GCSP | 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.

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.

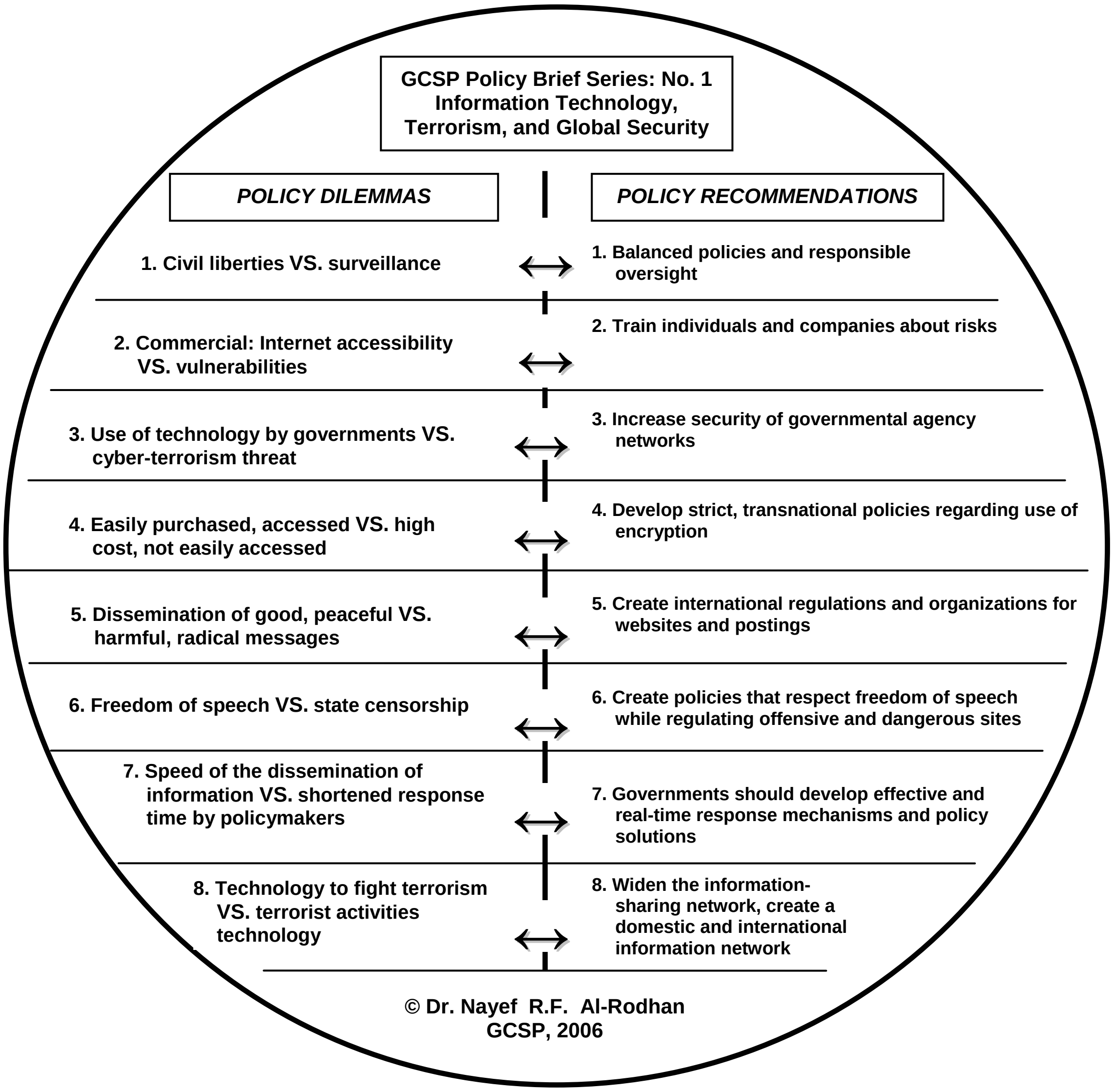
The era of cyber-crime is developing faster than most regulatory bodies are able to react. Mobile telephony provides a great opportunity for growth in both the private and public sectors. However, it also connects the world in a way that has never been the case previously. It allows for messages, both 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 determining 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.



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

POLICY DILEMMAS		*POLICY RECOMMENDATIONS*
1. Civil liberties VS. surveillance	⟷	1. Balanced policies and responsible oversight
2. Commercial: Internet accessibility VS. vulnerabilities	⟷	2. Train individuals and companies about risks
3. Use of technology by governments VS. cyber-terrorism threat	⟷	3. Increase security of governmental agency networks
4. Easily purchased, accessed VS. high cost, not easily accessed	⟷	4. Develop strict, transnational policies regarding use of encryption
5. Dissemination of good, peaceful VS. harmful, radical messages	⟷	5. Create international regulations and organizations for websites and postings
6. Freedom of speech VS. state censorship	⟷	6. Create policies that respect freedom of speech while regulating offensive and dangerous sites
7. Speed of the dissemination of information VS. shortened response time by policymakers	⟷	7. Governments should develop effective and real-time response mechanisms and policy solutions
8. Technology to fight terrorism VS. terrorist activities technology	⟷	8. Widen the information-sharing network, create a domestic and international information network

© Dr. Nayef R.F. Al-Rodhan
GCSP, 2006

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.