Cyber Security

In the last two decades the world has seen fast development and growth of Information Technology (IT) and cyber systems. They have penetrated in one form or another all aspects of life. Unfortunately, that has also induced new vulnerabilities, risks and threats. Therefore one definition might be that *cyber security consists of technologies, processes, practices and controls designed to protect systems, networks and data from digital attacks*. Cyber security in general involves people, organizations, processes and technology.

Cyber attacks have become a reality and a source of national fear: dangerous programs can secretly be executed on computer systems and send out confidential data straight to terrorists. As computer viruses and worms become “smarter” and better every day, cyber attacks on government and private industry represent an increasing threat to national security. Cyber attackers with different profiles have repeatedly demonstrated their capacity to jeopardize the functioning of the state and national infrastructure, and thus endanger security.

In relation to the previous there are various plans, methodologies and systems dealing with cyber security, starting from national levels down to individuals. Perhaps the most advanced segment of protection in EU, USA and China is in cyber domain. However, taking into consideration the constant evolvement of cyber systems and corresponding threats, it is necessary to remain vigilant and constantly update the cyber security.

INIS, with its international team of experts, partners and experience, is following closely the developments in cyber domain on the global level. Hence, INIS supports and participates in research, projects and publications related to cyber security.