Making global cyberspace more secure...

Security is becoming an increasingly important issue in the international landscape of cyberspace. Government, industry, and private citizens have become progressively more dependent on the Internet for information storage, data exchange, electronic commerce, social networking, gaming, electronic voting, banking, and professional advancement. With developments in technology and the increasing interconnectedness of global computer networks, the prevalence of information system bugs and vulnerabilities is growing and cyber threats are becoming more sophisticated, more diverse, more malicious, more effective, more affordable, and more readily available to hackers, organized criminals, rogue nations, and terrorists.

This study examines approximately seventy international, regional, non-governmental, and private-public organizations with varying degrees of commitment to developing an ecosystem of safety and security in cyberspace. These organizations have focused their efforts on local and regional policy initiatives, international harmonization of laws, basic research and technological innovation, law enforcement, education and training, incident response, and propagation of secure ICTs. But are they doing it well? Are these organizations presenting practical, innovative, collaborative, and sustainable solutions to address cyberspace’s security issues?

An initial study on the emergence of organizations working to secure cyberspace concluded in 2006 that, although many international initiatives were well underway, few metrics had been made publicly available to provide positive answers to these questions. Two years later, though the landscape of cyber security has grown and evolved in many ways, organizations are still not producing readily available standardized metrics on the progress of their efforts. This recurring challenge is discussed in more detail below, following a brief analysis of new and existing organizations emerging in the international realm of cyber security.

Further Analysis of Recent Advances in Cyber Security

International intergovernmental organizations like the United Nations (UN) and the North American Treaty Organization (NATO) are pursuing collaborative solutions to the various challenges presented by malicious online activity. The UN, primarily through the work of the International Telecommunication Union (ITU), has established subcommittees and working parties to address the security...
challenges facing today’s information society. Such organizations include the International Telecommunication Union’s Telecommunication Development Sector (ITU-D) and Corporate Strategy Division (CSD), as well as other affiliated organizations like the United Nations Office on Drugs and Crime (UNODC). In addition, the Organisation for Economic Co-operation and Development (OECD)’s Working Party on Information Security and Privacy (WPISP) has provided ongoing support to the security of cyberspace by advancing education and information sharing throughout member countries. Through the Group of Eight’s (G8) 24/7 Network of Contacts for High-Tech Crime and the NATO Computer Incident Response Capability-Technical Centre (NCIRC-TC), constituent nations now have central contacts for cybercrime-related incidents. In addition, INTERPOL regional working parties provide cybercrime law enforcement training and educational opportunities in various regions around the world.

Regional intergovernmental organizations are also contributing to the global effort to secure cyberspace. The European Union (EU) Parliament has issued numerous cyber security declarations, resolutions, and communications, while the Council of Europe (COE) established one of the most widely recognized precedents in agreement on international cyber security policy—the Convention on Cybercrime. Other organizations throughout Europe are also active in addressing the challenges of cyber security. Such organizations include the Organization for Security and Co-operation in Europe (OSCE)’s Action against Terrorism Unit (ATU), the European Telecommunications Standards Institute (ETSI), the European Committee for Standardization (CEN), and the Information and Communications Technologies Standards Board (ICTSB). Incident response for cyber attacks in Europe has been coordinated primarily by the European Task Force on Computer Security Incident Response Teams (TF-CSIRT), and Europol’s High-Tech Crime Centre has released ongoing threat assessments and other comprehensive reports on regional cybercrime.

The Asia-Pacific region is also making progress in information security and cybercrime prevention. The Asia Pacific Economic Cooperation (APEC)’s Telecommunications and Information Working Group (TEL), through the work of the Security and Prosperity Steering Group (SPSG), issued the Shanghai Declaration in 2002 and has since hosted various conferences and workshops on network security and cyber terrorism. The Association of Southeast Asian Nations (ASEAN)’s Regional Forum (ARF) and Telecommunications and IT Ministers (TELMIN) have focused on promoting cooperation and harmonization of security policies, as well as capacity-building and Computer Emergency Response Team (CERT) cooperation throughout the Asia-Pacific region. In addition, the Asia-Pacific Telecommunity (APT), the United Nations Economic and Social Commission for Asia and the Pacific (UN ESCAP), and China-Japan-Korea (CJK) have contributed in the areas of network security and electronic commerce. The Asia Pacific Computer Emergency Response Team (APCERT) has now taken an active role in coordinating CSIRTs throughout the region.