Prof. Dr. Udo HELMBRECHT June 2014

Executive Director
European Union Agency for Network and Information Security (ENISA)

Heraklion - Crete - Greece

High-level policy statement on the vision of WSIS

ITU speech, 11th June 2014

Information Technology (IT) is increasingly used, everywhere in society, and new technologies and business models offer us new opportunities. Yet, it is important to balance these opportunities against the risks; this is one of the main goals of information security.

The European Union Agency for Network and Information Security (ENISA) views the vision for WSIS beyond 2015 to be a continuation of past work. The vision is based upon solid principles and provides a good basis for collaboration. As an agency, we particularly support the objective of strengthening the trust framework including information security and network security. Indeed, this is one of the objectives of ENISA within the European Union. Similarly, we agree that a global culture of cybersecurity needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. In this context, we believe that there is still significant work to be done in order to promote more effective cooperation between different communities. It is clear that the multi-stakeholder approach is needed in order to realise this vision and indeed, ENISA also carries out its work using such an approach.

ENISA agrees that scientific knowledge is a key factor in the innovation process and that science is acknowledged as a common or public good that is to be shared universally.

ENISA supports the strengthening of the trust framework. Information security and network security, authentication, privacy and consumer protection, should continue to be a prerequisite for the development of the Information Society and for building confidence among users of information technology.

Community and Capacity building is essential and can be done by bringing together experienced communities to work on common problems to foster cooperation across geographical boundaries for cross-border security.

ENISA believes strongly in” learning by doing”; an example is the Pan-European exercise, Cyber Europe 2014, where European Member States test their operational capabilities in a cyber-crisis scenario. This exercise involves constant interaction between the operational units in the Member States. One of the exercise’s main results is the 'Standard Operating Procedures' for use in the cross-border crisis management.

A second example is the CERT - *Computer Emergency Response Team* - community, where we for example define suitable training scenarios and actively guide the training sessions.

Unfortunately with new technologies also new threats are coming up, like adversaries abuse web vulnerabilities to perform code injections or spreading malware. Therefore close cooperation with the operational communities are needed to identify methods and tools that work in real, operational environments. By spreading good practices to industry, they can avoid duplication of efforts and reduce costs.

Industry needs to become better at “security by design”, from the start. And all stakeholders need to become better at implementing security measures. This includes using and promoting cryptography.

To conclude, in this wide range of working methods, ENISA is proactively building a security culture to enable us to remain competitive and stay secure in the 21st century.

Thank you for your attention!