Cyberintelligence

The expanding typology of risks in the information age has led to growing uncertainty about the future of European and Euro-Atlantic security. In the near future, we could face hackers breaking security codes, terrorists getting access to biological weapons, states launching nuclear missiles, or cyber-spies gathering vital intelligence to state security.

Unprecedented technological development and emergence of virtual communities in a borderless cyberspace have opened a new battlefield. Therefore, one of SRI's recently assigned missions is to prevent and counter cyberattacks against critical infrastructure of the state - a mission meeting the threats specific to the beginning of the 21st century, when state communications and IT systems, as well as the data they manage tend to develop and function as a cyberspace in itself.

Why is this a threat? Because virtual environment development may have its advantages, but it can also bring on vulnerabilities in the absence of adequate security measures.

State and non-state entities having their own economic, political, or military interests can carry out cyberattacks. These hostile actions are directed against IT&C systems, which either form a critical infrastructure in itself (such as telecommunications or the Internet), or are essential for the functioning of other critical infrastructures of the state (e.g. air, rail, or road transportation infrastructure, energy, gas, oil or water supply systems, medical services, financial and banking system, etc.).

After its designation as national cyberintelligence authority by the Supreme Council of National Defense, SRI has set up a specialized structure, the **National Cyberint Center.**

Its main mission is to intertwine technical defense systems with intelligence capabilities in order to identify and provide legal beneficiaries with the necessary information to prevent, stop, and / or contain the consequences of acts of aggression on the IT&C systems representing critical infrastructures.

And because browsing the Internet securely is the first step each of us can take in order to protect ourselves against cyberattacks, please also visit the Security Advice section to learn about the best practices you should use.

0800 800 100
Anti-Terrorist Hotline

This website is optimized for browsers with HTML5 and CSS3 capabilities.