
SERVICIUL ROMÂN DE INFORMAŢII

# CYBER THREATS - A ROMANIAN PERSPECTIVE

**September 2013**

# AGENDA

I. Cyber threats in Romania

II. Current cybersecurity level in Romania

III. Intelligence estimate

IV. Legal framework

V. Institutional framework

VI. Private-public partnership

CYBER THREATS
A ROMANIAN PERSPECTIVE

# I. CYBER THREAT LEVEL IN ROMANIA

**STATE ACTORS** | CYBER CRIME | CYBER EXTREMISM | CYBER TERRORISM

- Cyber attacks are included in the offensive arsenal of some state actors, but also have build-up complex resources to cover and deny their involvement, including using hackers and organized cyber crime networks as proxies (e.g–"patriotic hackers"); IT&C companies, operating globally, could be used as attack vectors against nations
- Cyber espionage operations are an essential part for state actors effort to reduce its dependency on foreign technologies and has the potential to supply cyber systems with subtle altered components
- Romania has been confronted with state-sponsored cyber attack, operation Red October, investigated by SRI since 2011, as national authority in cyberintelligence, in cooperation with other national institutions with responsibilies like STS, SIE and CERT-RO and with foreign partners. The investigations revealed that hostile cyber entitites are aiming to obtain access to national strategic networks and gather intelligence

# I. CYBER THREAT LEVEL IN ROMANIA

STATE ACTORS | **CYBER CRIME** | CYBER EXTEMISM | CYBER TERRORISM

- Cyber criminals are mainly aiming to obtain financial gains from online sales and banking systems, by means of cyber operations, employing a wide variety of methods, including phishing , spamming, social engineering, skimming, carding, as well as hacking techniques against targeted computer networks or personal workstations
- Two major cases involving cyber crime attracted the public eye, **operation PENE** - organized crime group specialised in electronic frauds, comprised by 24 that defrauded almost 350 persons from the US, Canada and UK, causing losses of over 8mil. USD – and **operation PĂUNESCU** - a crime group led by Mihai-Ionuţ Păunescu whose purspose was launching cyberattacks against various financial/bancking institutions in the US, like United States Postal Services and Bank of America, causing losses of aprox. 240 mil. USD.

SERVICIUL ROMÂN DE INFORMAŢII

# I. CYBER THREAT LEVEL IN ROMANIA

STATE ACTORS | CYBER CRIME | **CYBER EXTREMISM** | CYBER TERRORISM

- Next to state and crime involvement, hackers may have a large variety of motivations ranging from sheer misplaced (usually juvenile) assertiveness to some forms of ideological-type convictions
- As justification for their acts, they promote the idea of free access to information or attacking (on political, social or religious grounds) certain official decisions, stances and acts
- Romania was confronted with the actions carried by the members of Anonymous Romania who, starting January 2012, who launched a high number of cyber attacks against national public institutions. They have also been involved in initiating cyber attacks on foreign entities from the US, Czech Republic, Serbia, Poland and Brazil. Anonymous Romania also supported Anonymous International in attacking various IT systems outside Romania.

# I. CYBER THREAT LEVEL IN ROMANIA

| STATE ACTORS | CYBER CRIME | CYBER EXTREMISM | CYBER TERRORISM |
|---|---|---|---|

- No unanimously accepted definition for cyber terrorism

  - against computer systems managing CIs, aimed to produce direct, large scale, and terror-generating effects
  - for all terrorism-related activities (propaganda, recruitment, communications, financing, gathering information)

- No substantial indications of existing or imminent cyber terrorism capabilities to attack computer systems managing CIs
- In time, can achieve sufficient know-how by specializing themselves or recruiting like-minded specialists
- No evidence in Romania of such aggressions

# II. CURRENT CYBERSECURITY LEVEL IN ROMANIA

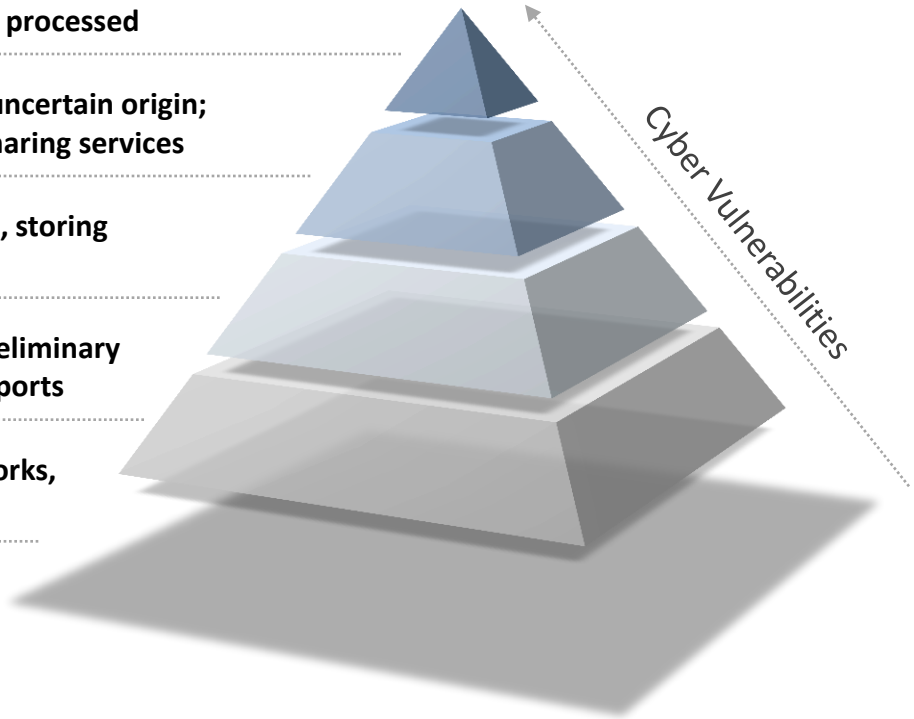
**Installing applications that allow file sharing, opening connection ports within the system where confidential data are stored and processed**

**Downloading / uploading in computer networks data of uncertain origin; installing and running unlicensed software through file sharing services**

**Connection to the Internet of sensitive computer systems, storing sensitive data on unauthorized workstations**

**Inadequate anti-virus software, data transfers without preliminary antivirus checks, inadequate use of external memory supports**

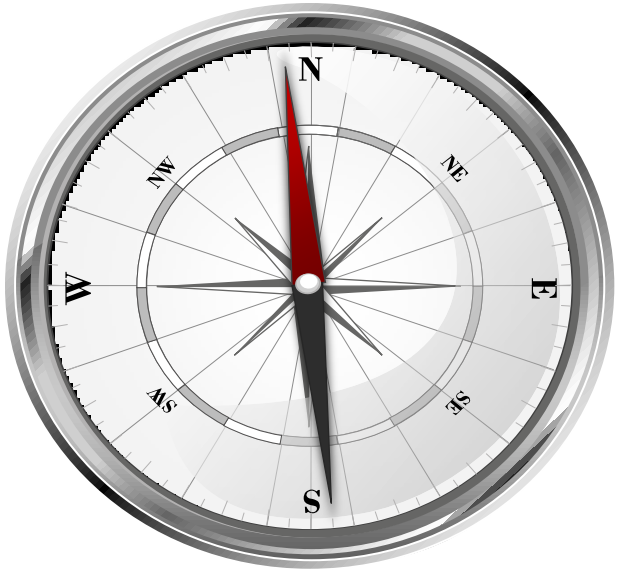
**Inexistent / lax policies for user access to computer networks, inexistence of audit systems and inadequate security**



# III. INTELLIGENCE ESTIMATE

## Intelligence Estimate

- Due to the benefits, technical evolution and persisting vulnerabilities, will see increasingly sophisticated, automated and damaging cyber aggressions from state and non-state actors
- Besides general dynamics of cyber threat, Romania's foreign geopolitical and security environment may quickly augment the cyber risks and threats, especially by state entities
- The cyber threat condition is ELEVATED and has an GROWING trend for 2013



# IV. LEGAL FRAMEWORK

The national legal framework comprises:

| | | | |
|---|---|---|---|
| ✓ | **Law regarding the identification and assignment of national CIs** | March 2010 | Done |
| Law no. 18/2010 | | | |
| ✓ | **National Cyber Security Strategy** | February 2013 | Done |
| Approved by Governmental Decision no. 271/15.05.2013 | | | |
| … | **Law regarding cyber security** | end 2013 ? | Pending |

# V. INSTITUTIONAL FRAMEWORK

The national institutional framework should have in view:

| | | | |
|---|---|---|---|
| ☑ | **to continue the development of CERT-RO** | | Ongoing |
| ☑ | **to establish new specialized CERTs** | | Ongoing |
| ☑ | **to elaborate a national plan for management and reaction to cyber incidents** | end 2013 | Ongoing |

# V. INSTITUTIONAL FRAMEWORK

**The National CYBERINT Centre runs activities in order to:**

- Anticipate and know the Cyber Threats to national CII's
- Prevent Cyber Threats by disseminating intelligence products to policymakers
- Identify real time Cyber Attacks against national CII's, neutralize the attacks and limit the technical consequences

# VI. PUBLIC-PRIVATE PARTNERSHIP

the development of cooperation mechanisms between public and private sectors , both at national and international level, as a priority in order to insure the prevention, identification, analysis and reaction to cyber events.

**Public private partnership** should focus on:

raising awareness through organizing workshops, seminars and presentations on cyber security issues

SERVICIUL ROMÂN DE INFORMAŢII

# THANK YOU !

## CYBER THREATS
## A ROMANIAN PERSPECTIVE