The Current State and Future Landscape of Cybersecurity: A View from Russia

Presentation Summary

Igor Kotenko, Ph.D.

The first part of Dr. Kotenko's presentation provides a broad survey of the current and future state of information and communication technologies (ICT) as well as the current and emerging security issues related to ICT. The second area of his discussion outlines Russia's policy response to IT security. In the final section, he shares some of his thoughts on international collaboration in the area of cyberspace security.

In the first part of his talk, Dr. Kotenko discusses the trends defining the future of ICT as follows:

- a worldwide broadband network based on fiber optics, communication satellites, cellular and microwave communication;
- increasing availability and accessibility of "anytime, anywhere" face-to-face, voice-to-voice, person-to-data and data-to-data communication systems;
- the 'Internet of things': the ubiquitous availability of computers will facilitate automated control and make continuous performance monitoring and evaluation of physical systems routine; and
- a rapid increase in the number of homes with integrated systems (and a consequent rise in smart and smarter integrated homes) with the ability to plug into the global communications network at increased speeds.

He also briefly outlines some of the common computer attack trends:

- increasing level of automation and penetration speed of attack tools;
- increasing sophistication of attacks;
- increasing speed of 'vulnerabilities discovery';
- exploitation of global internet security policy gaps; and
- increasing number of entities (countries included) with the capacity to develop cyberweapons.

Dr. Kotenko points out that modern and future malicious software have what he calls "key peculiarities" that pose serious challenges for crafting appropriate cybersecurity policy strategies and responses. Among those malicious software features are:

- a flexible control system – minimizes the risks of successful detection and disinfection;
- a stage-by-stage infection scheme – allows the maximum extent of invisibility up to the final destructive stages (e.g., up to the execution of the module implementing a viral functionality);
- a module-based scheme of the update process – provides functional and structural variability to the forming mixed (mashup) malicious software;
- effective mechanisms of concealing presence from the attacked host (these include mechanisms focused on the active stage of the malware life cycle);
- presence of active mechanisms for counteracting against the host's anti-malware software;
- use of cryptographic algorithms; and
- use of cloud computing.

The ICT revolution continues to pose challenges because the Internet was not initially designed to be a critical part of the economic infrastructure. The current and emerging problems and concerns stemming from its pervasive use arose from the unanticipated trajectory of ICT development on a global basis. Dr.Kotenko raises some of these issues, emphasizing that these have serious implications for national security:

- the Internet will triple the number of people now connected, from one billion to three billion in the next 3-5 years;
- there will be additions of billions – perhaps even hundreds of billions – of devices in the virtual globe (e.g., sensors, tags, micro-controllers);
- net-delivered services will continue to reshape the world;
- user-generated content is leading to a massive increase in the creative flow of content and processes;
- there will be increasing pressure to address the need to balance between the perceived need for control with the creativity that spawns innovation (and profit);
- there is a need to examine the question of whether the future is going the way of tethered appliances or generative technology;
- current architectures are open to security breaches, privacy invasion and identity theft; and
- criminals and terrorists will have at least the same access to the Internet as most people, and in the future they will be better educated, more insidious and will use the newest technologies.

The future of the Internet is one of great complexity in information technologies and systems. The key is to have collaborative end-to-end security and trust in highly complex networks and services. Dr. Kotenko asserts that non-functional requirements such as trustworthiness should be a part of the design and construction of future systems. He defines trustworthy ICT as technologies that are secure, reliable and resilient, can survive attacks, guarantee a desired level of service, protect user data and privacy, and provide usable and trusted tools to support the user.

In ending the first part of his presentation, Dr. Kotenko briefly mentions what he considers to be one of the most important and intriguing direction of current research in the area of cybersecurity:

the creation of auto-adaptive, survivable, self-generative systems. These systems have at least three key features: provide 100 percent critical functions at all times in spite of attacks; able to learn own vulnerabilities to improve survivability over time; and able to regenerate service after attack.

His discussion of Russia's response to growing cybersecurity concerns focuses on two official documents: the "National Security Strategy of the Russian Federation to 2020" (Presidential Decree No. 537, issued in May 12, 2009), and the "Strategy for Developing an Information Society in Russia" (authorized on February 7, 2008). The first document is a provision in the "Organizational" section (Section V) of the national security strategy subtitled "Legal-normative and informational foundations of the realization of the given strategy." It decrees that in order for Russia to develop a "system of Situational Centres" in the intermediate term, "it will be necessary to overcome technological lag in the most important areas of IT, telecommunications, and interconnectivity, which determine the state of national security." The provision also calls for Russia to "develop and introduce technologies of information security into systems of government and military administration, systems of management of ecologically dangerous products and critically important sites, and to create conditions for the harmonization of the national information infrastructure with global information networks and systems."

The second document outlines the steps for Russia to transform itself into one of the world's leaders in "post-industrial development and significantly bolster its information security" and aims to see Russia's share of ICT-based production increase to at least eight percent of total national exports by 2015. This is in part Russia's initiative that articulates its support for the two phases of the World Summit on the Information Society (WSIS) in Geneva (2003) and Tunis (2005), as well as its approval of the Okinawa Charter on Global Information Society that was signed by the G8 leaders on the occasion of the G8 Summit in Kyushu-Okinawa in 2000. The charter aims at "integrating efforts to bridge the digital divide into a broader international approach."[1] Special attention is given to the international negotiating processes revolving around three aspects: military-political (including informational and psychological) security, cybercrime and cyberterrorism.

In the third and final part of his presentation, Dr. Kotenko shares his thoughts on cyberspace security as an emerging area for international collaborative research. He stresses that in response to the economic loss and destabilization on the global scale caused by growing cyberattacks, governments and the professional communities must increase collaborative efforts now and in the future. According to him, the bottom line of these efforts must be the development of mutual trust between specialists that he hopes will lead to the development of mutual trust between governments around the world.

Notes

[1] Alfredo M. Ronchi, *EČulture: Cultural Content in the Digital Age* (Google eBook, 2009): xvi.