Cybersecurity: Definition & Relevance

Paolo PRINETTO

Director
CINI Cybersecurity National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

License & Disclaimer

License Information

This presentation is licensed under the
Creative Commons BY-NC License

To view a copy of the license, visit:

http://creativecommons.org/licenses/by-nc/3.0/legalcode

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided "as is" without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Acknowledgments

- The presentation includes material from
  - Alessandro ARMANDO
  - Riccardo FOCARDI
  - Nicolò MAUNERO
  - Gianluca ROASCIO

  whose valuable contributions are here acknowledged and highly appreciated.

Prerequisites

- Lecture:
  - *CS_1.1 - Security – An Introduction*

Goal

- Focusing on Cybersecurity and on its impacts on enterprises and society.

Outline

- Cybersecurity definitions
- Cybersecurity impacts
- Cybersecurity fields

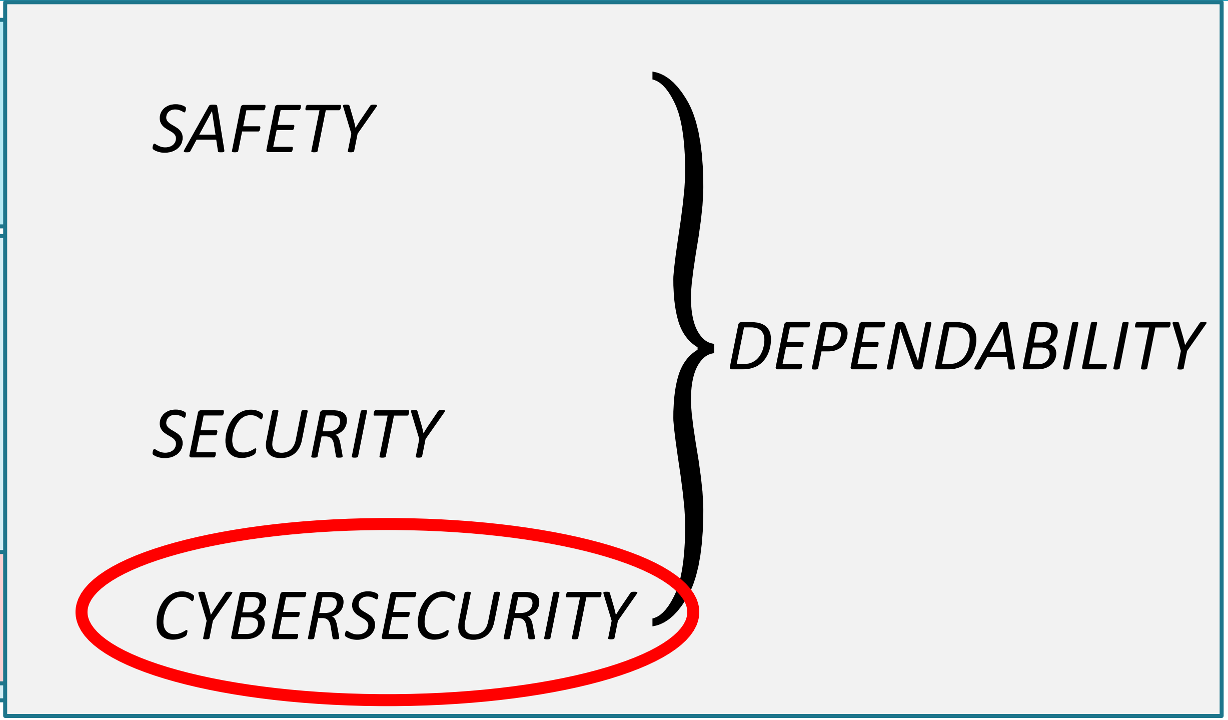
Outline

- Cybersecurity definitions
- Cybersecurity impacts
- Cybersecurity fields

Protecting what

- People
- Environment

- Objects
- Computers
- Information
- Cyberspace



SAFETY

SECURITY

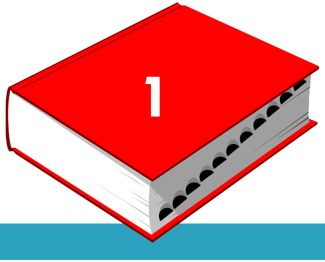
CYBERSECURITY

DEPENDABILITY

Cybersecurity

- A plenty of definitions…

Cybersecurity



- Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

[CNSSI 4009-2015 (NSPD-54/HSPD-23)
NISTIR 7621 Rev. 1 under Cybersecurity (CNSSI 4009-2015)]

Cybersecurity

- The prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.

[NISTIR 8074 Vol. 2 under Cybersecurity]

Cybersecurity

- The process of protecting information by preventing, detecting, and responding to attacks.

[NISTIR 8183 under Cybersecurity (Framework for Improving Critical Infrastructure Cybersecurity, version 1.0]

Cybersecurity

- Refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

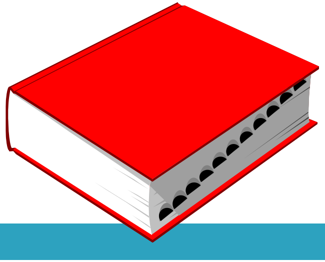
[HM Government, UK, “National cyber security strategy 2016–2021,” 2016. https://www.gov.uk/government/publications/national-cyber-security- strategy-2016-to-2021]

Cybersecurity

- That practice that allows an entity (organization, citizen, nation, ...) to protect its physical assets and confidentiality, integrity and availability of its information from threats that come from *cyberspace*

[standard ISO/IEC 27000:2014 e ISO/IEC 27032:2012]

Cyberspace



- That complex resulting from the interaction of people, software and services on the Internet by means of technologies, devices and networks connected to it

[standard ISO/IEC 27000:2014 e ISO/IEC 27032:2012]

Cyberspace

- The *most complex* thing that man has ever built:

Cyberspace

- The *most complex* thing that man has ever built:
  - union of thousands of networks
  - stratifications of software programs and protocols
  - heterogeneity of devices and terminals

Cyberspace

- The *most complex* thing that man has ever built:
  - union of thousands of networks
  - stratifications of software programs and protocols
  - heterogeneity of devices and terminals
  - Internet though as a *friendly* collaboration tool and with *best-effort* services
  - …

Cyberspace

- Allows us to:
  - communicate and interact anywhere, anytime
  - carry out more and more activities per unit of time
  - store and manage larger and larger amounts of data
  - overcoming space-time barriers (including borders)

Cyberspace

- Alessandro Baricco called it l'*oltremondo*

Cyberspace

- The *most complex* thing that man has ever built
- Complexity generates *vulnerabilities*
- As in the real world, in the cyberspace our *vulnerabilities* and *weaknesses* are exploited by cyber-criminals to launch *attacks*
- They use the cyberspace to attack not the cyberspace itself, but the *real world*!!

Outline

- Cybersecurity definitions
- Cybersecurity impacts
- Cybersecurity fields

Why taking care of it

- The computerization of society and the digitization of goods, merchandise, and services, both public and private, obliges us to pay great attention to the security of all IT and OT assets.

Why taking care of it

Critical Infrastructures

Cybersecurity & Critical Infrastructures

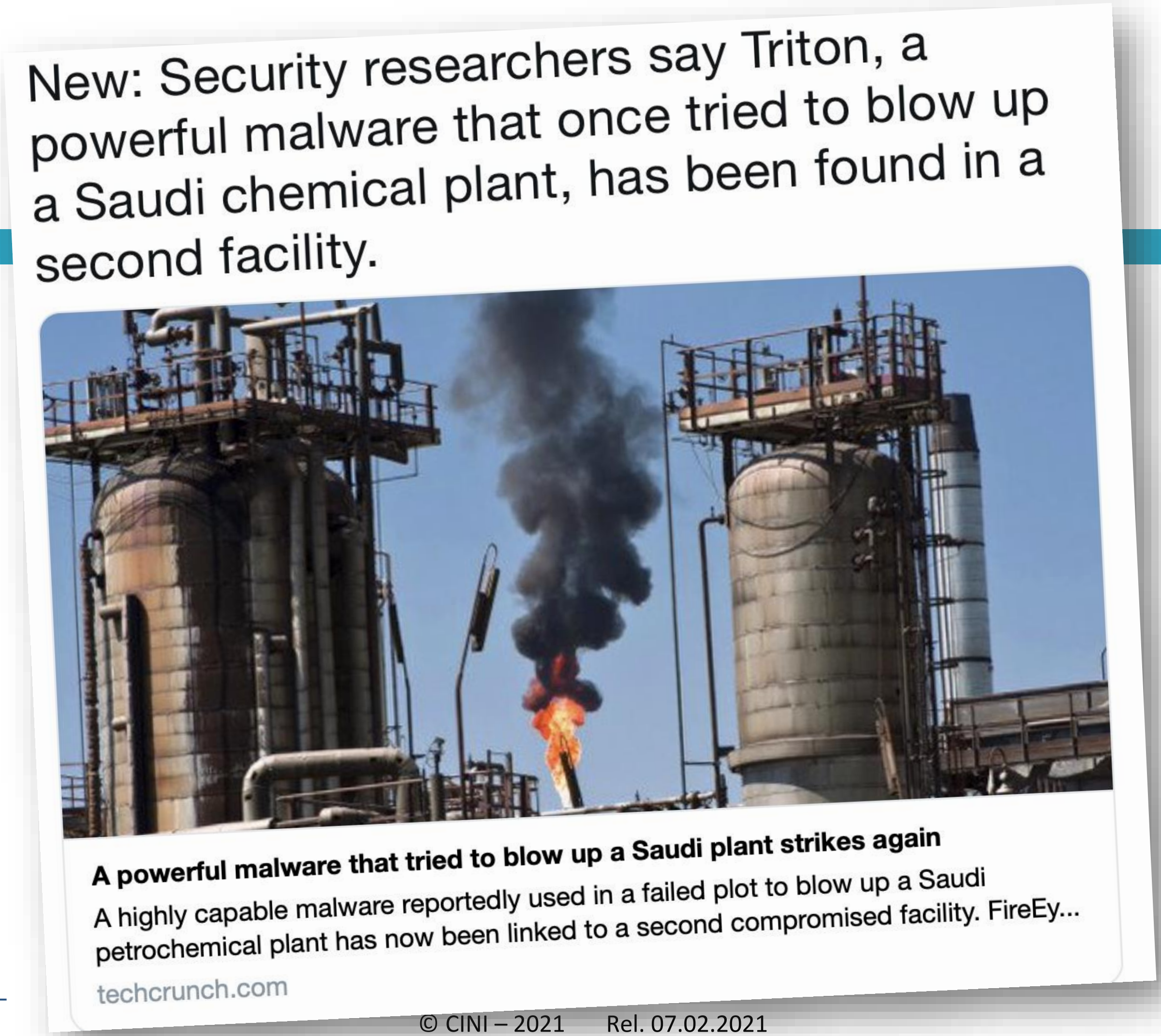
- Cyber attacks endanger the safety of citizens when they affect the distribution networks of essential services such as health, energy, transport, i.e., the *critical infrastructures* of modern societies.

U.S. Critical Infrastructure Full of Security Holes

By Ann R. Thryft 06.04.2020 0

The coronavirus pandemic has spawned a huge increase in cyberthreats and attacks. While much of this is aimed at consumers, a lot has also targeted companies whose employees must now access critical infrastructure, such as industrial control systems (ICS) and operational technology (OT) networks, from home.

But that critical infrastructure, which keeps modern society going even during a pandemic, is seriously under-protected against cyberattacks, say recent reports from cybersecurity companies.



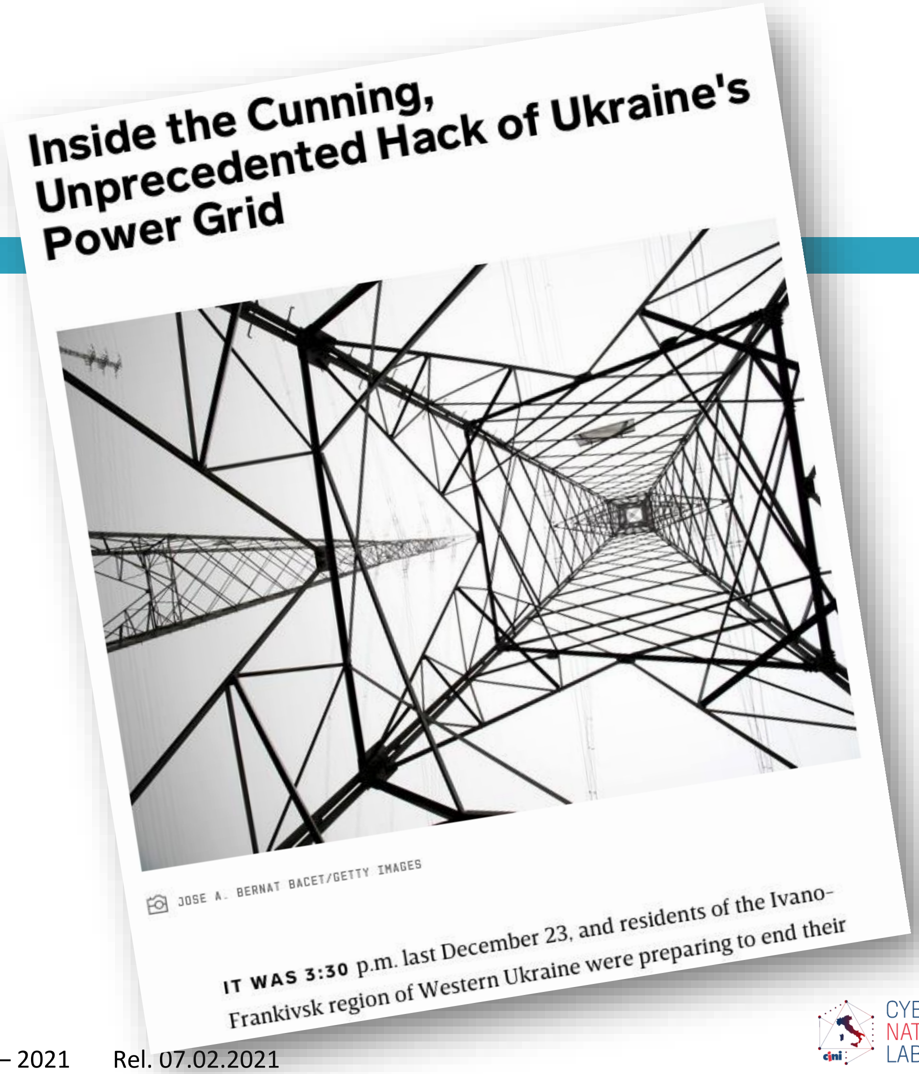
New: Security researchers say Triton, a powerful malware that once tried to blow up a Saudi chemical plant, has been found in a second facility.

A powerful malware that tried to blow up a Saudi plant strikes again

A highly capable malware reportedly used in a failed plot to blow up a Saudi petrochemical plant has now been linked to a second compromised facility. FireEy...

techcrunch.com

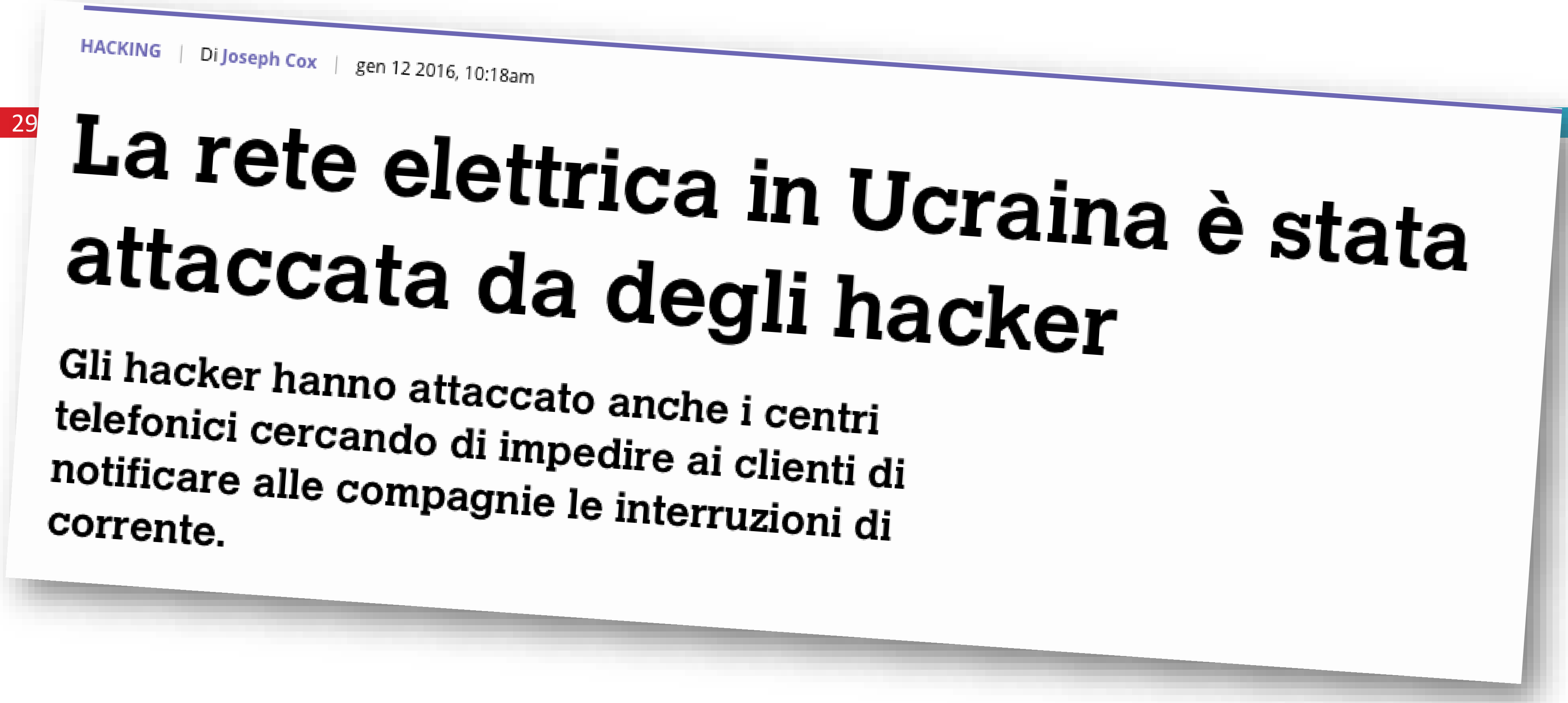
2015, Dec. 23rd



Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

JOSE A. BERNAT BACET/GETTY IMAGES

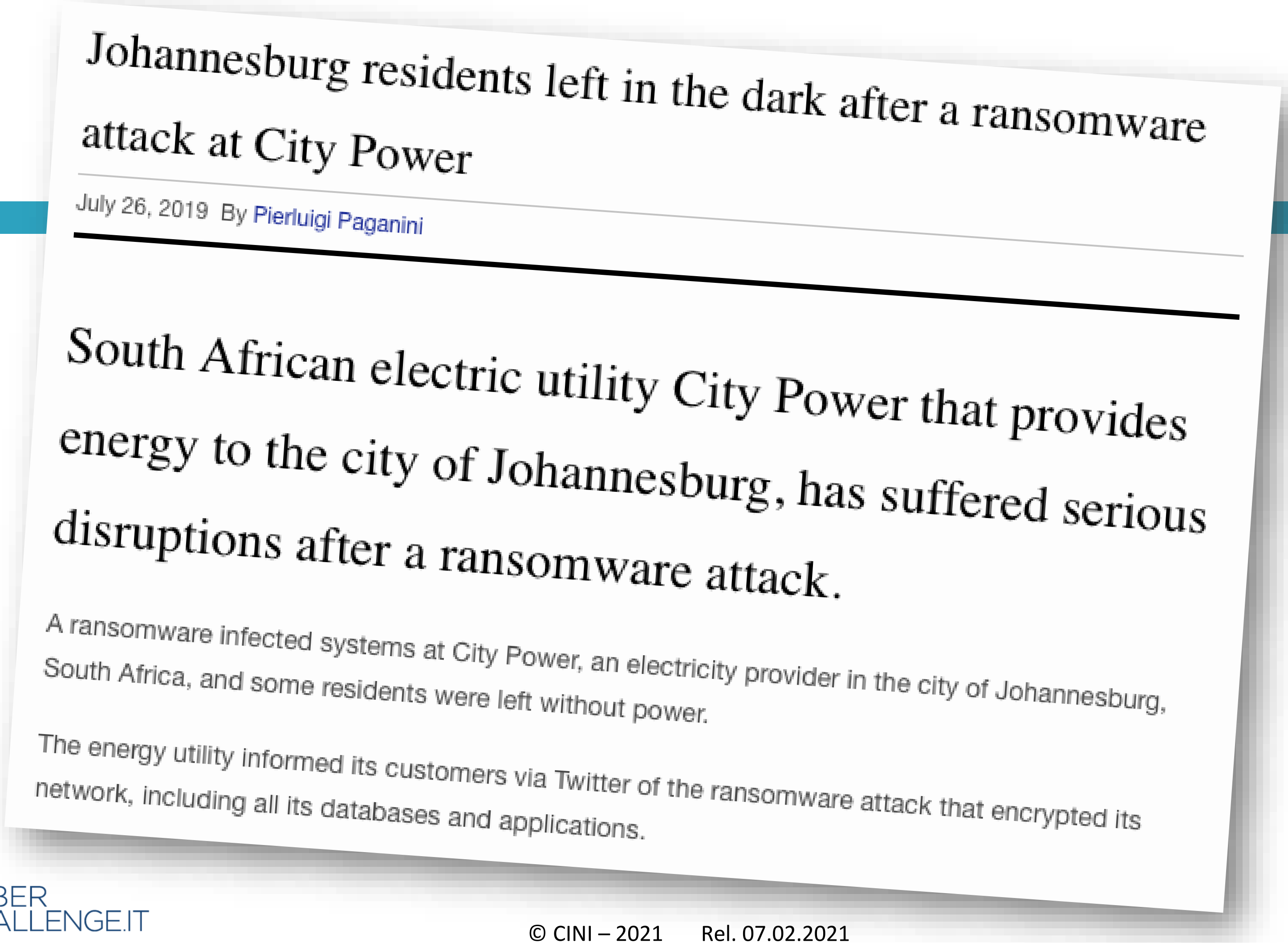
IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their



HACKING | Di Joseph Cox | gen 12 2016, 10:18am

La rete elettrica in Ucraina è stata attaccata da degli hacker

Gli hacker hanno attaccato anche i centri telefonici cercando di impedire ai clienti di notificare alle compagnie le interruzioni di corrente.



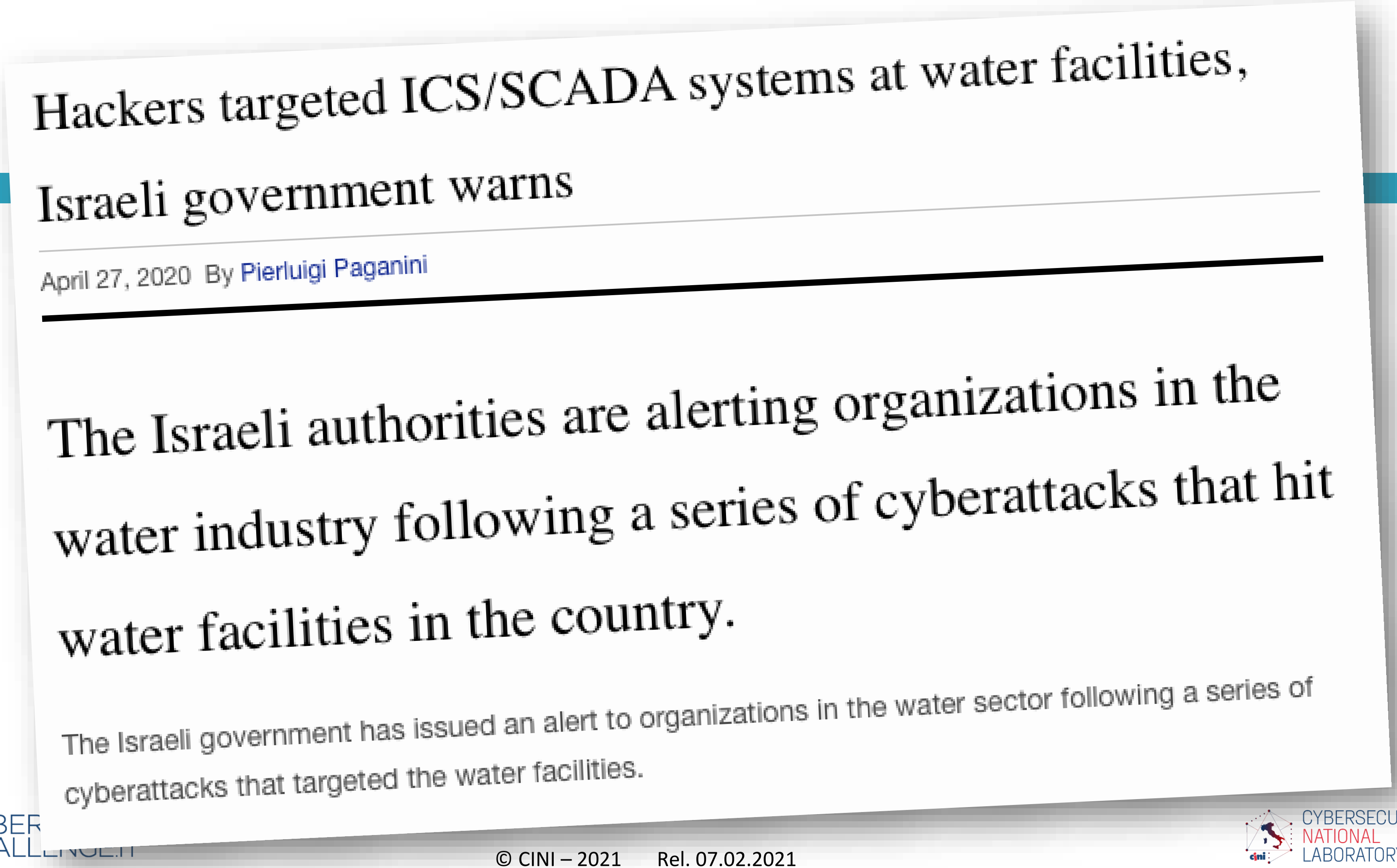
Johannesburg residents left in the dark after a ransomware attack at City Power

July 26, 2019 By Pierluigi Paganini

South African electric utility City Power that provides energy to the city of Johannesburg, has suffered serious disruptions after a ransomware attack.

A ransomware infected systems at City Power, an electricity provider in the city of Johannesburg, South Africa, and some residents were left without power.

The energy utility informed its customers via Twitter of the ransomware attack that encrypted its network, including all its databases and applications.



Hackers targeted ICS/SCADA systems at water facilities, Israeli government warns

April 27, 2020 By Pierluigi Paganini

The Israeli authorities are alerting organizations in the water industry following a series of cyberattacks that hit water facilities in the country.

The Israeli government has issued an alert to organizations in the water sector following a series of cyberattacks that targeted the water facilities.

Why taking care of it

Critical Infrastructures

Enterprises

Cybersecurity & Enterprises

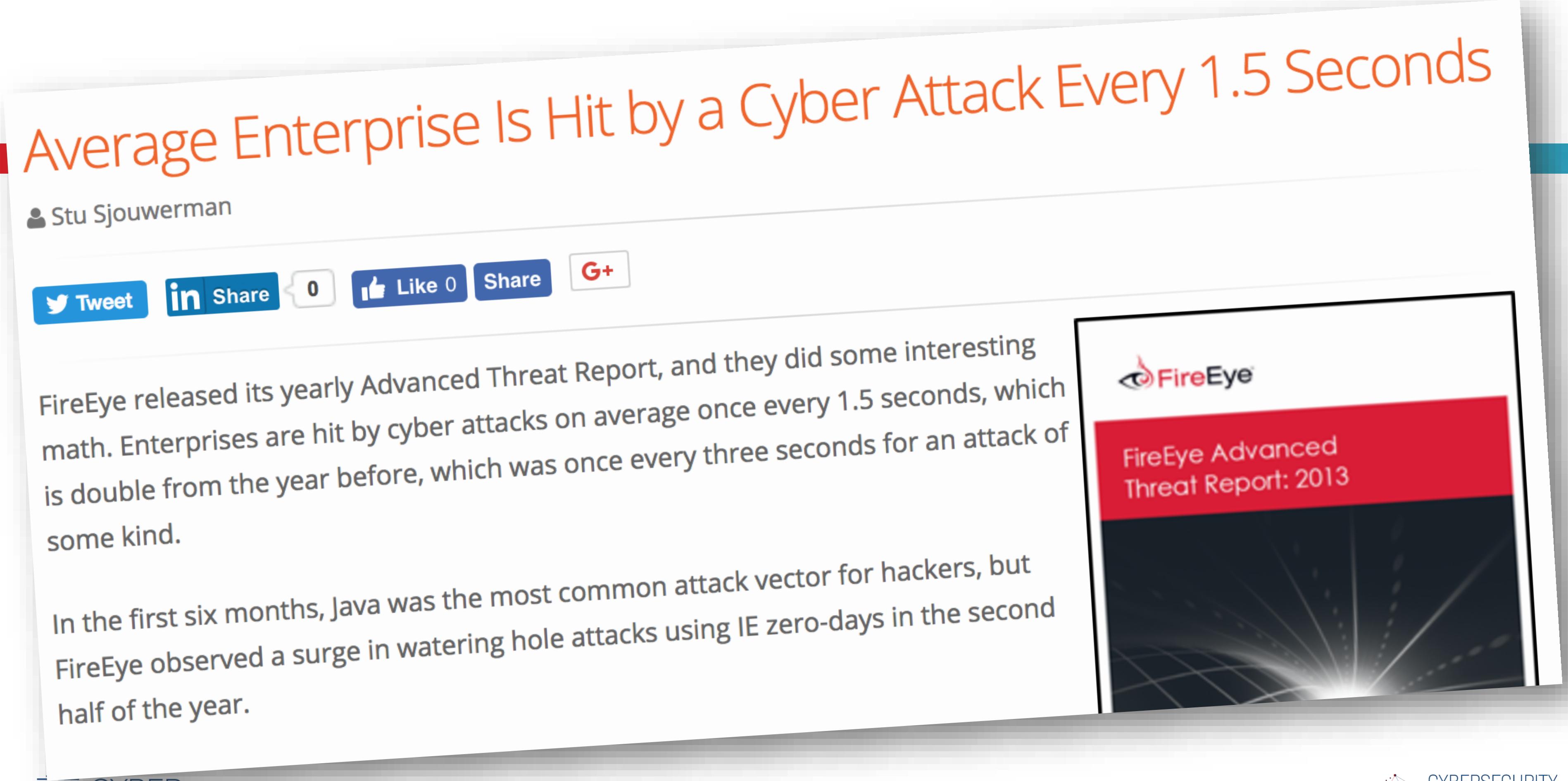
- A successful cyber attack could represent a moment of no return for the credibility of a company, the development of its business, its ability to sell useful products in a regime of healthy competition.

Company clustering…

- Companies can be clustered in 2 sets:
  - the one that have been attacked

Company clustering…

- Companies can be clustered in 2 sets:
  - the one that have been attacked
  - the one that do not know they have been attacked



Average Enterprise Is Hit by a Cyber Attack Every 1.5 Seconds

Stu Sjouwerman

FireEye released its yearly Advanced Threat Report, and they did some interesting math. Enterprises are hit by cyber attacks on average once every 1.5 seconds, which is double from the year before, which was once every three seconds for an attack of some kind.

In the first six months, Java was the most common attack vector for hackers, but FireEye observed a surge in watering hole attacks using IE zero-days in the second half of the year.

FireEye

FireEye Advanced Threat Report: 2013

Status

[Claudia Biancotti: “The price of cyber (in)security: evidence from the Italian private sector”. *Questioni di Economia e Finanza 407*, Banca d’Italia, Dicembre 2017]

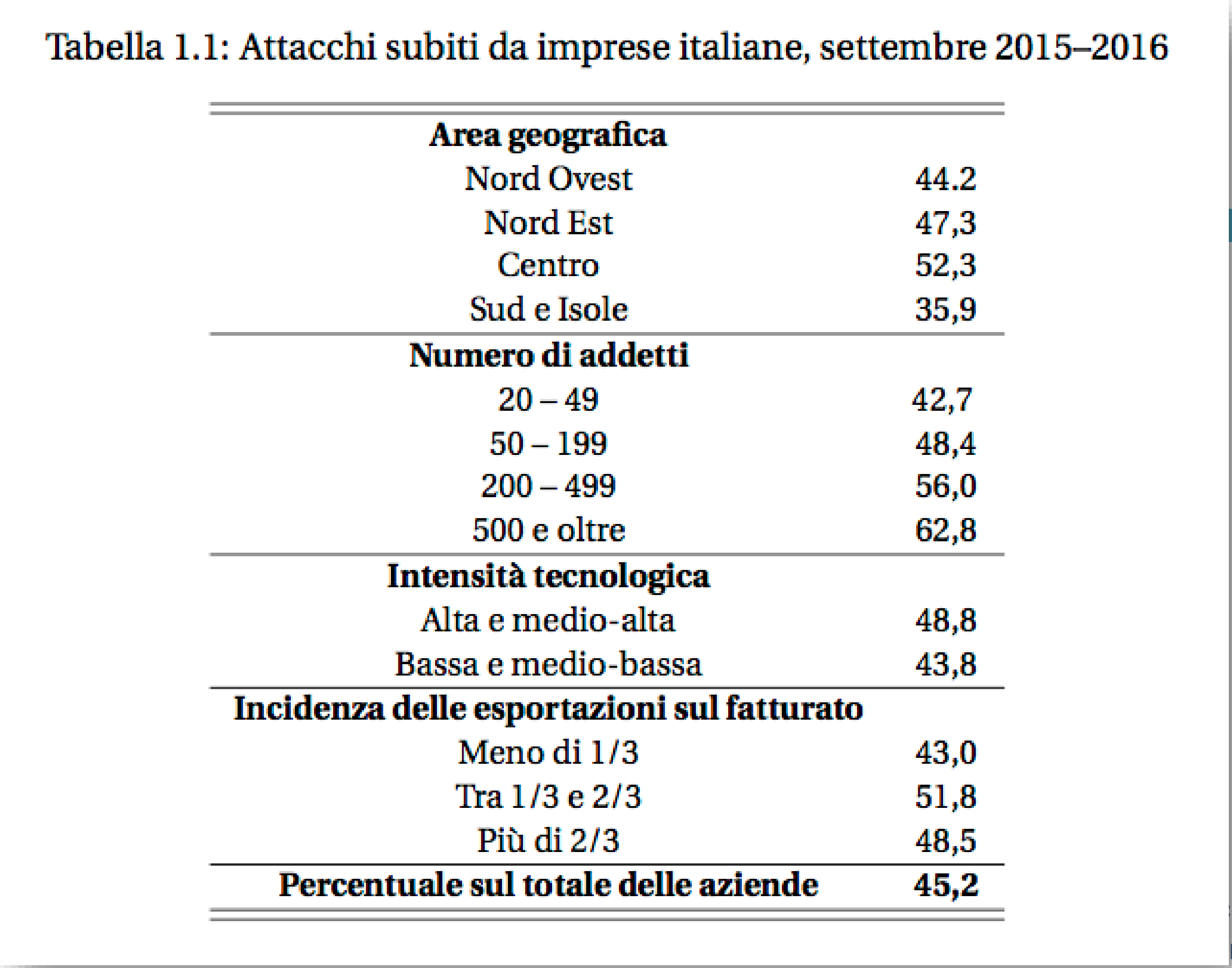


Tabella 1.1: Attacchi subiti da imprese italiane, settembre 2015–2016

Area geografica	
Nord Ovest	44.2
Nord Est	47,3
Centro	52,3
Sud e Isole	35,9
Numero di addetti	
20 – 49	42,7
50 – 199	48,4
200 – 499	56,0
500 e oltre	62,8
Intensità tecnologica	
Alta e medio-alta	48,8
Bassa e medio-bassa	43,8
Incidenza delle esportazioni sul fatturato	
Meno di 1/3	43,0
Tra 1/3 e 2/3	51,8
Più di 2/3	48,5
Percentuale sul totale delle aziende	**45,2**

Why taking care of it

Critical Infrastructures

Enterprises

Country Level

Cybersecurity at the Countly level

- A successful cyber attack could destabilise the stock market and plunge entire countries into chaos, or block gas supplies in winter or the urban waste cycle: what political scenario would then follow?

Why taking care of it

Critical Infrastructures

Enterprises

Country Level

Rights

Cybersecurity & Rights

- Information security coincides today with the security of data and information that define us as citizens, voters, workers, consumers.
- If the security of data and information is lacking, it is our privacy that suffers, which is the precondition for exercising the right of opinion, expression, news, association, movement, business, property.

Outline

- Cybersecurity definitions
- Cybersecurity impacts
- Cybersecurity fields

Cybersecurity Fields

- Cybersecurity is becoming an important element in everyday life
- However, the foundational knowledge on which the field of cyber security is being developed is fragmented, and as a result, it can be difficult to map coherent paths of progression through the subject.

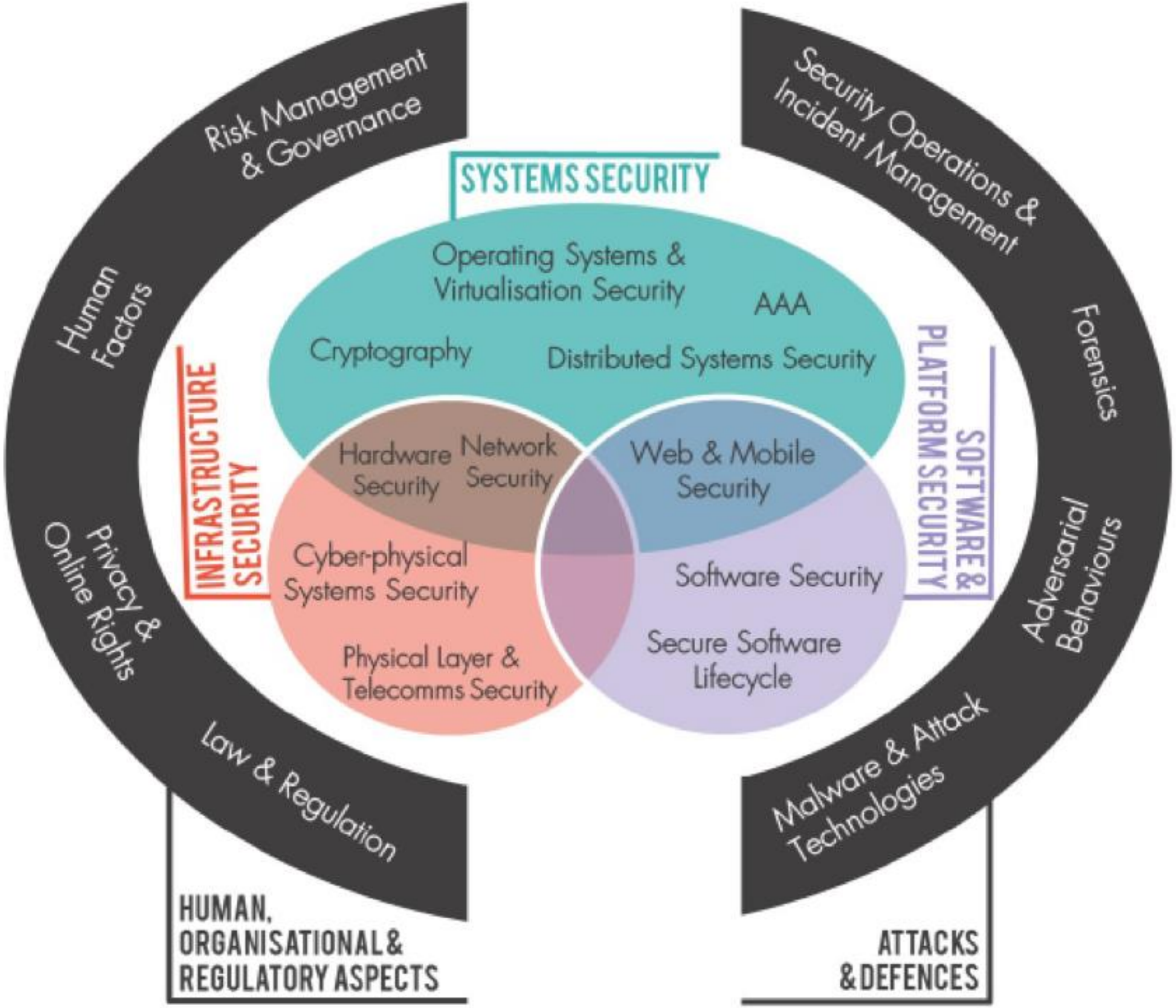
The Cyber Security Body of Knowledge (CyBOK)

The Cyber Security Body of Knowledge (CyBOK)

- The CyBOK is divided into 19 top-level Knowledge Areas (KAs), grouped into 5 broad categories:

- *Human, Organisational, and Regulatory Aspects*
- *Attacks and Defences*
- *Systems Security*
- *Software and Platform Security*
- *Infrastructure Security*

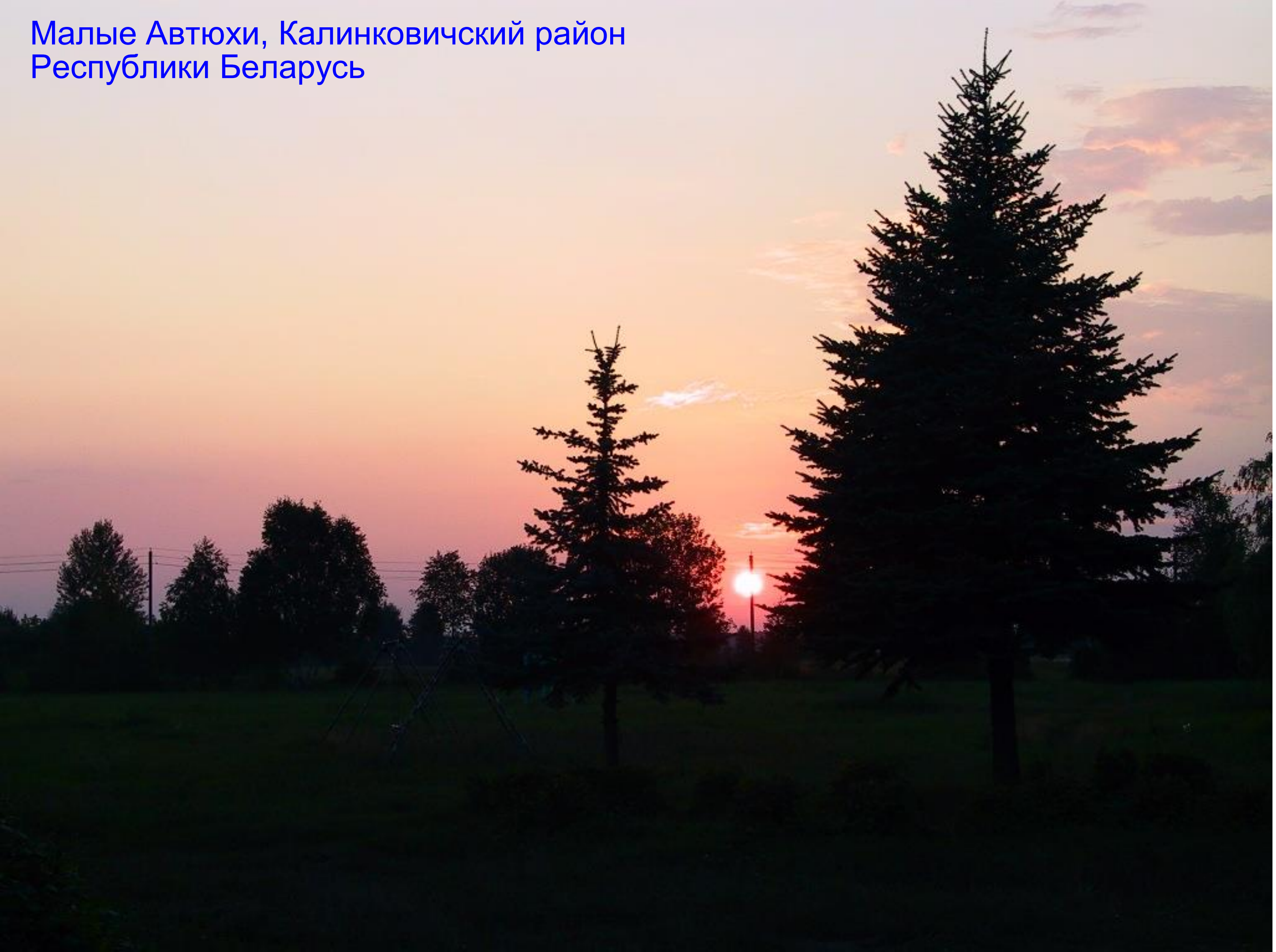
CyBOK categories


Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
AAA
Cryptography
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Web & Mobile Security
Cyber-physical Systems Security
Physical Layer & Telecomms Security
Software Security
Secure Software Lifecycle
SOFTWARE & PLATFORM SECURITY
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

CYBER CHALLENGE.IT

Cybersecurity Glossary

- https://csrc.nist.gov/Glossary



Малые Автюхи, Калинковичский район
Республики Беларусь

Paolo PRINETTO

Director
CINI Cybersecurity National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it