SAPIENZA
UNIVERSITÀ DI ROMA

Master Degree in Cybersecurity

The EU Cybersecurity Legal Framework

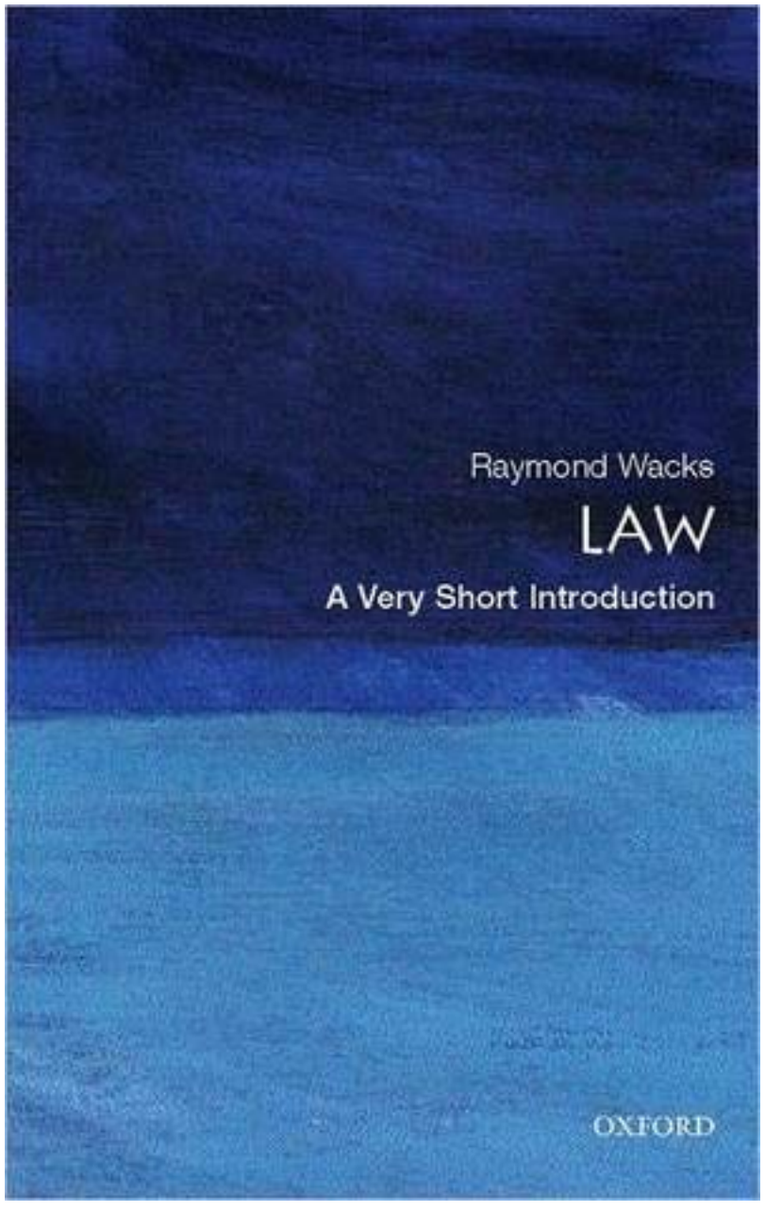
April 22, 2020

Andrea Monti
Adjunct professor of Public order and security
University Gabriele d'Annunzio, Chieti-Pescara (IT)
amonti@unich.it - lawfirm@andreamonti.net

Agenda

- **Law, a very short introduction**
- **The EU legal and political system**
- **The EU legal instruments (Directives and Regulations)**
- **The legal and political relationship between the EU and member States**
- **Missing points: no EU Constitution, no common defense and law enforcement system, no common intelligence bodies**
- **The role of ENISA**
- **Protection of Personal Data vs Protection of Critical Infrastructure**
- **The General Data Protection Regulation**
- **The Network and Information System Directive**
- **From law to market: building a cyber security oriented start-up**

Textbook



Raymond Wacks
Law. A Very Short Introduction
II Edition 2015
Oxford University Press
ISBN-13: 978-0198745624
Available on Amazon Kindle

SAPIENZA
UNIVERSITÀ DI ROMA

What Is Law

- What Is Power
- From Power To Law
- From Rights to Law
- Law and Justice
- The Western Legal System

SAPIENZA
UNIVERSITÀ DI ROMA

What Is Power

Power is the ability to make others actually do what we want them to do.

It manifests itself in every sphere of social life, in the family, in personal relationships, in the workplace, in the relationship between citizens and the State and in the relationship between States.

The sources of Power are different. As for the relationship between State and citizen, six can be identified:

- Physical force-> control over the army and the police.
- Wealth-> control over money->currency and cryptocurrency
- Power of the State-> use of law and bureaucracy
- Social standards->softpower-> public and private rituals
- Ideas(ologies)->"social drive"->religion, philosophy, activism
- Crowd-> a large number of people with an interest generate power

What Is Law

NATURALISM is the belief that law consists of a set of universal moral principles in accordance with nature. A variant is the equation of "nature" with "God", thus creating a link between Law and Religion.

LEGAL POSITIVISM law is little more than a collection of valid rules, commands, or norms that may lack any moral content.

* * *

Others perceive the law as fundamentally a vehicle for the protection of individual rights, the attainment of justice, or economic, political, and sexual equality.
Few consider that the law can be divorced from its social context. The social, political, moral, and economic dimensions of the law are essential to a proper understanding of its workaday operation.

From Power to Law

The first form of Power's management has been the monarchy

Monarchy is absolute, unaccountable, free to rule with no duty of coherence

As soon as the border of the kingdom grows, the monarch's autonomy weakens and technology is the key to preserve power

Rules are needed to manage the increasing complexity of social interaction

Intermediate levels in the management of power are created. Examples: Proconsul and Propraetor, Feudatory

While the Power is no more solely into the monarch's hands, formally he's not bound by any limit.
Superiorem Non Recognoscens

The Rule of Law

The Rule of Law is the principle stating
that nobody is above the Law
***Legum servi sumus ut liberi esse possimus* (Cicero)**

The roots of the Rule of Law may be found in
Magna Carta of 1215 which rejected the idea
of unchecked, unaccountable royal power

The Rule of Law is the limit set forth by a social contract
to the unaccountable power of the monarch

For the Rule of Law to work,
Power must be shared with consociates

SAPIENZA
UNIVERSITÀ DI ROMA

From Rights to Law

Law gives Rights

The word “Right” has a double meaning:
a - the prerogatives attributed by Law to a category of subjects
b - a social prerogative that a big enough group of subjects ask to be acknowledged by a Law by their political representatives

The rule of Law is the limit set forth by a social contract to the unaccountable power of the monarch

For the rule of Law to work,
Power must be shared with consociates

SAPIENZA
UNIVERSITÀ DI ROMA

Law and Justice

In the words of the 20th-century English judge Lord Denning:
The law as I see it has two great objects: to preserve order and to do justice; and the two do not always coincide.

The pursuit of justice must lie at the heart of any legal system.
But there is no commonly accepted definition of the "Justice" word's meaning.

While the virtual equation of law with justice has a long history dating back to Ancient Greek times, there are legal theories that challenge this assumption.

The Legal Positivism claims that since Law is a formal system, ethics and "larger-than-life" motives are beyond the reach of Law

The Western Legal System

The Western legal tradition has a number of distinctive features, in particular:

• A fairly clear demarcation between legal institutions and other types of institutions; legal authority in the former exerting supremacy over political institutions.

• The nature of legal doctrine which comprises the principal source of the law and the basis of legal training, knowledge, and institutional practice.

- **The concept of law as a coherent, organic body of rules and principles with its own internal logic.**
- **The existence and specialized training of lawyers and other legal personnel.**

The European Union Political and Legal System

- The EU is a sort of ‘association’: member States preserves their own individuality but decided to delegate a series of prerogatives to a new entity,
- The European Union is made of two treaties: The European Union Treaty and the Treaty on functioning of the European Union
- The treaties separate the matters reserved to the EU from those that remains under the control of member States
- In theory, criminal law, national security and public security are out of reach for the EU legislator. In practice, the EU is aggressively eroding the space
- This happens because of the missing points in the EU political structure: no common intelligence, law enforcement, judicial and security powers
- Sometimes this is made by way of ‘technical’ provisions, sometimes with a deliberate ‘crowbar’ attitude such as in data protection, hate speech and copyright

The European Union Political and Legal System

- The political and governance structure of the EU is made of
  - European Council (political body, settles the political goals of the Union)
  - Council of the European Union (act as a legislature, made of members' ministers)
  - European Parliament (act as a legislature, is the EU Commission's watchdog)
  - European Commission (executive power, submits legislative proposal to the EU Parliament)
  - European Union Court of Justice (judicial power)
  - Agencies: administrative bodies appointed of specific tasks. ENISA is the agency competent for cybersecurity. It does not have an actual 'field role' acting mainly as an advisor body

The EU legal instruments (Directives and Regulations)

- The EU has plenty of legal instruments in its ruler's toolbox
- For the sake of this seminar, we only focus on directives and regulations
- Both are approved by the EU Parliament
- Directives need to be enforced in every single member State
  - enforcement might differs from State to State because of the different legal systems
  - in theory there is a term fixed by the directive itself for the local enforcement, rarely though the adoption happens at the same time
- Regulations are directly effective in member States
  - can not be amended by locally-passed laws
  - override non-coherent legislation
  - when, as the GDPR, a regulations is too wide, creates problem of enforcement

Information Matter

SAPIENZA
UNIVERSITÀ DI ROMA

What Is Privacy Supposed To Be

That's None of Your Business

SAPIENZA
UNIVERSITÀ DI ROMA

What Privacy Is Associated To

Secrecy

Anonymity/
Personal Identity

Self-Determination

Personal Image Control

Family Life Respect

SAPIENZA
UNIVERSITÀ DI ROMA

Are these rights unattended?

Western Constitutions and Laws already protect:

- **Secrecy of communications** (reading someone else personal correspondence is a criminal offense, only the State can eavesdrop communication),
- **Personal Image** (no use of personal image is allowed that violate human dignity),
- **Family Life** (private home can be accessed only by way of a Court order, snooping into private matters is a criminal offense),
- **Self-Determination** (discriminations of all sort are forbidden),
- **Anonymity/Personal Identity** (with some exceptions, anonymity is generally allowed, Identity Theft is a criminal offense)

Do These Rights Necessary Belong to the Privacy Domain?

NOT VERY!

Secrecy of communications and Anonymity are factual conditions that matter, for **criminals** (who don't wont to be arrested), **unfaithful partners** (who don't want their extra-marital intercourse to be discovered), **journalists and political activists** (who want to protect their sources and plans), **whistleblowers** (who need to stay unknown to report illicit behaviours.)

Self-determination is better served by public exposure rather than by keeping things in the hide,

Family life deserves protection in public spaces too, **personal image** infringements can threat **dignity** and **honour**.

On the other side, **National Security**, ***Ordre Publique***, and **Law enforcement by Police and Courts** activities are better controlled by the Due Process Right rather than by "Privacy"

In these cases, there are not privacy issues at stakes!

SAPIENZA
UNIVERSITÀ DI ROMA

The Privacy Misunderstanding

- Privacy is a Common Law legal concept, recognised as a right by way of the Courts decision, therefore there is no need for a specific law to acknowledge the existence of a “new right”,
- Civil Law systems only acknowledge a right that can be derived by an already existing law,
- But the word “right” has a double meaning
  - is a claim of a big enough social group that feel like it deserve to be allowed to something (e.g. right to divorce or abortion, arising from politically active citizen who ask for their “right” to be officially acknowledged)
  - is the technical outcome of a political mediation process, “nailed” into a provision, thus making it actually enforceable

Does A Right to Privacy Exist?

- From a Civil Law perspective, as there is neither a Constitution nor an Ordinary Law that acknowledge the existence of a "right to privacy" in the same way, for instance, of the "right to private property", a right to privacy doesn't exist

- Furthermore, if we stay stuck to the traditional definition of "privacy", an autonomous right is of no use, as the already existing laws cover all the needs

Does The European Union Data Protection Regulation Fills The Gap? Or: Is Data Protection the New Privacy?

- There is a wide spread attitude in the Western Legal Community to equal Privacy to Data Protection
- As we will see in a moment, not all Personal Information are Personal Data
- Personal Information are not defined by a specific provision, while Personal Data are mentioned in Article 7 of the EU Charter of Fundamental Rights and defined in Article 4, First Paragraph of the GDPR
- The GDPR doesn't mention the word "Privacy"

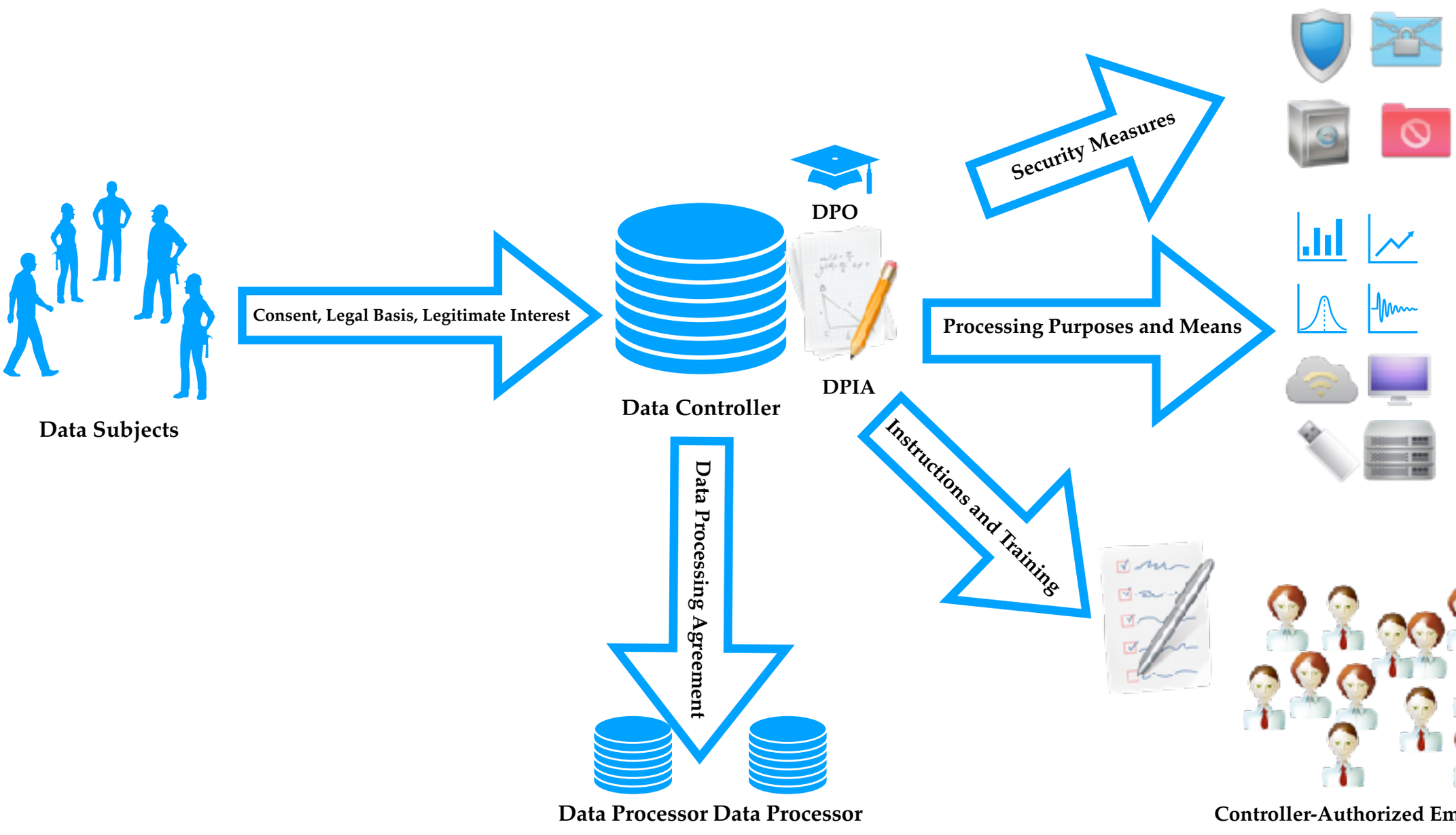
Why Does the Difference Between Privacy and Data Protection Matters?

- From a taxonomy perspective, privacy is (conceived as) a fundamental right, while Data Protection is instrumental to protection of Fundamental rights
  - GDPR Whereas n. 4 states that ***The right to the protection of personal data*** **<u>is not an absolute right</u>**; ***it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications,***
- From an enforcement perspective,
  - Whether the old-fashioned "right to be alone" or a more contemporary privacy definition is chosen, the right to Privacy only works to protect the personal information sphere
  - Data Protection, in contrast, regulates a far wider spectrum of issues such as data integrity, availability and reliability that are not connected to the right to Privacy and is more effective as a tool to protect rights - such as freedom of information and political activity - that are not "covered" by the right to Privacy

The GDPR In a Nutshell

- The General Data Protection Regulation 679/2016 enforces Art 7 of the EU Charter of Fundamental Rights
- Being a Regulation it dictates same provisions all around the EU and it has immediate executive power
- Regulates (mainly) digital processing, not data
- Meant to protect NATURAL PERSON as Data Subjects and their liberty and fundamental rights
- Details various legal alternatives to mere consent for the legitimacy of the processing
- **Profiling** gets a legal (and rather vague) definition, as well as **Pseudonymisation**
- **Right to be forgotten** moves from Court (Google Spain/Costeja) to Law
- **Data Portability** becomes a legal right
- **Security of the processing** becomes mandatory and specific duties of **Data Protection by design** and **by default** is a specific duty of the Data Controller
- Turns the legal compliance from a **prescriptive model** into a **Self Assessed, Feedback Oriented, Dynamically Enforced, Accountability Based, Self Incriminating architecture**
- GDPR is enforceable if personal data are processed
  - by an EU entity, abroad,
  - if an Extra-EU entity processes personal data within the EU
  - if a controller is not established in the Union, but in a place where Member State law applies by virtue of public international law.

How Does (or Should) GDPR Work In Practice



GDPR and IT security

- Security is meant to protect the data-subject and not the data-controller
- Security is NOT meant to protect other assets
- Security is self-assessed and not prescribed. The data-controller makes his own choices, and the data protection authority controls ex post
- Security choices are matched against an impossible parameter: the risk for fundamental rights and freedom of each single data-subject, and not against data-subjects as a category. That makes the risk analysis impossible

SAPIENZA
UNIVERSITÀ DI ROMA

Critical issues in the actual enforcement of the GDPR

⚠ **National Legislative Fragmentation.** The GDPR cannot be modified by Member States, but they can "harmonise" it with the local legislation. Knowing the GDPR only is not enough to be compliant.

⚠ **Data Protection Authorities' Different Views.** Each Data Protection Authority has its own interpretation of the GDPR. While there is an effort to be "speak with a single voice" by way of the European Data Protection Board, difference may be relevant.

⚠ **Data Protection is meant as a Privacy synonym.** At a theoretical level the difference between Privacy and Data Protection is clear. Nonetheless, even Data Protection Authorities call themselves "Privacy Commissioner". Furthermore, there is a widespread assumption that "Privacy" or "Data Protection" are some sort of "SuperConstitutional Rights"

⚠ **Many professionals have a poor legal understanding of the Regulation.** The market is flooded by professionals coming from non-legal background, or by legal people with no actual expertise in Data Protection. The results is a flourish of odd interpretations that make the interaction between controllers and between controllers and processors very difficult.

⚠ **Confusion among GDPR, Critical Infrastructure Protection an Network Security.** The GDPR assessments are meant to protect "freedom and other fundamental rights" of the Data Subject, while the EU legislation on the protection of critical infrastructure, network security etc. have other purposes and requirements. It might make sense to coordinate all these legal provisions, nonetheless the differences must not be forgotten

⚠ **Lack of commitment to an actual compliance.** The GDPR is seen by the Data Controllers as a mere bureaucratic burden. The compliance is often just made by way of internal policy and legal texts that are hardly followed by an actual enforcement of the legal provisions

⚠ **Anti-competitive effect of the lack of general compliance.** The GDPR compliance has a huge price in terms of financial effort and business strategies. Companies who don't comply - and that are not immediately fined - shall maintain a competitive advantage over virtuous players.

Critical Infrastructure Protection

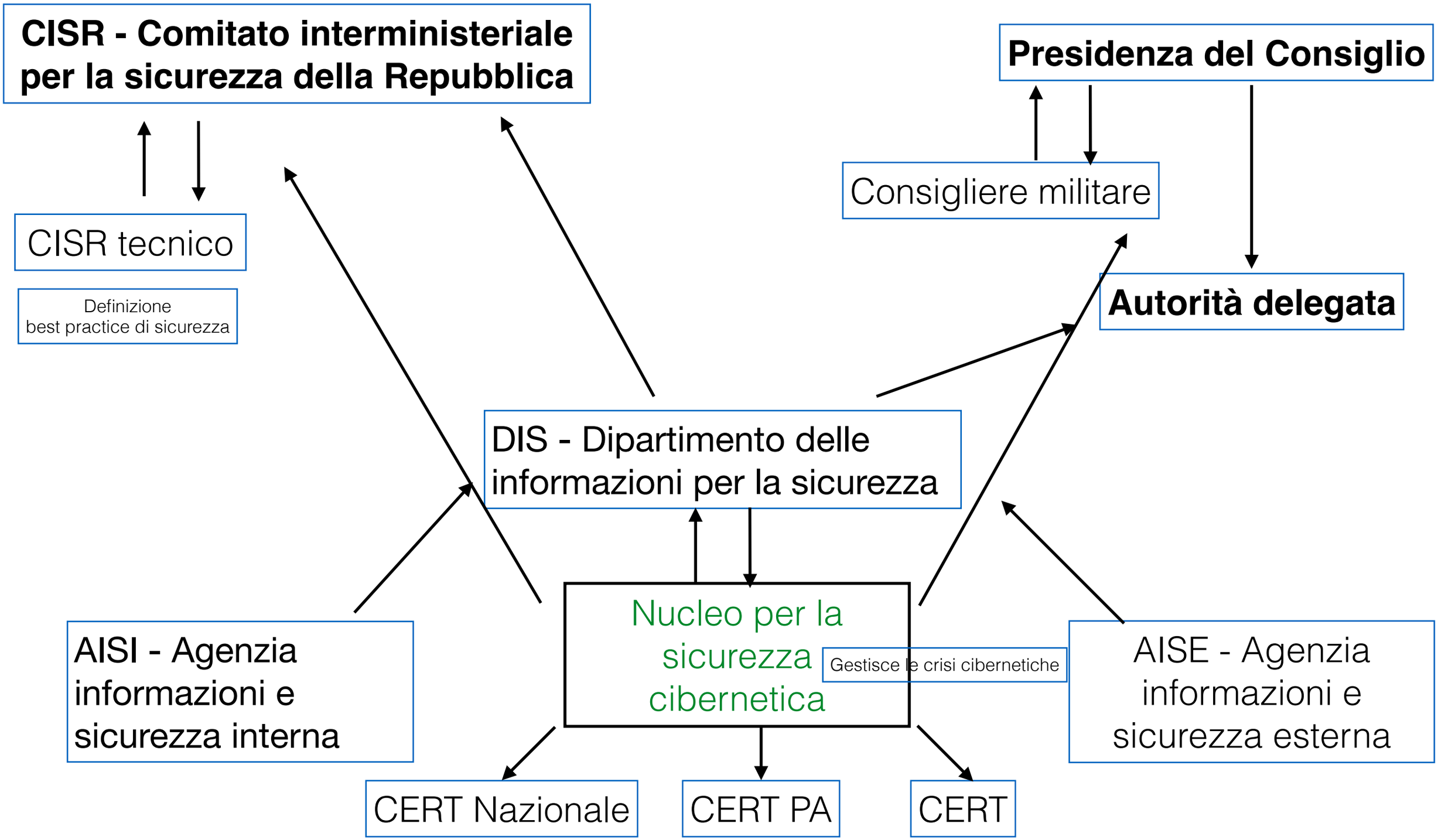
- The critical infrastructure protection is a directive, this means that must be enacted by each member State with a specific law
- The core of the directive is the identification of specific infrastructures that deserve to be protected at the highest level
- In contrast to the GDPR, the legal scope of the NIS directive is to protect national security and not individual freedoms
- The security requirements to protect a critical infrastructure are entirely different from those required by the GDPR
- Still, GDPR and NIS are often presented as essentially the same thing, but this is a paramount mistake because it affects the security design and enforcement

The NIS Directive in three points

- National Capabilities Development
- Cross-border collaboration
- National supervision on critical sectors

SAPIENZA
UNIVERSITÀ DI ROMA

Italian National Security Organisation in the 2017 Presidency of Minister Decree



And now, let’s stop with legalese, and talk about business!

SAPIENZA
UNIVERSITÀ DI ROMA

A word to the wise

Ain’t no such things as
“cyberspace”

As I stared at it in red Sharpie on a yellow legal pad
my whole delight was
that it meant absolutely nothing

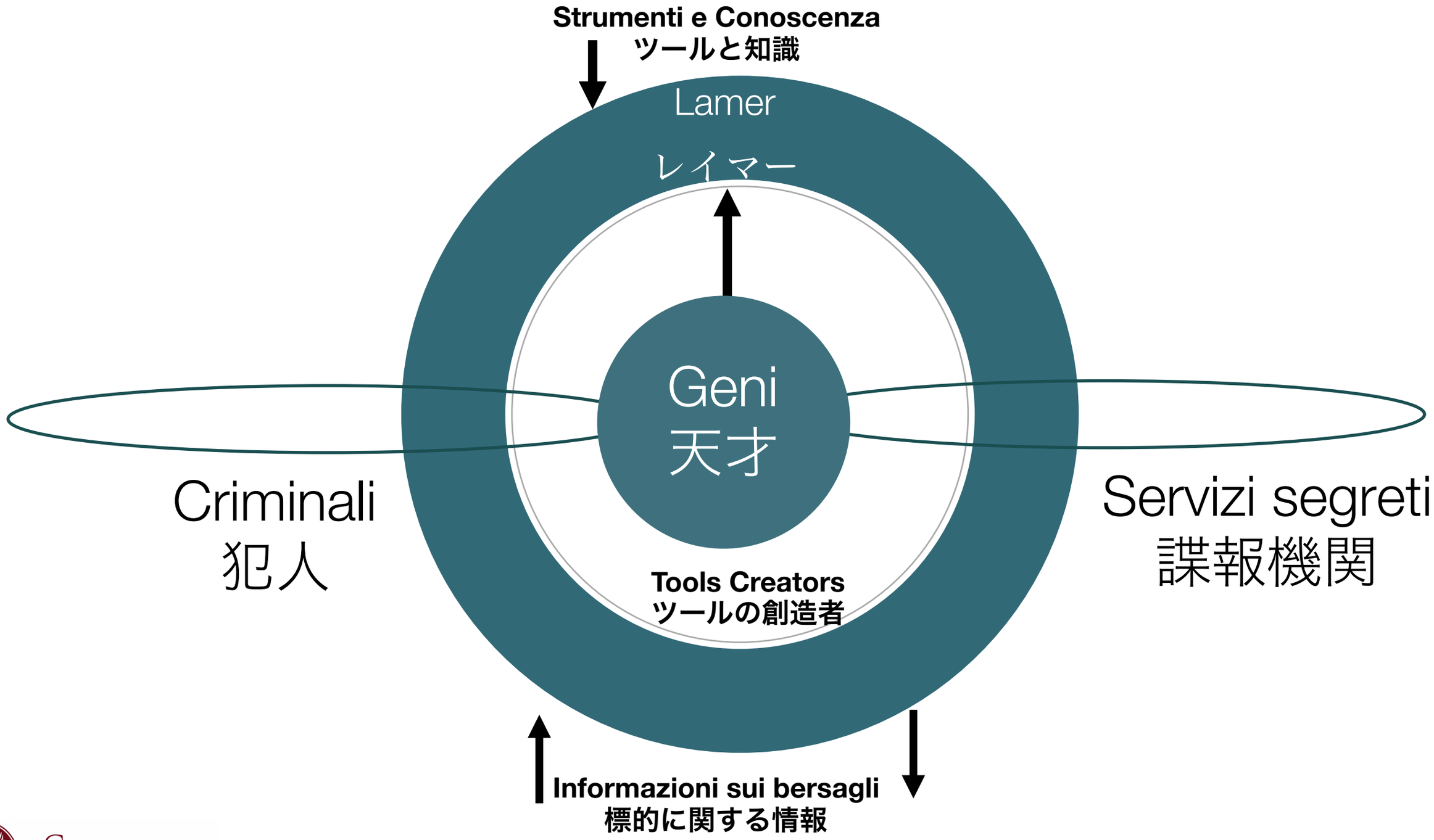
William Gibson, author of *Neuromancer*

Cybernetics Is About
Human-Machine Interaction

N. Wiener *Cybernetics, or Control and Communication in the Animal and the Machine* (1948)

SAPIENZA
UNIVERSITÀ DI ROMA

From Hackerland to Crimeland



SAPIENZA
UNIVERSITÀ DI ROMA

Further elaboration of a graph published by Winkler, I. ***Corporate Espionage*** Prima Publishing 1997 - p. 86

The Hackers'Role in the Evolution of the IT Security Market

- **1985** Altos and Altger's and the early IRC-based hackers' communities
- **1990** Targeting the Telcos: Phone Phreaking and Social Engineering
- **1994** Software Industry, BBS and the Italian Crackdown
- **2000** (about) hackers are "discreetly" hired by multinationals to run penetration tests
- **2001** Ettercap by Alberto Ornaghi and Marco Valleri
- **2002 - 2004** Telindus Bug, The Hacker Goes Business, Defacement As Marketing Tools
- **2008** - The Telecom Sismi Scandal
- **2010 - Today** The Big Four Enter the Market

Suggested Readings

- **The Cuckoo's Egg** - C. Stoll
- **Hackers** - B. Sterling
- **When The Wizards Stay Up Late** - K. Hafner - M. Lyon
- **The Cathedral and the Bazaar** - E. Raymond
- **The Codebreakers** - D. Kahn
- **The Puzzle Palace** - J. Bamford
- **Approaching Zero** - P. Mungo
- **Spaghetti Hacker** - S. Chiccarelli - A. Monti
- **Le Tigri di Telecom** - A. Pompili

Startup 101

- A startup makes two things
  - something nobody did before
  - a new way of doing things that have been already done
- A ‘new’ product/service comes:
  - from a intuition, verified by market research
  - from the decision to impose a product (Henry Ford, Steve Jobs)
- Money to fund a startup comes from
  - venture capital
  - public funding
  - private funding
- When you get funded by somebody, the first thing you relinquish is the control over the company. You responsibility is product development, but, de facto, you are not the sole in command anymore

Critical issues in a cybersecurity startup

- Legal limitation for a specific kind of product
  - trojans and malware are for institutional client only (Hacking Team)
  - forensics tool might have a broader customer base
  - offensive security is illegal in some countries such as Italy
- Legal compliance
  - threat assessment tools might infringe specific regulations (labour law)
  - red teaming might be forbidden
  - Mind the product liability issues
- That affects markets, market shares and the definition of price

Solutions?

- Hire a good lawyer right after you've hired your best software engineer!
- Kidding apart, embedding a legal analysis into the product design reduces the risks of future problems one the startup hits the market
  - think of the criticism raised against Zoom for privacy and security concerns