Cyber security: what a decision maker should know[1]

By Elisabetta ZUANELLI[2]

The paper recalls three problematic areas of conceptual reference in cybersecurity for institutional decision makers:

- *notions and definitions such as: cyber space, cybersecurity, cybercrime, cyber crime ware, etc.*
- *the assumed shared knowledge: investigation/analysis, applications, defence, resilience*
- *the shared strategies: public/private collaboration, national and international cybersecurity strategies.*

The assumptions underlying these conceptual areas should be reconsidered from an external viewpoint that presses for a faster collaboration and concrete solutions at a global level.

To do this the contribution poses questions concerning the relation between cybersecurity and cybercrime, who the players/stakeholders are, what the implications, what the solutions.

A new global approach to cybersecurity issues is therefore elicited that exceeds local views and faces the challenge of complex trans-boundary connections in order to contrast cybercrime economy and guarantee cybersecurity.

Table of Contents

---

1 Paper presented at the international Seminar on Global Challenges, organized by the CASD (Centre of high studies of the Italian Ministry of Defense), March 23rd 2015.

2 University of Rome "Tor Vergata" - Coordinator of the Observatory on cyber security/University of Rome "Tor Vergata" - President of the Centre for econtent R&D (CReSEC,www.cresec.com)

List of Figures

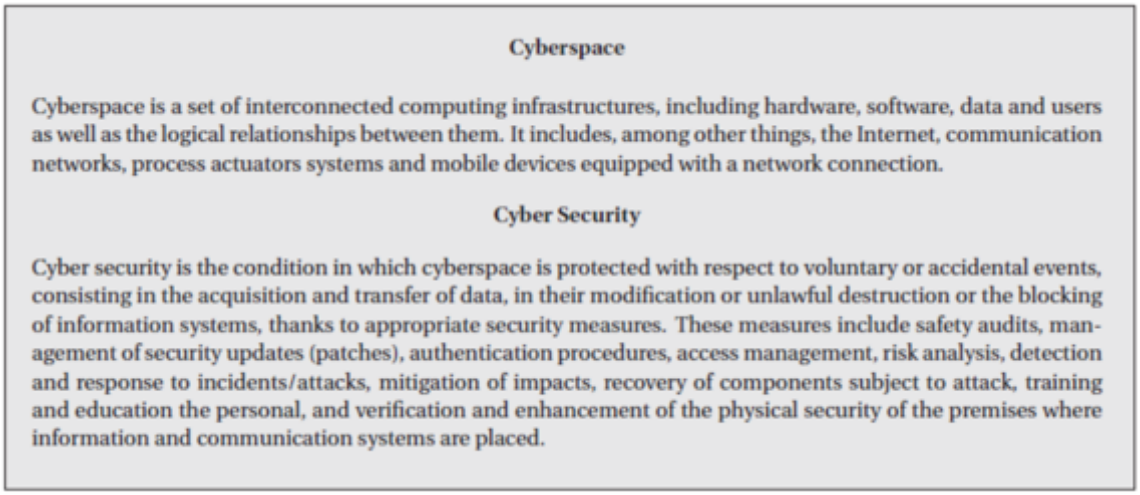
The observer's paradox

The observer's paradox consists in the limitation of our vision when we take part in and stay inside the phenomenon we undertake to analyse.

If we take a look at cybersecurity from the outside, we need to check **definitions**, the **shared knowledge** and the **shared strategies** related to the notion without preliminary assumptions.

As for definitions, if the notion of cyber space refers to the virtual world where we interact daily for buying and selling, teaching and learning, doing administrative, political and institutional work as well as banking and financial activities, managing a company, releasing online services, etc., the need for **security in our virtual interactions** becomes dominant just as much as security for our activities in the physical world and in every-day's life.

Cyberspace can be defined in different ways. According to the 2013 Report on *Critical Infrastructure and Other Sensitive Sectors Readiness*, by the University of Rome "La Sapienza", the technological definition is proposed as follows:



Cyberspace

Cyberspace is a set of interconnected computing infrastructures, including hardware, software, data and users as well as the logical relationships between them. It includes, among other things, the Internet, communication networks, process actuators systems and mobile devices equipped with a network connection.

Cyber Security

Cyber security is the condition in which cyberspace is protected with respect to voluntary or accidental events, consisting in the acquisition and transfer of data, in their modification or unlawful destruction or the blocking of information systems, thanks to appropriate security measures. These measures include safety audits, management of security updates (patches), authentication procedures, access management, risk analysis, detection and response to incidents/attacks, mitigation of impacts, recovery of components subject to attack, training and education the personal, and verification and enhancement of the physical security of the premises where information and communication systems are placed.

Figure 1 - Cyberspace and Cybersecurity Definitions

In this regard, cyber security is a condition for free, safe, democratic life in the global digital world.

The Armament Of Cyber Attacks

If these activities are menaced for fraudulent criminal aims against the individuals,

groups, entities, societies then we face what is called **cybercrime**, which is made up of individuals, groups, entities that practise criminality **through or by means of digital technologies** as their institutional mission.

This is the core business of **cyber warfare,** an extended use of cyber attacks where cyber attacks tend to disrupt digital activities for diverse aims.

Parts of these criminal digital activities are carried out by means of **cyber malware**, namely digital software specifically developed for cyber crime[3]. **Cyber crime-ware** is, therefore, **an important resource for cyber crime as it represents the armament of cyber attacks.**

If we agree on these definitions, we accept the shared knowledge in documents, analyses, reports, legal acts, legislation where we read of **typologies of attacks, typologies of crimes, statistical trends of information security attacks, defence technologies and digital vulnerabilities, both human and technological.**

We also share the need for defence that has generated **cybersecurity strategies** which are made up of national strategies, of the European nations as well as of the USA, the alarm signals of formal institutions, for instance the recent American NIST framework for information security of critical infrastructures, the setting up of central boards, various organisms, LEA's activities, private and public collaboration, the CERTs implementation and the **acceleration on investigation activities, data exchange, knowledge dissemination,** etc.

Yet it is clear that so far there is no definite solution to the problem, neither technological nor behavioural. The challenge calls us to face a global permanent attack as global is the Internet world where cyber armies cannot be localized and detected and social, economic, political, institutional partners represent the liquid variable that must be faced within a global vision.

The Five Questions

In order to make the point clear, let put a few questions.

Why Cyber Attacks And What For?

Question 1 sounds like this: ***why cyber attacks and what for?***

Cyber attacks are meant to **violate, corrupt or subtract** personal or institutional information systems (from personal computers to corporate servers) and are performed:

1. to get money back straight from the solution of corruption;
2. to create severe problems in the management/activities of an institution or a

---

[3] *S. Gordon, R. Ford, "on the definition and classification of cybercrime", J Comput Virol, 2006*

company (for instance, by political or industrial competitors);
3. to slow down or block the services offered by a company or an institution.

As for the **subtraction of information/data** the aim and the targets are:

1. individuals whose identity is the target for 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.

Other perspectives are assumed when we consider cybercrime as the use of the Internet for delinquent activities such:

1. child abuse, pedo/pornography;
2. drugs market;
3. prostitution market;
4. migration market.

Finally, the answer to question 1 includes **criminal propaganda and antagonist objectives** such as:

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

Which Are The Cybersecurity Players?

Let us come to question 2 that touches on the definition of **cybersecurity players.**

Who are the players in this global digital criminality? Whose responsibility are cybersecurity flaws, such as the ones in cloud services, social platforms, apps for mobile, online sales, etc.?

In the criminal perspective, hacktivists/cybercriminals act as single entities, group cyber attackers, cybercrime companies who get money and power **straight from cyber attacks, viruses inoculation, malware,** etc. or **selling attacks, selling data, selling criminal services in general to other players**. These other players are industrial, political, military stakeholders and physical managers of criminal activities such as prostitution, pornography, etc.

So question 3 makes the point.

We face the challenge of a ***cybercriminal economy*** **that is sponsored by diverse players in our global society** and the question should include the market share interests not only on the side of the offer but also on the side of demand. In othe terms who are the buyers, not only the sellers, of cybercrime services? In other terms, the cybercrime economy has a triangular composition: **cybercriminals, victims** and **final beneficiaries.**

According to an Italian report elaborated by CLUSIT in 2014 victims are listed as follows.

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%

Figure 2 Tipologies of Victims in 2011 and 2012

The list is not utterly satisfactory because it hints at vast and generic social domains such military/intelligence activities, online services/cloud, banking and finance, etc.

As for the typology of attacks the same report offers this synthetic prospect:

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			

Figure 3 Typologies of Attacs

where the categories of cybercrime, hacktivism, espionage, sabotage, cyber warfare imply a very complex sub-categorisation.

As have stated, the cybercrime economy provides vast black-markets. And the cybercrime black-market is partially visible as any digital market place.

An Internet site sums up the global black market for stolen personal data in a visual scheme as follows:

Figure 4 - The Global Market for STolen Personal Data

The global black-market for stolen personal data is here represented geographically and mainly associated with Brazil, China and Russia; price lists are given as follows:

Figure 5 - Price List of Stolen Personal Data in Brasil

The Brazilian black-market as opposed to the Russian and Chinese ones seems specialized in account/credit card credentials and phone numbers whereas the Chinese market seems to be characterised for email and entertainment/gaming credentials.

Figure 6 - Price List of Stolen Personal Data in China

As for the Russian blackmarket, prices include credit cards and IP addresses.

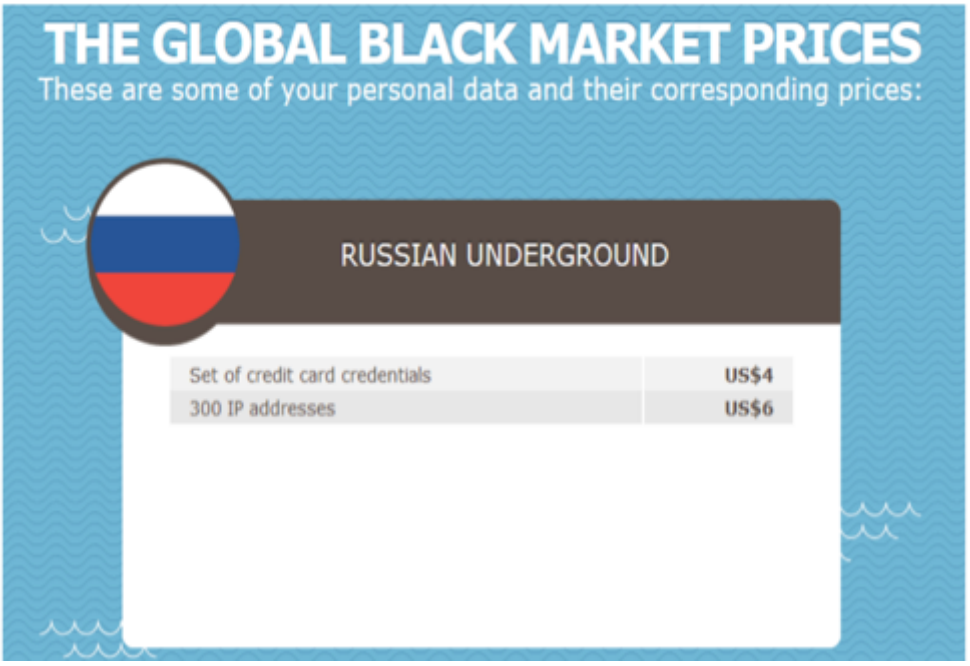


Figure 7 - Price List of Stolen Personal Data in Russia

What Are The Solutions?

The situation briefly represented leads us to question 4: What are the solutions?

It is important to stress the coordination of public and private responses and the urgence to accrue investigation, protection, limitation of damages/resilience as well as legislation and responsibilities in the level of services offered by on line service providers etc.

Reports such as Gardner's 2014 stress the need for a new adaptive approach based on continuous monitoring and analytics.

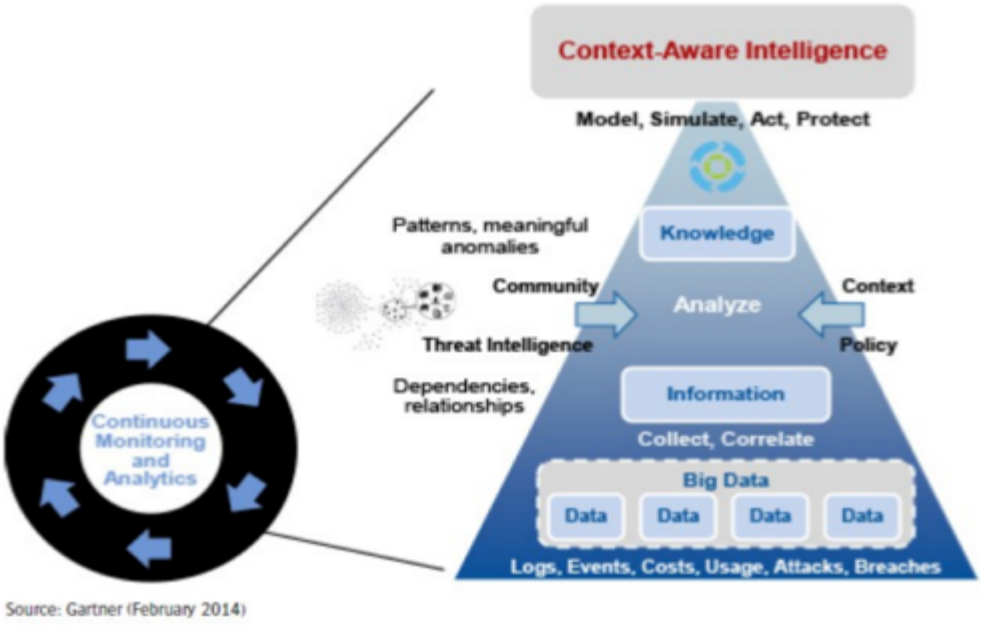


Figure 8 - Continuous Monitoring for an Adaptive Protection Architecture

The need for a better human organization in companies and institutions in order to prevent cyber attacks is stressed by the NIST in the framework for critical infrastructures security 2014. These are necessary guidelines for risk management. The scheme should be implemented for a defence strategy that reduces risks.

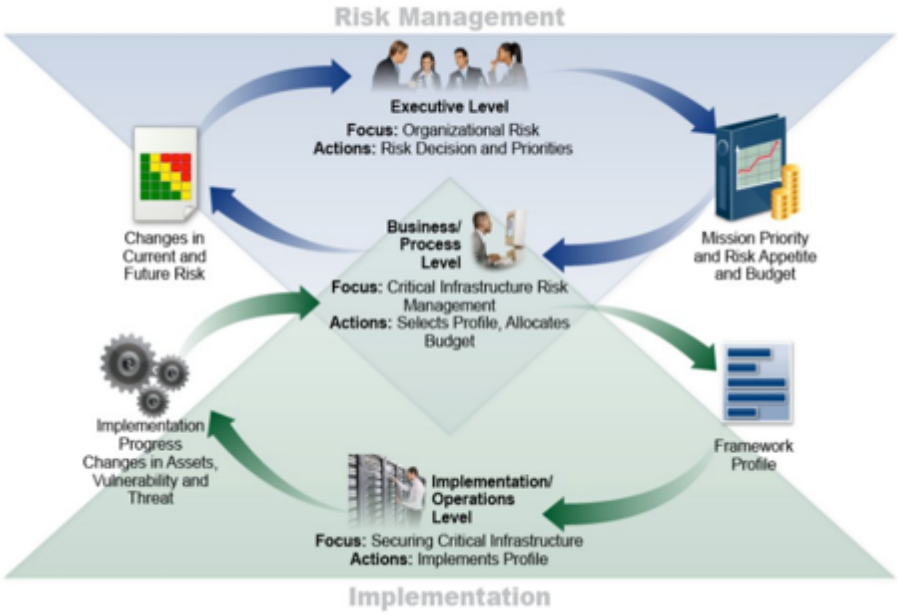


Figure 9 - Notional Information and Decision Flows within an Organization

Activities for risk management are visually summarized and schematic checklists for risk assessment are proposed to be implemented.

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

Figure 10 - Function and Category Unique Identifiers

Is this is enough? Of course it is not.

We must consider that cyber-criminality serves a global market that must be globally prosecuted: we need an attack strategy against cybercrime on the side of demand as well as on that of supply.

Economic, political, institutional environment is at risk: the task is quite difficult.

Therefore question 4 stresses the urgency of new specific lines of intervention.

What Is The Role Of Rules?

Question 5 is: 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 to be considered as a basic economic asset in public and private domains, used for all kind of human activities:** institutional, political, industrial, military, social.

Digital information is the economic revolutionary asset of the third millennium.

The Holistic Approach

Lines of analysis and intervention in national/international strategies, to be assumed by decision makers, should include the prosecution of deep Internet, investigation and intelligence on cyber security black markets, the detection of supply and demand of cyber attacks on one side.

On the other side strategies should implement international cooperation (NATO and other institutions) to solve the **paradox of the holistic approach:** measures must be found at a global level reinforcing specific sectors: governments, industries, service providers, etc. as well as improving technological and behavioural risk assessment and resilience which calls for investments in information security R&D, awareness, dissemination of information at different levels for specific purposes. In sum we must extend the perspective of the European Parliament on information security as related to cloud computing services.

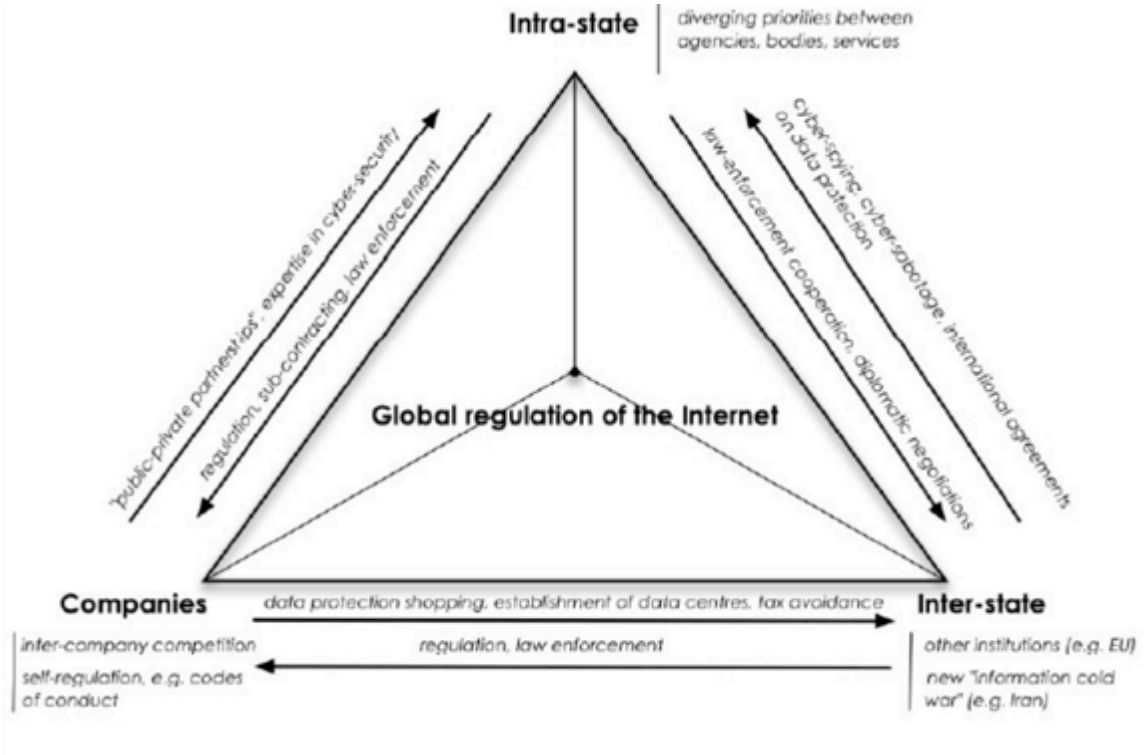


Figure 11 - The Triangular Diplomacy of Cloud Computing from the Point of View of the Global Regulation of the Internet

An international trans-boundary effort requires the setting up of a ***cybersecurity diplomacy*** and a quick move towards **trans-boundary rules** (what is the function of national strategies in the Internet global domain?). Jurisdictional, procedural limitations must be overcome and the **prosecution of supply and demand in the cybercrime market** must be quick and severe.

Cyber-criminality is a powerful economic arena where technological defence can only limit damages.

The growth of awareness is one of the tools for **institutional decisors**. Multifaceted analysis of the implied themes, economic, juridical, technological, social is another tool; dissemination of information, education, training, R&D are further activities to be fostered and coordinated.

The global vision, however, is the missing element of this mosaic for achieving success in this highly complicated puzzle of the third millennium.