Introduzione alla Sicurezza

Paolo PRINETTO
Director
CINI Cybersecurity National Laboratory
Paolo.Prinetto@polito.it
Mob. +39 335 227529

cini
Cybersecurity
National Lab

www.consorzio-cini.it

License & Disclaimer

License Information

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

Thanks

- The presentation includes material from several contributors, whose valuable help is here acknowledged and highly appreciated.

Contributors

- CyberChallenge.IT
- Giuseppe AIRO' FARULLA
- Jean ARLAT
- Alessandro ARMANDO
- Roberto BALDONI
- Rocco DE NICOLA
- Arturo DI CORINTO
- Giorgio DI NATALE
- Eugene KASPERSKY
- Rosario PUGLIESE
- Francesco VESTITO
- Stefano ZANERO

Outline

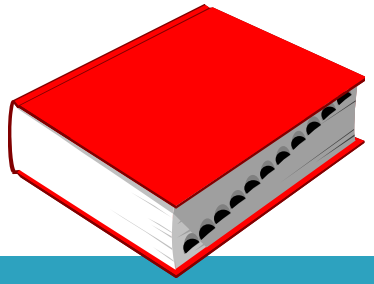
- Introduzione
- Rilevanza & Costi
- Vulnerabilità & Attacchi
- Formazione
- Aspetti etici e legali
- Privacy
- Security by Design

Roberto BALDONI
Rocco DE NICOLA
Paolo PRINETTO

cini
Cybersecurity
National Lab

www.consorzio-cini.it

Sicurezza



- Condizione oggettiva esente da pericoli, o garantita contro eventuali pericoli

Sicurezza – Accezioni diverse

Accezione

- Physical
- Safety
- Security

Sicurezza – Accezioni diverse

Accezione	Protezione di cosa:
Physical	Spazi fisici
Safety	
Security	

Sicurezza – Accezioni diverse

Accezione	Protezione di cosa:
Physical	della persona
Safety	dell'ambiente circostante
Security	

Sicurezza – Accezioni diverse

Accezione	
Physical	See Lecture 1
Safety	
Security	

Sicurezza – Accezioni diverse

Accezione	Protezione di cosa:
Physical	dei computer
Safety	delle informazioni
Security	del cyberspace

Sicurezza

- È funzione dell'insieme dei pericoli e delle minacce (***threat***) dalle quali si vogliono proteggere i propri ***asset***

Sicurezza

- È funzione dell'insieme dei pericoli e delle minacce (***threat***) dalle quali si vogliono proteggere i propri ***asset***

Caveat

- I threat assumono significati diversi nelle varie accezioni

Sicurezza – Accezioni diverse

Accezione	Protezione di cosa:
Physical	dei computer
Safety	delle informazioni
Security	del cyberspace

Computer security

- Deals with the prevention and detection of unauthorized actions by users of a computer system

Computer security

- Deals with the prevention and detection of unauthorized actions by users of a computer system

- *Authorization* is central to definition
- Sensible only relative to a *security policy*, stating who (or what) may perform which action

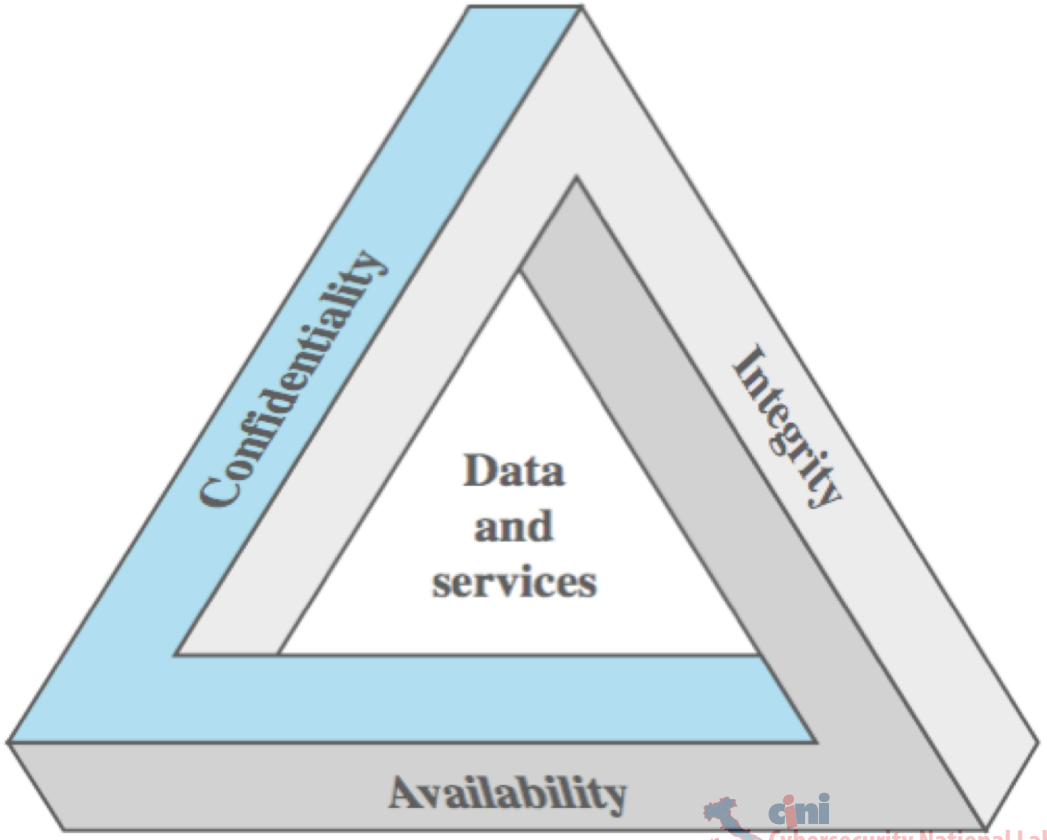
Computer security

- Measures and controls that ensure *confidentiality*, *integrity*, and *availability* of information system assets including hardware, software, firmware, and information being processed, stored, and communicated

[The NIST Internal/Interagency Report NISTIR 7298
- Glossary of Key Information Security Terms, May 2013
(**NIST** = U.S. National Institute of Standards and Technology)]

The CIA triad

- *Confidentiality, Integrity, Availability* form what is often referred to as the *CIA triad*



Secure Systems Basic Pillars

- *Confidentiality*
  - Ensuring that information is accessible only to those authorized
- *Integrity*
  - Ensuring that information has not been modified
- *Availability*
  - Legitimate users have access when they need it

Confidentiality

It covers 3 related areas:

- *Data*
- *Individuals (Privacy)*
- *Organizations (Secrecy)*

Confidentiality

It covers 3 related areas:

- *Data*
- *Individuals (Privacy)*
- *Organizations (Secrecy)*

- Assures that confidential information is not disclosed to unauthorized individuals

Confidentiality

It covers 3 related areas:

- *Data*
- *Individuals (Privacy)*
- *Organizations (Secrecy)*

- Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Confidentiality

It covers 3 related areas:

- *Data*
- *Individuals (Privacy)*
- *Organizations (Secrecy)*

- Is sometimes used in the sense of *anonymity*, keeping one's identity private

Confidentiality

It covers 3 related areas:

- *Data*
- *Individuals (Privacy)*
- *Organizations (Secrecy)*

- Pertains to confidentiality for organizations, such as commercial companies or governments

Integrity

It covers two related concepts:

- *Data integrity*: Assures that information and programs are changed only in a specified and authorized manner
- *System integrity*: Assures that a system performs its operations in unimpaired manner, free from unauthorized manipulation

Availability

- Assures that systems work promptly and service is not denied to authorized users.

Secure Systems Additional Pillars

- *Resilience*
  - Ensuring that attacking previous basic pillars will be difficult o limiting the potential damage
- *Non-repudiation*
  - Ensuring that the originator of the communication cannot deny later
- *Authenticity*
  - Ensuring that information comes from trusted source
- *Access control*
  - Unauthorized users cannot have access

Sicurezza – Accezioni diverse

Accezione	Protezione di cosa:
Physical	dei computer
Safety	delle informazioni
Security	del cyberspace

Information security

- Information security is even more general
- It deals with information, independently of computer systems

Information security - Remark

- Information is more general than data
- Data convey information
- But information may also be revealed, without revealing data, e.g., by statistical summaries
- Constitutes a basic right: protection of self (possessions, ...)

Quotazioni dei dati nel Dark Web

data di nascita, social security number

informazioni su carte di credito

social media account

cartelle sanitarie

Quotazioni dei dati nel Dark Web

- 3 $
  data di nascita, social security number
- 0.75 - 40 $
  informazioni su carte di credito
- 16 - 325 $
  social media account
- 500 - 1200 $
  cartelle sanitarie

Sicurezza – Accezioni diverse

Accezione	Protezione di cosa:
Physical	dei computer
Safety	delle informazioni
Security	del cyberspace

Cybersecurity

- Quella pratica che consente a una entità (organizzazione, cittadino, nazione, …) la protezione dei propri asset fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyberspace

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

Cyberspace

- Quel complesso risultante dall'interazione di persone, software e servizi su Internet per mezzo di tecnologie, dispositivi e reti a esso connesse

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

Cyberspace

- La cosa *più complessa* che l'uomo abbia mai costruito:

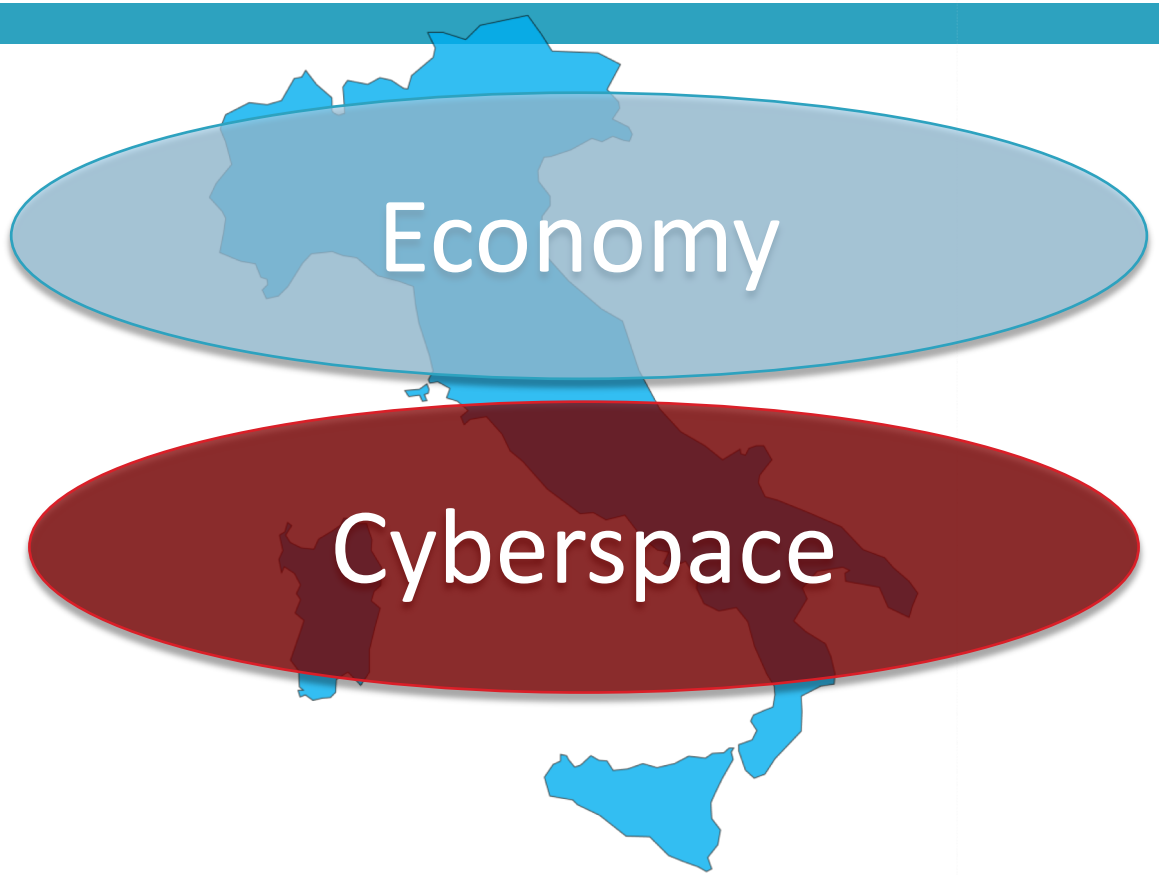
Cyberspace

- La cosa *più complessa* che l'uomo abbia mai costruito:
  - unione di migliaia di reti
  - stratificazione di programmi software e protocolli
  - eterogeneità di apparati e terminali

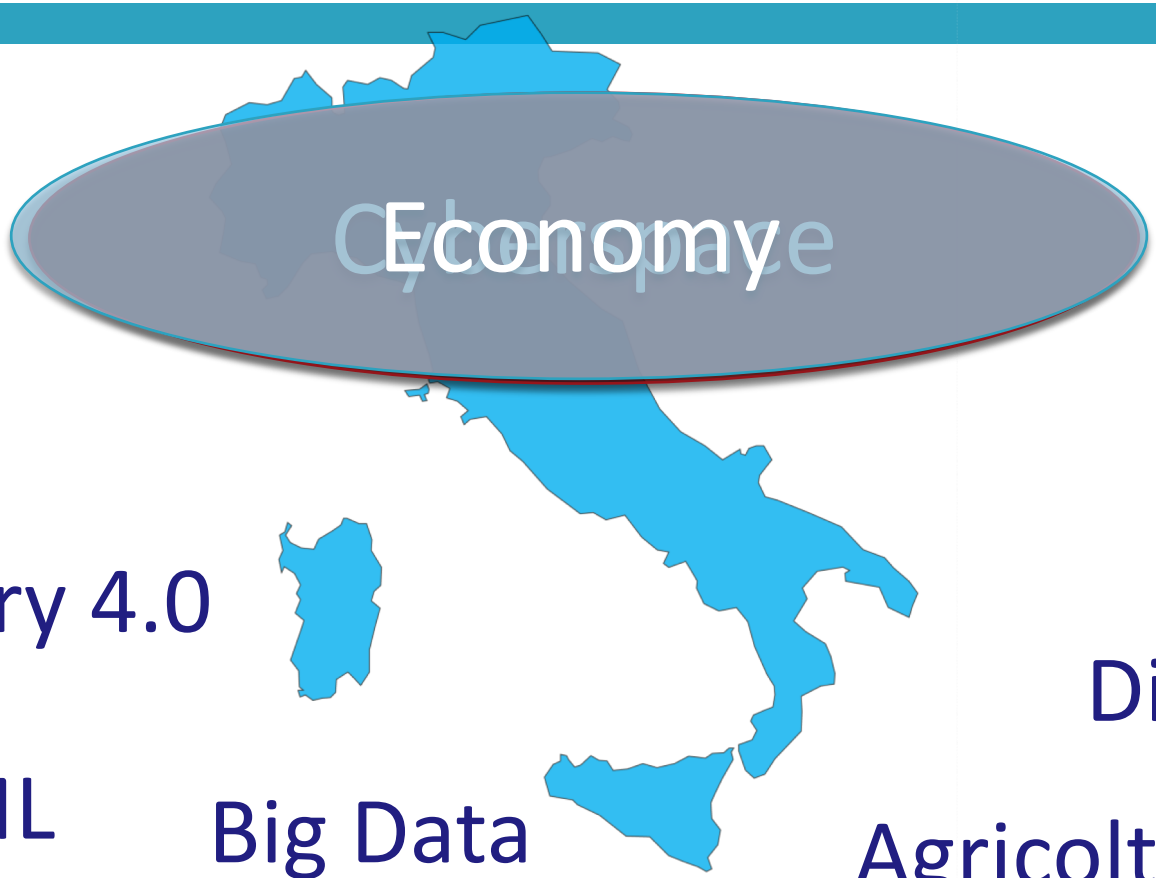
Cyberspace

- La cosa *più complessa* che l'uomo abbia mai costruito:
  - unione di migliaia di reti
  - stratificazione di programmi software e protocolli
  - eterogeneità di apparati e terminali
  - Internet pensata come strumento di collaborazione *friendly* e con servizi *best effort*
  - …

Il cyberspace è pervasivo



Il cyberspace è pervasivo



IoT

Drones

Industry 4.0

AI & ML

Big Data

Robotics

Smart Cities

Digital Currencies

Agricolture 4.0

Threat

Minacce agli ***asset*** di un'entità target che, basandosi su agenti software malevoli (***threat agent***) e sfruttando delle ***vulnerabilità***, anche umane, del target stesso, sono in grado di ***attaccare*** (penetrare) il suo sistema informatico e/o la sua rete.

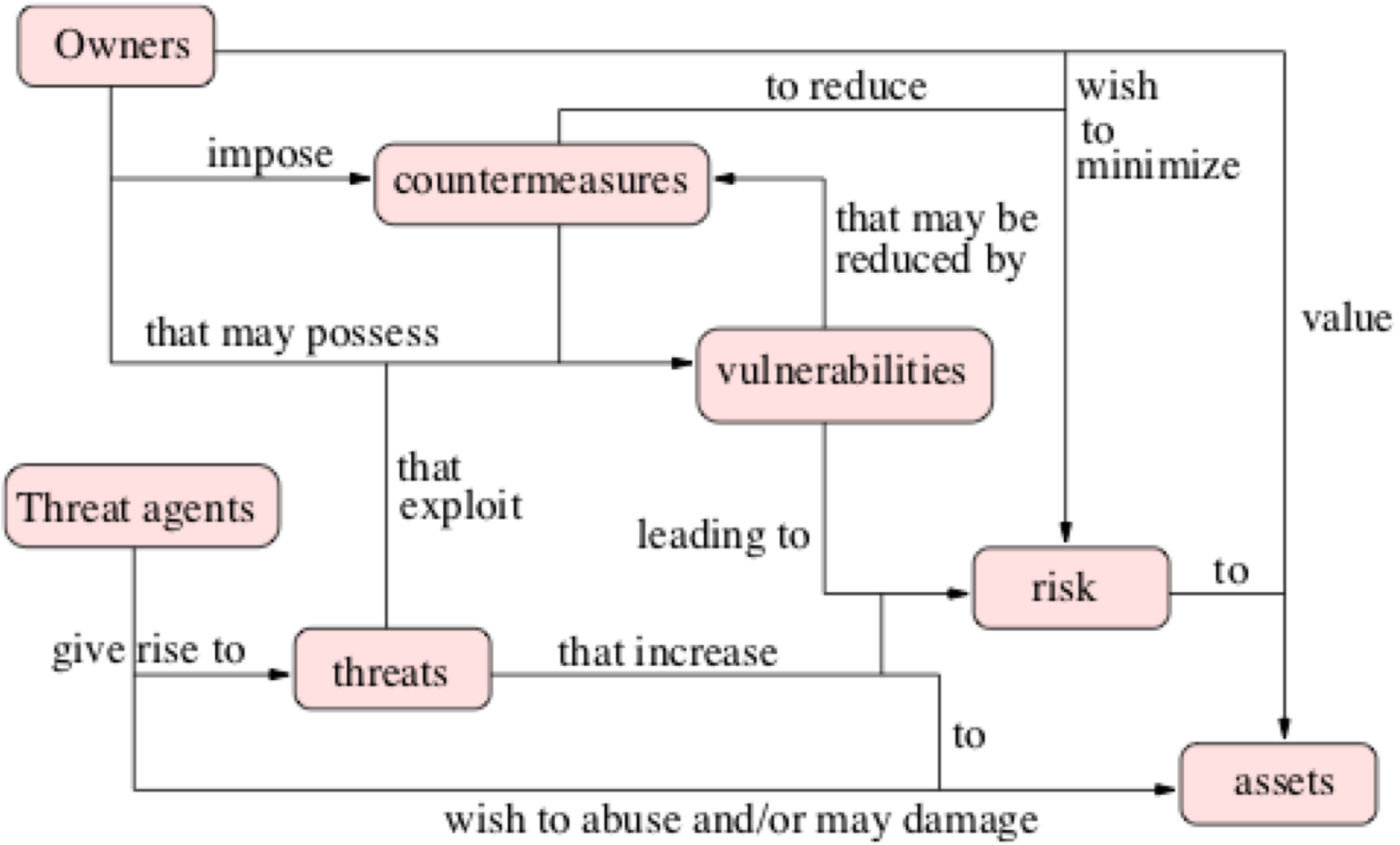
Risks

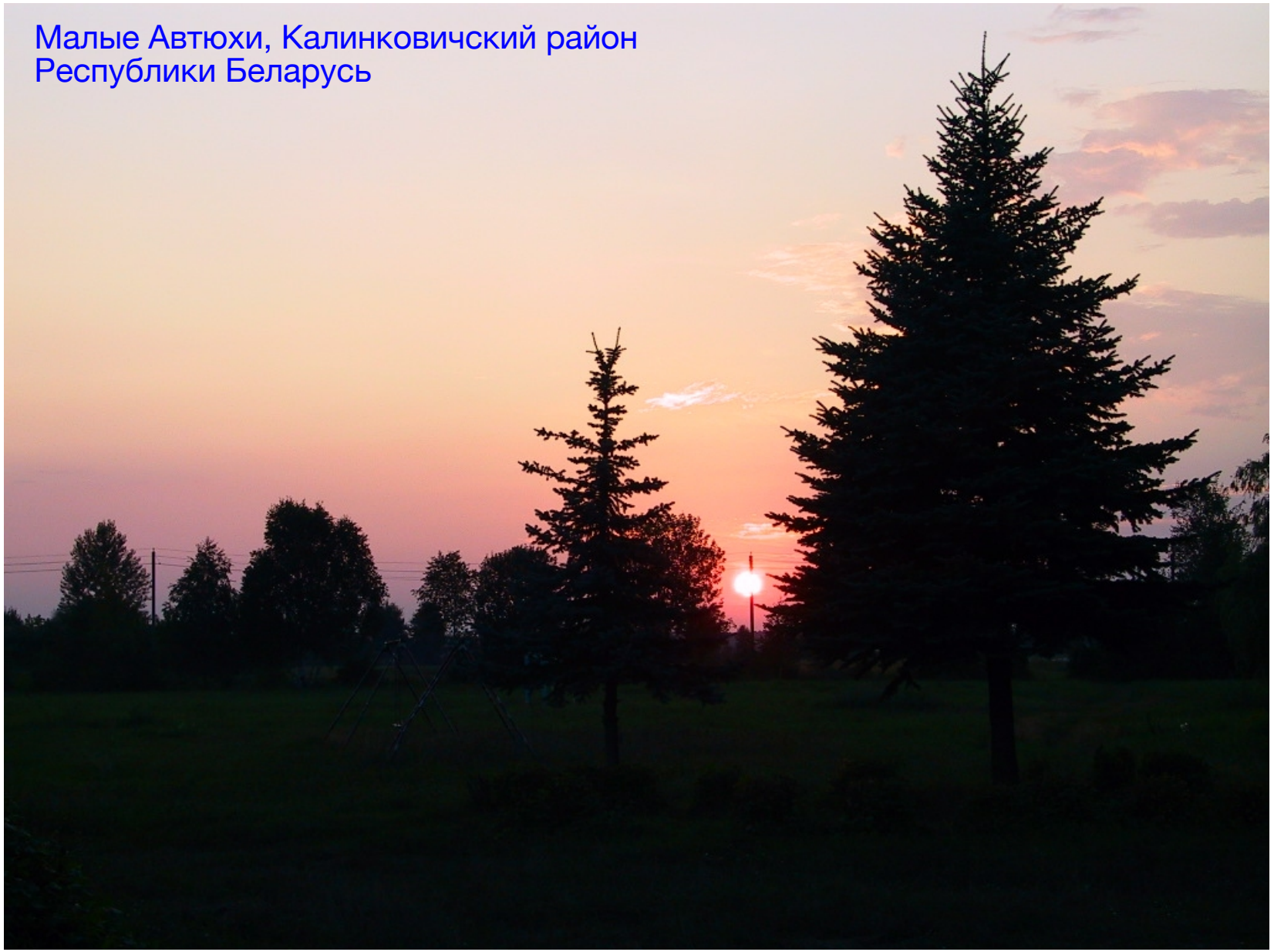
- Owners analyse threats to determine which ones apply; these are the *risks* that can be costed
- This helps the selection of *countermeasures*, which reduce the *vulnerabilities*

Residual Risks

- Vulnerabilities may remain, leaving some residual risk
- Owners seek to minimise that risk, within other constraints (feasibility, expense)

Fundamental concepts and interrelationships





Paolo PRINETTO
Direttore
Lab, Naz. Cybersecurity
Paolo.Prinetto@polito.it
Mob. +39 335 227529

cini
Cybersecurity
National Lab

cini
consorzio
interuniversitario
nazionale
per l'informatica

www.consorzio-cini.it