



Itu regional workshop

"Key Aspects of Cybersecurity in the Context
of Internet of Things (IoT)"

Natalia SPINU

18 September, 2017 Tashkent, Uzbekistan

AGENDA

1. INTRODUCTION

2. Moldovan
public policy
on
cybersecurity

3. RECOMMEN
DATIONS

A person wearing a dark suit and a blue shirt is holding a white smartphone with both hands. The background is a blurred cityscape with buildings and lights, suggesting an urban setting. The overall tone is professional and modern.

Introduction

WHY THIS MATTERS TO YOU

Growing space with rapid expansion	<ul style="list-style-type: none">▪ Across all sectors: individuals, commerce, governments▪ Growing pervasiveness in everything we do
Many threats	<ul style="list-style-type: none">▪ Cyber criminals, hacktivists, terrorists, state-sponsored, hackers, amateurs, insiders, trusted partners and many other
Cyber Security is an unclear concept	<ul style="list-style-type: none">▪ Considerable uncertainty, broad scope, and ever-changing dimensions▪ Cyber security definitions vary widely and lack true conformity
Cyber is a chaotic and ungoverned environment	<ul style="list-style-type: none">▪ Increasing tension between governments, individuals, private enterprises, commerce.▪ What is cyber defense?
Early stages of cyber expansion	<ul style="list-style-type: none">▪ Technological advancement▪ Fast and intense competition▪ An uncertain future of the cyber domain, the internet and more
Government roles increasing in number and importance	

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

WHY?

3) Complex Trust relationships between cyber domains

Cyber security affects every person who

Trust is foundational

- Who is not connected in some way?
- Uses a smart phone, computer, automated banking, GPS, and modern medicine
- Rapid expansion. The Internet of Things....
- Machine to machine interaction

How do organizations find the right balance of trust, transparency, and privacy?



HOWEVER, WHAT DO WE KNOW ABOUT CYBERSPACE?

Globally connected

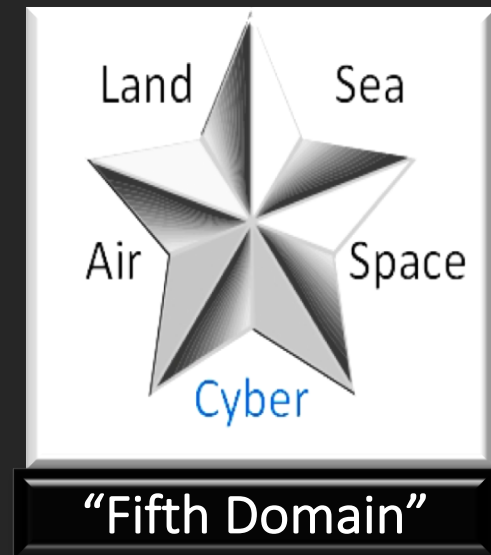
Contested environment

Mostly in private hands

Great deal of anonymity

Changing environment

New form of warfare?





Moldovan public policy on cybersecurity

DIGITAL CONTEXT

ICT contributes ~10% of GDP:

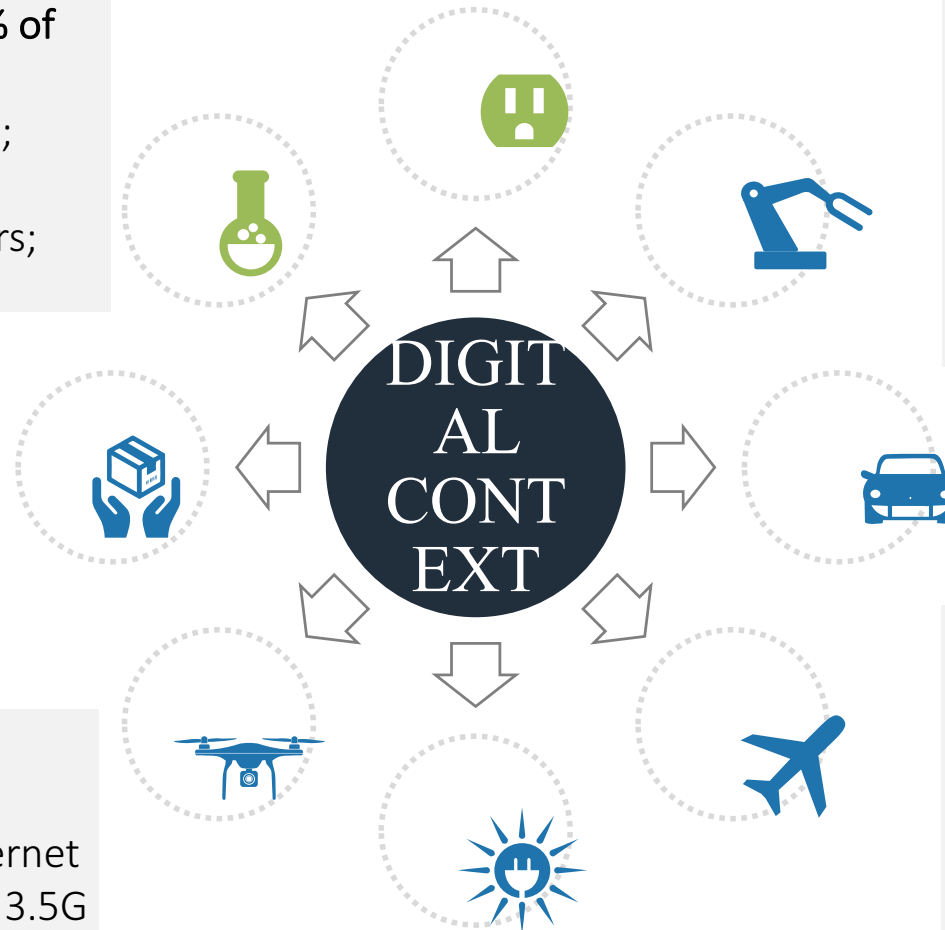
- 153 IT companies;
- 7 major ISPs;
- 3 mobile operators;

Governmental Services

- 522 available
- 125 are electronic

Mobile penetration – 110%:

- High speed 3G internet access since 2008, 3.5G since 2010, 4G since 2012;



Internet penetration:

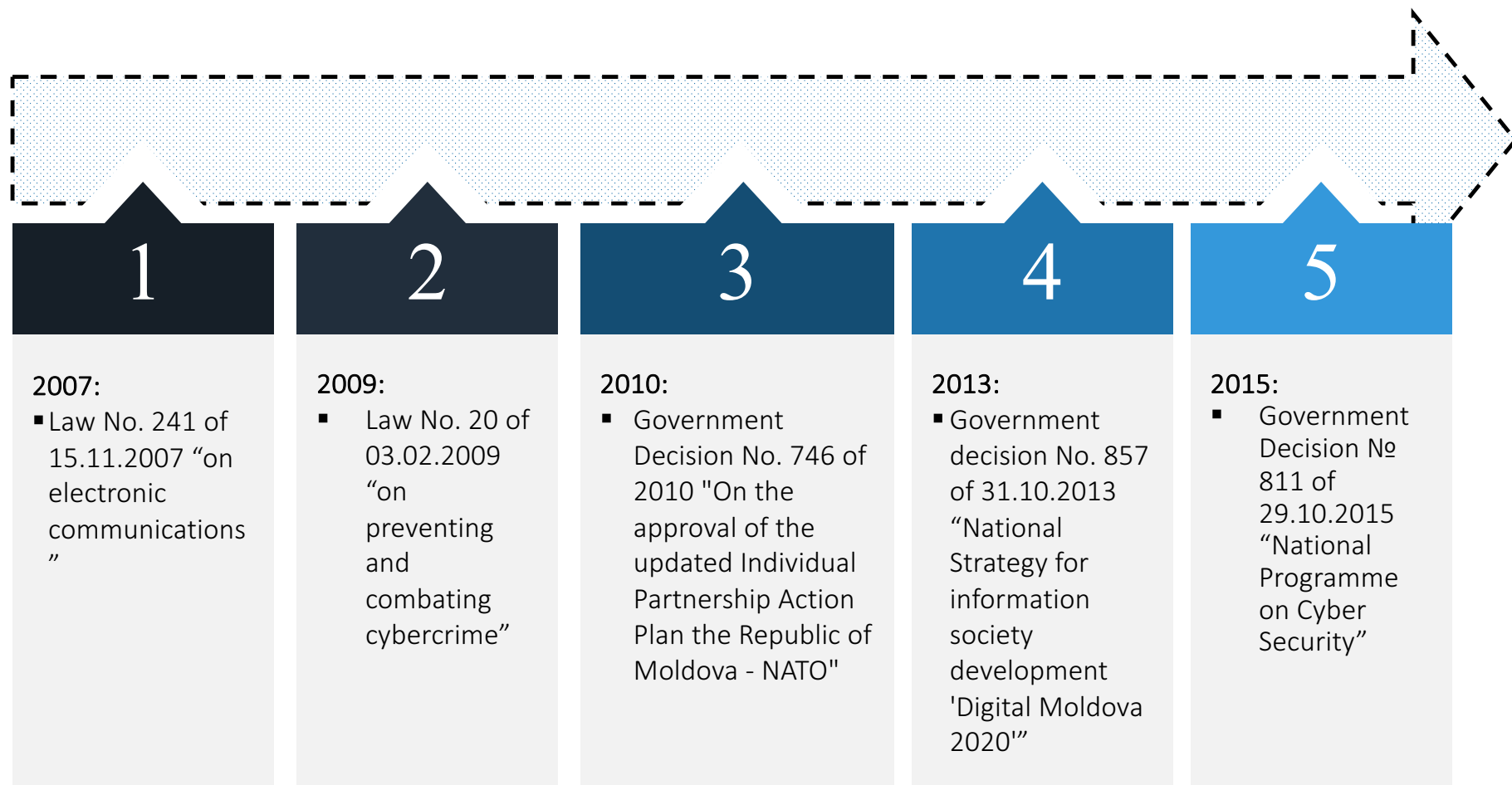
- Overall - 50%;
- Broadband – 11%;
- Since 2010 some ISPs offer 100/100Mbit for 250 MDL (~13 USD);

Infrastructure:

- Fiber link to 99% of localities, last mile is Ethernet;
- Separate 100Mbps dark fiber network serving central public administration

EVOLUTION

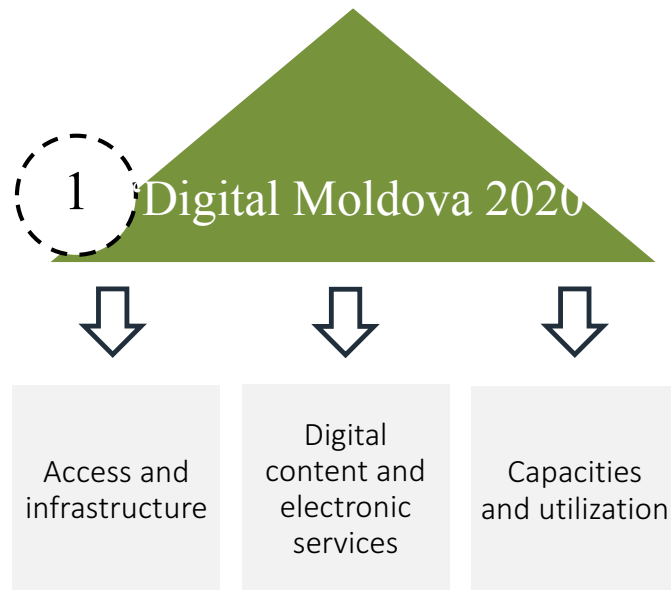
of Moldovan Public Policy on Cybersecurity



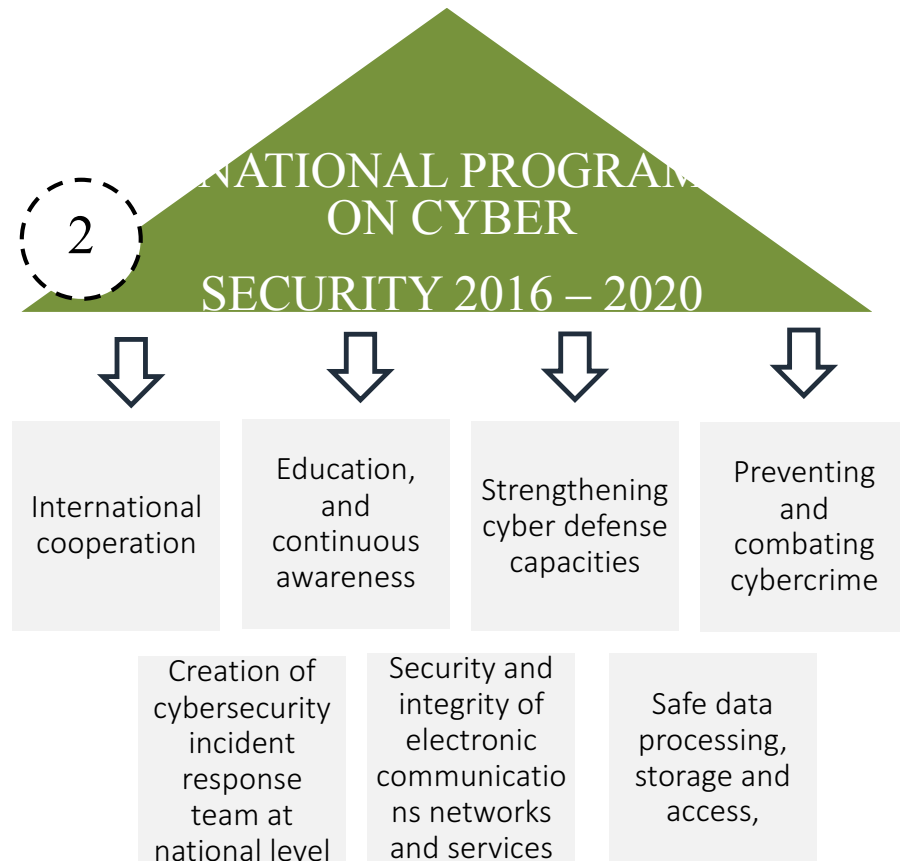
DUALISM OF DEVELOPMENT VECTORS

of Moldovan Public Policy on Cybersecurity

OVERALL OBJECTIVE: To create secure environment for development of information society



GOAL: To create and implement national cybersecurity management system



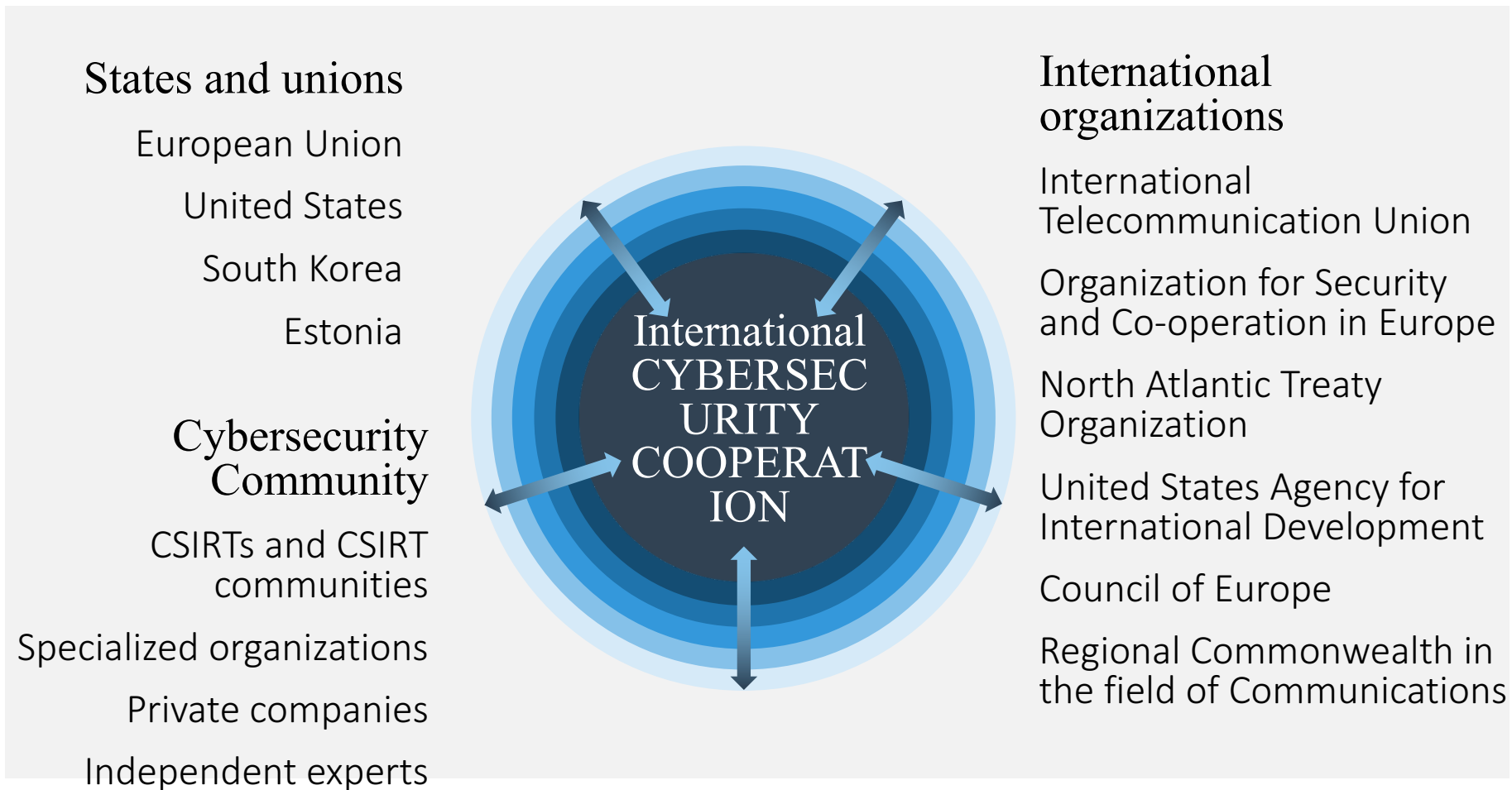
KEY ASPECTS

of Moldovan Public Policy on Cybersecurity



INTERNATIONAL COOPERATION

Most active cooperation partners of Moldova on cybersecurity



MAIN CHALLENGE

” Insufficiency of international cooperation in identifying risks, vulnerabilities, other events occurring in the world cyberspace, and preventing cross-border cyber threats and attacks.

National Programme on Cyber Security

Government Decision № 811 of 29.10.2015

INTERNATIONAL COOPERATION

Approved course of actions



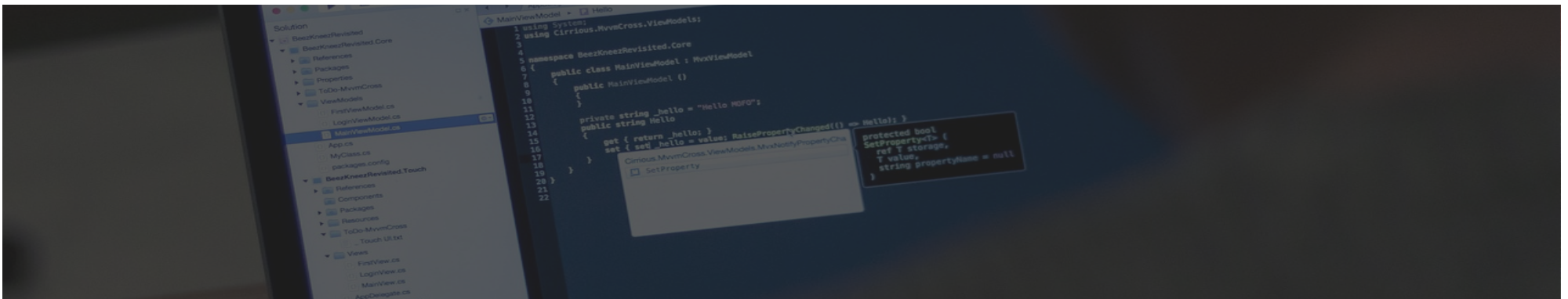
EDUCATION AND CONTINUOUS AWARENESS

Core problems

(1) Citizen are not conscious that their electronic devices might be already hacked







- “In spite of a big number of cybersecurity victims, only a few citizen are conscious that their electronic devices (mobile phones, tablets, notebooks, computers, etc.) might be compromised by cyber attacks through the Internet. That fact significantly contributes to the grow of cyber crimes exploiting the vulnerability of human character.” (National Program on Cybersecurity)

(2) Lack of continuous education and awareness in cybersecurity area



EDUCATION AND CONTINUOUS AWARENESS

Policy plan

 Awareness campaigns	Development of awareness in the regard of existing risks of cyberspace
 Educational curriculum	Augmentation of cybersecurity educational curriculum
 Awareness portal	Creation of awareness portal for informing about current cyber threats
 Competence requirements	Adoption of the requirements to the competence of employees in cybersecurity domain both in private and public sectors
 Cybersecurity trainings	Organization and implementation of trainings and workshops on cybersecurity for public and private personnel, holders of critical infrastructure
 Cybersecurity laboratory	Creation of cybersecurity laboratory

EDUCATION AND CONTINUOUS AWARENESS

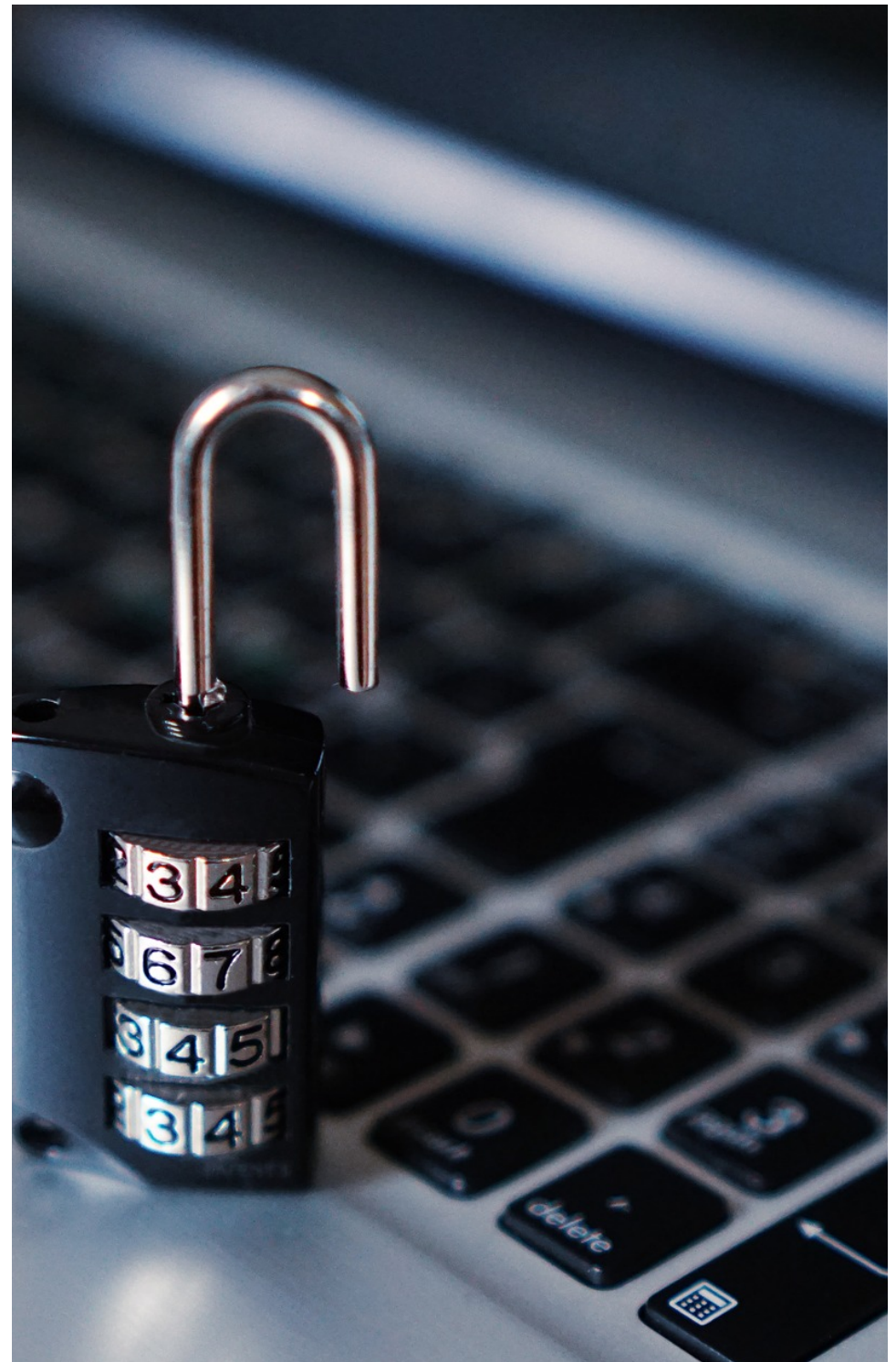
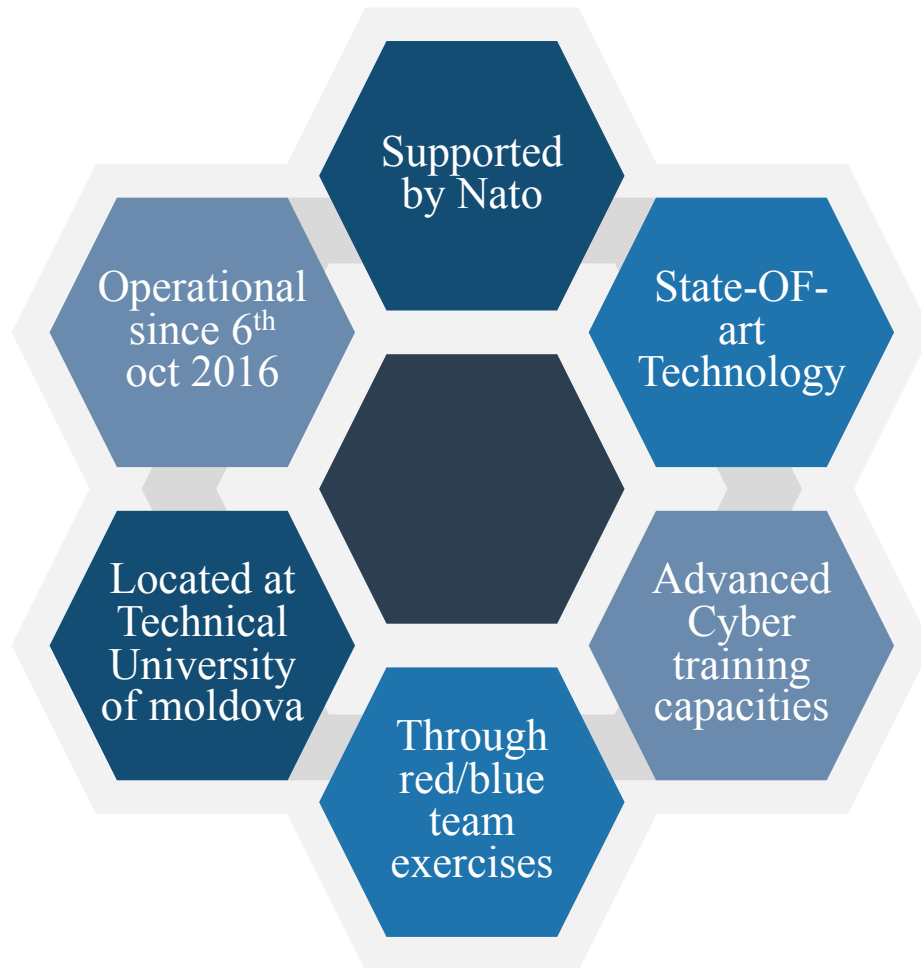
Policy implementation achievements. Cybersecurity trainings



Joint educational activities supported by EU

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

POLICY IMPLEMENTATION ACHIEVEMENTS



A blurred background image of a business meeting. Several people in business attire are gathered around a table, looking at documents and charts. The charts include a bar graph and a pie chart. The overall color palette is dark blue and grey.

RECOMMENDATI ONS

RECOMMENDATIONS

Tips for Implementing a Cybersecurity Program

FOCUS ON CRITICAL INFORMATION	What effect does an attack on your business have and what can be done about it?
EVALUATE A CYBER INCIDENT RESPONSE PLAN	What vulnerabilities have been identified and how have they been resolved?
LOOK OVER THE BUDGET	Is the cybersecurity budget being used appropriately?
BE INFORMED ABOUT KEY RISK INDICATORS	Do you know enough about defence, monitoring, risk and data protection?
WORK WITH INTERNAL AND EXTERNAL SPECIALISTS	Are you constantly being briefed on new developments in technology and cybersecurity?
FOLLOW THE SAFETY RULES OF EXTERNAL PROVIDERS	What are the privacy and security policies of external providers? Do they meet your requirements?
COMPLY WITH LAWS/REGULATIONS FOR CYBERSECURITY	Are you keeping up-to-date with the latest cyber threats and new laws?

RECOMMENDATIONS

Tips for dealing with challenges

CHALLENGES



Change the mass culture



Keep the cyber strategy in mind



Ensure effective national and international collaboration



Allocate resources and budgets



Understand the influence of newly emerged cyber threats



THANK YOU!

Natalia SPINU

natalia.spinu@cts.md

natalia.spinu@cert.gov.md