



ROLE OF CERT-GOV-MD and cooperation at national level

Natalia SPINU,
Chief, CERT-GOV-MD, S.E. CTS

AGENDA

1. Introduction
2. CERT-GOV-MD:
organization and operational capacities
3. CYBERSECURITY INCIDENTS: CHALLENGES, CURRENT SITUATION AND PAST ATTACKS
4. Future:
Cybersecurity in moldova
5. CONCLUSION
S

”

There are only two types of companies: Those that **have been hacked**, and those that **will be**.

Robert Mueller, FBI Director, 2012

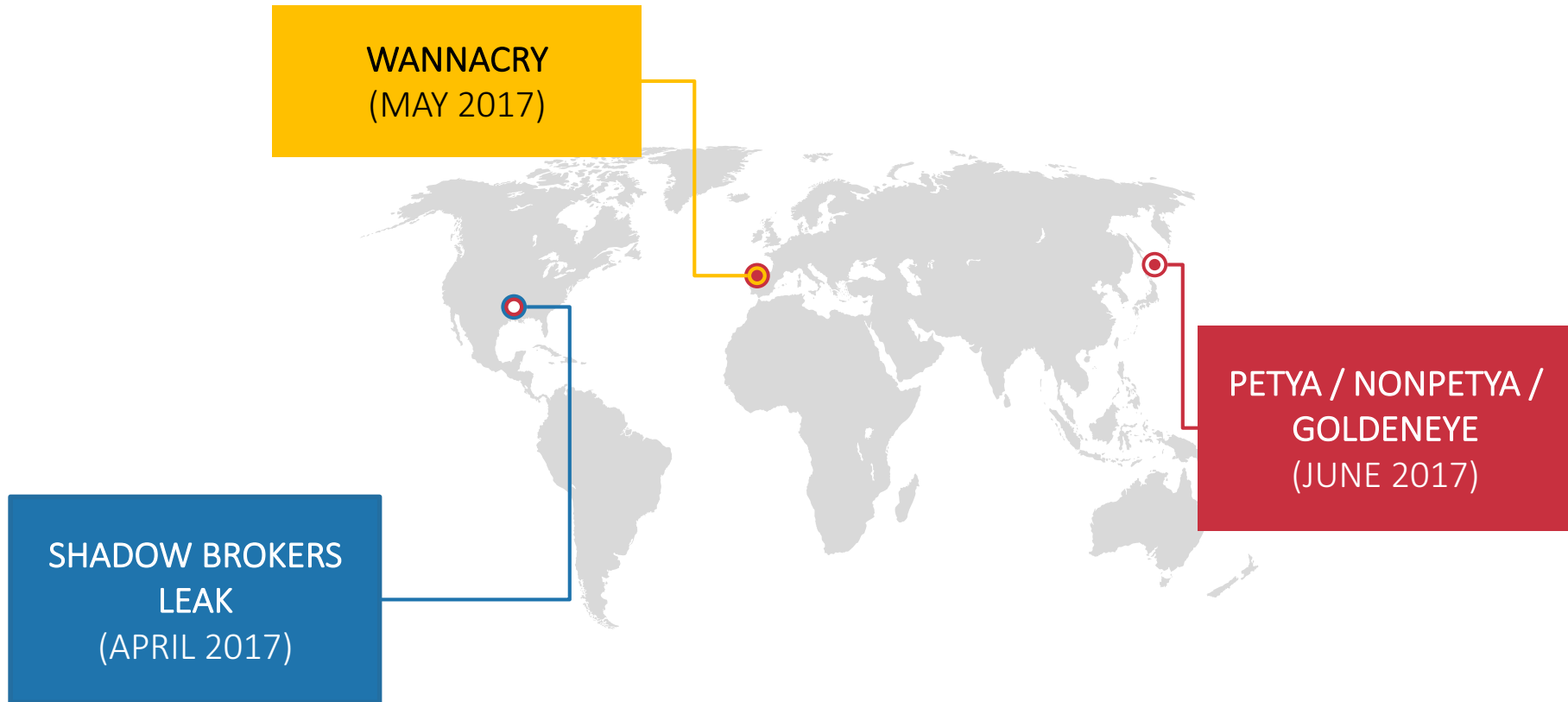


A top-down view of a person wearing a grey hoodie sitting at a desk. The desk is cluttered with computer equipment: a laptop on the left, a large monitor in the center displaying code with a 'Copy From' dialog box, another large monitor on the right displaying code, a keyboard, and a mouse. The person's hands are on the keyboard. The background is a dark wooden desk.

Introduction

CYBER THREATS ARE INTERCONNECTED

CYBER THREATS 2017



SHADOW BROKERS LEAK

August 2016

- Shadow brokers group claimed to obtain NSA spy tools.

April 2017

- The most significant leak of spy exploits done by the group.

April's leak led to the most serious consequences.



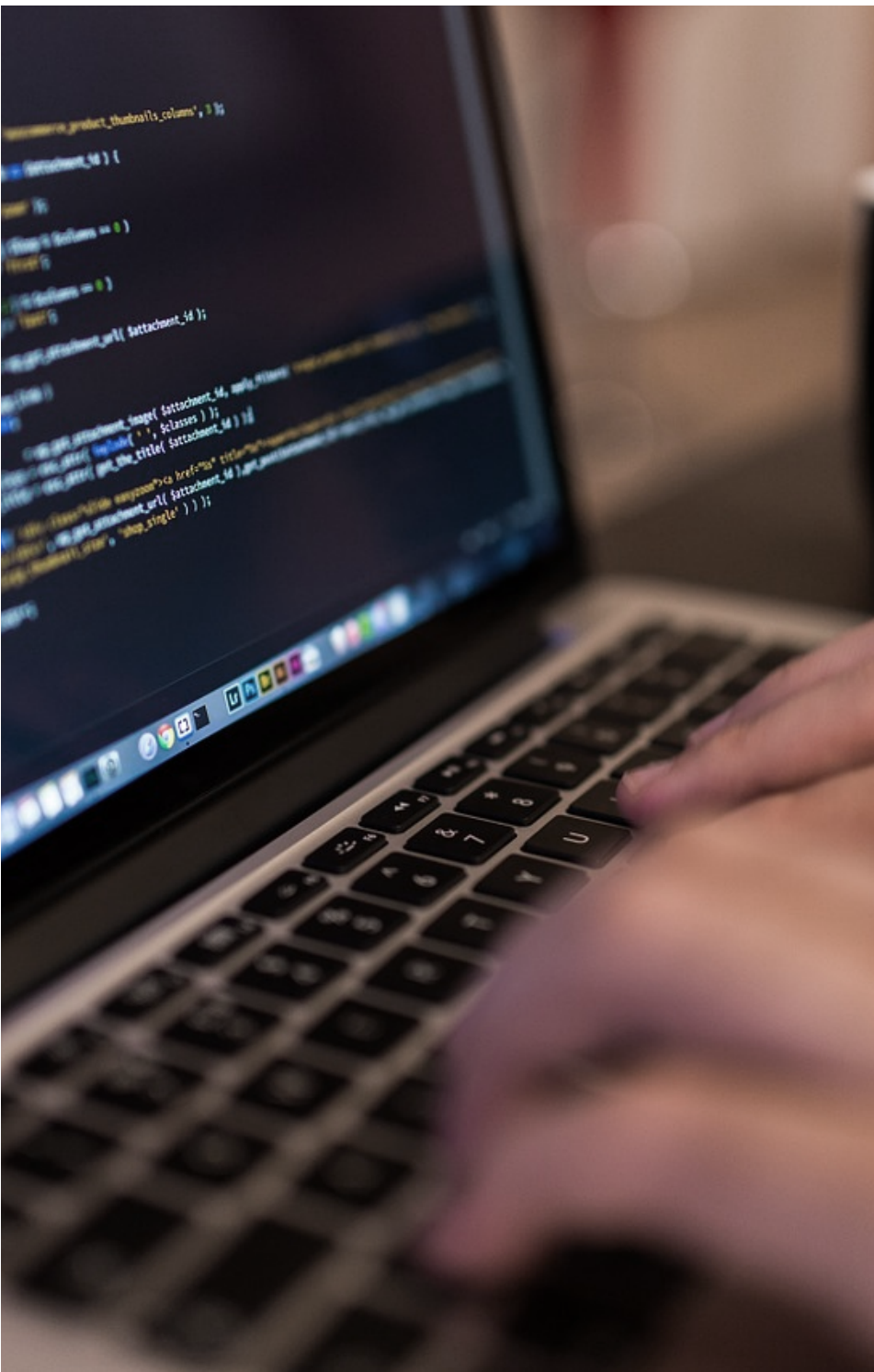


WANNACRY

- On **May 12** a strain of ransomware called WannaCry spread around the world.
- The ransomware used leaked by Shadows Brokers exploit to attack the targets.

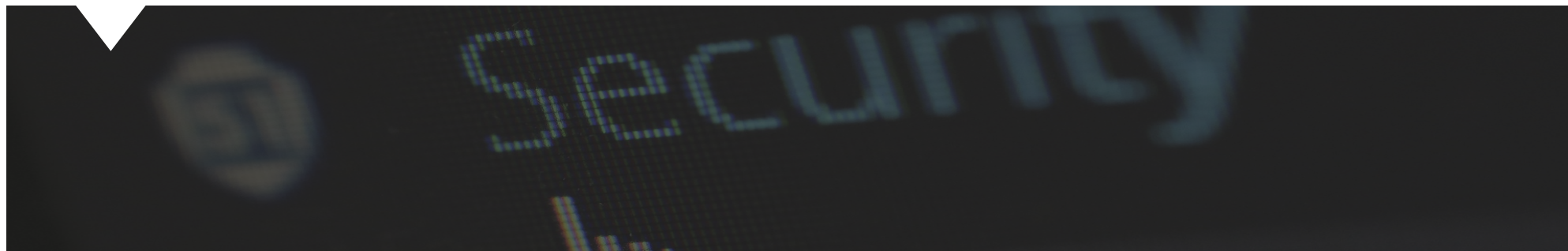
PETYA / NONPETYA / GOLDENEYE

- A month or so after WannaCry, another wave of ransomware infections that partially leveraged Shadow Brokers Windows exploits hit targets worldwide



WHY THIS MATTERS TO YOU

- **Growing space with rapid expansion**
 - Across all sectors: individuals, commerce, governments
 - Growing pervasiveness in everything we do
- **Many threats**
- **Cyber Security is an unclear concept**
 - Considerable uncertainty, broad scope, and ever-changing dimensions
 - Cyber security definitions vary widely and lack true conformity
- **Cyber is a chaotic and ungoverned environment**
 - Increasing tension between governments, individuals, private enterprises, commerce.
 - What is cyber defense?
- **Early stages of cyber expansion**
 - Technological advancement
 - Fast and intense competition
 - An uncertain future of the cyber domain, the internet and more



THE CYBER SECURITY CHALLENGE...

When...

- In the Cyber world, security was an afterthought
- The Cyber world lacks a single central cyber architect
- The Cyber world is a system of insecure systems
- The Cyber world is not static but constantly evolving
- Innovation is constant, and highly unpredictable



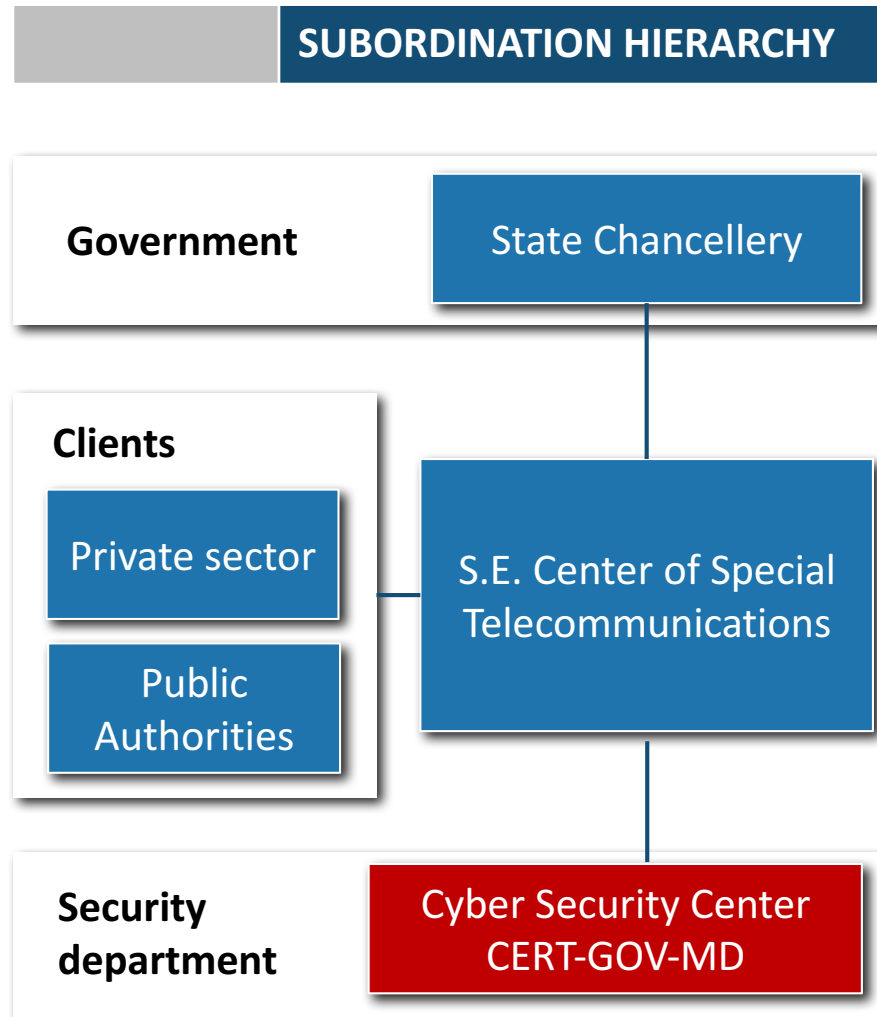
The background of the slide features a blurred image of a person in a blue uniform pointing at a screen. Overlaid on this is a semi-transparent graphic consisting of a padlock icon in the center, surrounded by several concentric circles that resemble signal waves or a target. The overall color palette is dark blue and black.

CERT-GOV-MD

ORGANISATION AND OPERATIONAL CAPACITIES

WHO WE ARE?

SUBORDINATION HIERARCHY



FACTS

- 2010** Established by Government decision № nr. 746 of 18.08.2010
- 2013** Implemented ISO 27001
- 2014** CERT-GOV-MD became accredited by Trusted Introducer
- 2016** FIRST membership



Benefits of CERT-GOV-MD

- Serve as a trusted point of contact
- Develop an infrastructure for coordinating response
- Develop a capability to support incident reporting
- Conduct incident, vulnerability & artifact analysis
- Participate in cyber watch functions
- Help organizations to develop their own incident management capabilities
- Provide language translation services
- Make security best practices & guidance available
- Provide awareness, education & trainings



A top-down view of a person wearing black gloves typing on a keyboard. The person is seated at a desk with a wooden surface. There are three computer monitors and a laptop, all displaying green code on a black background, reminiscent of the Matrix movie. The room is dimly lit, with the primary light source being the screens. The person is wearing a dark, long-sleeved garment. The overall atmosphere is mysterious and technical.

THREATS

CYBERSECURITY

THREATS

Threats in Cyberspace

INFORMATION & ABUSE

- Targeted government control and influence of citizens
- Propaganda
- Consciously communicating false information
- State espionage
- Data breach
- Identity theft
- Hackers
- Internet crimes, encouraging sedition
- Terrorism



THREATS

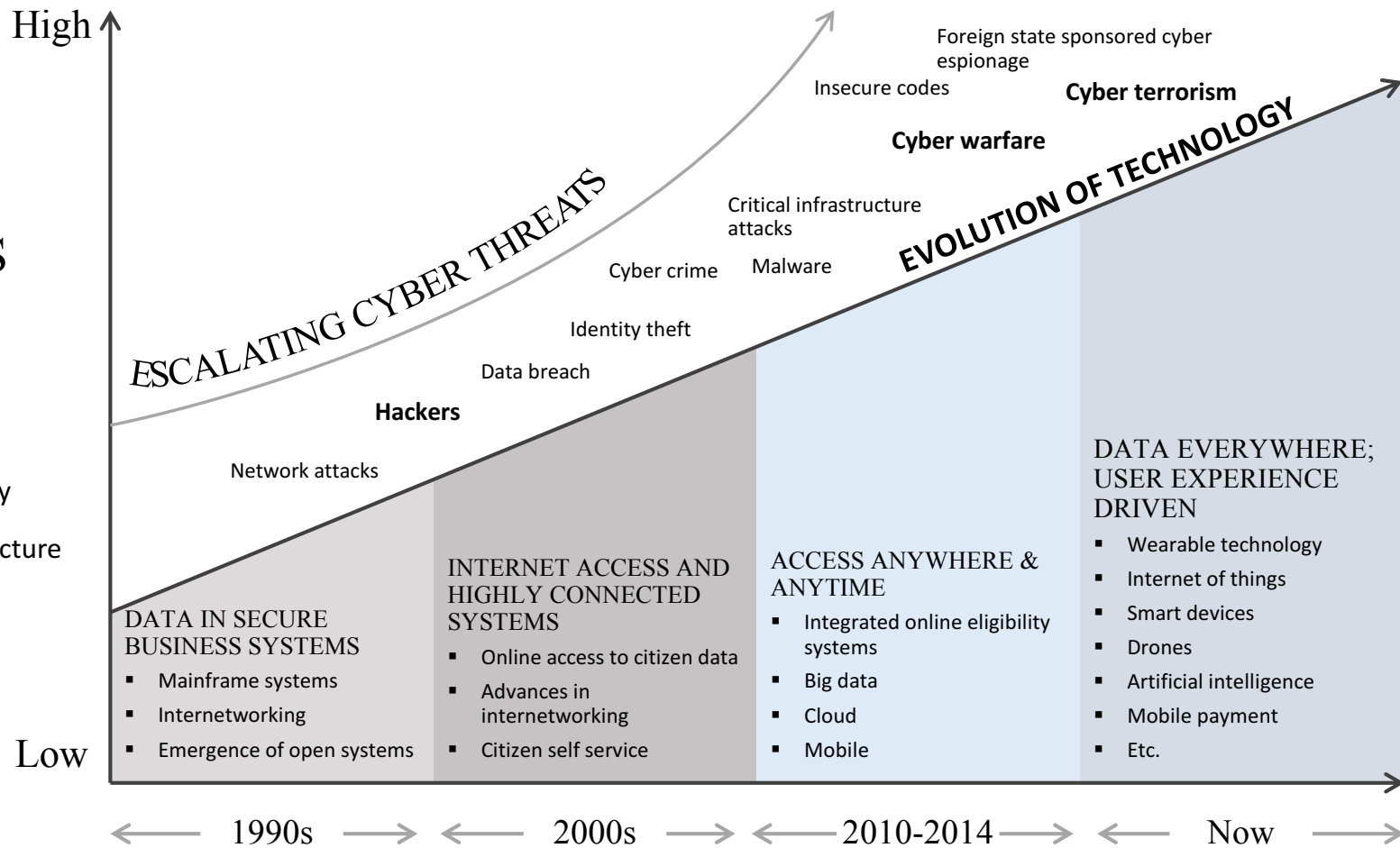
Threats are Becoming
More Complex



THREATS

BUSINESS IMPACT:

- Citizen trust
- Cost to protect
- Legal/ regulatory
- Critical infrastructure



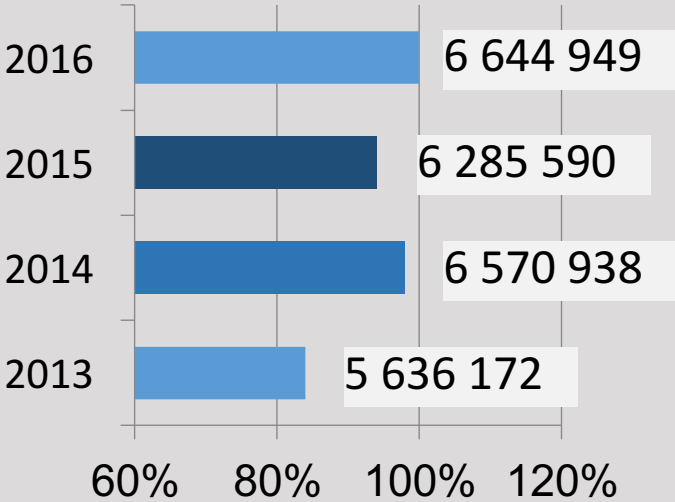


CYBERSECURITY INCIDENTS

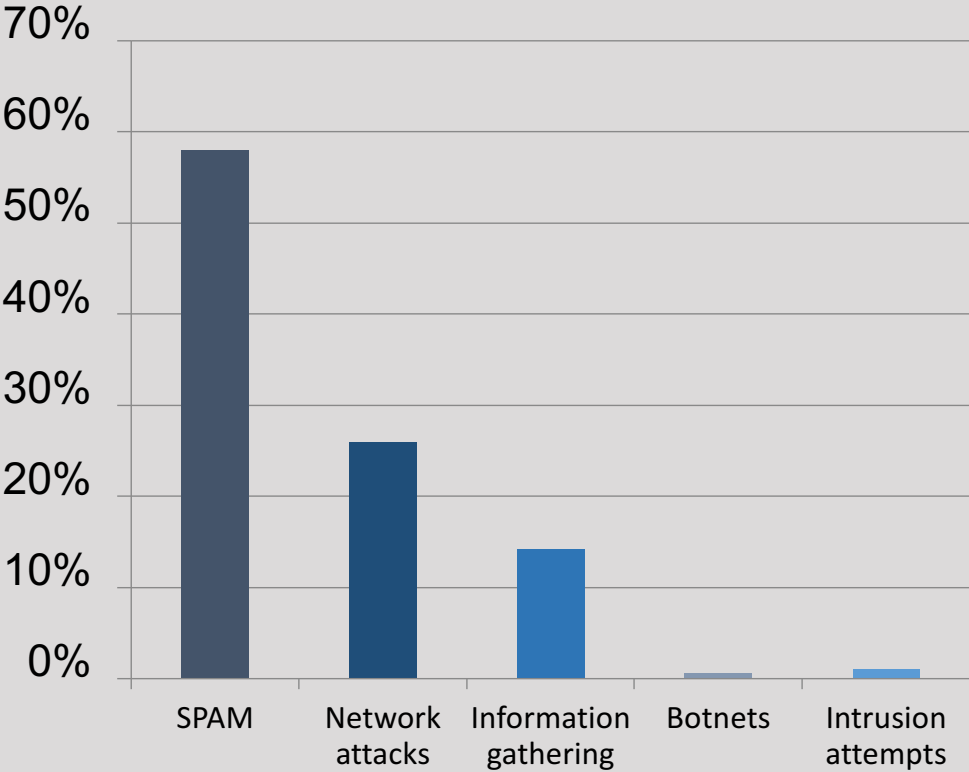
CHALLENGES, CURRENT SITUATION AND PAST ATTACKS

CYBER INCIDENTS IN GOVERNMENTAL SECTOR

NUMBER OF INCIDENTS



INCIDENTS BY CATEGORY (2016)



THREATS

3 882 529 unsolicited emails blocked as of 2016

SPAM

Seems legitimate and are sent to an email account

Many email accounts have spam filtering

Contains often dangerous links (to download) or invoices for alleged online orders

Can also be sent on social networks or apps



THREATS

57 575 malware blocked as of 2016

ATTACKER



Various new forms of malware appear on the internet every day.

TROJANS & WORMS

ARE SENT VIA INFECTED EMAILS



Can transfer sensitive data such as passwords, banking information, personal data

VICTIM



Next undetected in computer systems or creep in during downloads



THREATS

3 678 Botnets infections detected

ATTACKER

Networks consisting of several computers



BOTNETS CONTROLERS



INFECTED

Can send infected and dangerous (spam) emails



Can send infected and dangerous (spam) emails

TARGET



Can attacks all IT systems

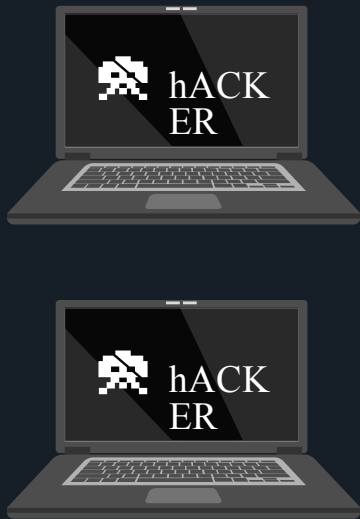


THREATS

124 575 Distributed Denial-of-service (DOS) attacks stopped

ATTACKER

Networks consisting of several computers



BOTNETS CONTROLERS

Are also used as a distraction while malicious software is being installed



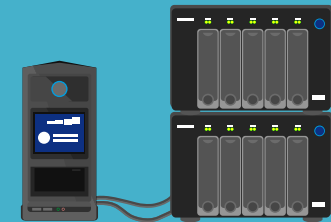
INFECTED



TARGET



Block internet services



Its purpose is to interrupt web servers which then causes a mass of data packets to be sent to the server

CAPACITY BUILDING

Cyber Security Trainings and Workshops

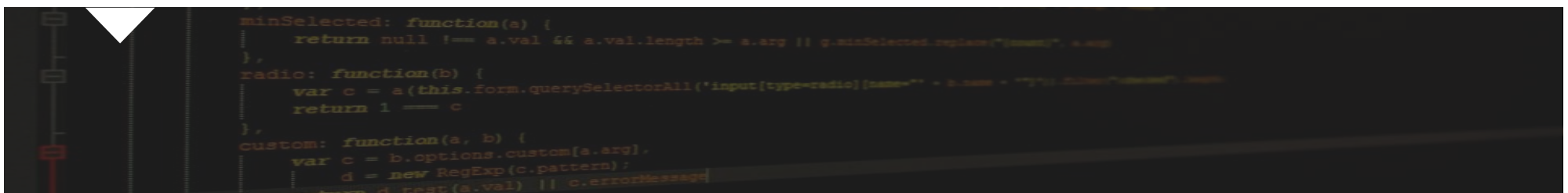


Joint educational activities

```
minSelected: function(a) {
    return null !== a.val && a.val.length >= a.arg || g.minSelected.replace("min", a.arg);
},
radio: function(b) {
    return g.minSelected.replace("min", a.arg) + a.val + " " + "The minSelected" + a.arg;
},
custom: function(a, b) {
    var c = b.options.custom[a.arg];
    d = new RegExp(c.pattern);
    return d.test(a.val) || c.errorMessage;
}
```

INFORMATION SECURITY AWARENESS

CERT-GOV-MD's awareness activities



POWER OF PARTNERS



Working together to ensure high level of cybersecurity

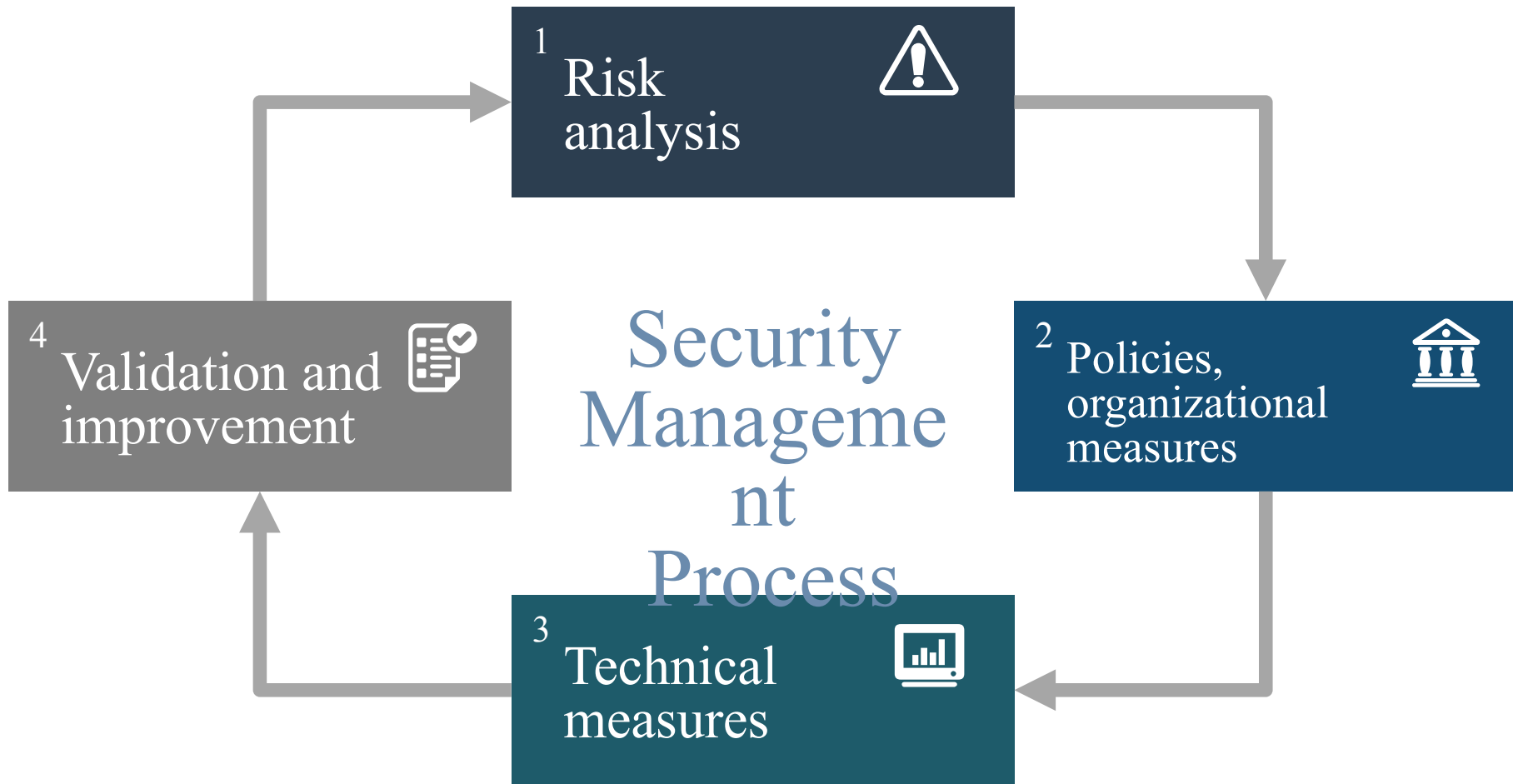


FUTURE

CYBERSECURITY IN MOLDOVA

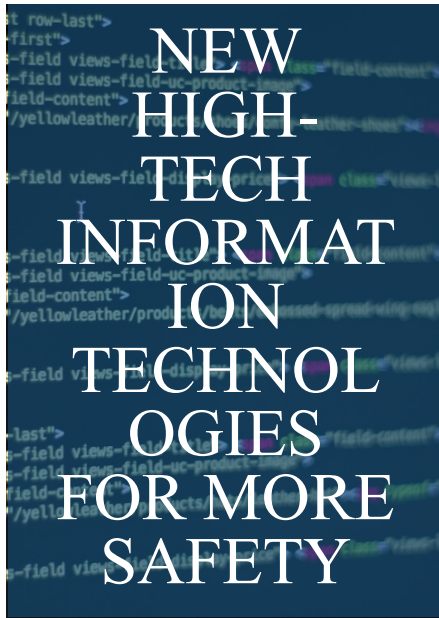
SECURITY

Continuous Steps of a Security Management Process

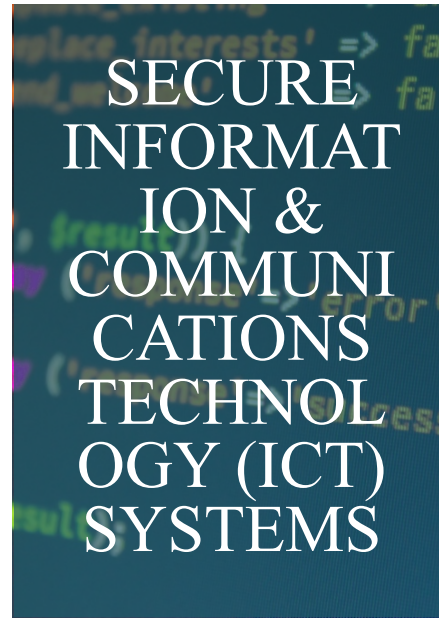


FUTURE

New Research Program of the Government with Four Focus Areas



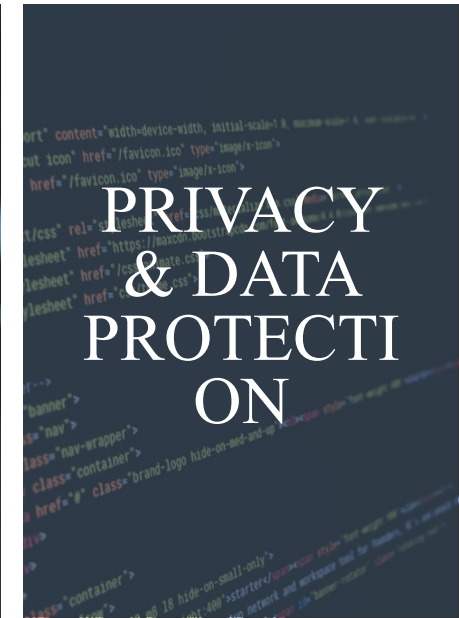
New encryption capabilities
and security measures



Security measures and
solutions for networked
systems



Protection of critical
infrastructures and
networked industrial plants



More control over citizens'
personal data on the
Internet



CONCLUSIONS

CONCLUSION



Cyber security is a **global problem** that has to be addressed globally by all governments jointly;



No government can fight cybercrime or secure its cyberspace in isolation;



International cooperation is essential to securing cyberspace;



It is **not a technology problem** that can be 'solved'; it is a **risk to be managed** by a combination of defensive technology.





THANK YOU!

Natalia SPINU

natalia.spinu@cts.md

natalia.spinu@cert.gov.md