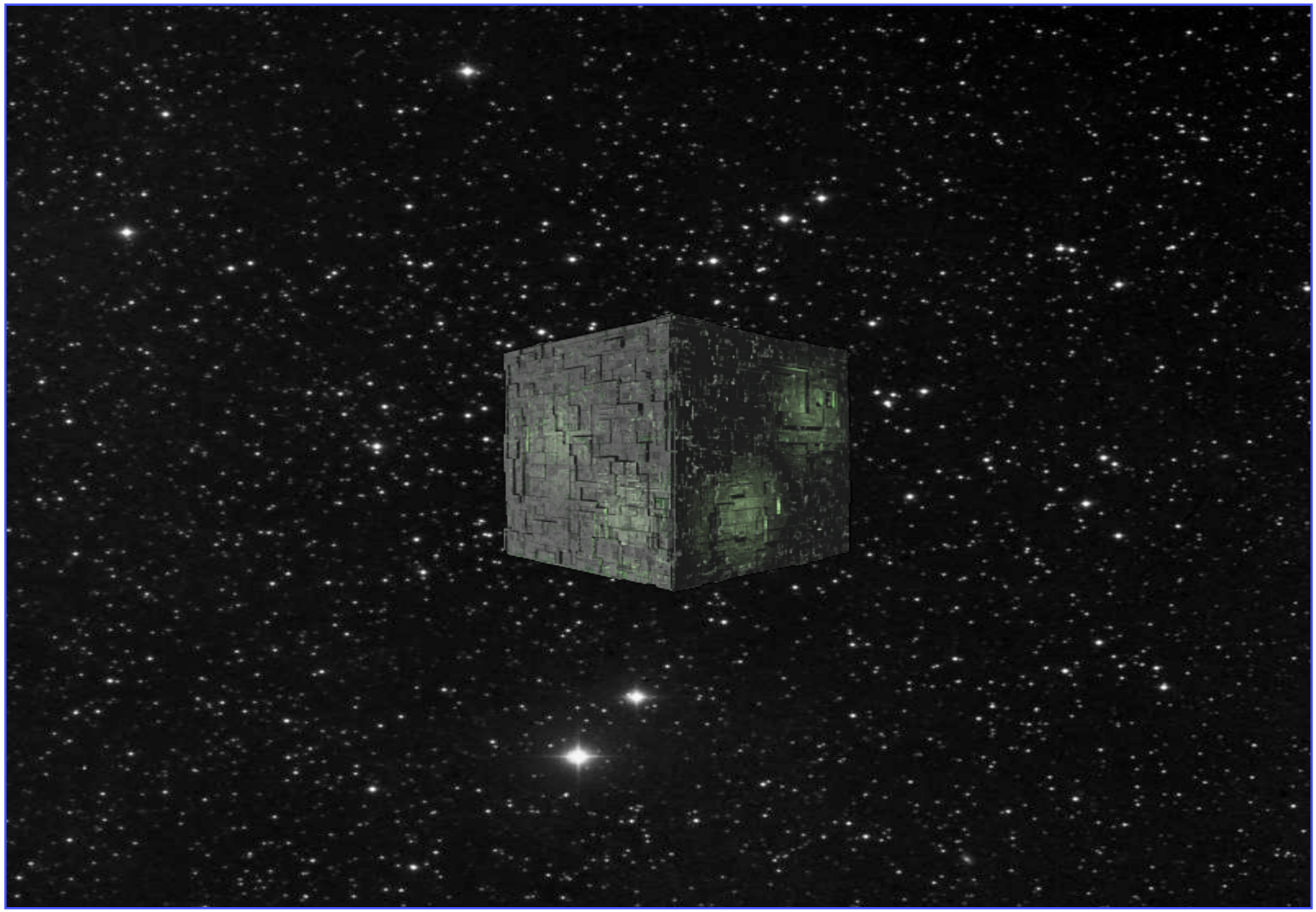
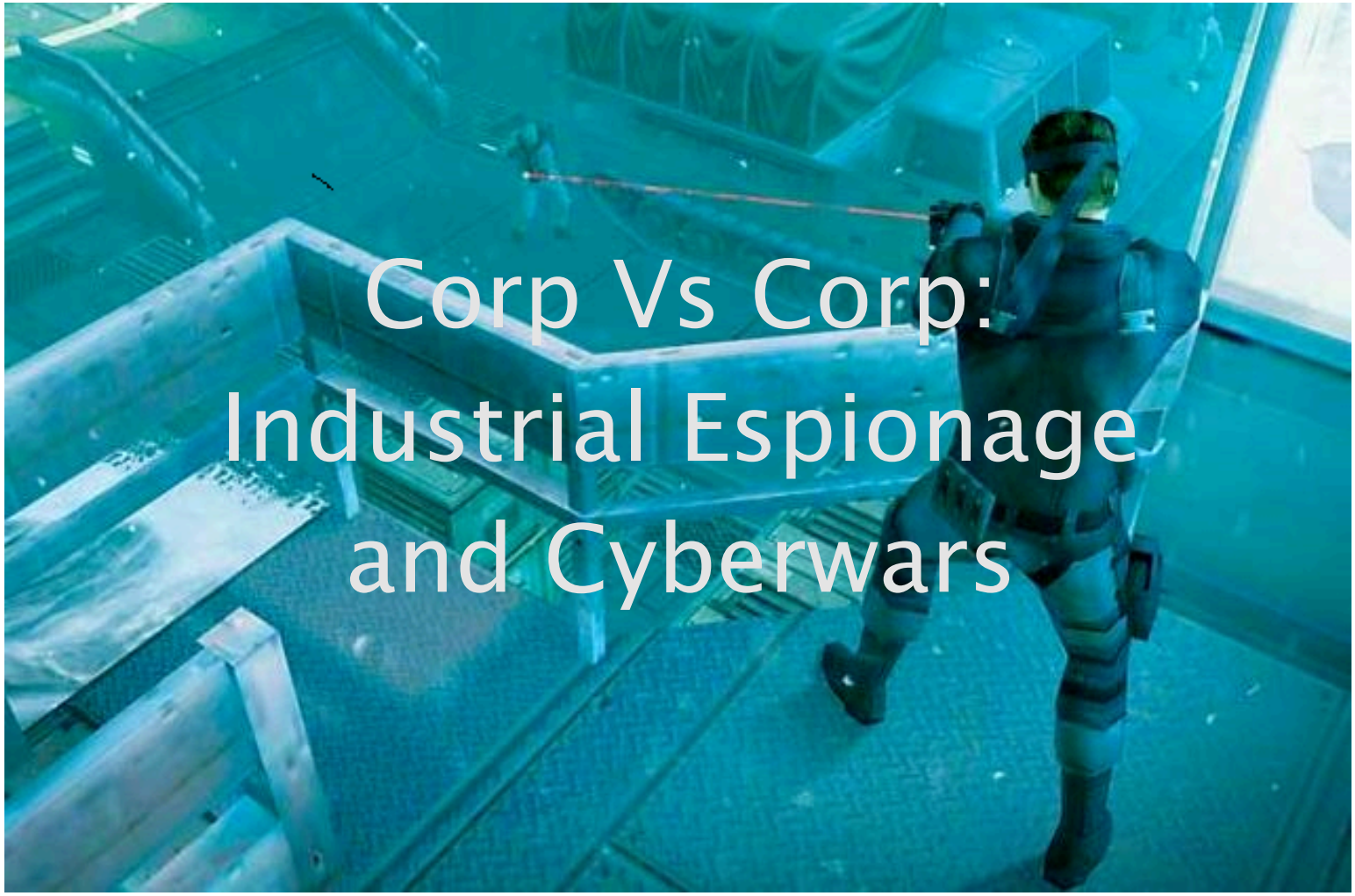
THE LECTURERS

Fabio Ghioni

Roberto Preatoni




Corp Vs Corp:
Industrial Espionage
and Cyberwars


BLACK HAWK DOWN

INDEX

1) Introduction: old and new threats after September 11th
2) Industrial Espionage: state-sponsored espionage
3) Cyber defense methodology: from digital identification of attacker to counterattack strategy
4) Cyber counterattacks: information leakage, Injected Interception

In the aftermath of September 11th, security issues came into the limelight… everybody focalized their attention on increasing anti-terrorist measures and countering the increasing number of hacker attacks to business and government networks…





… but hardly anyone has ever mentioned a more insidious and widespread criminal activity: INDUSTRIAL ESPIONAGE

WHY ?

Companies are often reluctant to publicly admit that they have been victims of industrial espionage for two main reasons:

- it implicitly means that THERE WAS SOME KIND OF VULNERABILITY to be exploited
- it implies the unveiling of MORE CONFIDENTIAL lines of business

WHAT exactly is INDUSTRIAL ESPIONAGE?

The illegal acquisition of intellectual property and trade secrets, in other words THEFT!

The techniques to steal information from outside a company range from the traditional eavesdropping to social engineering tactics…

The FBI generally defines economic espionage as "government-directed, sponsored, or coordinated intelligence activity, which may or may not constitute violations of law, conducted for the purpose of enhancing that country's or another country's economic competitiveness by the use of the information by foreign government or by providing it to foreign private business entity thereby giving that entity a competitive advantage in the marketplace,..."

Since the 1990s Western Intelligence Agencies appear to have focused most of their time and resources on industrial espionage

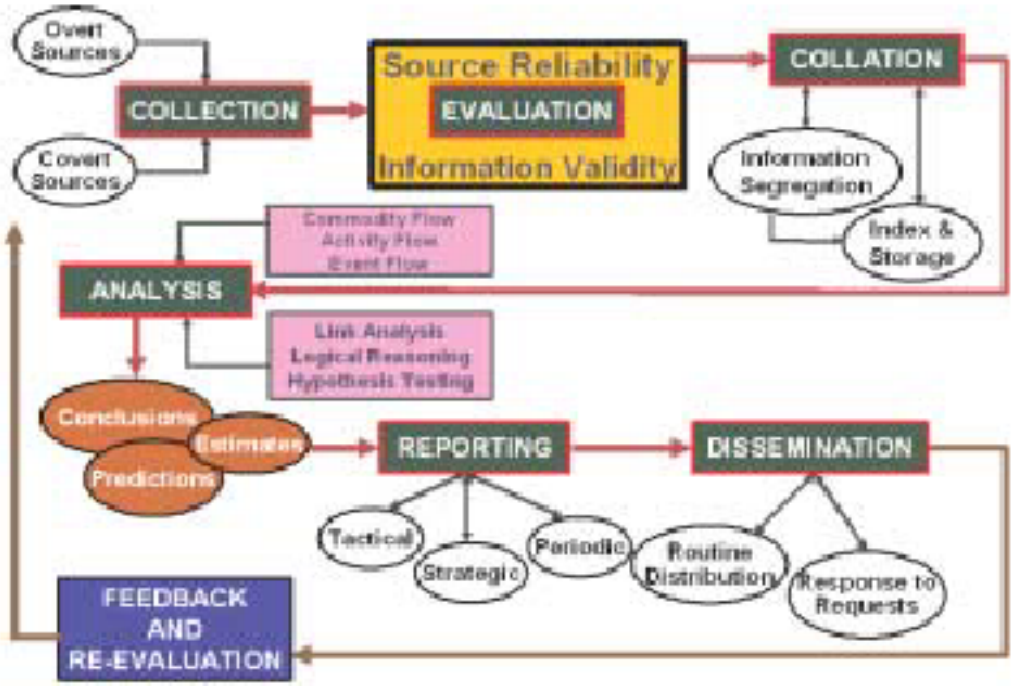
In most countries corporations rely on Government Agencies to carry out investigations whose results can be used to boost the National economy…

France, the United States and Israeli have often been accused to spying on competitors' industrial secrets through scanning systems such as Echelon or the Helios 1A satellite up until the more recent Carnivore software

Conversely, the INDUSTRIAL INTELLIGENCE process consists of researching information on public source documents in order to draw inferences about what competitors might be going to do and provide the basis for possible counteraction

Situational Awareness is the key word…

The classic Intelligence Cycle



Source: Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies

http://www.cops.usdoj.gov/mime/open.pdf?Item=1396

". . . attaining one hundred victories in one hundred battles is not the pinnacle of excellence.

Subjugating the enemy's army without fighting is the true pinnacle of excellence."

Sun Tzu, The Art of War

"There are but two powers in the world, the sword and the mind. In the long run the sword is always beaten by the mind."

Napoleon Bonaparte

Nevertheless, there is sometimes a fine line between the legitimate tactics of competitive intelligence gathering and the illegitimate practice of industrial espionage…

Information may be obtained through the use of unethical but legal techniques, such as social engineering or the exploitation of competitors' errors or negligence (e.g. e-mail hijacking)

Today, indeed, companies can rely on cyber-based techniques and methodologies to react to attacks coming from the real world…

The Internet and the Web have dramatically impacted the classic intelligence cycle

More information is migrating to the Web as companies use it to automate their value chain and build tight linkages with their business parties

THE ATTACKS

Distributed Denial Of Service

- Set up of botnets or drones instructed to perform synchronized attacks

Information leakage and data manipulation

- Intranet access due to loose access policies
- Weak corporate applications
- Exploitation of insiders

CASE STUDIES 1/4

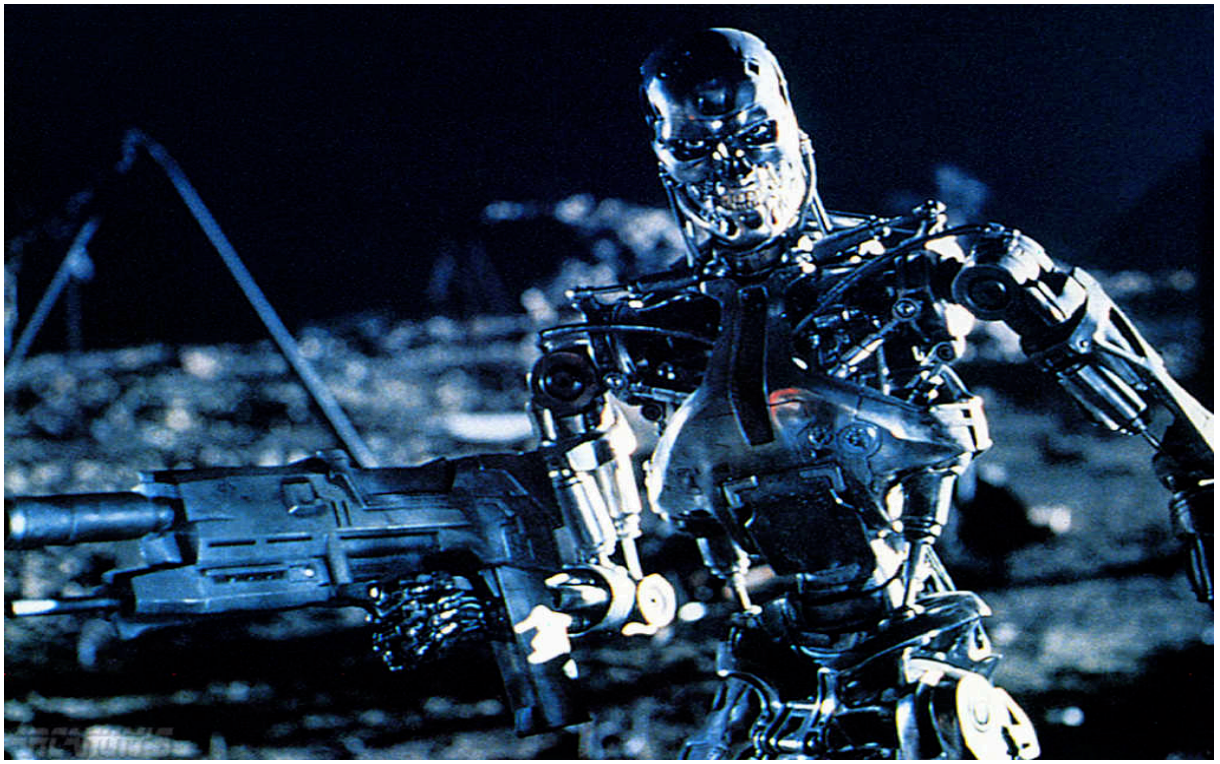
T-Mobile

- At the end of 2003 a hacker got access to the T-mobile users' accounts and stole private material from jet-set users as well as a C.I.A. document located on a T-Mobile transit e-mail account belonging to a C.I.A. agent. The hacker exploited a Bea Weblogic interface flaw.

CASE STUDIES 2/4

Skynet 1.0

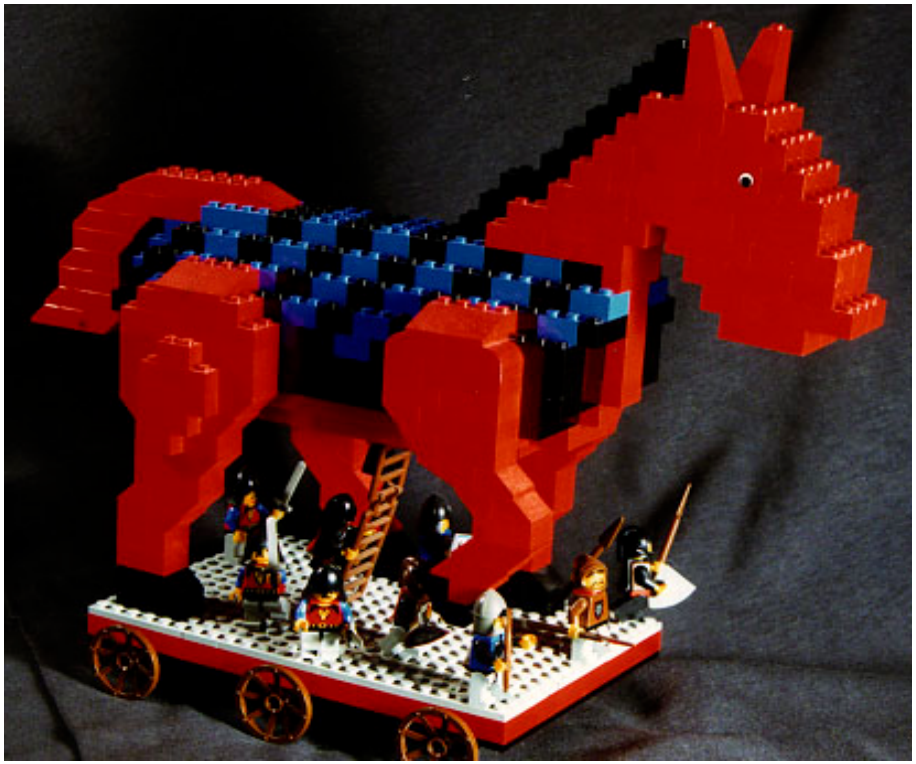
- A new application of Artificial Intelligence
- Set up of intelligent networked agents
- Underground work is in progress



CASE STUDIES 3/4

Israel Trojan Horse

- In 2005 Israel was put in a difficult situation by an industrial espionage scandal involving several corporation and dozens of people.
- Once again data were stolen using a trojan and social engineering.
- Trojan-based attacks are growing rapidly and are considered as among the most important security risks for today's corporations.



CASE STUDIES 4/4

Chinese Trojan Attacks

- Several American corporations got compromised in the last year by trojan attacks perpetrated by chinese citizens, according to the attacks' logs.
- Myfip, the trojan used for most of the attacks appeared to be one of the most sophisticated ever and one of its peculiarity was that it tried to steal also CAD/CAM files, usually related to engineering design works.
- According to an IBM report, in the first half of 2005, 'customized‘ attacks against governments, corporations and financial institutions jumped to 50 per cent.

THE DEFENSE METHODOLOGY 1/2

Digital Identification of the Attacker

- Understanding the originating path
- "Digital fingerprinting" and pre-analysis of the attack methodology

Passive Observation and Tracking

- Logging the identified activity
- Spotting the attacker

THE DEFENSE METHODOLOGY 2/2

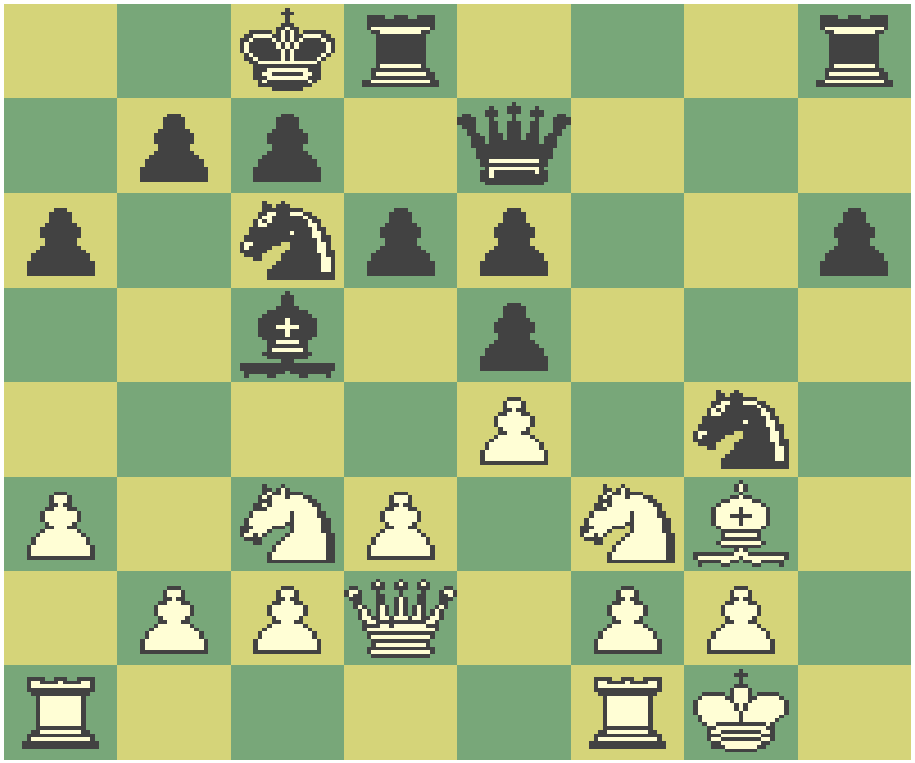
Active Honeypots and Honeynets

Situational Awareness

- Case mapping

Definition of Counterattack Strategy

- Resource selection and allocation
- Definition of timing, effort and techniques



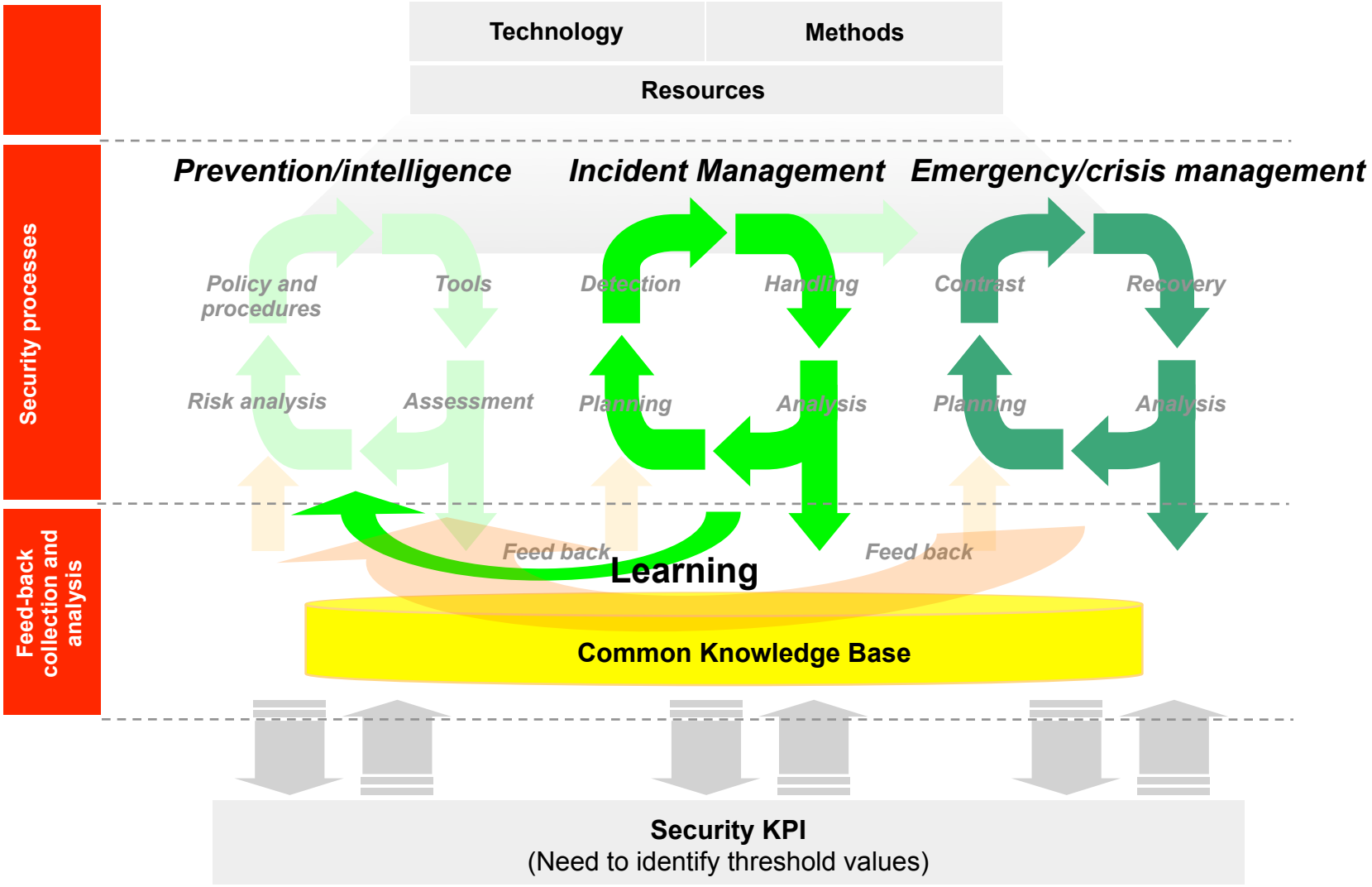
CYBER COUNTERATTACKS

An example…

Injected Interception

•allows to trace the IP address of a target and gain direct access to all data contained on the computer no matter what is the means of data transport (i.e. physical or digital)

The security management learning model



Questions?
English

¿Preguntas?
Spanish

أَيَّة مَطَالِبِ
Arabic

Domande?
Italian

вопросы?
Russian

Ερωτήσεις?
Greek

tupoQghachmey
Klingon

質問
Japanese