Geneva Centre for Security Policy
Centre de Politique de Sécurité, Genève
Genfer Zentrum für Sicherheitspolitik

Program on the Geopolitical Implications of Globalization and Transnational Security

GCSP Policy Brief Series

The GCSP policy brief series publishes papers in order to assess policy challenges, dilemmas, and policy recommendations in *all aspects* of transnational security and globalization. The series was created and is edited by Dr. Nayef R.F. Al-Rodhan, Senior Scholar in Geostrategy and Director of the Program on the Geopolitical Implications of Globalization and Transnational Security.

GCSP Policy Brief No. 1
Information Technology, Terrorism, and Global Security

Mr. Marc Finaud
Faculty Member
Geneva Centre for Security Policy

Marc Finaud, born in France in 1953, holds a Certificate of Proficiency in English from the University of Cambridge, a Master's Degree in International Law from the University of Aix-en-Provence, and is a Graduate of the Paris Institute of Political Studies. Since 2004, he has been a faculty member of the Geneva Centre for Security Policy seconded from the French Government. As a diplomat, he was posted in Leningrad at the CSCE; the Staff of the Secretary-General, Warsaw; Geneva (Conference on Disarmament); the Information Department, Tel Aviv, and as Consul-General in Sydney. He was also a lecturer on arms control and disarmament at the Marne-la-Vallée University.

June 19, 2006

To comment please, email Bethany Webster at b.webster@gcsp.ch.

Avenue de la Paix 7bis
P.O. Box 1295
CH-1211 Geneva 1

Telephone +41 22 906 83 17
Telefax +41 22 906 16 49
www.gcsp.ch info@gcsp.ch

Abstract

The information technology (IT) revolution that the world has been experiencing over the last two decades has had a significant impact not only on the world economy but also on global security, and in particular on international terrorism. Indeed, IT advances have allowed terrorists to gain easy access to sensitive information, spread their ideology, recruit supporters or operatives, plan and carry out their operations, and conduct criminal activities. IT networks can also offer targets for terrorists who aim to disrupt or destroy critical infrastructure by launching cyber-attacks. But IT can also be exploited by governments as a counterterrorism and an intelligence tool: it permits the surveillance of potentially malicious groups, the detection of planned attacks, the mitigation of eventual attacks, and can facilitate the countering of ideological support for terrorism. Some progress has already been made in raising awareness of risks and levels of preparedness, but there is a need for more international cooperation and public-private partnership in harmonizing legislation, improving the security of cyberspace, and promoting better law enforcement.

Policy Challenges

The revolution in the field of information technology (IT) that the world has witnessed over the past two decades has accelerated and kept pace with the process of globalization. Developments in ICT have been characterized by increasingly greater speeds of data transmission, increased capacity for data storage, more mobility, and the integration of various functions. The results of this evolution on a global scale, especially in terms of economic impact, have exceeded most predictions. A 2002 forecast of the annual growth of world ICT spending (hardware, software, and services) for 2003-2007 was updated in 2005 from 8 percent to nearly 10 percent (over 12 percent for Europe, the Middle East, and Africa). This spending grew from $2.1 trillion in 2001 to $3 trillion in 2005 and is expected to reach $3.7 trillion in 2008 [Have these figures been adjusted to take into account the declining value of the dollar?]. Its share of world GDP reached 7.4 percent in 2001 and is now stable at around 7 percent.[1] ICT spending will total $15 trillion in the present decade, as compared to $6 trillion during the first 40 years of the existence of such technology.[2] Globally, Internet usage increased more than fourfold from 2000 to 2005,[3] with the total number of users exceeding one billion in 2005.[4] In spite of the "digital divide" between developed economies (with 300 secure e-commerce servers for every 1 million people) and developing nations (with only two secure e-commerce servers for every 1 million people), the latter have considerably increased their access to ICT: between 1980 and 2005, the number of telephone subscribers in developing countries increased thirty fold, reaching a world share of 60 percent, against 20 percent in 1980, thanks to their "leapfrogging" in mobile telephony.[5]

Developments on such a scale could not but have an impact on security, one of the conditions influencing how economies develop and what policies states implement. If the "new economy" is increasingly dependent on ICT, then ICT infrastructure can certainly be the target or conduit of hostile actions. Thus, in addition to being a major factor in terms of growth, ICT can also cause certain vulnerabilities. International terrorism has become one of the main challenges to global security. It is not surprising that this phenomenon used all the advances offered by IT to thrive, thus exacerbating challenges for decision-makers tasked with ensuring national security.

1. The IT revolution has helped the development of terrorism

a. *IT facilitates access to sensitive information of interest to terrorist groups*

Transparency is a fundamental element of any democratic society. With this comes the right of citizens to have access to information, with certain limitations on the grounds of national security. The widespread use of ICT has made the regulation of such access and related limitations more difficult to enforce. Moreover, the academic community, the force behind the initial development of information sharing through the Internet, at times overlooks the risk of the ill-intentioned use of this information. There are numerous websites that explain ways of producing explosives or weapons of mass destruction (WMD) in terms that are accessible to

people with an average level of expertise.[6] Even websites that are intended to warn and prepare people against the use of such explosives or weapons contain information that may be of direct interest to terrorists.[7] Aerial and satellite images and maps of critical infrastructure can also be found on the Internet. It was revealed in March 2006 that the names of thousands of covert CIA operatives are available in Internet databases.[8]

b. *IT allows terrorist groups to spread their ideology and facilitates recruitment*

Cyberspace experts now talk of a "virtual caliphate" of some 4,000 pro-Al-Qaeda websites, blogs, and chat rooms disseminating *jihadist* messages or propaganda.[9] These are used for training; recruitment; disseminating tactics, techniques, procedures; financing (through Internet pay sites); and garnering support. By spreading propaganda and showing videos of executions of hostages or successful strikes, the Internet contributes to the radicalization of young Muslims.[10]

c. *Terrorists use IT tools to plan and carry out operations*

The attackers of September 11, 2001, used the Internet to plan their operations by booking air tickets online and communicating with one other through Internet-based telephone services and chat rooms. It has also been reported that some terrorist groups use sophisticated technological devices such as optoelectronics, encrypted communications equipment, GPS systems, and remote electronic bomb detonators.[11] Al-Qaeda computers seized in Afghanistan contained models of dams and computer programs that could have been useful in attacks against such infrastructure.[12] Here again, law enforcement personnel are handicapped by the accessibility, versatility, speed, and transnational character of cyberspace, which allows almost total impunity.

d. *The possibility of computer attacks by terrorists against critical infrastructure or information networks is real*

Although it has not yet materialized and the possibility is debated by experts, one cannot disregard the risk that terrorist groups will use IT not only as a weapon but also as a target, e.g., by launching cyber-attacks against supervisory control and data acquisition (SCADA) systems and networks controlling sensitive infrastructure (air-traffic control systems, power grids, dams, industrial plants or nuclear installations, communications systems, financial services, etc.) or computers containing critical data. At this stage, this is more the domain of individual or organized "hackers, crackers, and hacktivists" acting on the basis of personal, economic, ideological, or criminal motives. But if the activity of these individuals is an natural by-product of an IT society, it is an increasingly worrying phenomenon. In 1988, only six incidents of hacking were reported to the Carnegie-Mellon University Computer Emergency Response Team (CERT); in 2001, this number reached 52,658.[13] In 2002, Computer Economics Inc. estimated the annual cost to the U.S. economy of computer virus and worm attacks to be $17 billion.[14] If terrorist networks acquire the necessary skills, opting for cyber-

attacks would be only a matter of strategic choice. Inferring from their past behavior, one can predict that they would not hesitate to use IT to target critical infrastructure if it allowed them to attain their objectives: massive fatalities and/or major disruption of economic, political, and social life in the targeted country, either independently or in conjunction with a physical attack, and subsequent widespread media coverage, .

e. *Terrorist groups and organized crime often use opportunities offered by IT*

International terrorists and organized criminal groups both use IT advances, such as encryption or anonymizer features on computers, and hire highly qualified hacking specialists of these systems who conduct their transnational operations without fear of detection.[15] Terrorist groups often conduct additional criminal activities of their own, such as money laundering, trafficking in drugs or human beings, credit card fraud, and selling counterfeit goods, in order to fund their organizations. Just like multinational corporations, terrorist groups capitalize on the advantages of Western societies (openness, IT development) and those of developing countries (legislative loopholes, weak law enforcement, corruption, cheap labor).[16] They use the Internet to produce forged identity documents for themselves, their operatives, or the people they smuggle into Western countries. They enjoy the flexibility of electronic fund transfers and covert banking. The challenge for governments is to increase the legal and technical obstacles standing in the way of those activities in order to make law enforcement more effective.

2. IT can be used by governments as a counterterrorism and intelligence instrument

In 2003, the United States[17] identified several areas where the use of IT was critical to the fight against terrorism: prevention, detection, and mitigation of terrorist attacks. In addition, IT can be of invaluable assistance in countering ideological support for terrorism.

a. *IT can help in the prevention of terrorist attacks*

Prior to any potential terrorist attack, law enforcement and intelligence services rely heavily on the surveillance of electronic communications and Internet use to identify significant patterns of behavior among suspected groups or individuals. Techniques have been developed for modeling the evolution of social groups in Web chat rooms, newsgroups, and bulletin boards, with the specific goal of detecting potentially harmful groups.[18] Progress made in information fusion, i.e., the aggregation of data from various sources, combined with powerful search engines, may enable well-equipped and properly trained specialists to uncover terrorist plans.

b. *IT can help security services detect an imminent terrorist attack*

The collection and rapid analysis of intelligence through electronic means can prove critical in detecting and attributing planned terrorist attacks. The failure of the US intelligence community to properly interpret the signals it received prior to the September 11 attacks was one of the main flaws criticized by the 9/11 Commission, which led to the reorganization of the

US intelligence architecture. On the other hand, excessive reliance by the US intelligence community on electronic signals prior to the invasion of Iraq, in light of subsequent revelations about the absence of WMD and the underestimated insurgency, was another failure.

c. *The use and protection of IT are crucial in mitigating and managing the consequences of a terrorist attack*

Emergency first responders (fire-fighters, police, paramedics, other health-care workers, etc.) need to be able to have confidence in the capacity of their IT systems to allow for their communications, coordination, and information sharing. For such agencies, the challenge is to keep their systems up-to-date and protected from attacks, to train their staff adequately how to use such systems, and to share good practices and lessons learned with other agencies. Private businesses also need support from governments to increase their resilience to terrorist attacks.[19]

d. *The use of IT is necessary to raise awareness of risks and to counter ideological support for terrorism*

Governments can take advantage of the vast spectrum of opportunities offered by the digital revolution to increase knowledge and awareness among the public of the terrorist risk. They can use official websites or create dedicated websites to publicize information about threats, encourage the public to report incidents, and engage the various communities of stakeholders (academia, the business world, civil society). Governments can also seek allies among the same groups targeted by terrorists for recruitment or support as a part of their own counterterrorism policy. Indeed, *jihadism* is more an internal struggle among extremist and moderate Muslims than a clash of civilizations between the West and the Muslim world.[20]

Responses

Reminiscent of the arms race during the Cold War, the world is now witnessing a similar contest between terrorist groups on the one hand, which try to exploit the potential of IT for their own purposes, and governments and international organizations on the other hand, which try to harness the power of IT to prevent terrorist acts before they happen. The temptation exists to deal with this threat on a national basis, while it clearly requires international cooperation.

1. Until now, most efforts have focused on preventing cyber-attacks:

The 2003 US National Strategy to Secure Cyberspace, designed by the new Department of Homeland Security,[21] details a policy aimed at preventing cyber-attacks against critical US infrastructure, reducing vulnerabilities to attacks, and improving preparedness for possible attacks. The European Union adopted in 2005 a Framework Decision on Attacks against Information Systems,[22] which provides for harmonized penalties applicable to cyber-criminals and a 24/7 Network of operational points of contact for exchanging data on attacks against

information systems. Since 2001, Interpol's High Tech Crime Unit has been implementing an early-warning system consisting of national specialized contact officers for standardized police communication.[23]

2. The international community needs to improve IT-based counterterrorism tools and prevention through law enforcement cooperation

Law enforcement and intelligence agencies still have difficulties in successfully detecting, tracking, identifying, and neutralizing terrorist groups, which benefit from the anonymity of cyberspace. The IT industry is reluctant to let governments regulate the Internet or strengthen standards on its use, and companies fear for their image if they report incidents.[24] However, a public-private partnership, as part of a single national architecture, is required to agree on measures that would be both efficient and acceptable in terms of privacy, such as improving the resilience of Internet protocols, extending record-keeping rules for Internet service providers, or developing filtering systems for forged source addresses. The international harmonization of criminal legislation also appears to be indispensable in order to plug existing loopholes used by terrorist groups. The Council of Europe's 2001 Convention on Cyber Crime[25] was recommended as a model by the 2005 Interpol Conference on Cyber Crime,[26] but the progress made so far in this direction has been minimal. The Internet Governance Forum, to be convened in November 2006 under the auspices of the UN,[27] will have a heavy workload in this respect.

Dilemmas

Governments and decision-makers are confronted with the following dilemmas:

1) How to prevent the spread of information useful to terrorists and at the same time promote the dissemination of information needed for public awareness and preparedness;
2) How to reconcile some control of means of communication with freedom of speech, which can be abused to promote violence, racial hatred, or religious intolerance;
3) How to strike the proper balance between the need to preserve privacy and efficiency in counterterrorism; and
4) How to strike the right balance between electronic and human intelligence as a source of information in countering terrorism.

Implications

1) If governments want to reduce terrorists' access to sensitive information, they need to explain the risks and convince the public of what is necessary. A culture of vigilance must be part of the training of all staff involved in making information available.
2) Enacting or adapting legislation to make the spread of racial hatred or incitement to violence a criminal offense would impose new constraints on terrorist groups. The 2003 Additional Protocol to the Council of Europe's Convention on Cyber Crime[28]

offers a model, but there are still fundamental differences between the approaches taken by Europe and the US, with the latter being more reluctant to hinder freedom of speech.

3) If governments decide to reduce civil liberties in the name of the fight against terrorism, this needs to be publicly debated and decided on the basis of a broad consensus. This has been illustrated by recent debates in the United States about the wiretapping of private communications without a court order; in Britain and France about government demands on Internet service providers or telephone companies to keep records for a longer period; as well as by the transatlantic dispute over the ECHELON interception network.[29]
4) Increased recourse to electronic intelligence requires adequate investment in new technologies, research and development, and training. If human intelligence is to retain its importance, there should be investment in analysis capacity.

Future Trajectories/Scenarios

Future scenarios, based on such technological advances as the expansion of broadband Internet, 3G/4G mobile phones, multimedia messaging, wireless technology, will only exacerbate the existing race between terrorists and law enforcement officials. On the one hand, the more the global economy becomes dependent on IT, the more it becomes vulnerable. On the other hand, further technological advances may also result in progress in the surveillance and detection capacity of intelligence and law enforcement agencies.

Policy Recommendations

Governments should:

1) Adopt a national strategy, where such a strategy does not exist, for countering the use of IT by terrorists, based on a broad national consensus and distribution of tasks among stakeholders;
2) Encourage and invest in scientific research and industrial development of IT systems that are more resistant to terrorist use and facilitate law enforcement agencies to combat these illegal acts by implementing current legislation and providing these agencies in countries that do not have the means for acquiring and supporting them.
3) Harmonize anti-terrorism legislation on an international level, on the basis of Council of Europe conventions, in order to deprive terrorists of loopholes that can be exploited.
4) Cooperate with developing countries in designing adequate legislation on both terrorism and organized crime and in strengthening law enforcement capacities to combat both phenomena.

References

[1] "Digital Planet 2004 Update – The Global Information Economy", World Information Technology and Services Alliance (WITSA), October 2005, http://www.witsa.org/digitalplanet/DigitalPlanet2004Update_execsummary.pdf.
[2] J. Gantz, Chief Research Officer, IDC, "Information Technology: An Engine for Global Economic Growth", April 16, 2002, Microsoft, http://www.microsoft.com/presspass/features/2002/apr02/04-16glcqa.mspx.
[3] World Bank, "Information and Communication for Development 2006 – Global Trends and Policies", http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/282822-1141851022286/IC4D-Summary.pdf.
[4] http://www.internetworldstats.com/stats.htm.
[5] *Op. cit., note 3*, World Bank.
[6] See, for example, the website of the Federation of American Scientists: http://www.fas.org/nuke/intro/index.html.
[7] See the website of "WMD First Responders," which includes all the available literature in English on WMD risks and measures to take either in dissemination prevention or in case of attack: http://www.wmdfirstresponders.com/.
[8] http://www.chicagotribune.com/news/nationworld/chi-060311ciamain-story,1,123362.story?ctrack=1&cset=true.
[9] A. de Borchgrave, Director, Transnational Threats, Center for Strategic and International Studies (CSIS), "Evolving Counterterrorism Strategy", Subcommittee on International Terrorism and Nonproliferation, US House of Representatives, October 28, 2005, http://wwwc.house.gov/international_relations/109/bor092905.pdf.
[10] CENTCOM Senior Leaders Talking Points, February 1, 2006, http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&folder=2558&paper=2592.
[11] "Computer Attack and Cyber Terrorism – Vulnerabilities and Policy Issues for Congress", CRS Report, October 17, 2003, http://www.fas.org/irp/crs/RL32114.pdf.
[12] *Ibid*.
[13] E. Gelbstein and A. Kamal, "Information Insecurity – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security", United Nations ICT Task Force, September 2002, p. 17.
[14] *Ibid*.
[15] L. I. Shelley, "Organized Crime, Terrorism and Cybercrime", in A. Bryden, P. Fluri (eds.), *Security Sector Reform: Institutions, Society and Good Governance*, (Zürich: 2003), see http://www.american.edu/traccc/resources/publications/shelle31.pdf.
[16] *Ibid*.
[17] "Information Technology for Counterterrorism: Immediate Actions and Future Possibilities", http://bob.nap.edu/html/IT_counterterror/.
[18] http://www.cs.rpi.edu/news/stories/story-04152004a.html.
[19] A Resilience Benchmark Survey was conducted by the UK financial service tripartite authorities in London after the July 2005 attacks, showing that the IT systems of financial companies were resilient and that their recovery time was short, but that there was a need for a better understanding of interdependencies with suppliers and counterparties, as well as for guidance on good practices. See http://www.fsc.gov.uk/upload/public/Files/9/Web%20-%20Res%20Bench%20Report%2020051214.pdf.
[20] See, for instance, the initiative of Yusuf al-Qaradawi, a Qatar-based Egyptian religious scholar, to establish websites and networks promoting a cosmopolitan interpretation of Islam: Peter Mandaville, "Toward a Virtual Caliphate: Al-Qaeda is not the Only Muslim Group Harnessing the Power of Globalization", *YaleGlobal*, October 27, 2005, http://yaleglobal.yale.edu/display.article?id=6416.
[21] http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.
[22] http://register.consilium.eu.int/pdf/en/04/st15/st15010.en04.pdf.
[23] http://www.interpol.int/public/icpo/pressreleases/pr2003/pr200331.asp.
[24] H. N. Miller, "Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing", statement before the US Senate Committee on the Judiciary, March 28, 2000, http://www.itaa.org/eweb/upload/CyberAttacks3-2000.pdf.
[25] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
[26] http://www.interpol.int/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp.
[27] http://www.un.org/apps/news/story.asp?NewsID=17534&Cr=internet&Cr1=.
[28] http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.
[29] See the 2001 report of the European Parliament on ECHELON: http://www.fas.org/irp/program/process/rapport_echelon_en.pdf.

Program on the Geopolitical Implications of Globalization and Transnational Security

GCSP Policy Brief Series

The GCSP policy brief series publishes papers in order to assess policy challenges, dilemmas, and policy recommendations in *all aspects* of transnational security and globalization. The series was created and is edited by Dr. Nayef R.F. Al-Rodhan, Senior Scholar in Geostrategy and Director of the Program on the Geopolitical Implications of Globalization and Transnational Security.

Editorial of GCSP Policy Brief No. 1
Information Technology, Terrorism, and Global Security

Dr. Nayef R.F. Al-Rodhan
Senior Scholar in Geostrategy and
Director of the Program on the
Geopolitical Implications of Globalization
and Transnational Security
Geneva Centre for Security Policy

June 19, 2006

To comment, please email Bethany Webster at b.webster@gcsp.ch.

Avenue de la Paix 7bis
P.O. Box 1295
CH-1211 Geneva 1

Telephone +41 22 906 83 17
Telefax +41 22 906 16 49
www.gcsp.ch info@gcsp.ch

Review and Critique

The introduction of a new technology into a society can have a profound impact on its structure and development. Over the past fifteen years, we have seen the impact that the Internet has had on global society. Communication has taken on a new significance, as traditional means have given way to the era of Internet telephony, instant messaging, and 3G technology. While it is only natural that governments and political entities benefit from such technology, they also face new challenges as a result of it.

One of these challenges is the impact that such technology has on the ability of terrorists to recruit members, spread their ideologies, and plan and launch attacks around the world. New technologies provide clear advantages in the ease of communication. Unfortunately, this is the same ease in the case of peaceful purposes as for coordination in the terrorist domain. At the same time, however, technology also provides government and law enforcement agencies with the ability to monitor terrorist activities with greater awareness. So while the technology offers a global venue for terrorist groups, it also grants authorities the tools with which to combat illegal operations.

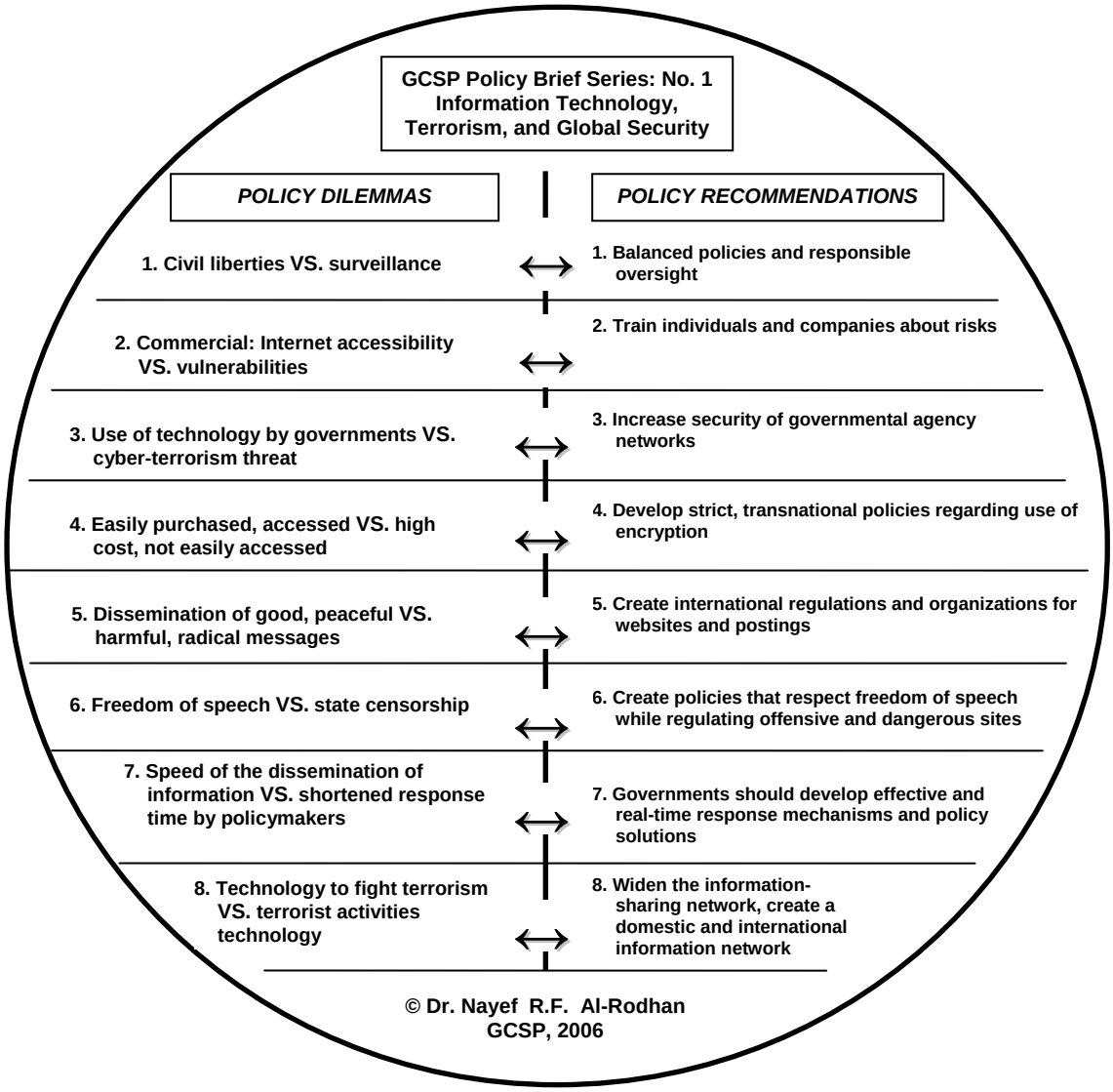
The era of cyber-crime is developing faster than most regulatory bodies are able to react. Mobile telephony provides a great opportunity for growth in both the private and public sectors. However, it also connects the world in a way that has never been the case previously. It allows for messages, both well-intentioned and not, to be transmitted in a matter of seconds. How are these challenges being dealt with and what are the current responses to them?

Marc Finaud outlines two major challenges posed by states with regard to information technology (IT) and terrorism.[1] The first is that "the IT revolution has helped the development of terrorism." Second, he argues that "IT can be used by governments as a counterterrorism and intelligence instrument." In terms of the development of terrorism, he convincingly argues that the Internet provides an easily accessible resource for distributing sensitive information, such as how to construct bombs or purchase weapons. In addition, the use of computers as a recruitment tool and as a means of attacking targets through cyberspace is a real threat, which Mr. Finaud gives due credibility. He provides sound justification for the use of IT in countering terrorism and concludes that proper utilization of such tools can be a means of properly managing such threats.

The policy brief addresses a vital part of the globalization debate. As the Internet connects communities and countries, this connectivity opens itself up to information sharing, which can lead to positive developments but can also open the door for dissemination of harmful information and accessibility to government systems. When utilized properly, this technology also provides solutions to dealing with such issues.

Dilemmas and Recommendations

The introduction of new technologies presents both challenges and opportunities for states. The development of new policies concerning use of the Internet and other technologies by terrorists is fiercely debated in policy and academic circles. Government agencies and states will need such policies in the years to come to properly handle these challenges and dilemmas. How best to regulate these matters has been widely discussed in recent years, yet detemining the best way to move forward, especially in the entire international system, is much more difficult. This is an extremely important task since it will require transnational cooperation and cross-border regulations. Presented here are eight dilemmas in this area and corresponding recommendations for appropriate policy responses.



The policy dilemmas and recommendations that appear here are clearly issues that states are currently facing in terms of information technology and the utilization of such technologies by terrorists. The most noteworthy of these dilemmas and recommendations involve balancing the proper level of privacy with civil liberties. In order to solve this dilemma, states must ensure a balance of policies and monitoring that is transparent enough to guarantee the

preservation of civil liberties. One other major dilemma facing states is the lack of coherence in the security of systems both on the commercial and governmental levels. For industries that operate within security-sensitive areas such as airlines, measures should be implemented that make certain that a level of security exists that can prevent a breach.

In addition, states face issues of balancing freedom of speech and state censorship. Policies must be developed that respect this fundamental freedom while regulating offensive and dangerous sites. This is also important in the monitoring of good, peaceful messages versus harmful and radical messages. States must create international regulations and organizations that can monitor the creation of websites and the information traffic that passes through them. A widening of the information-sharing network is also key in utilizing technology as a means of fighting terrorism, in the form of cyber-crime, as well as in other cases.

Finally, states and policy-makers must find a way to solve problems related to the speed in which information is spread, which leads to shortened response times. The development of effective and real-time response mechanisms and policy solutions by governments is the most efficient way to move forward in this area. Without it, shortened response times can be a crucial flaw in any response that is developed.

Conclusion

The international system greatly benefits from the technological advances that the Internet and other new information tools provide. The connectivity made possible by these developments in technology brings us closer to those whose interests contribute to global security and stability, as well as to those whose interests do not. An important challenge is how to encourage states to create harsher penalties for the misuse of this technology, as well as to provide incentives for furthering international cooperation in combating this phenomenon.

References

[1] For the brief in its entirety, please see the policy brief series as a part of the Geneva Centre for Security Policy's Program on the Geopolitical Implications of Globalization and Transnational Security at http://www.gcsp.ch/e/publications/Globalisation/index.htm.