CASD

Global challenges

March 23rd 2015

Cyber security: what a decision maker should know

Elisabetta Zuanelli

University of Rome "Tor Vergata"

President of CReSEC (Center for econtent R&D)

Coordinator of the Observatory on information security

The observer's paradox

What do we know about cybersecurity:

definitions, shared knowledge, shared strategies

The observer's paradox

What do we know about cybersecurity:

definitions, shared knowledge, shared strategies

Definitions

- Cyberspace
- Cybersecurity
- Cybercrime
- Cyber warfare
- Cyber malware
- Cyber crimeware
- etc.

Shared knowledge

- Typologies of attacks
- Typologies of crime
- National & international data/statistics
- Cybercrime technologies
- Cybersecurity vulnerabilities: social networks, online services, cloud computing, mobile devices (services, apps, etc.)/ human behaviour and technological flaws

Shared strategies

- National strategies (in Europe 2011 and 2013)
- NIST framework for critical infrastructures security
- Central boards
- Number of organisms
- LEAS's
- Private public collaboration
- CERTs
- Investigation, data exchange, knowledge

Question 1

Why cyber attacks and what for:

to violate and corrupt personal or institutional/company information systems (from personal computers to corporate servers)

1. to get money back straight from the solution of corruption

2. to create severe problems in the management of an institution or a company activities (i.e. subtraction of economic data by political/industrial competitors)

3. to slow down or block the services by a company or institution

...Question 1

To subtract information/ data:

1. personal individual identity theft, forgery, etc. to be used for illegal purposes
2. corporate data for insider industrial espionage and economic competition
3. institutional, social and economic data to be used in the political and financial arena
4. political, industrial, military espionage for international competition

...Question 1

The use of Internet for fraudolent activities/ cybercrime activities:

1. child abuse, pedo/pornography
2. drugs market
3. prostitution market
4. migration market
5. dirty money market

...Question 1

Criminal propaganda and antagonist objectives:

1. cyber terrorism/ terrorism recruitment
2. racist propaganda
3. antagonist actions (sites defacement)

Question 2

- Who are the players:

- hacktivists/cybercriminals acting as single entities, group cyber attackers, cybercrime companies getting money straight from cyber attacks,viruses inoculation, malware, etc.)

- **or**

- selling attacks, selling data, selling criminal services in general to others:

- industrial, political, military stakeholders

Question 3

- who are the players in the **Cybercriminal economy**
- what are the market share interests
- who are the buyers (not only the sellers)
- the triangular market of cybercrime economy: cybercriminals,victims, final beneficiaries

The victims (CLUSIT Report 2014)

VITTIME	2011	2012	TOT	INCR.
Mil, LEAs, Intelligen.	153	374	527	244,44%
Others	97	194	291	200,00%
Entertainment / News	76	175	251	230,26%
Online Services / Cloud	15	136	151	906,67%
Research / Education	26	104	130	400,00%
Banking / Finance	17	59	76	347,06%
Softw./ Hardw. Vendor	27	59	86	218,52%
Telco	11	19	30	172,73%
Contractors/Consulting	18	15	33	-16,67%
Security Industry	17	14	31	-17,65%
Religion	0	14	14	1400,00%
Health	10	11	21	110,00%
Chemical / Medical	2	9	11	450,00%
TOTALE	**469**	**1183**	**1652**	**252,24%**

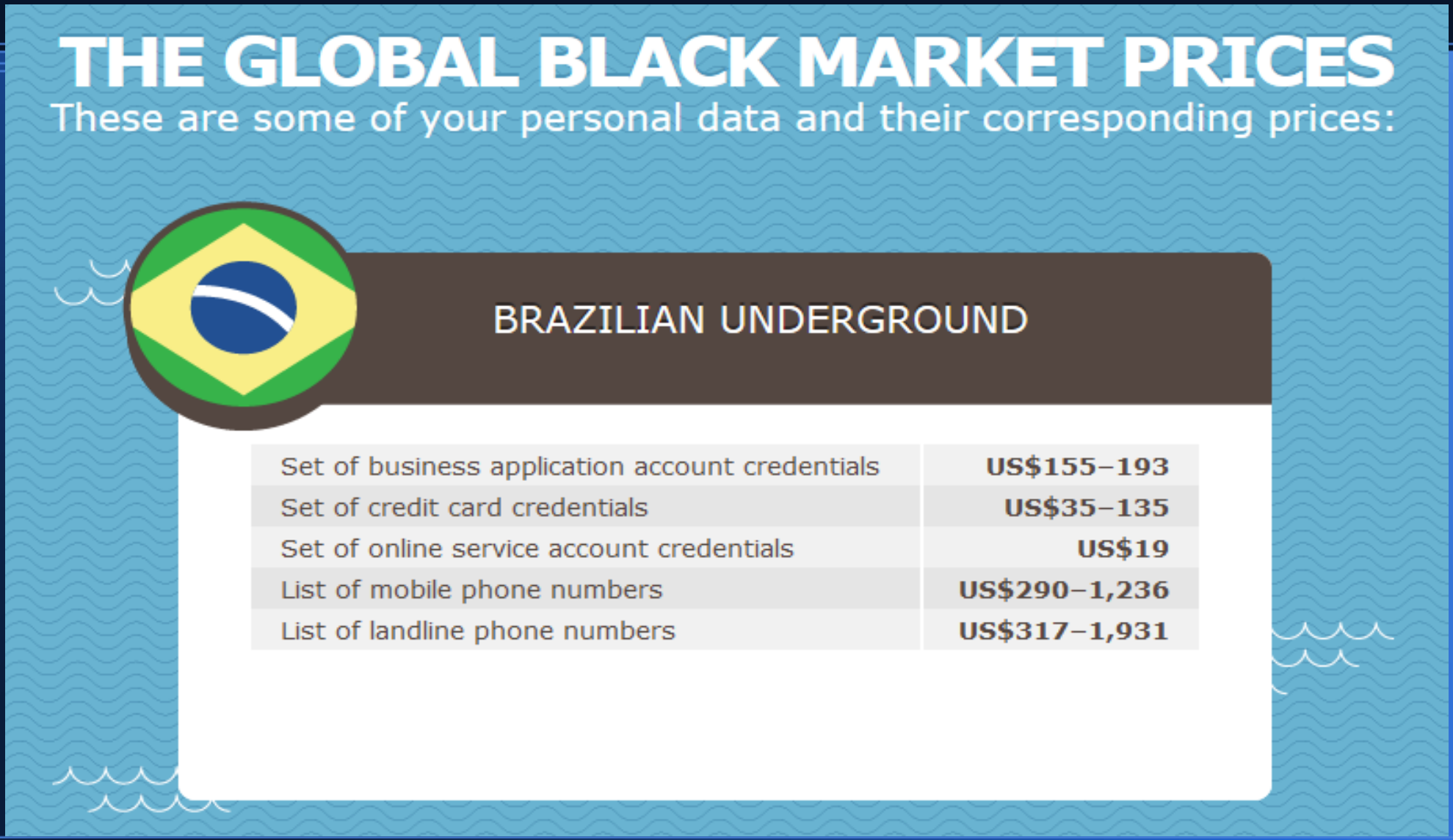
Attacchi per tipologia di vittime nel 2011 e nel 2012

The typologies of attacks (CLUSIT Report 2014)

ATTACCANTI PER TIPOLOGIA	2011	2012	2013	Variazioni 2012 su 2011	Variazioni 2013 su 2012	Variazioni 2013 su 2011
Cybercrime	170	633	609	272,35%	-3,79%	258,24%
Unknown	148	110	0	-25,68%	-100,00%	-100,00%
Hacktivism	114	368	451	222,81%	22,55%	295,61%
Espionage / Sabotage	23	29	67	26,09%	131,03%	191,30%
Cyber warfare	14	43	25	207,14%	-41,86%	78,57%
TOTALE	469	1.183	1.152			

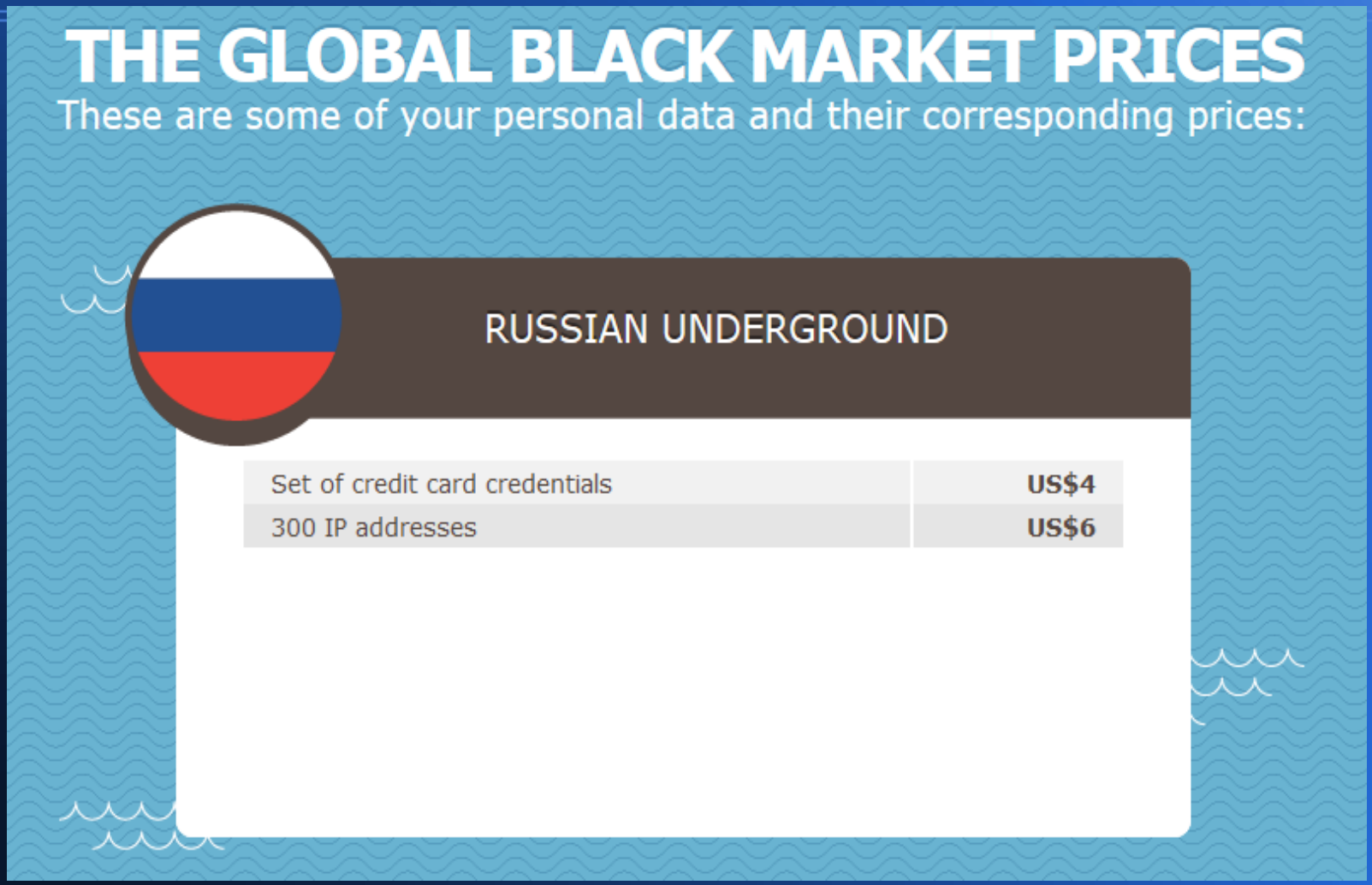
The blackmarket of stolen personal data

The prices


THE GLOBAL BLACK MARKET PRICES
These are some of your personal data and their corresponding prices:
BRAZILIAN UNDERGROUND
Set of business application account credentials
US$155–193
Set of credit card credentials
US$35–135
Set of online service account credentials
US$19
List of mobile phone numbers
US$290–1,236
List of landline phone numbers
US$317–1,931

The Chinese blackmarket

The Russian blackmarket



Question 4

What are the solutions:

public and private responses

- investigation
- protection
- limitation of damages/resilience
- legislation and responsibilities in the level of services offered by players
- etc.

The NIST framework for critical infrastructure security 2014

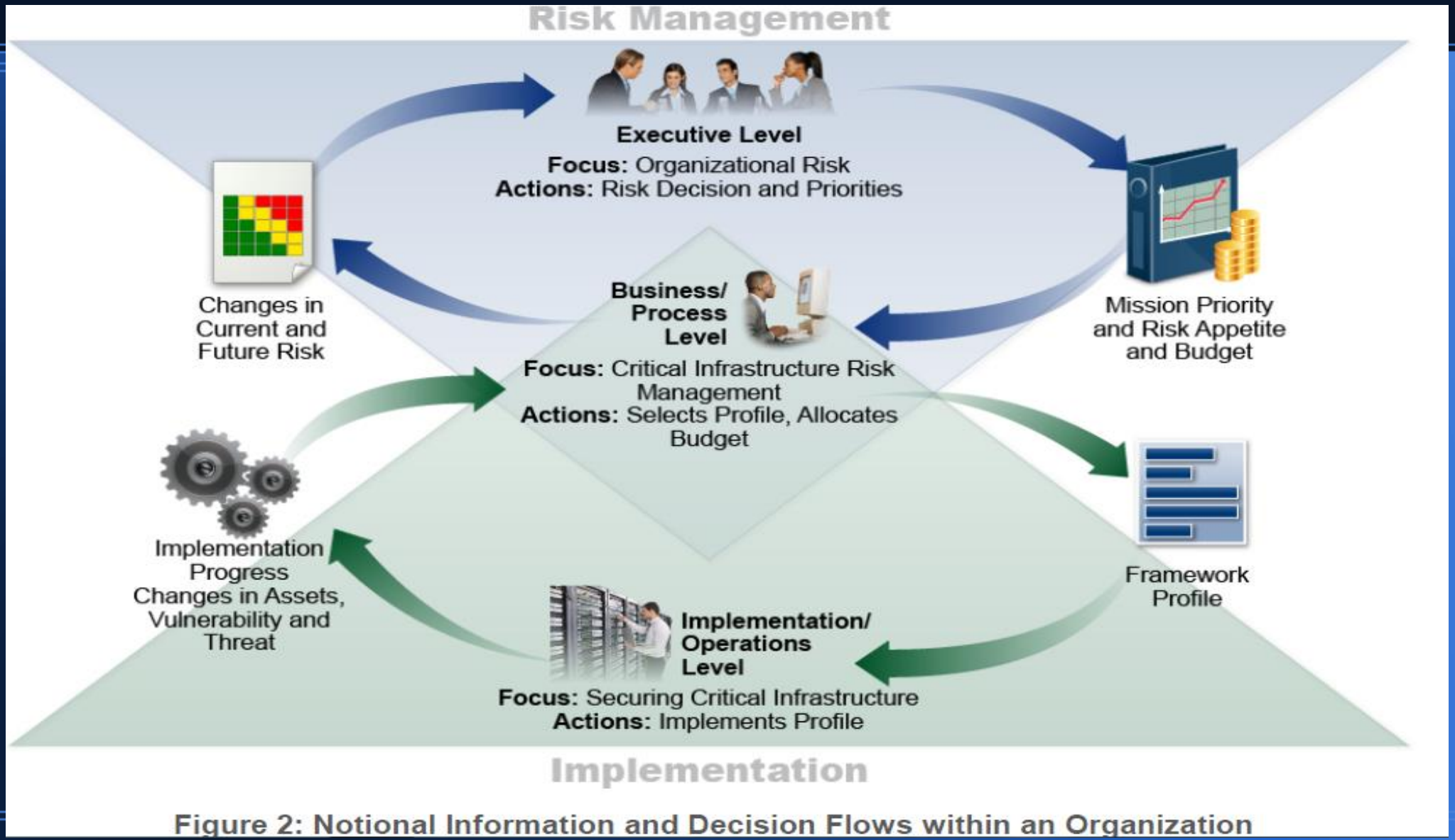


Figure 2: Notional Information and Decision Flows within an Organization

The activities by private stakeholders: the defense

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Cybercriminality serves a global market that must be globally prosecuted: the attack strategy

- on the side of demand as well as on that supply
- economic, political, institutional environment is at risk: quite a difficult task

Question 5

What is the role of rules:

necessary but insufficient if generic and only addressed to attackers/hacktivists and the supply side

cyber warfare includes the fundamental economic value of digital INFORMATION/KNOWLEDGE being used for all kind of human activities:

The cybersecurity chain: lines of analysis and intervention in national/international strategies

- deep Internet
- the cyber black market
- the law of supply and demand

- international cooperation (Nato and other institutions)
- the paradox of the holistic approach: measures must be found at a global level

The international transboundary effort

- **Cybersecurity diplomacy**

- Transboundary rules (what is the function of national strategies in the Internet global domain); jurisdiction, procedures
- The prosecution of supply and demand in the cybercrime market
- Cybercriminality is a powerful economic arena

The missing tessera: the global vision

That's all. Thank you