information systems. For example, in 2000, a disgruntled consultant hacked into a waste management control system and let loose millions of gallons of raw sewage on the town (Berinato, 2002). While this potential problem may be alleviated through comprehensive employee screening processes, such security measures may be decreasingly feasible as a result of deregulation. Second, deregulation potentially leads to an increased risk of cyberterrorism. An amplified focus on profitability has forced utility companies and other critical infrastructure businesses to move increasing proportions of their operations to the Internet in search of greater efficiency and lower costs. This may result in further risk and exposure to cyberterrorist threats. Growing cross-border interdependency will play an increasingly important role in the vulnerability of vital networks. For example, strong links between Canadian and U.S. critical infrastructure were demonstrated during the 2003 Canada-U.S. blackout, in which a transformer station in Cleveland malfunctioned, causing power outages affecting 40 million people in Canada and the north-western United States.

In sum, despite current concerns over the vulnerabilities of military, security and intelligence, government and critical infrastructure systems, the nature of these systems currently suggests that such concerns are generally unfounded, though a potential threat is present. While dangers to critical infrastructure systems exist, in the form of insider action and deregulation, a “digital Pearl Harbour” has yet to occur.

***An Exaggerated Threat?***

The relatively insignificant threat of a cyberterrorist attack brings forth the question of why the threat is exaggerated. The reasons behind this are four-fold (Weissman, 2005: 131-134). First, as Dorothy E. Denning, a professor of computer science speaking before the U.S. House Armed Services Committee, has observed, "cyberterrorism and cyberattacks are sexy right now. It’s novel, original, it captures people’s imagination” (Denning, 2001; United States Congress: House Committee on

Armed Services, 2000). As such, the concept of cyberterrorism has symbolic power that creates compelling and frightening scenarios, influencing perceptions and contributing to the remaining three reasons below. In addition to the symbolic impact of cyberterrorism, the mass media frequently fail to distinguish between hacktivism and cyberterrorism, often exaggerating the threat of the latter. As mentioned above, the two are not analogous. Additionally, misunderstandings between computer crime and cyberterrorism have also surfaced (Stone, 2000). Ambiguity about the very meaning of "cyberterrorism" has confused the public and given rise to many misrepresentations. Third, there is a general fear of the unknown. Despite the advent of Third Wave society, many people, including most lawmakers and government officials, still do not fully understand and therefore tend to fear both computer technology and terrorism. As a result, psychological distress and the desire for self-preservation increase the likelihood of accepting unnecessary measures to combat an exaggerated threat. Fourth, some groups are eager to exploit this ignorance. National security officials are inclined to take measures to increase their presence and influence in government, while the computer technology industry, still recovering from the collapse of the high-tech bubble, seeks to regain its economic foothold. Any response to a cyberterrorist threat requires enhanced technology, training and maintenance. Some politicians have “played the role of prophets of doom” (Weissman, 2005: 133), purposely stoking fears of cyberterrorism, whether out of genuine conviction or from a desire to create public anxiety in order to advance a political agenda.

While the potential threat of cyberterrorism is currently exaggerated, many analysts predict an increase in the actual threat. Looking at the various trends in military transformation, technological innovation and terrorist sophistication, the threat of cyberterrorism and computer-based attacks in expected to increase in the future for three principal reasons. First, the next generation of terrorists is now growing up in an increasingly digital world, alongside or integrated into post-industrial society, and will therefore be progressively more proficient in the use of information and computer technologies (Weissman, 2005: 146). An example of recent activity, though not classified as cyberterrorism, is *Titan Rain*, the name given to a series of attacks against the U.S. since 2003, in which the networks at Lockheed martin and NASA (among others) were infiltrated.

Second, cyberterrorism may also become more attractive as the real and virtual worlds become more closely coupled. Increasing demands for efficiency and

interoperability in critical infrastructure, government systems and potentially intelligence systems will ultimately result in elevated degrees of exposure to outside networks, and therefore cyberterrorist attacks. For example, the push by the U.S. military towards the network-centric warfare doctrine has resulted in new attempts at military transformation and integration. The Global Information Grid, which seeks to encompass the end-to-end set of information capabilities, is a primary example. In terms of supervisory control and data acquisition (SCADA) systems, they are no longer only on stand-alone networks – connections between SCADA systems via the Internet are perceived as better for business. While SCADA systems are solely for the management and supervision of critical infrastructure (such as power-grid systems), their intentional or unintentional misuse can still cause damage. During a no-notice exercise performed by the U.S. Department of Defence, operators at a power management station were fooled by manipulated SCADA data into taking actions that would have damaged the system.

Third, success in the "war on terror" on the traditional battlefield may result in terrorists turning increasingly towards unconventional weapons such as cyberterrorism. The cost-effectiveness (in both human and economic terms), anonymity, abundance of critical targets and geographical freedom provide several incentives for terrorists to experiment with this new method. As such, while the current conjecture regarding the cyberterrorist threat is exaggerated, the expected increase in cyberterrorist activity demands that legal and technological remedies be explored.

## Counter-Terrorism I: Securing a Network Society – Modes of Prevention

The conclusion of the previous section of this paper, indicating that no acts of cyberterrorism have occurred, does not necessarily imply that the potential cyberterrorist threat should not be addressed. Irwin Cotler argues that the nature of security legislation, particularly in regards to terrorism, is preventative rather than reactive (Cotler, 2002: 23-24) – that it is necessary to stop acts of terrorism, including cyberterrorism, before they occur. While the extent and scope of preventative approaches should be questioned, the following portion of this paper examines current and potential legal and political mechanisms at various scales for combating the threat of cyberterrorism.

***Existing Domestic Law***

Canadian domestic legal mechanisms are insufficient for addressing terrorism, and especially cyberterrorism. The transnational nature of the threat, as mentioned above, severely limits the utility of federal or sub-federal law. Of particular interest here is the lack of geographic restrictions on acts of cyberterrorism. Not only can cyberterrorism occur from outside the territorial boundaries of the state, but acts can originate from numerous foreign states simultaneously. Therefore, domestic mechanisms such as the U.S. terrorism watch lists are either inadequate (in that not enough states with a cyberterrorism capacity are considered) or inefficient (in that too many states with a cyberterrorism capacity, but that do not pose a legitimate threat, are considered). The dilemma rests on the rise of the network society and increasing dependence on information and computer technologies for the production of everyday life.

Additionally, considerations of national sovereignty and issues of jurisdiction emerge when investigating or prosecuting transnational criminal acts. The same can be said for addressing cyberterrorism. While Canadian security legislation, such as the *Anti-Terrorism Act* (ATA), addresses acts of terrorism against Canadian citizens abroad, it cannot take legal action against cyberterrorism without the consent of the foreign government from which the cyberterrorist act originated. National sovereignty remains enforced and universal jurisdiction is currently non-existent. As such, existing domestic legal mechanisms are insufficient.

***Bilateral Agreements***

Bilateral agreements may not be feasible due to the mobility and deployability of cyberterrorism, as well as bureaucratic impracticability. First, as indicated above, cost-effectiveness, the global extension of computer technologies and lack of geographic restrictions suggests that cyberterrorist attacks can originate in almost any country. Second, with over 200 countries enjoying access to the Internet and related communications technologies (Internet World Stats, 2007), bilateral agreements are bureaucratically unfeasible. As such, governments must approach the issue at the international scale. Whereas Canada's *Securing an Open Society* is a national strategy, securing a network society requires approaching the issue transnationally.

*International Agreements I: Combating Terrorism.* Common international platforms are required to address the terrorist threat, and there are two components of international agreements worth considering: international law and policy harmonization. International law originating within international, multilateral institutions can most successfully address cyberterrorism. While there has been disagreement over whether a universal definition of terrorism can be ascertained (for example, see Cronin, 2003; Martin, 2003), the United Nations has successfully issued international legislation concerning weapons of terrorism (United Nations, 1997), and regarding supporters of terrorism (United Nations, 1999). Multilateral institutions are particularly crucial because of the variegated definitions of terrorism and the legitimacy that comes from agreements among several states in an open and transparent forum. The legislating of any international law on cyberterrorism should consider three factors.[1] First, a definition of what constitutes a cyberterrorist act should be established. As indicated above, distinctions can and should be made between acts of cyberterrorism and acts of cyberdissent or hacktivism. Second, a designation of what actions are required for a legal response should be determined. This includes whether a target should be notified before retribution for a cyberterrorist act is executed, and under what circumstances. Third, the agreement should promote transnational cooperation. National interests should be compromised to the minimal extent possible when addressing the attribution of cyberterrorist attacks and subsequent potential retribution.

Policy harmonization is a consequence of common international platforms. International requirements for the legislating of domestic policies on cyberterrorism increase domestic and international security and transnational cooperation. An instructive example, addressed specifically at terrorism, is *UN Security Council Resolution 1373* (and *UNSCR 1377*). A second example is the *Council of Europe Convention on Cyber-Crime*. Signed by Canada in 2001, this treaty is "the first-ever international treaty to address criminal law and procedural aspects of various types of criminal behaviour directed against computer systems, networks or data and other types of similar misuse" (de Borchgrave, 2001: 33). While not addressed specifically at cyberterrorism, the cybercrime treaty requires states to criminalize certain forms of abuse of computer systems and certain crimes when they are committed using computer systems. The treaty also supports international cooperation to detect, investigate and prosecute these criminal offences, as well as to collect electronic

evidence of any criminal offence. However, the *Convention on Cyber-Crime* does not include key elements of the terrorism definition. Specifically, it does not refer to political, ideological or religious motivations or objectives (as opposed to the *Anti-Terrorism Act* which indicates these in section 83.01(b)(i)(A)). Therefore, current international legal mechanisms are insufficient in addressing the cyberterrorist threat and new agreements must be established. The secondary danger is the collection of data by governments from commercial actors. This activity lacks transparency and accomplishes an "end-run around the checks otherwise applicable when government seeks personal information" (Galison & Minow, 2005). Information-gathering requires governmental regulation, oversight and transparency, a feature not common in the commercial harvesting of personal data.

### *International Agreements II: Addressing the Causes of Terrorism*

International agreements on combating terrorism necessarily require complementing initiatives on other issues that are perceived to be causes of individuals and groups turning to terrorist methods. The process of determining the causes of terrorism deserves much longer treatment than this essay can provide. However, international policies directed at the alleviation of poverty, war, repression and other forms of social, political and economic exploitation should be a counterpart of any counter-terrorism campaign. Information and communications technologies can assist in this process by extending the ability of governments to understand which regions require aid and to the development of a transnationally scaled civil society that seeks to drive marginalized individuals away from destructive forms of political action.

## Counter-Terrorism II: Technology-driven Surveillance and Intelligence

There are two methods of defending against cyberterrorism: passive defence and active defence. Passive defence is another name for target hardening, involving the use of technologies such as firewalls or cryptography to protect information technology assets and the data stored within (Goodman, 2007: 45). A considerable part of the problem is the combination of demands for large-scale connectivity and access, as well as the massive number of owners, operators and users of these systems and networks. As Goodman argues, "the domain of actors in cyberspace is much

larger and more diversified than is the case with more traditional security issues." (2007: 50-51). Analyses of private sector products and systems indicate that software quality assurance is problematic. Defective or poorly-designed products rushed to market without adequate concern for security raise many questions about whether regulation will be necessary. Additionally, in both the public and private sectors, the many legacy systems still in use were not designed with security in mind. Even presently, security is often perceived to be in conflict with design criteria focusing on accessibility and data throughput. Security is commonly identified with reduced efficiency and impaired functionality (Goodman, 2007).

Active defence seeks to determine the identity of the attacker and possibly initiate a counter-attack. One form of active defence, discussed here, is computer-driven surveillance. An effective response to the threat of terrorism and cyberterrorism requires international cooperation, but such cooperation must be reinforced with transnational surveillance mechanisms. Technology-driven intelligence gathering methods can be more effective and less intrusive than traditional forms of surveillance and intervention. As such, this section examines the various types of data collection systems, while the following portion provides an analysis of the legal and political implications of new technology in counter-terrorism efforts. While there are currently no global surveillance systems with the full participation of all countries, two more limited types of systems are presently in operation: domestic systems and transnational systems. Domestic systems, such as the (now defunct[2]) FBI surveillance system known as Carnivore, are inward-looking. While domestic systems may be more comprehensive than transnational systems (Todd & Bloch, 2003: 46-47), the former does not infringe upon the national sovereignty rights of foreign countries, not does it violate the jurisdiction of foreign intelligence and security services. As such, neither bilateral nor international agreements are necessary for the legal functioning of domestic surveillance systems. Transnational systems are a different breed altogether. These systems, such as ECHELON, are both inward-looking and outward-looking. Transnational systems are of a controversial nature due to a perceived lack of respect for national sovereignty rights and issues of jurisdiction. While transnational agreements or understandings are necessary for the functioning of transnational surveillance systems, such arrangements are often mired in secrecy. The features of transnational surveillance systems dictate

that the types of transnational or international agreements mentioned above (depending on the scope of surveillance) are necessary for their legal operation.

***ECHELON Transnational Surveillance System***

The ECHELON surveillance system began its current phase of development in 1971 as a component of the post-WWII UK/USA intelligence cooperation and information-sharing alliance.[3] Using electronic-intercept stations and space satellites, the purpose of ECHELON is generally signals intelligence (SIGINT), and specifically communications intelligence (COMINT). The transnational surveillance system additionally has the capability to acquire other forms of intelligence and information.[4] ECHELON captures military, political and diplomatic communications traffic from across the globe, though recent events have indicated that the system is also being used for economic purposes (Lowenthal, 2003: 239). ECHELON is not designed to eavesdrop on specific individuals. Instead, the surveillance system works on the basis of automated analysis. Messages and conversations are filtered though a computer system called Dictionary which detects keywords and phrases (Todd & Bloch, 2003: 46) – a method of processing information is known as "data-mining."

Five countries currently participate in the ECHELON system,[5] providing global coverage through intercept ground stations and space-based satellites. Australia and its Defence Signals Directorate (DSD) monitors Indochina, Indonesia and Southern China. The Government Communications Security Bureau (GCSB) of New Zealand covers the Western Pacific region. The United Kingdom's Government Communications Headquarters (GCHQ) monitors Europe, Africa and Russian territory west of the Urals. The National Security Agency (NSA) in the United States, possessing the most advanced and comprehensive surveillance infrastructure, covers Latin America, and Asia, as well as Asiatic Russia and northern China. Canada's Communications Security Establishment (CSE) monitors northern portions of the former Soviet Union, embassies around the world and central and southern parts of the Americas. Commentators argue that the nature of cyberterrorism demands that transnational surveillance systems be implemented to compliment international agreements, and that while legal issues and concerns over ECHELON in its current form will invariable arise, the basic transnational approach behind ECHELON is sound. The remainder of this essay examines these legal dilemmas and explores some

of the ways that surveillance systems such as ECHELON may gain increased or decreased legitimacy.

## Implications of Technological Intervention in the Age of Terrorism

Addressing matters of privacy and surveillance inevitably results in debates concerning oversight and the balancing of rights and security. The following portion of this essay discusses these issues in five parts: a contextual section that examines (1) the proportionality test, (2) the existence of a right to privacy in the Canadian context, and (3) the nature of automated surveillance; and an analytical section on (4) the balancing act between the right to privacy and security; and (5) a proposal to remedy the problem of oversight.

### *1. The Proportionality Test or "Oakes test.*

*"* Derived from *The Queen v. Oakes*, the "*Oakes test*" considers s.1 of the *Charter*, which provides that:

> 1. The *Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such *reasonable limits* prescribed by law as can be *demonstrably justified* in a free and democratic society. (Emphasis added)

In other words, the rights and freedoms under the *Charter* can be violated if the violation is reasonable and justifiable. The Supreme Court of Canada has defined a test for determining whether a violation is reasonable and justifiable. This test, referred to as the "*Oakes test*" or proportionality test, has two components: sufficient importance and proportionality. First, the government must demonstrate that its objective is sufficiently pressing and substantial to warrant the violation of a right or freedom. Second, the party invoking s.1 must show the means to be reasonable and demonstrably justified. Proportionality itself has three requirements: (1) the measures must be fair and not arbitrary (the means chosen to limit rights and freedoms must be rationally connected to the objective); (2) there must be a minimal impairment of rights in achieving the objective; and (3) the detriments of the violation must not outweigh its benefits (the more deleterious the effects, the more important the objective must be). The *Oakes test* was further solidified in Canadian law after *Dagenais v. CBC* (regarding publication bans).

***2. The Right to Privacy.***

While not expressed explicitly in the *Charter of Rights and Freedoms*, the right to privacy has been interpreted through the Supreme Court of Canada's purposive approach to s.8 of the *Charter*, which provides that:

> 8. Everyone has the right to be secure against unreasonable search or seizure.

Through precedence in case law,[6] the right to a reasonable expectation of privacy has been demonstrated in Canadian law. As La Forest J. stated in *R. v. Dyment*, "the restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state" (1988: 427-28). Historically, privacy was associated with private property, whose possession protected against intruders. "If the rights of private property were respected, and the curtains of the home (or the drawbridge of the castle) were pulled, the King's agents could watch from a distance but would have no way of finding out what was going on inside" (*R. v. Tessling*, 2004: para 16). However, technological developments diminished the protections provided by property rights, and new interpretations of law or new legislation were required. As a result, the Supreme Court of Canada (SCC) has indicated that s.8 of the *Charter of Rights and Freedoms* provides for the right to a reasonable expectation of privacy.

Canadian case law has identified three different types of privacy: (1) personal; (2) territorial; and (3) informational. Personal privacy includes the protection of bodily integrity, as indicated in *R. v. Golden* (regarding the legality of strip searches) and in *R. v. Stillman* (regarding the acquisition of bodily fluids by a third party). Territorial privacy includes the protection of privacy in the home, being the place where the most intimate and private activities are likely to take place. As per Cory J., in *R. v. Silveira*, "[t]here is no place on earth where persons can have a greater expectation of privacy than within their 'dwelling-house'" (1995: 363). Other forms of territorial privacy include: in the perimeter space around the home (*R. v. Wiley*, 1993: 273), in commercial space (*R. v. McKinlay*, 1990: 641), in private cars (*R. v. Mellenthin*, 1992: 615), in a school (*R. v. M. (M.R.)*, 1998: para 32), and in prison (*Weatherall v. Canada (Attorney General)*, 1993: 877). Territorial privacy is used as an analytical tool for evaluating the reasonableness of a person's expectation of privacy. Much more controversial than personal privacy and territorial privacy is informational privacy, defined as "the claim of individuals, groups, or institutions to

determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967: 7, cited in *R. v. Tessling*, 2004). The existence and lawfulness of a right to a reasonable expectation of informational privacy has been indicated in *R. v. S.A.B.* (regarding DNA information) and in *R. v. Law* (regarding commercial information). The "reasonable" nature of the expectation of privacy is derived from two factors: (1) the *Oakes test*; and (2) the "totality of the circumstances" test. First, the expectation of privacy can be violated if the objective is reasonable and demonstrably justified. As indicated above, the *Oakes test* demands that two requirements be met before the violation of a right or freedom can occur: sufficient importance of the objective, and proportionality between the limiting measure and the objective. Second the reasonable expectation of privacy is subject to the "totality of the circumstances" test set out by Cory J. in *R. v. Edwards*. Briefly, this test asks two questions: Did the respondent have a reasonable expectation of privacy? And if there was a reasonable expectation of privacy in this case, was it violated by police conduct? These questions must be specifically tailored, depending on facts of the case (*R. v. Tessling*, 2004: para 31).

Thus the expectation of privacy can "reasonably" be violated: (1) if the objective and means of the violation is in accordance with s.1 of the *Charter*; and (2) if there is either no reasonable expectation of privacy, or if a reasonable expectation of privacy was violated by the lawful conduct of law enforcement. A potential third factor affecting the "reasonable" nature of the expectation of privacy is s.33 of the *Charter*, though the relevance of the non-withstanding clause would depend on the nature of the violating legislation (and whether it has invoked s.33). Nonetheless, the development of case law suggests that Canada is either progressing towards or already situated at a position in which the right to privacy in constitutionally protected, but subject to the context of the crisis or emergency at hand.

### *3. Automated Surveillance and the "Veil of Ignorance."*

The nature of ECHELON and other electronic surveillance systems is such that information is automatically filtered by computer systems. As indicated above in the section on surveillance systems, ECHELON is not designed to eavesdrop on specific individuals. Instead, the surveillance system works on the basis of automated analysis. Messages and conversations are filtered though a computer system called Dictionary which detects keywords and phrases. This structure is analogous to John

Rawls' conception of a "veil of ignorance."[7] While those developing the surveillance system are not completely disinterested, automated analysis removes personal biases that pervade other forms of intelligence gathering. Automated systems, while not immune from subjectivity due to their construction by humans, are more capable of eliminating the discrimination often witnessed in human intelligence (HUMINT) or in law enforcement. The use of computer-based keyword and phrase analysis results in amplified complexities and increased difficulties in manipulating the system. Currently, electronic surveillance systems are the most objective components of the intelligence apparatus. However, the analysis of electronically-gathered information is the realm in which increased subjectivity and bias come into play. As such the issue concerns how the data is analyzed rather than how information is collected.

***4. Balancing the Right to Privacy and Security.***

Taking into consideration the threat of cyberterrorism, the preventative nature of law, the reasonable expectation of privacy and the automated nature of transnational surveillance, the "*Oakes test*" can be employed in analyzing the balance between the privacy and security. When situating the risk in relation to national security, a tangible threat of cyberterrorism is non-existent, yet a potential threat remains. In the post-9/11 security environment, increasingly driven by information technology, preventative measures are necessary for the maintenance of security. The potential number of casualties resulting from a cyberterrorist attack on critical infrastructure, or government systems (since military and intelligence systems are as of yet shielded) is sufficient to warrant a limitation on the right to privacy. Therefore the first requirement of the "*Oakes test*" is satisfied. In the second component of the "*Oakes test,*" the rational connection requirement is satisfied due to the transnational nature of cyberterrorism (as well as other characteristics indicated previously in this paper). Transnational surveillance is a prerequisite for any success derived from international agreements. However the issue becomes more problematic when considering the final two requirements: proportionality between the effects of the violation and the objective; and the minimal impairment of rights. This complexity is the result of the secretive nature of the ECHELON system. To what extent does ECHELON eavesdrop on the global communication networks? Who has ultimate control over the intelligence acquired? What restrictions exist on access to and

operationalization of the intelligence collected? These questions are of significant importance in analyzing the balance between rights and security.

Without a deeper understanding on the functioning of the ECHELON surveillance system, the application of the "*Oakes test*" cannot be fully realized. However, a consideration of the automated nature of analysis in combination with an appreciation of the potential threat posed by terrorism and cyberterrorism may be sufficient to establish that a balance between rights and security in the utilization of ECHELON can be achieved. If further information on the functioning of ECHELON is unavailable for logistical or security reasons, oversight mechanisms will increase confidence in the stability, legality and efficiency of the ECHELON surveillance system. An analysis of potential transnational oversight mechanisms is discussed below. A potential issue, though outside the scope of this paper, is the prospective balance required between transnational privacy and international security. While citizens may tolerate domestic surveillance within reasonable limits, it remains to be seen whether surveillance by a foreign government will be as acceptable.

***5. Oversight.***

The problematic of oversight, prevalent and reoccurring in historical analyses of Canadian security services, is further complicated when considering ECHELON, due to the system's transnational nature. The issue of oversight can be considered in both a Canadian context and a transnational context. The Canadian contribution to the ECHELON surveillance system is through the Communications Security Establishment (CSE). This presents a problem for oversight. While security and/or intelligence agencies such as the Royal Canadian Mounted Police (RCMP) and the Canadian Security and Intelligence Service (CSIS) are regulated and restricted by the *RCMP Act* and *CSIS Act*, respectively, the CSE has no specific legislation governing or guiding its actions.[8] While privacy and oversight are present in numerous forms of legislation in other fields, such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA, regarding personal information in the private sector), the *Privacy Act* (regarding personal information in the public sector), the *Telecommunications Act*, and the *Competition Act*,[9] the CSE has very little evidence of its existence outside of Orders-in-Council and a headquarters on Heron Road in Ottawa, Ontario. The CSE ultimately reports to the Minister of National Defence and is not subject to the oversight mechanisms in place for other agencies (such as the

Security and Intelligence Review Committee, or SIRC, with regards to CSIS). As such, domestic oversight of Canada's participation in the ECHELON system is generally absent.[10]

In the transnational context, oversight becomes additionally complex. While international cooperation in addressing cyberterrorism is already perceived as a monumental task, the development of transnational oversight mechanisms for the ECHELON surveillance system seems almost impossible. And yet, the completion of such a task is necessary to establish confidence in the balance between rights and security. Four types of oversight are worth briefly considering here: governmental oversight, judicial oversight, public oversight, and civilian oversight. Governmental oversight is possible through internal watchdogs. This is a relatively common occurrence in national governments, however here it is recommended that an independent organization outside the government be responsible for oversight (due to its transnational nature and to prevent any conflict of interest). Judicial oversight is a potential solution, though no international court suitable to addressing this issue currently exists. Both the International Criminal Court (ICC) and the International Court of Justice (ICJ) have mandates outside the scope of assessing transnational surveillance systems (United Nations, 1978; United Nations 1998). However, if the participating members of the ECHELON system establish themselves as an international institution or agency, approaching the ICJ becomes a possibility. Public oversight, through the media for example, is impractical due to the confidential nature of the intelligence collected. Civilian oversight, similar to SIRC, is potentially the most feasible and the most effective form of oversight currently available. While the process of establishing transnational oversight mechanisms is not within the scope of this paper, the issue must be considered before an analysis of the ECHELON surveillance system under the framework of the "*Oakes test*" can be completed.

## Conclusion: Where to Go From Here

The coinciding of the rise of the network society in the Information Age with the re-emergence of asymmetric threats in the Age of Terrorism signals the need for new approaches to old, established ideas. While information and communications technologies enable new modes of terrorism, they also provide avenues for defence. The preservation of civil liberties is predicated on the distinction between technology-

driven terrorism and virtual forms of activism and dissent. By providing greater anonymity, the protection of the right to privacy may also be increasingly possible as society becomes more integrated with information and computer technologies. The political and legal approaches to addressing terrorism in a network society are necessarily transnational. However, legal questions on the transparency of surveillance systems or, alternatively, oversight mechanisms for regulating electronic modes of intelligence-gathering, must be answered before such systems can be considered compatible with Canadian law. Preventing acts of terrorism or cyberterrorism in a network society requires a sustained, multi-scalar effort by governments and security agencies – not only to maintain the safety of citizens, but also to ensure that rights and freedoms are not unnecessarily trampled upon.

## Footnotes:

1. More in-depth analysis can be found in de Borchgrave et al, 2001.
2. Defunct in name only, as the system was renamed DCS1000 and subsequently "un-named'" when the FBI selected a commercially available Internet tracking tool to replace Carnivore/DCS1000.
3. For detail, see Todd & Bloch, 2003: 4, 44-47, 53-56, 64, 127; Lowenthal, 2003: 196-197, 239.
4. For a detailed analysis of the various forms of intelligence acquisition, see "Collection and the Collection Disciplines" in Lowenthal, 2003.
5. Although there are currently attempts to bring other countries, such as Spain and Germany, into the UK/USA alliance; as indicated in Todd & Bloch, 2003: 45.
6. For example, *R. v. Tessling*, 2004; *R. v. Buhay*, 2003; *R. v. Law*, 2002; *R. v. Wong*, 1990; *R. v. Dyment*, 1988.
7. Rawls supposes that a (virtual) committee of rational but not envious persons will exhibit mutual disinterest in a situation of moderate scarcity as they consider the concept of right: (1) general in form; (2) universal in application; (3) publicly recognized; (4) final authority; (5) prioritizes conflicting claims. Rawls claims that rational people will unanimously adopt his principles of justice if their reasoning is based on general considerations, without knowing anything about their own personal situation. Such personal knowledge might tempt them to select principles of justice that gave them unfair advantage - rigging the rules of the game. This procedure of reasoning without personal biases Rawls refers to as "The Veil of Ignorance;" As outlined in Rawls, 1999.
8. Although it should be noted that this may be in the process of changing after the Canadian Government's 2005-2006 National Defence Act Review, in which a CSE watchdog was proposed.
9. This list is indicative and not comprehensive.
10. The *Modernization of Investigative Techniques Act* (MITA), which was previously rejected by the House of Commons but is now back on the table, does not address the CSE.

## Bibliography


Alexander, Yonah and Michael S Swetnam, eds. (1999). Cyber Terrorism and Information Warfare. New York: Oceana Publications.

Alphabetical List of Countries. Internet World Stats. Retrieved 08 March 2007 from <http://www.internetworldstats.com/list2.htm>.

Ball, Kirstie and Frank Webster, eds. (2003). The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age. London: Pluto Press.

Berinato, Scott (2002). "The Truth About Cyberterrorism." CIO Insight (15 March 2002).

De Borchgrave, Arnaud et al., eds. (2001). Cyber Threats and Information Security: Meeting the 21st Century Challenge. Washington DC: CSIS Press.

Brown, Michael, eds. (2003). Grave New World: Security Challenges in the 21st Century. Washington DC: Georgetown University Press.

Castells, Manuel (2000). The Rise of the Network Society. Oxford: Blackwell.

Center for Strategic International Studies Press (1998). Cybercrime, Cyberterrorism, Cyberwarfare; Averting an Electronic Waterloo. Washington: CSIS Press.

Cordesman, Anthony H. and Justin G. Cordesman (2002). Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland. London: Praeger.

Cotler, Irwin (2002). "Terrorism, Security and Rights: The Dilemma of Democracies," in Mendes, Errol P. and Debra M. McAllister, eds.: 13-70. Between Crime and War: Terrorism, Democracy and the Constitution. Toronto: Thomson Carswell.

Cronin, Audrey Kurth (2003). "Behind the Curve: Globalization and International Terrorism." International Security 27: 38-58.

Denning, Dorothy (1999). "Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in Arquilla, John and David Ronfelt, eds.: 239-288. Networks and Netwar: The Future of Terror, Crime and Militancy. Washington DC: RAND.

Denning, Dorothy (2001). Is Cyber Terror Next? Social Sciences Research Council. Retrieved 08 March 2007 from <http://www.ssrc.org/sept11/essays/denning.htm>.

Galison, Peter and Martha Minow (2005). "Our Privacy, Ourselves in an Age of Technological Intrusions," in Ashby Wilson, Richard, ed.: 258-294. Human Rights and the War on Terror. New York: Cambridge University Press.

Goodman, S.E. (2007). "Cyberterrorism and Security Measures," in Kumar, Arvind et al, eds.: 43-54. Science and Technology to Counter Terrorism. Washington DC: The National Academies Press.

Green, Joshua (2002). "The Myth of Cyberterrorism." Washington Monthly (November 2002). Retrieved 08 March 2007 from <http://www.washingtonmonthly.com/features/2001/0211.green.html>.

Lesser, Ian O. et. al., eds. (1999). Countering the New Terrorism. Washington DC: RAND.

Libicki, Martin (1996) What is Information Warfare?. Washington DC: National Defense University.

Lowenthal, Mark M. (2003). Intelligence: From Secrets to Policy, 2nd Edition. Washington DC: CQ Press.

Mandel, M. (1982). "Discrediting the McDonald Commission." Canadian Forum (March 1982): 14-17.

Martin, Gus (2003). Understanding Terrorism: Challenges, Perspectives and Issues. London: Sage Publications.
Mendes, Errol P. and Debra M. McAllister, eds. (2002). Between Crime and War: Terrorism, Democracy and the Constitution. Toronto: Thomson Carswell.
Mitchell, Paul T. (2003). Small Navies and Network-centric Warfare: Is There a Role? Naval Warfare College. Retrieved 08 March 2007 from <http://www.nwc.navy.mil/press/Review/2003/Spring/art5-sp3.htm>.
Rawls, John (1999). A Theory of Justice. Cambridge: Harvard University Press.
Richard, Cleroux (1990). Official Secrets: The Story Behind the Canadian Security Intelligence Service. Montreal: McGraw-Hill.
Sloan, Elinor (2002). The Revolution in Military Affairs. Montreal: McGill-Queens University Press.
Sofaer, Abraham D. et al. (2001). The Transnational Dimension of Cyber Crime Terrorism. Stanford: Hoover Institution Press.
Stone, Martin (2007). "Canada Called Hotbed of Cyberterrorism." Newsbytes. Retrieved 01 February 2007 from <http://www.newsbytes.com/pubNews/00/146343.html>.
Todd, Paul and Jonathan Bloch (2003). Global Intelligence: The World's Secret Services Today. New York: Zed Books.
Toffler, Alvin (1980). The Third Wave. New York: William Morrow & Co.
Weissman, Gabriel (2005). "Cyberterrorism: The Sum of All Fears?" Studies in Conflict & Terrorism 25: 129-149.
Westin, Alan F. (1967). Privacy and Freedom. New York: Atheneum.

## Legislation and Governmental Documents

Anti-Terrorism Act
Canadian Charter of Rights and Freedoms
Canadian Security Intelligence Service Act
Competition Act
Convention on Cyber-Crime (23 November 2001). ETS No. 185, Council of Europe.
Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, Retrieved 08 April 2007 from <http://www.ocipep-bpiepc.gc.ca/critical/nciap/synopsis_e.asp>.
Government of Canada (January 1999). The Report of the Special Senate Committee on Security and Intelligence.
International Convention for the Suppression of Acts of Nuclear Terrorism (13 April 2005). UN Resolution 59/290, United Nations.
International Convention for the Suppression of Terrorist Bombings (25 November 1997). UN Resolution 52/653, United Nations.
International Convention for the Suppression of the Financing of Terrorism (09 December 1999). UN Resolution 54/109, United Nations.
Modernization of Investigative Techniques Act
Personal Information Protection and Electronic Documents Act
Rome Statute of the International Criminal Court (17 July 1998). United Nations.
Royal Canadian Mounted Police Act
Statute of the International Court of Justice (14 April 1978). United Nations.
Telecommunications Act

United Nations Security Council Resolution 1373 (28 September 2001). United Nations.
United Nations Security Council Resolution 1377 (12 November 2001). United Nations.
United States Congress: House Committee on Armed Services (2000). Terrorist Threats to the United States: Hearing Before the Special Oversight Panel on Terrorist of the Committee on Armed Services, 23 May 2000. Washington DC: U.S. G.P.O.
United States Congress: House Committee on Government Reform: Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census (2003). Cyber security: the challenges facing our nation in critical infrastructure protection: hearing before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census of the Committee on Government Reform. Washington: U.S. G.P.O.
United States Joint Staff (1999). Joint Strategy Review 1999. Washington DC: The Joint Staff.

## Case Law

Dagenais v. Canadian Broadcasting Corp., [1994] 3 S.C.R. 835.
R. v. Buhay, [2003] 1 S.C.R. 30.
R. v. Dyment, [1988] 2 S.C.R. 417.
R. v. Edwards, [1996] 1 S.C.R. 128.
R. v. Golden, [2001] 3 S.C.R. 679.
R. v. Law, [2002] 1 S.C.R. 10.
R. v. McKinlay Transport Ltd., [1990] 1 S.C.R. 627.
R. v. Mellenthin, [1992] 3 S.C.R. 615.
R. v. M. (M.R.), [1998] 3 S.C.R. 393.
R. v. Oakes, [1986] 1 S.C.R. 103.
R. v. S.A.B., [2003] 2 S.C.R. 678 .
R. v. Silveira, [1995] 2 S.C.R. 297.
R. v. Stillman, [1997] 1 S.C.R. 607.
R. v. Tessling, [2004] 3 S.C.R. 67.
R. v. Wiley, [1993] 3 S.C.R. 263.
R. v. Wong, [1990] 3 S.C.R. 36.
Weatherall v. Canada (Attorney General), [1993] 2 S.C.R. 872.

## ABOUT THE AUTHOR:

***Eliot Che*** **is a Researcher at the Carleton University in Canada. He specializes on Counter-terrorism, information technology, privacy, surveillance, and terrorism.**

## RIEAS PUBLICATIONS:

**RIEAS** welcomes short commentaries from young researchers/analysts for our web site **(about 700 words),** but we are also willing to consider publishing short papers (**about 5000 words**) in the English language as part of our publication policy. The topics that we are interested in are: transatlantic relations, intelligence studies, Mediterranean and Balkan issues, Middle East Affairs, European and NATO security, Greek foreign and defense policy as well as Russian Politics and Turkish domestic politics.

**Marco Rosa**, "Cooperation Between European Armed Forces: What Consequences on National Security and Defense Cultures?", RIEAS: Research Paper No. 112, (August 2007).

**Mahjoob Zweiri and Mohammed Zahid**, "Religion, Ethnicity and Identity Politics in the Persian Gulf", RIEAS: Research Paper, No. 111, (July 2007).

**Florina Cristiana (Cris) Matei**, "Shaping Intelligence as a Profession in Romania: Reforming Intelligence Education After 1989", RIEAS: Research Paper, No. 110, (June 2007).

**Yannis A. Stivacthis**, "Understanding Anti-Americanism", RIEAS: Research Paper, No. 109, (May 2007).

**Mahjoob Zweiri and Mohammed Zahid,** "The Victory of Al Wefaq: The Rise of Shiite Politics in Bahrain", RIEAS: Research Paper, No. 108, (April 2007).

**Koturovic Darja**, "Serbian Foreign and Security Policy in 21st Century", RIEAS: Research Paper, No.107, (January 2007).

**Michelle Buckley,** "China and the United States", RIEAS: Research Paper, No. 106, (December 2006).

**Aya Burweila,** "Libya After Rapprochement: Implications on energy security", RIEAS: Research Paper, No.105, (November 2006).

**Hamilton Bean,** "Tradecraft Versus Science:" Intelligence Analysis and Outsourcing", RIEAS: Research Paper, No. 104, (November 2006).

**Andrew Liaropoulos, and Ioannis Konstantopoulos,** "Selected Bibliography on Intelligence", RIEAS: Research Paper, No. 102, (November 2006).

**Maria Alvanou,** "European Responses to Islamic Terrorism Threat: The Italian Case Study", RIEAS: Research Paper, No. 101, (October 2006).

**Andrew Liaropoulos**, (2006), "A (R)evolution in Intelligence Affairs? In Search of a New Paradigm", RIEAS: Research Paper. No. 100 (June 2006).

**Andrea K. Riemer**, (2006), "Geopolitics of Oil: Strategic and Operative Causes for the Iraq Intervention", RIEAS: Research Paper. No.99, (February).

**Andrea K. Riemer**, (2005), "Nation Building: Concepts, Definitions, Strategic Challenges and Options", RIEAS: Research Paper. No.98, (November).

**Pine Roehrs,** (2005), "Weak States and Implications for Regional Security: A Case Study of Georgian Instability and Caspian Regional Insecurity", RIEAS: Research Paper, No. 97, (October).

**Vassiliki N. Koutrakou**, (2005), "Insights into the Post 2000 WTO- Inspired Development Policies Sponsored by the G 8 and the European Union", RIEAS: Research Paper, No.96, (June).

**Andrea K. Riemer**, (2005), "The Kurds: Between Ankara and Baghdad in Search of Independence", RIEAS: Research Paper, No. 95, (May).

**Yannis A. Stivachtis**, (2005), "The European Security and Defense Policy (ESDP): Evolution and Challenges", RIEAS: Research Paper, No. 94, (March).

**John M. Nomikos**, (2004), "Greek Intelligence Service (NIS-EYP) and Post 9 / 11 Challenges", The Journal of Intelligence History, Germany.

**Andrea K. Riemer**, (2004), "Turkey: In a European-U.S. Crunch?" RIEAS: Research Paper, No.93, (November).

**John M. Nomikos**, (2004), "European Union Intelligence Service: A Necessary Institution for Confronting Terrorism?" RIEAS: Research Paper, No.92, (April).