

Jerusalem, 4 April 2017

“Cyber Security: National Threats & State Audit - Special Seminar for Heads of SAIs”- Conclusions and Recommendations

The “Cyber Security: National Threats & State Audit - Special Seminar for Heads of SAIs” was held at the State Comptroller and Ombudsman Office of Israel in Jerusalem, from April 2nd to April 5th, 2017. The SAIs of the following countries attended the Seminar¹: Austria; Estonia; Finland; Germany; India; Ireland; Latvia; Lithuania; Netherlands; Poland; Spain; Sweden; USA.

The participating SAIs agreed on the following conclusions and recommendations:

Our world is more interconnected than ever before and our extensive use of computer networks will only grow in the coming years with the fruition of cloud-computing, internet-of-things (IOT) autonomous cars, etc. Yet, for all its benefits, increased connectivity brings bigger risks of theft, sabotage, fraud, harm and abuse. Sophisticated cyber adversaries maintain and develop capabilities to threaten, disrupt and halt the delivery of essential services, steal information and money and (virtually) destroy the basic infrastructure of modern society. Indeed, in recent years we have witnessed an alarming increase in cyber security threats, directed at undermining the core foundation of our democracies. Some of these threats have grown to potentially catastrophic scales, putting in danger national security, critical infrastructures, financial systems and more. Without a doubt, the cyber security risk, with its very high chance of realisation, is one of the top risks any nation faces, especially developed ones.

Furthermore, this is a global threat. Therefore, international cooperation is necessary.

This Cyber Security Seminar in Jerusalem, in which we have gained further knowledge about the magnitude of the threat and the actions required to combat and safeguard against it, has strengthened our conviction that Supreme Audit Institutions must consider this peril as a central part of their national, local and intra-organisational risks maps.

However, as a border-crossing global threat which requires global action, we are of the opinion that this subject should also be addressed by the international state audit community.

Therefore, in order to achieve the most effective outcome, considering the scale and complexity of this task, it is advisable to exchange practical experiences, ideas and best practices with a view to raising awareness among national audit offices and developing a framework for international cooperation on cyber security and its audit, in the fields of capacity building, knowledge sharing and professional standards - under the umbrella of the multilateral organisations of Supreme Audit Institutions, with consideration of views of a range of relevant stakeholders.

¹ For the list of participants, please see the document attached.