ATTACHMENT 4

UNITED NATIONS SYSTEM **CEB**

Chief Executives Board
for Coordination
Second Regular Session for 2013 12 November 2013

Issue note on Cybersecurity/Cybercrime and Policies on Information

I - Introduction

1. We live in a world where technology has become pervasive and omnipresent. There are today nearly as many cell phones as people.[1] Ninety per cent of the world is already covered by a mobile signal[2] with mobile broadband rapidly expanding, especially in developing countries where subscriptions doubled over the last 2 years[3], while the number of Internet users is growing at around 9% annually[4]. Today, the Information and Communication Technology (ICT) sector can account for anything up to 15% of GDP of an economy[5], while global Business-to-Consumer e-commerce sales were reported to have topped $1 trillion for the first time in 2012[6]. As an increasing proportion of human activity now happens online, recent events, including various cyber-attacks and *government-led Internet surveillance activities,* have underscored the need to promote, protect and preserve trust, safety, security and privacy in cyberspace within a truly democratic framework, ensuring their adequacy, proportionality, due process and judicial oversight.

2. Cybersecurity is multi-dimensional and complex, touching upon fundamental elements of sovereignty such as national security and governance, while encompassing universal values of freedom of expression and privacy. The Internet today is a global public good, the value and utility of which can only be protected through the involvement and goodwill of all stakeholders. Any discussion of cybersecurity must reflect the multi-stakeholder reality of the information society and provide an equitable forum for all stakeholders in policy and decision-making processes.

> *Cyberattacks have the potential to destabilize on a global scale. Cybersecurity must therefore be a matter of global concern. We need to work together to bolster confidence in our networks, which are central to international commerce and governance.*
>
> *We need to strengthen national legislation … push for international frameworks for collaboration … and adopt the necessary measures to detect and defuse cyber threats.*
>
> - Mr. Ban Ki Moon, UN Secretary-General, Seoul Conference on Cyberspace, Seoul, Republic of Korea, 17 October 2013

[1] http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf
[2] http://www.itu.int/net/pressoffice/stats/2010/06/#.UoEJ_18o6by
[3] http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2013-SUM-PDF-E.pdf
[4] ITU World Telecommunication/ICT Indicators Database.
[5] Depending on countries' economic structure, and how ICT is defined. World Bank/ITU workshop in Egypt, 2009.
[6] http://www.emarketer.com/Article/Ecommerce-Sales-Topped-1-Trillion-First-Time-2012/1009649

3. Yet there remains a lack of a comprehensive and inclusive international framework for cooperation to promote cybersecurity at the global level, although various bilateral and regional frameworks attempt to address the issue.

II - An issue that affects the entire UN family

4. Because society has become more connected, a secure information environment has become fundamental to the broad range of issues and principles that concern the UN system, including the rule of law, peace and security, development, governance, gender equality, human rights, and disaster risk reduction, preparedness and mitigation. For example:

- When the inviolability of communication becomes questionable, it becomes increasingly difficult for Member States to comply with **International Law.** According to Article 24 of the 1961 Vienna Convention on Diplomatic Relations, "the archives and documents of the mission shall be inviolable at any time and wherever they may be" while Article 27 states that 'The receiving State shall permit and protect free communication on the part of the mission for all official purposes'. As the virtual world is borderless, concepts of national sovereignty may prove difficult to apply or enforce.

- Many UN agencies function as custodians of a wide variety of information entrusted to it by the Member States, individuals and employees. A major breach of trust relating to this information could have a very damaging effect on the reputation of the UN. Would agencies even know if Member States or individuals are reluctant to share information with the UN system in whole or in part because of a perceived lack of proper controls and precautions? For example, people may be reluctant to give full and complete information to doctors or medical staff about their personal habits, lifestyle or HIV status, if they believe that their personal data could be "hacked" or shared publicly. Furthermore, data collected by UN agencies could endanger the lives of those the Organizations serves if released or compromised. For example, detailed ethnic maps may be used during civil strive for targeted killings; data from victims of sexual abuse or human rights violations might serve perpetrators to intimidate those victims and witnesses; information gathered from political parties or armed opposition groups may tip the balance in peace negotiations; etc.

- As e-commerce has grown to become a major driver of economic and social development, insecurity can diminish the confidence in the use of ICTs and force public and private sector entities to increase spending to mitigate the effects of an insecure environment. These actions can have profound economic implications and undermine ICTs for development efforts, including achievement of the Millennium Development Goals.

- Improvements in technology have overtaken considerations regarding privacy, enabling actors, both state and commercial, to collect significant personal information. This includes the tracking and reporting of computer usage, normally without the knowledge of the user, and tracking has become prevalent in the physical world as well, through the deployment of activities such as device "location services" and monitoring cameras in public spaces. Member States have reacted strongly to recent revelations about violations of privacy, the mass surveillance of private communications and the indiscriminate interception of the personal data of citizens, including for purposes of protecting national security and countering domestic and international terrorism. In a recent statement, the UN Secretary-General noted "*Concerns about national security and criminal activity may justify exceptional and narrowly-tailored use of surveillance but surveillance without safeguards to protect the right to privacy hampers fundamental freedoms*"[7]. These acts raise issues of **human rights, including freedom of speech and the right to privacy** as outlined in the Universal Declaration of Human Rights and articles 17 and 19 of the International Covenant on Civil and Political Rights**.**

- ICT's have been used for trafficking and sexual exploitation, among other gender- and child- related violations. In particular, ICTs may expose children to new forms of violence, exploitation and abuse, which have harmful consequences for their safety, personal development and wellbeing. This may include exposure to violent images and other inappropriate content, cyberbullying and online grooming of children for sexual exploitation. National governments and the business sector alike have an important role to play to ensure that children have safe access to resources without exposure to risks that may lead to serious harm.

- Agencies and Member States require a new approach to **disaster risk reduction**, preparedness and mitigation as current global and UN strategic plans of action on disaster risk reduction exclude any risks occurring in the virtual world. It is vital to address challenges from cyber-threats to ensure business continuity of national infrastructure services (such as energy plants, air-control, water systems, health systems, food distribution, the financial environment).

- Many UN programmes are based around conferences and negotiations of various types, and the preparation and supervision of these by the UN involve the sharing of information, which can include negotiating positions and draft documents not intended to be seen outside small groups. Cyber-insecurity means that the protection of an organization's (or State's) continuity, privacy and information integrity can no longer depend on physical security alone with the physical perimeter insufficient as new working methods have been introduced (including email, the exchange of electronic documents, teleworking, remote participations, video, phone conferences, and collaborative working), and data may be located anywhere. Addressing this requires **a fundamental shift in risk mitigation** where physical security and cybersecurity go hand-in-hand.

III - ONE UN - An effective response

5. Addressing these issues requires a new approach which takes into account both the "real" and "virtual" worlds, and the growing interaction between them. **As agencies depend increasingly on global communication networks and services, the physical and virtual domains have converged. Nevertheless, this convergence has yet to be reflected or mainstreamed in UN System agency policies and programmes and requires enhanced coordination to be effective.**

[7] http://www.un.org/sg/statements/index.asp?nid=7046.

6. This point was underscored when the UN General Assembly received earlier this year the report of the UN Secretary-General[8] on the developments in the field of information and telecommunications in the context of international security from the Group of Governmental Experts. The report offers recommendations for Member States, including that international law is applicable to activities online. The report also points to the **leading role for the UN "in promoting dialogue among Member States to develop common understandings on the security of and in the use of ICTs, encourage regional efforts, promote confidence-building and transparency measures and support capacity-building and the dissemination of best practices"**.

7. As our physical and cyber worlds overlap, there is increased need for a high-level dialogue that addresses the challenge of balancing security, human rights and economic development with the rule of law and good governance. The UN family is well-placed to play the role of a global facilitator for this dialogue, not just among Member States, but also among all other stakeholders – including the private sector and civil society. Various agencies have mandates in different aspects – some on cybersecurity, some on cybercrime, and some on the normative dimensions such as privacy, freedom of expression and human rights, including the rights of women and children. However, in order to facilitate a global dialogue effectively, all agencies must work together in a coordinated and coherent manner, contributing to this endeavor within their mandate and expertise.

8. Beyond the technical issues that information security raises, agencies must first address many policy questions, keeping in mind that cybersecurity does not exist in isolation from the deployment of modern information and communication technologies. As noted in the HLCM strategic plan, "New technologies open entirely new horizons to re-shape the operational models of UN organizations…HLCM is embracing the use of ICT as an agent of change, improved knowledge management and increased collaboration within the system and with other partners." Embracing technology that improves the delivery of mandates also demands new working methods, and includes integration of information security into risk management strategies.

IV - Framing Questions

- **How can the system ensure effective internal preparation to cope with cyber-threats, among individual agencies and across the UN system, including policy and resource obstacles that may prevent agencies from acting together to jointly protect the UN system better through, for example, the inclusion of cybersecurity in risk assessment and risk management frameworks?**

- **How can agencies better integrate and mainstream cybersecurity and counter cyber-threats as part of programme planning and, in particular, the post-2015 development agenda?**

[8] UN Secretary-General Report to the General Assembly (A/68/98 of 24 June 2013).

- **How can agencies of the system ensure coherence and coordination in its assistance to Member States and avoid duplication of efforts?**

- **How can agencies facilitate discussions with member states that ensures that the international community arrives at a common understanding of, and takes action on, the need for a comprehensive and inclusive international framework for cooperation in the field of cybersecurity?**

- **When conducting their work, how can agencies balance the need for privacy and confidentiality with the transparency that stakeholders demand?**

–––

Annex – Background

1. While extremely broad in scope, most actions within the UN-system related to cybersecurity, cybercrime and information policies fall into three main categories: intergovernmental, UN agency support to Member States and UN agency internal actions.

Intergovernmental activities within the context of the UN

2. Member states began to recognize the risks posed by information technology to international security many years ago, and in 1998 the General Assembly passed resolution A/53/70 "Developments in the field of information and telecommunications in the context of international security" from a recommendation of the First Committee. Successive GA sessions passed similar resolutions. The most recent resolution, 67/27, calls upon member states to, *inter alia*, promote strategies "to address the threats emerging in this field, consistent with the need to preserve the free flow of information". The Committee is has again proposed a similar resolution for the 68th session.

3. More recently, and in the wake of a statement by Brazil during the General Debate opening the 68th GA session that drew attention to recent spying revelations. member states have reacted by, among other actions, submitting a draft resolution through the Third committee. The draft version of this resolution, to be addressed by the Committee during its fall session, calls upon member states to, inter alia, respect and protect privacy, "including in the context of digital communication" and to "…take measures to put an end to violations of these rights and to create the conditions to prevent such violations…".

4. Finally, the Second Committee regularly considers reports of the Secretary-General regarding follow-up to the outcomes of the World Summit on the Information Society, the most recent (A/68/65 – E/2013/11) published in March 2013. This report notes several cybersecurity-related activities in regions, and highlights the activities of the UN system in responding to action line 5, "Building confidence and security in the use of ICTs".

System-wide activities

5. With activities within all three pillars of the CEB, the topic of cybersecurity and cybercrime has received significant attention by agencies. The CEB first raised these issues at its First Regular Session of 2010, where it agreed on the seriousness of the growing risk of cyber-threats and cybercrime, both as a global threat, as well as with regard to the operations of the United Nations system itself. The Board requested both HLCM and HLCP to take up this issue and report back to CEB for further consideration as appropriate.

6. The 2003 and 2005 World Summit on the Information Society (WSIS) placed as a top priority the need to strengthen the trust framework, including information security and network security, authentication, privacy and consumer protection, as a prerequisite for the development of the Information Society and for building confidence among users of ICTs. In order to achieve this, a global culture of cybersecurity needs to be further promoted, developed and implemented in cooperation with all stakeholders, including the UN System, and international expert bodies. Many UN agencies along with the UN Regional Commissions have been actively involved in this process, and will take stock of progress during the WSIS+10 review process.

UN Agency support to Member States

7. HLCP has just endorsed an UN-wide framework on cybersecurity and cybercrime to enable enhanced coordination among UN entities in their response to the concerns of Member States regarding cybercrime and cybersecurity. This framework represents an important milestone in achieving the overall objective of ensuring more efficient and effective response mechanisms within governments, involving various stakeholders. The framework document includes a compendium of UN mandates related to cybersecurity and cybercrime, which brings together all of the action on this issue across the system Agencies have been requested to integrate the policies embodied in the framework into their programme development activities, and to contribute to the compendium to ensure it portrays a comprehensive view of directions by member states.

8. The UN and several agencies, notably ITU, UNESCO and UNCTAD, facilitate the discussions amongst member states on the issue of a more secure "cyber" environment and have produced material that demonstrate the grave risks that an insecure information society poses to social and economic development. Building on the recommendation of the governmental experts, the UN and its agencies can further facilitate the dialogue and promote best practices.

UN agency internal actions

9. The HLCM has also responded to the CEB mandate by integrated cybersecurity into its strategic plan, with the results framework including two activities intended to strengthen the system-wide capacity to address cyber-threats. First, in recognition that an agency's workforce is the first defense against cyber-intrusions, the Network has created a basic, standard information security awareness training syllabus that agencies adapt and deliver to staff members. Many agencies have already adopted this material and the Network is urging all agencies to make this mandatory, similar to other security trainings.

10. The ICT Network is nearing completion of a charter for a UN system information security response capacity. Building on the experience gained by the World Bank, this facility will provide a mechanism for agencies to share information and pool resources to address cybersecurity incidents.