United Nations

General Assembly

12 April 2014

Sixty-eighth Session
Agenda item 94

Resolution #1

Development of a Comprehensive International Cooperative Framework to Ensure Global Cybersecurity

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011 and 67/27 of 3 December 2012 on developments with respect to information and communication technologies (ICTs) in the context of international security,

Reaffirming its resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on combating the criminal misuse of ICTs, 57/239 of 20 December 2002 on the creation of a global culture of cybersecurity, and 58/199 of 23 December 2003 and 64/211 of 21 December 2009 on the creation of a global culture of cybersecurity and the protection and taking stock of national efforts to protect critical information infrastructures, *and stressing* that a robust culture of cybersecurity among all States must be vigorously promoted and implemented to ensure confidence and security in the global use of ICTs,

Noting that increased dependence on ICTs by the world's population and increased connectivity of critical infrastructures have made cybersecurity essential to the functioning of a modern State, and thus cybersecurity must be an intrinsic part of every State's national security planning,

Expressing grave concern that cyber threats are rapidly on the rise internationally with cybercrime victimization rates (particularly for online credit card fraud, identity theft, "phishing" and other unauthorized ICT access) significantly higher than for conventional forms of crime, making such cyber threats to individuals and State ICT infrastructures one of the most serious challenges of the 21st century, which could substantially adversely affect State and international peace and security,

Emphasizing that it is necessary to prevent the use of ICTs for criminal or terrorist purposes in order to maintain the integrity of information delivered over ICTs and the integrity of private and State ICT infrastructures,

Highlighting the need for enhanced coordination and cooperation among States in combating the criminal misuse of ICTs and in implementing national cybersecurity measures,

Endorsing the work of relevant regional and international organizations with respect to assisting States in enhancing their cybersecurity measures and in fostering international cooperation in such matters, such as the United Nations Office on Drugs and Crime (UNODC)'s cybercrime studies and technical and capacity-building assistance to States; the United

Nations Institute for Disarmament Research (UNIDR); the International Telecommunication Union (ITU)'s cybersecurity initiatives, particularly its Global Cybersecurity Agenda; the Internet Governance Forum (IGF); the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence; the Association of Southeast Asian Nations Regional Forum (ARF), the International Multilateral Partnership Against Cyber Threats (IMPACT), and the Forum for Incident Response and Security Teams (FIRST), *but concerned* that such international efforts are sometimes fragmented, and participation is often limited since it is voluntary and there has not been a broader recognition until now of the global need for all States to participate in some minimum cybersecurity measures and hopefully more in the future after further consensus is reached with respect to additional multilateral collaborative confidence, security and capacity-building measures, *and recommending* that a more uniform international framework is necessary to achieve an effective global culture of cybersecurity,

Recognizing that gaps in access to and use of ICTs by certain States can inhibit the effectiveness of international cooperation in combating criminal use of ICTs and in furthering a global culture of cybersecurity, *and exhorting* the need for enhanced efforts to close that digital divide by facilitating the transfer of ICTs, cybersecurity best practices and training and similar capacity-building measures to developing countries,

Welcoming the productive studies conducted in 2009-10 and 2012-13 by two different groups of governmental experts composed of highly qualified ICT professionals from States representing geographically diverse interests, *and embracing* the assessments and recommendations contained in the two reports to the Secretary-General of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,

1. *Declares* that international law, and particularly international human rights law, international law of armed conflict and the Charter of the United Nations, including existing universally recognized norms of behaviour governing international relations among States, apply to all activities in cyberspace. All activities in cyberspace by States and non-State actors within the jurisdiction of each State shall be governed by such international laws and norms;

2. *Determines* that State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory;

3. *Establishes* the United Nations Institute for Cybersecurity (UNIC), a unifying international agency to coordinate the efforts of other regional and international entities (such as UNODC, UNIDR, ITU, IGF, NATO and ARF), and to assist States in implementing the requirements of this resolution. The UNIC will also, after further collaborative input and consensus from States, formulate and develop the following: (a) common understandings among States about further norms, codes of conduct and standards for use of ICTs by States and State behaviour towards cybersecurity activities, (b) additional confidence, transparency, security and capacity-building measures in order to maintain peace and security in cyberspace, (c) further legislative and regulatory frameworks for States' international responsibilities for their acts or omissions in cyberspace as outlined in paragraph 7 below, (d) a framework for accurately determining the attribution of cyber-attacks to States or their proxies, and (e) methodologies for encouraging States' implementation of UNIC's common rules and guidelines;

4. *Requires* each State to enact by 31 December 2015 laws prohibiting the use of ICTs (a) for criminal or terrorist purposes, including without limitation the use of ICTs to carry out hostile events or acts of aggression, and (b) to attack, disable or otherwise harm hospitals, schools, water facilities, electrical and gas power networks and/or financial systems. States shall also cooperate with UNIC and other States in combating criminal and terrorist activities that use ICTs;

5. *Finds* that since actors who maliciously use ICTs exploit vulnerabilities in systems where ICT security or the

related legal framework is not as strong due to disparities in national laws and practices, there is a pressing need for a minimum level of harmonization among States. Accordingly, *further instructs* each State to commit to harmonize its national legislation and enforcement practices with other States in the following areas under UNIC's guidance: (a) confirming general principles of availability, confidentiality, competitiveness, integrity and authenticity of data and networks, privacy and protection of intellectual property rights; (b) development of international model provisions to criminalize "core" cybercrime offenses in order to eliminate safe havens; (c) development of international model provisions to implement effective investigative powers to prevent, suppress and prosecute crimes involving ICTs and electronic evidence, including the preservation and admissibility of electronic evidence and direct access to extraterritorial data by law enforcement authorities, because in this age of cloud computing, data centres and interconnecting servers in different countries, the role of evidence "location" needs to be reconceptualised; (d) engaging the private sector, particularly Internet service providers, to combat cybercrime. The cooperation of the private sector is indispensable since most Internet services and ICTs are operated by private companies; and (e) settle disputes resulting from the application of this resolution and subsequently adopted international ICT norms through peaceful means and to refrain from the threat or use of force. International human rights law represents an important reference point for harmonizing such criminalization and procedural enforcement provisions;

6. *Further requires* that by 31 December 2014 each State must establish and maintain a Computer Emergency Response Team (CERT), to be accredited by FIRST, and must designate a national point of contact to handle communications among States related to ICT security incidents. *And strongly encourages* States to create and strengthen their ICT incident response capabilities (such as early warning mechanisms and law enforcement units that specialize in cybercrimes) and to enhance channels of communication and cooperation among States to address such cyber-attacks;

7. *Holds* that States shall be responsible for: (a) internationally wrongful cyber activities attributable to them, including the internationally wrongful activities in cyberspace of any State-backed proxies acting on the State's instructions or under its direction or control, (b) malicious cyber activity originating from within its territory or sphere of control or travelling over its networks of which they have knowledge and do nothing to minimize or end such attacks, and (c) facilitating lawlessness in cyberspace, for example, by knowingly tolerating the storage of illegally collected personal data on their territory. States should also take all necessary measures to ensure that their territories are not used by other States or by non-State actors for purposes of unlawful use of ICTs against other States or their interests;

8. *Further determines* that each State shall be obligated to report to the Secretary-General and UNIC by the end of each calendar year on its compliance with this resolution and the other matters described in paragraph 3 of resolution 67/27;

9. *Decides* that each State with mature or highly developed ICT security capabilities shall provide, in conjunction with UNIC or other regional or international organizations such as NATO's or the United Kingdom's respective cybersecurity centres or capacity-building initiatives, the following: ICT expertise, funds and ICTs to developing countries to manage ICT security incidents, to improve the security of their ICT infrastructures, and to assist such countries in creating and maintaining cybersecurity awareness-raising and training programmes.