Balancing Liberty, Stability, and Security

just attended the Fourth International Forum “Partnership of State Authorities, Civil Society, and the Business Community in Ensuring Information Security and Combating Terrorism” sponsored by the Security Council of the Russian Federation, Moscow State University, and the Internet Corporation for Assigned Names and Numbers. Attendance at the forum by high-level Russian and US dignitaries signaled a willingness of the two countries to explore common ground in addressing the governance of cyberspace (www.nytimes.com/2010/04/16/science/16cyber.html).

A central theme at the forum was that terrorists and criminals have the ability to degrade the stability and security of cyber ecosystems, which in turn can have calculated or unintended effects outside of cyberspace. For example, a terrorist organization can reach out to disaffected members of society, give them a sense of identity and a new set of values, and press these new recruits into committing acts ranging from sabotaging air traffic control systems to disabling a political leader’s Web-addressable pacemaker. However, this isn’t news to many of us: threats to cyber ecosystems were discussed long before the Internet went public (see, for instance, ARPA Network Working Group RFC 602 dated December 1973; www.faqs.org/rfcs/rfc602.html).

Attribution of malefactors’ acts in cyberspace was another hot-button issue at the forum. To prosecute in a court of law, attribution must be made to the individual who committed the crime. For military responses, of which going to war is the most violent, the standard of evidence isn’t as strict. But military responses, along with deterrence and operational arms control measures pertaining to offensive cyber weapons—another important theme of the forum—require reliable all-source intelligence to be workable (www.technologyreview.com/computing/25060/).

Several proposals attempted to make attribution a “solvable” problem: providing for strong identification of the users themselves rather than just strong identification of user terminals; curtailing civil, political, and cultural liberties; and making all “cyber footprints” (such as blog postings, email, instant messages, and Web content) available for examination by government authorities. But none of these proposals made sense—we must be careful not to adopt a Manichean view of cyberspace (that is, that it can be partitioned into good and evil). Any cyber ecosystem can serve as a dark network for criminals and terrorists to use. Today, it isn’t technically or economically feasible to effectively monitor all activity on our international cyber–social ecosystem (the Internet). What protection of rights will be afforded to law-abiding people who unwittingly share ecosystems with criminals or terrorists? Steve Bellovin makes a convincing argument that the proposals revolving around attribution, some of which are Draconian, are impossible to achieve as long as current operating systems can be compromised (“Identity and Security,” IEEE Security & Privacy, vol. 8, no. 2, 2010, p. 88).

Regardless of your view on the merits of curtailing liberties in the name of maintaining stability and security, practical issues must be addressed, such as the fact that an individual’s cyber footprints can cross multiple legal jurisdictions. We need to respect nations’ sovereign rights and their sensitivities to disclosing data or cooperating with other nations—one of the points Fred Schneider made about managing the tension between accountability and anonymity (“Accountability for Perfection,” vol. 7, no. 2, 2009, pp. 3–4).

A key nontechnical enabler for thwarting the commission of crimes and acts of terrorism is cooperation among nations, between the public and private sectors, and within the private sector. Until we can make significant progress in fostering trust to realize the requisite level of cooperation, in tandem with applying workable technical solutions, criminals and terrorists will continue to find safe haven for destabilizing cyberspace and making it a dangerous place to operate.