



Con il patrocinio di



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

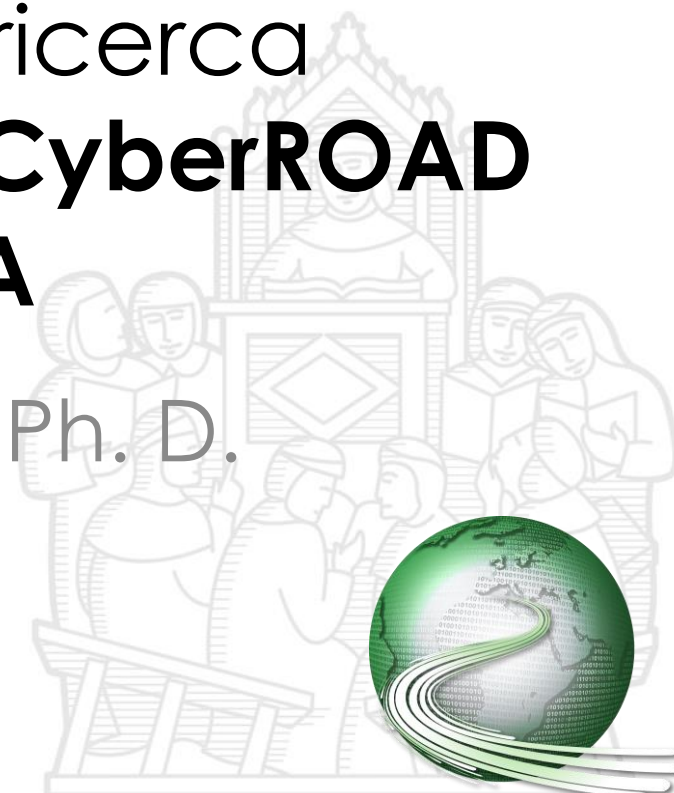
Cybersecurity e ricerca scientifica: i progetti **CyberROAD** e **DOGANA**

Ing. Davide Ariu, Ph. D.



Dogana

ADVANCED SOCIAL ENGINEERING AND
VULNERABILITY ASSESMENT FRAMEWORK



CYBER ROAD



Sant'Anna
Scuola Universitaria Superiore Pisa

Corso di base «Introduzione alla Cyber-Security», Pisa 4-8 luglio 2016

Who I Am...

- I'm a Post-Doc with the Pattern Recognition and Applications Lab (University of Cagliari – <http://pralab.diee.unica.it>)
- I'm an electronic engineer with a Ph.D. in Computer Security
- Together with several colleagues, I've recently founded **Pluribus One** (<http://www.pluribus-one.it>)

Personale docente:

[Luca Didaci](#)
[Giorgio Fumera](#)
[Giorgio Giacinto](#)
[Gian Luca Marcialis](#)
[Fabio Roli, Lab Director](#)

Studenti di dottorato:

[Mohanad Abukmeil](#)
[Mansour Ahmadi](#)
[Amra Demontis](#)
[Alessandro Carcangiu](#)
[Muhammad Ahmed Khfagy](#)
[Bahram Lavi](#)
[Paolo Russu](#)

Disseminazione e valorizzazione risultati:

[Matteo Mauri](#)
[Fabio Roli](#)

Assistente di progetto:

[Carla Piras](#)

Ex collaboratori

[Laureandi](#)

Ricercatori post-doc:

[Davide Ariu](#)
[Battista Biggio](#)
[Igino Corona](#)
[Davide Maiorca](#)
[Duc-Tien Dang-Nguyen](#)

Collaboratori:

[Luca Ghiani](#)
[Luca Piras](#)
[Amaia Abanda](#)
[Elena Chiappe](#)
[Matteo Contini](#)
[Marco Melis](#)
[Luigi Meloni](#)
[Alessio Mulas](#)
[Valerio Mura](#)
[Guido Mureddu](#)
[Giulia Orrù](#)
[Enrico Salis](#)
[Enrica Santucci](#)
[Roberto Tronci](#)
[Pierluigi Tuveri](#)

Visiting professors

[Visiting students](#)



Why I'm here today?

- Currently, I'm mostly responsible for the management of several EU funded research projects

ILLBUSTER



Dogana

ADVANCED SOCIAL ENGINEERING AND
VULNERABILITY ASSESSMENT FRAMEWORK



CYBER ROAD

maven

Management and Authenticity Verification of multimedia contENts

- Just trying to explain how much you can learn from international research projects...



An Open, Safe, and Secure Cyberspace

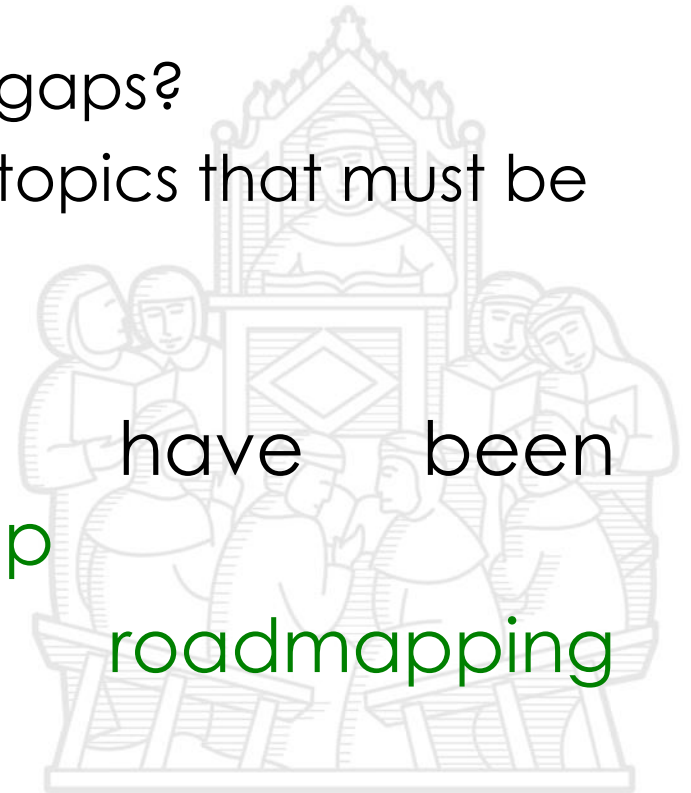
- EU Strategic Priorities and Actions*
 - **Achieving Cyber Resilience**
 - **Drastically Reducing Cybercrime**
 - Develop cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
 - Develop the industrial and technological resources for cybersecurity
 - Establish a coherent international cyberspace for the EU and promote core EU values

*Cybersecurity Strategy of the European Union - 2013

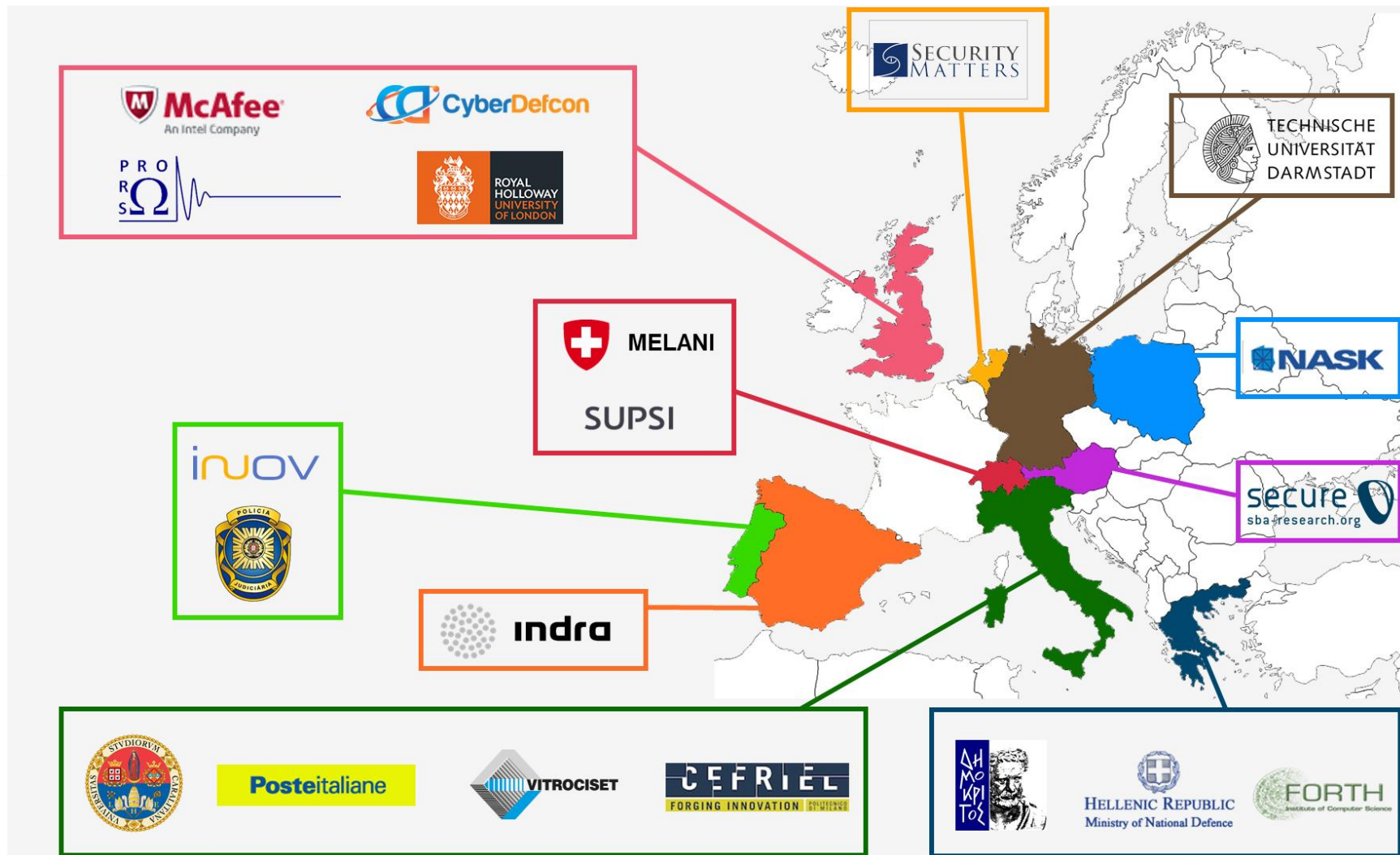


Why CyberRoad?

- The project call: Topic SEC-2013.2.5-1 Developing a **cyber crime** and **cyber terrorism** research agenda
 -
 - What are the major research gaps?
 - What are the major research topics that must be addressed to fill the gaps?
 -
- Research agenda: we have been committed to do a **roadmap**
- Based on a solid **roadmapping methodology**

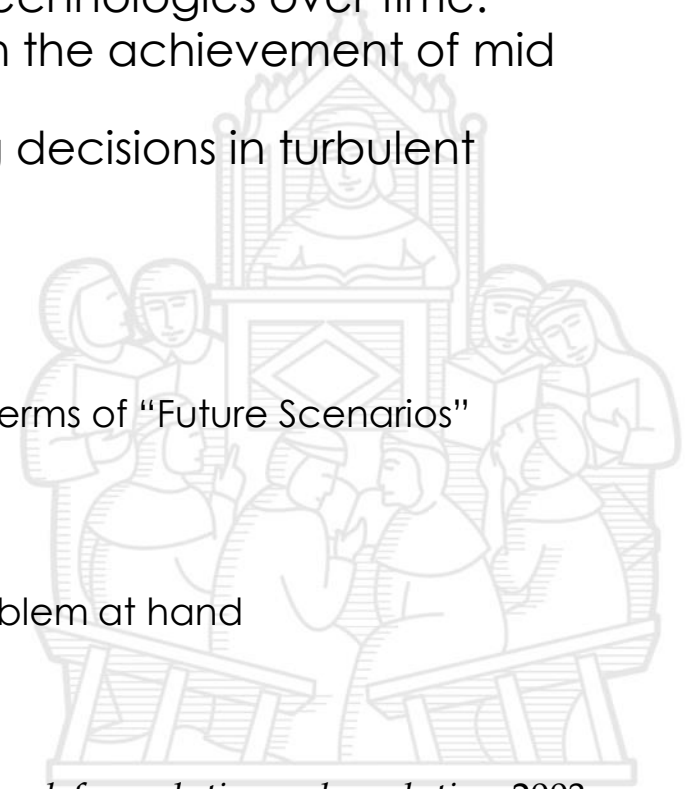


The CyberRoad team



Why to Roadmap?

- **Roadmapping techniques can be used to support strategic & long-range planning***
 - Technology roadmapping is widely used especially by the companies for exploring and communicating the relationships between evolving and developing markets, products, and technologies over time.
 - Can be also used by governments to plan the achievement of mid and long term goals
 - It can in general help making challenging decisions in turbulent environments
- **Data sources**
 - Experts in the domain of interest
 - Generally provide their views on the future in terms of “Future Scenarios”
 - Stakeholders
 - Usually express their needs
 - Empirical Data
 - Provide concrete evidence regarding the problem at hand
 - Scientific Literature



*Robert Phaal et. Al., *Technology roadmapping – A planning framework for evolution and revolution*, 2003



Why to Roadmap?

- Was in 2007-2008 (when Apple marketed the iPhone and Google released Android) possible to foresee the current scenario of Mobile (in)Security?

Technical facts

- (relatively) High Computational Power
 - Moore's Law known since '60s
- Always-on connectivity
 - 1st generation iPhone soon replaced (in 2008) by the 3G version

Economical facts

- Huge size of the Mobile market, even before the Smartphone era
 - E.g. Since 2004 in Italy we have more mobile devices than citizens
 - Quickly enlarging markets
- Pressure from the Internet Providers

Experience from past cyber-attacks

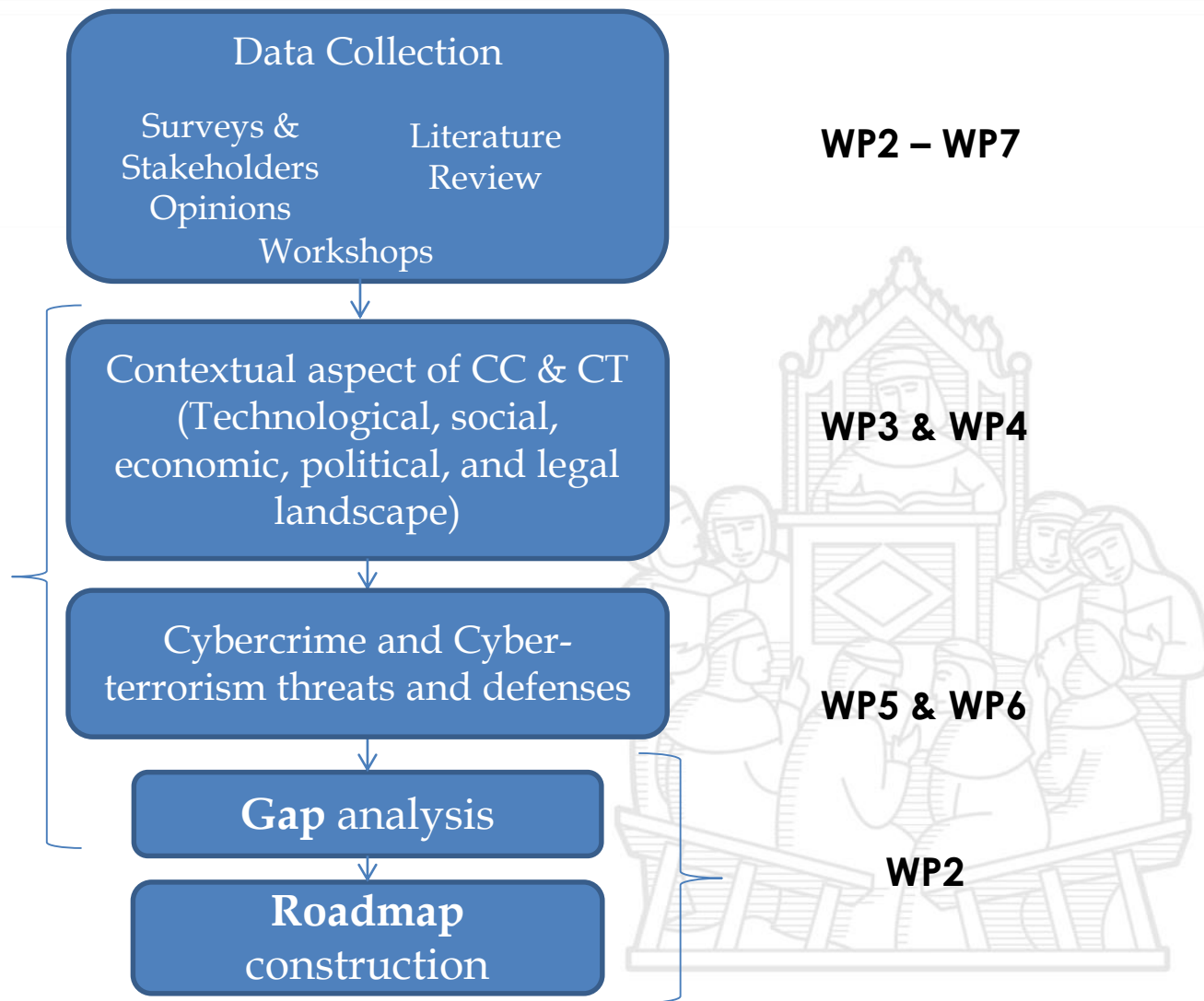
- Platforms with many users are strongly appealing
- Always connected devices are more exposed



How we did the roadmap

Exploratory
roadmap using
scenario building
and **gap analysis**

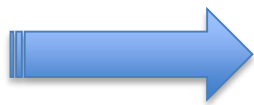
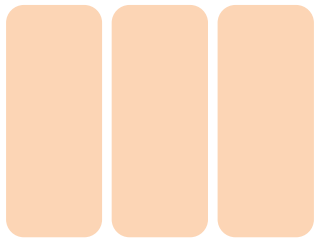
Creation of
actual & future
scenarios



Gap Analysis

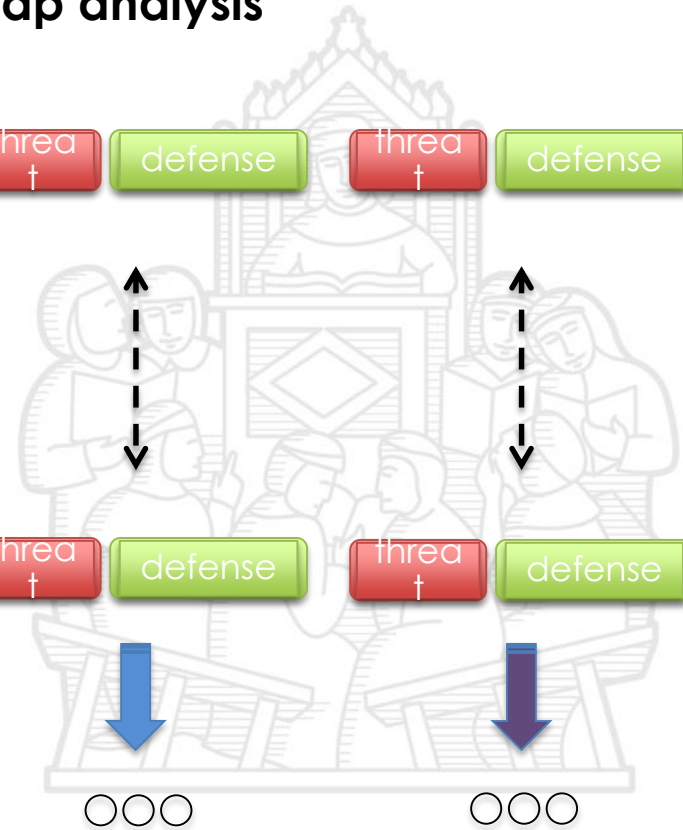
GAP ANALYSIS: the process of comparing actual and future views (i.e., the current knowledge and future needs) in order to identify **research gaps**

Set of actual scenarios



Gaps ○○

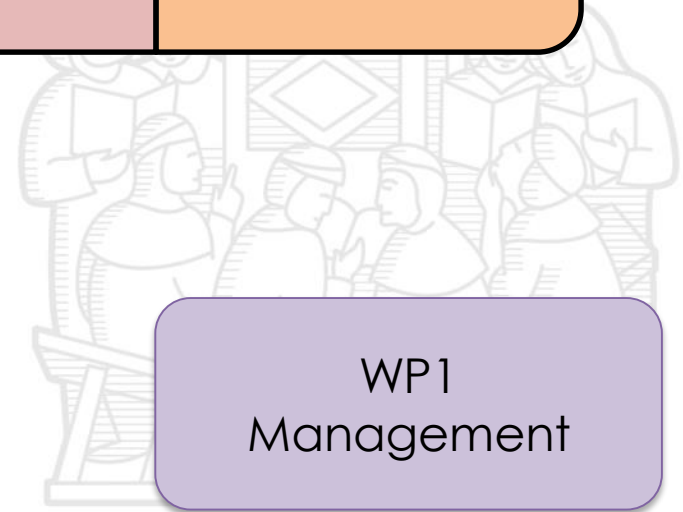
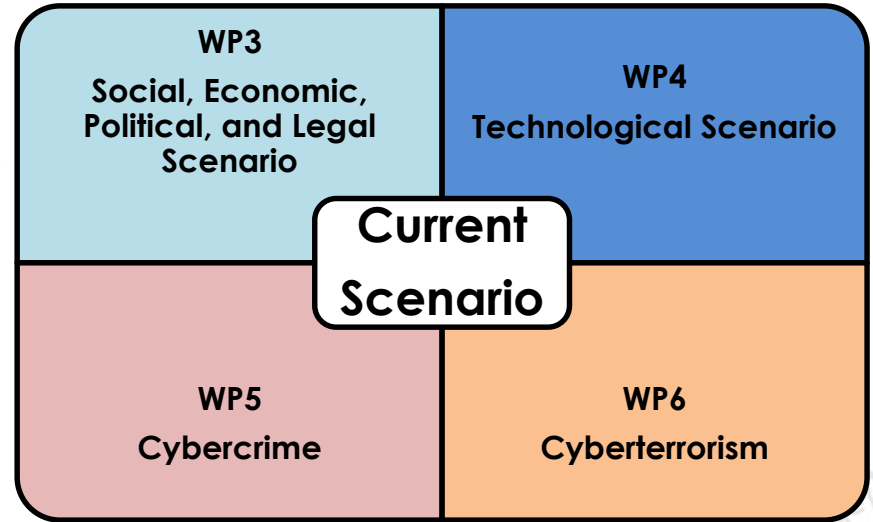
Gap analysis



WP organization

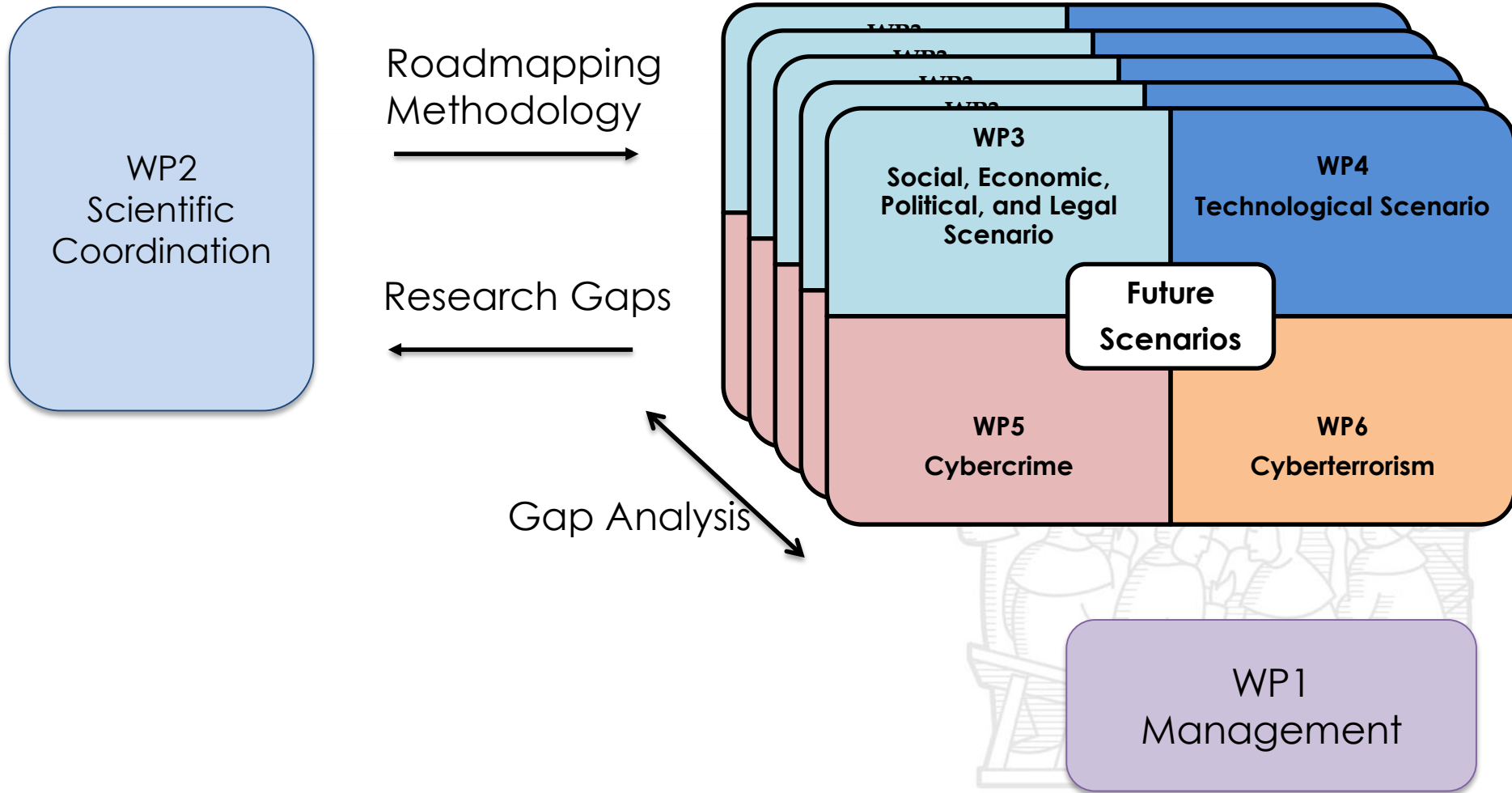
WP2
Scientific
Coordination

Roadmapping
Methodology

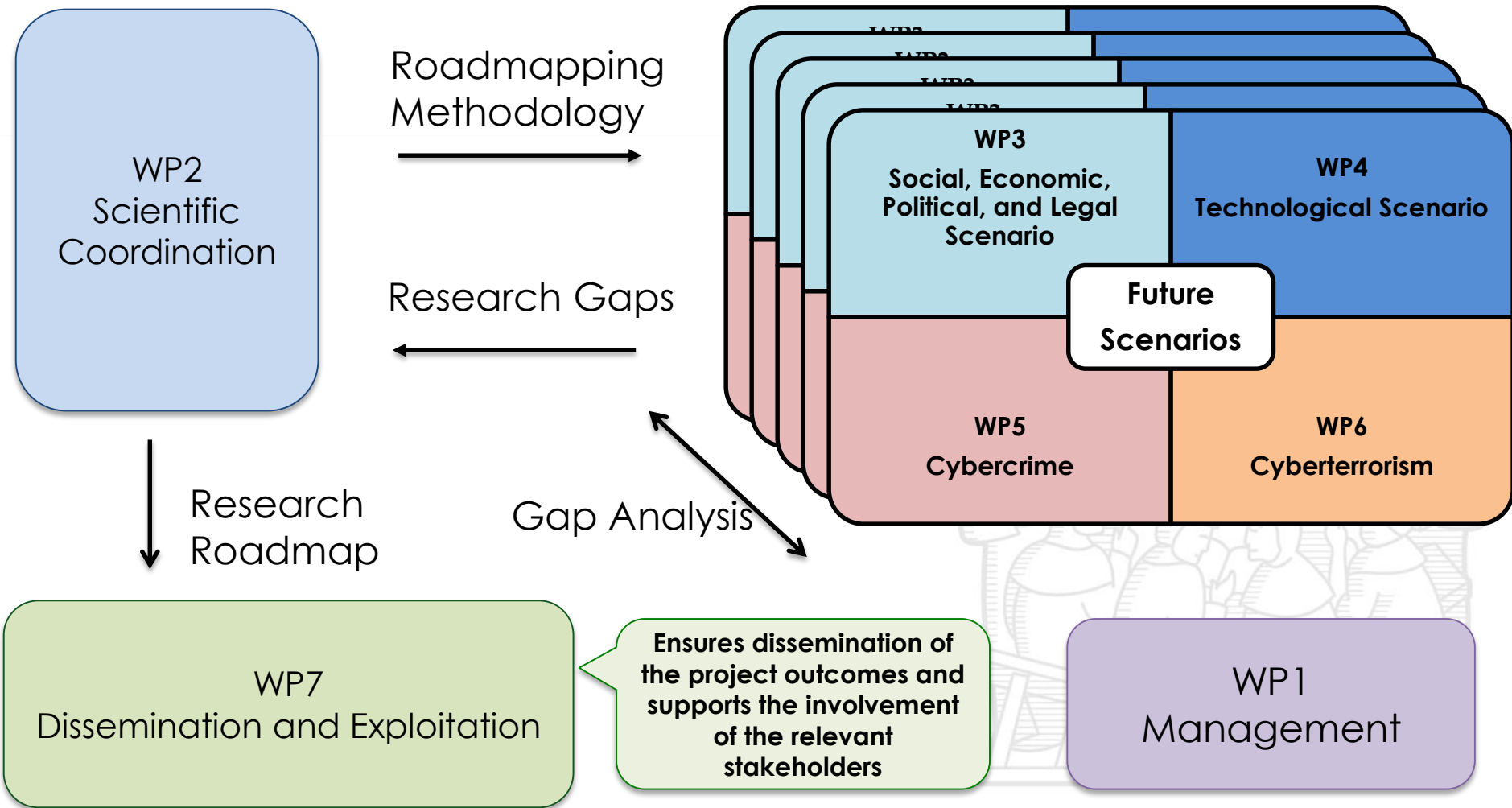


WP1
Management

WP organization



WP organization



Cybercrime Surveys



CYBER ROAD
DEVELOPMENT OF THE CYBERCRIME AND
CYBER-TERRORISM RESEARCH ROADMAP
www.cyberroad-project.eu



- 2,200 English or Polish speaking stakeholders, in the EU and 20 other countries, responded to the wide-ranging, Delphi-based, survey questions.
- The findings provide a snapshot of cybercrime-related, real-life experiences across a diverse landscape of technology-enabled scenarios.

2016 - Cybercrime Surveys Report

Authors – Jart Armin & Bryn Thompson (CyberDefcon) & Piotr Kijewski (NASK)

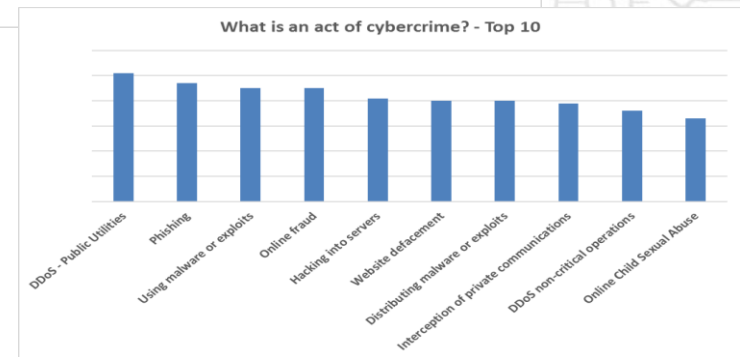
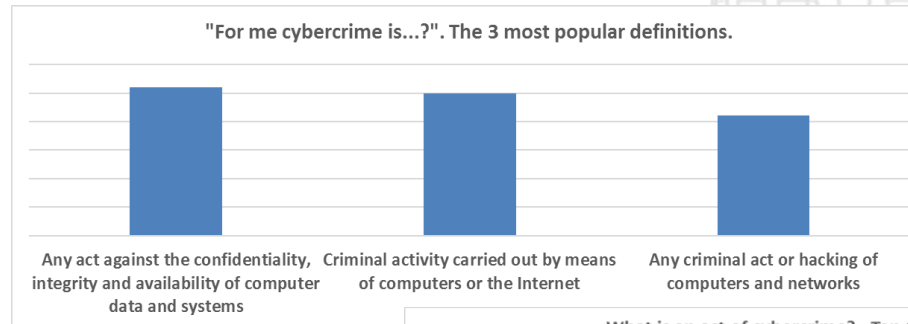
Table of Contents

1	Overview of the Cybercrime Surveys	2
1.1	Introduction	2
1.2	Methodology	2
2	Results and Findings	4
2.1	Definitions of cybercrime	4
2.2	What activities are considered to be cybercrimes?	4
2.3	Best practices and workplace policies	5
2.4	Cyber security responsibility	8
2.5	Security solutions	9
2.6	Sources of data and information on cybercrime	10
2.7	Personal experiences of cybercrime	10
2.8	Consumer rights	12
2.9	Cybercrime research – Return on Investment (ROI)	12
2.10	Information sharing	14
2.11	Cyber Threats	15
3	Analysis from the stakeholder surveys – What are the research gaps?	16
3.1	Gap Analysis	16
4	Conclusions	18

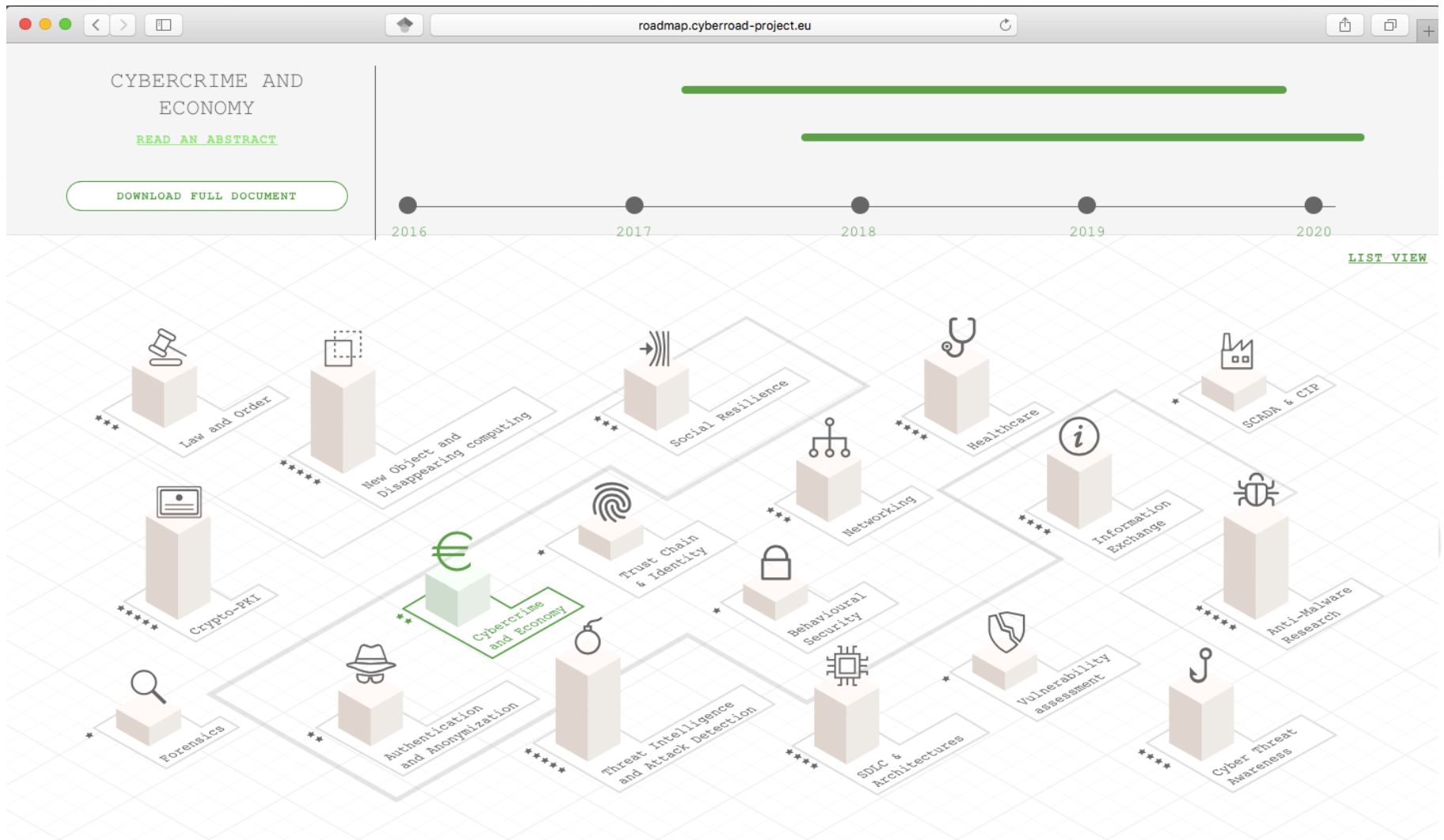
Acknowledgements

The authors would like to provide grateful thanks to all the many survey participants & respondents who gave up valuable time to complete the surveys, this report is primarily for you. To the European Commission Seventh Framework Programme, that made this possible. APWG, MAAWG, ENISA, and the wider cyber security community. LinkedIn, Survey Monkey, Google, & the CyberROAD team;

UNIVERSITÀ DEGLI STUDI DI CAGLIARI, TECHNISCHE UNIVERSITÄT DARMSTADT, INDRA, POSTE ITALIANE, SECURITY MATTERS, VITROCISET, FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS, INOV, DEMOKRITOS, SBA, PROPRS, MINISTÉRIO DA JUSTIÇA (PORTUGAL), CEFRIEL, SUPSI, ROYAL HOLLOWAY, MINISTRY OF NATIONAL DEFENCE, GREECE, MELANI



The Roadmap

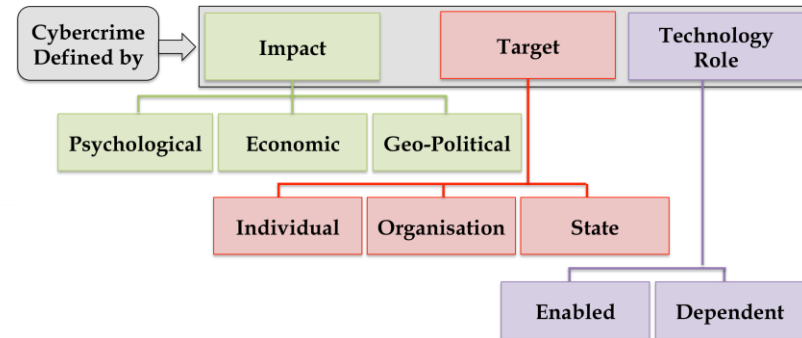


CyberROAD Main Achievements

A S.E.P.L. perspective on Cybercrime

- **Provided a categorisation of cybercrime along three dimensions:**

- Impact
- Target
- Technology Role



- **Highlighted the role of social means of protecting against and responding to cybercrime and cyberterrorism, suggesting as possible research gaps:**
 - Evaluation of the **role of social resilience** in both defending and absorbing the social and economic impact of cybercrime;
 - **Exploration of the roles of trust relationships** in both defending against and absorbing the social and economic impact of cybercrime;
 - Exploration of the perceived **costs of cybercrime to nation-states and to individual communities.**
- **Raised the following fundamental research questions:**
 - How should cyber crime be quantified and economically evaluated?
 - How can cybercrime be defined and agreed upon on an international level?
 - Is trust possible in the digital age?

CyberROAD Main Achievements

Cybersecurity Solutions Taxonomy

- Derived from existing sources (either scientific/non-scientific)
- Applied to the technological Paradigms, Trends, and Threats devised in D4.1

Attacks

- **Security Violation (Attacker's Goal)**
 - Confidentiality, Integrity, Availability
- **Attack Specificity (Attacker's Goal)**
 - Indiscriminated, Targeted
- **Attack Surface (Attacker's Capability)**
 - Relevant HW & SW Components / Communication Means
- **Attack Influence (Attacker's Capability)**
 - Causative, Exploratory
- **Attacker's Skill and Motivations**
 - Low, High
- **Technology Role**
 - Enabled, Dependent
- **Exploitation Tools and Techniques**
- **Victims and Targets**
 - Individuals, Organisations, States
- **Impact Type**
 - Direct, Indirect

Characterization of the Attack Scenario				
High-level Attack Categorization		Cybercrime Cyberterrorism	✓	
Attacker's Goal - Security Violation		Confidentiality (Privacy) Integrity Availability	✓	
Attacker's Goal - Attack Specificity		Indiscriminated Targeted	✓	
Attacker's Capability - Attack Surface		Relevant Hardware and Software components Communication means (e.g. Wi-Fi, Bluetooth, etc.)	✓	
Attacker's Capability - Attack Influence		Causative Exploratory	✓	
Attacker's Skills and Motivations	Low Skills (Low-tech/Low-Medium Expertise)	Young, Unskilled (Script Kiddies)		
		Soft Skilled (Online Social Hacker)		
		Internal, Low-Medium Skilled (Employee)	✓	
	High Skills (High-Tech, High Expertise)	Infrastructure Use (Tools User, Deployer)	Infrastructure Delivery (Provider, Developer, Operator)	
			Paid Nonchalant (Espionage) National Mission	
			Paid Nonchalant (Espionage) Corporate Mission	✓
			Socially Motivated Citizens (hacktivist)	
			Ideologically Motivated (cyber terrorist)	
			Profit Oriented (cyber criminal)	
			Nationally motivated citizens (cyber fighter)	
Technology Role		Technology-enabled Technology-dependent	✓	
Exploitation Tools and Techniques		No-one Research prototype Mature with open solutions existing Mature with commercial solutions existing Mature with solutions existing on the black market Cyberweapons	✓	
Victims & Targets		Individuals Organizations National States	✓	
Impact type	Direct	Failure of services (unavailability)		
		Failure of data (no more integrity)		
		Failure of restrictions (no more confidentiality)	✓	
	Indirect	Economical		
		Psychological		
		Geo-political Reputational damage	✓	

CyberROAD Main Achievements

Cybersecurity Solutions Taxonomy

- Derived from existing sources (either scientific/non-scientific)
- Applied to the technological Paradigms, Trends, and Threats devised in D4.1

Countermeasures

- **Technological**
 - Hardware Security
 - Network Security
 - Software Security
 - Data Security
- **Organisational**
 - Training, Audit, Media Protection, Role-based Organisation
- **Procedural**
 - Security Authorisation Process
 - Device Management
 - Incident Response
- **Awareness**
 - Security Awareness Training
 - Incident Response Training

Countermeasures				
Countermeasures	Technological	Hardware Security	Anti-Tampering	✓
			Hardware Hardening	
		Network Security	Intrusion Detection	✓
			Intrusion Prevention	
			Unified Threat Management	
			URL Filtering	
		Software Security	Sandboxing	
			Penetration Testing and Patching (Security Updates)	✓
			Vulnerability Assessment	
		Data Security	Software Hardening	
	Encryption			
	Data Loss Prevention			
	Insider Threat Detection		✓	
	Organisational	Training Policies		
		Audit and Accountability Policies		
		Media Protection Policies	✓	
		Role-based organization		
	Procedural	Security Authorization processes	✓	
		Device Management processes		
		Incident Response Procedures		
Awareness enhancements	Security Awareness Training			
	Incident Response Training	✓		

A bit more on the Research Topics

#	Title	#	Title
1	ANTI-MALWARE	10	LAW AND ORDER
2	AUTHENTICATION AND ANONYMIZATION	11	NETWORKING
3	BEHAVIOURAL SECURITY	12	NEW OBJECTS AND DISAPPEARING COMPUTING
4	CRYPTOGRAPHY AND PUBLIC-KEY INFRASTRUCTURES (PKIS)	13	SCADA & CRITICAL INFRASTRUCTURES PROTECTION
5	CYBERCRIME AND THE ECONOMY	14	SOCIAL RESILIENCE
6	CYBER THREAT AWARENESS	15	SDLC & ARCHITECTURES
7	FORENSICS	16	THREAT INTELLIGENCE AND ATTACK DETECTION
8	HEALTHCARE	17	TRUST CHAINS AND IDENTITY
9	INFORMATION EXCHANGE	18	VULNERABILITY ASSESSMENT

From several of the CyberROAD Research Topics emerged issues concerning the Social Engineering

SOCIAL ENGINEERING

The clever manipulation
of the natural human
tendency to trust.



Definition

“The art of intentionally *manipulating* behaviour using specially crafted *communication techniques*.”

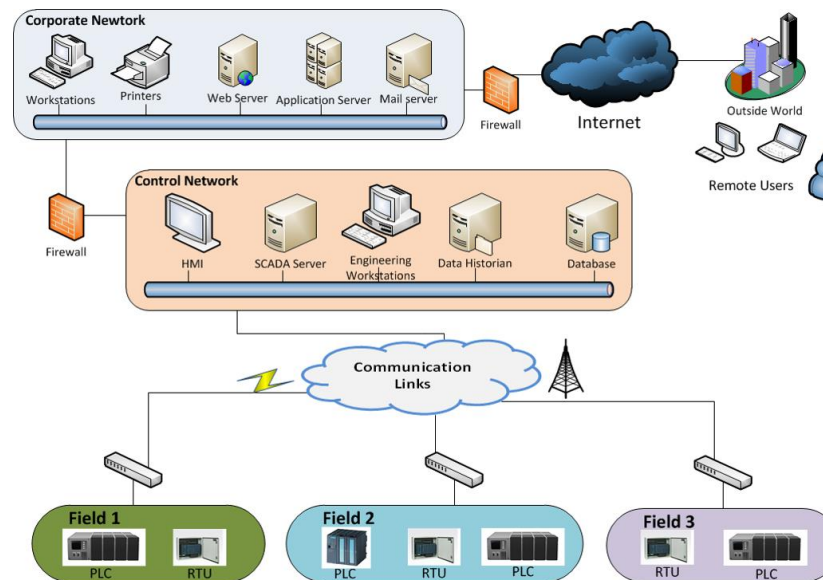
“Social engineering is the ‘art’ of utilizing *human behavior* to breach security without the participant (or victim) even realizing that they have been *manipulated*.”



S.E. – Examples from the CyberROAD Topics

Energy/Utilities

- A utility is an organization that maintains the infrastructure for a public service and that often also provides services that use such infrastructure.
 - E.g. Electric, Natural Gas and Water Firms and are essential services that play a vital role in economic and social development.
 - Controlled by the means of SCADA/ICS networks



S.E. – Examples from the CyberROAD Topics

Energy/Utilities

- Threat to water utilities is the loss of sensitive information (e.g. customers' personal data) that is stolen by cybercriminals. [...]
- [...] Techniques used to steal information include social engineering and phishing e-mails used to install malware for the exfiltration of the data criminals are interested in. [...]
- [...] Targeted attacks, where attackers employ specifically developed malware and zero-day exploits aiming at an exact target, are on the rise. [...]
 - [...] In order to provide remote accessibility, elements of SCADA systems, used to monitor and control the plants and equipment, are connected to the Internet through corporate networks. These SCADA elements expose the control network and pose a risk of attacks like scanning, probing, brute force attempts, and unauthorized access of these devices. [...]

"It's a milestone because we've definitely seen targeted destructive events against energy before—oil firms, for instance—but never the event which causes the **blackout**," John Hultquist, head of iSIGHT's cyber espionage intelligence practice"

First known hacker-caused power outage signals troubling escalation

Highly destructive malware creates "destructive events" at 3 Ukrainian substations.

by Dan Goodin - Jan 4, 2016 9:36pm CET

Share Tweet Email 112



December 23rd (2015) Ukrainian Power Outage (A.k.a. Black Energy 3)

BlackEnergy 3 plug-ins*:

- [...]
- **ki.dll — Keylogger**
- **ss.dll — Screenshots**
- **vs.dll — Network discovery, remote execution**
- **rd.dll — Simple pseudo “remote desktop”**
- [...]

According to ESET, the Ukrainian power authorities were infected using booby-trapped macro functions embedded in Microsoft Office documents.

Black Energy 2 (from 2014) leveraged vulnerabilities in ICS directly connected to the Internet to deliver malware. In contrast, the new **Black Energy 3 variant appears to have been launched using a spear phishing campaign with malicious Microsoft Office (MS Word) attachments.**

In March 2015, an email appearing to be from the Supreme Council of Ukraine was sent to multiple state institutions ... One of the targets in this campaign was a power company situated in the western part of the Ukraine. **The spear-phishing email contained an XLS attachment with a macro in it.**

- R. Piggin, Cyber security trends: What should keep CEOs awake at night, Elsevier, 2016
- arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/
- https://blogs.mcafee.com/mcafee-labs/blackenergy_ukrainian_power_grid/

S.E. – Examples from the CyberROAD Topics

Healthcare

- Over 90 percent of healthcare organizations faced a data breach in 2014 and 40 percent had over five incidents in the last two years .
- This trend also explains why the healthcare industry sees 340 percent more security incidents than the average industry :
“**The rapid digitization of the healthcare industry, when combined with the value of the data at hand, has led to a massive increase in the number of targeted attacks against the sector**” .
 - **Targeted Attacks** are among those that more efficiently **exploit Social Engineering techniques to facilitate data breaches**. Despite not being one of the most common attacks so far, the likelihood of an attack of this type on hospitals is very high for data breaches, in particular due to the structural and security problems of several Patient Ecosystems.
 - **Threatening of hospital patients and infiltration through the external nodes**. [...] An interesting menace comes from the abuse of patients' dataspace and medical information, for example through specialized ransomware , which uses Social Engineering techniques against weak targets (elderly, patients etc.)



S.E. – Examples from the CyberROAD Topics

Healthcare

Hollywood hospital's systems held hostage by hackers

The Hollywood Presbyterian Medical Center, an "acute-care facility" located in Los Angeles, has had its computer systems compromised by hackers. The attackers are asking for 9,000 Bitcoin (approximately \$3.6 million) in exchange for giving the hospital access to the systems again.

Community Health Systems data hack hits 4.5 million

18 August 2014 | Technology



Community Health Systems has 206 hospitals across the US

A major US hospital group said it was the victim of a cyber-attack resulting in the theft of 4.5 million people's personal data.

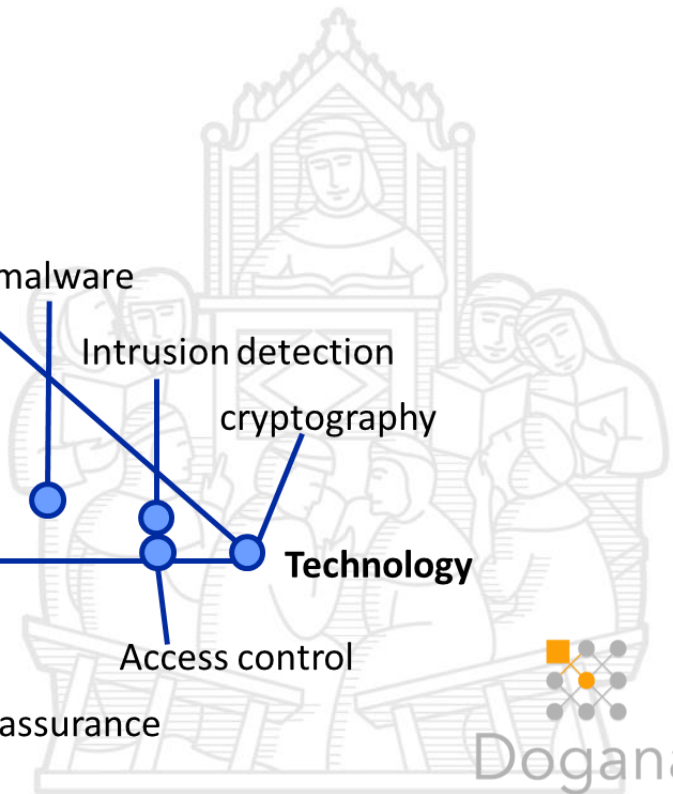
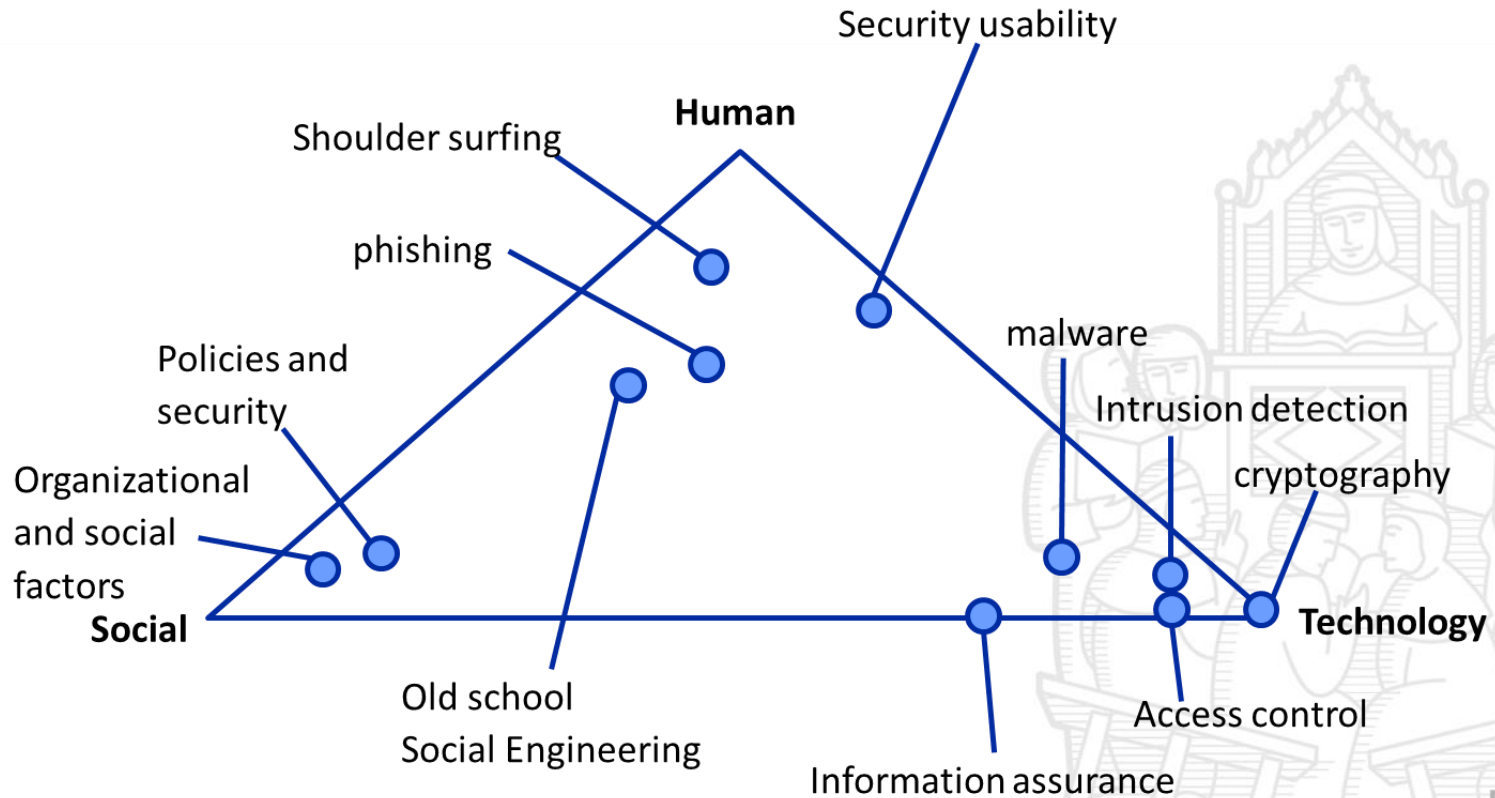
HACK BRIEF: HEALTH INSURER EXCELLUS SAYS ATTACKERS BREACHED 10M RECORDS



Anthem: Hacked Database Included 78.8 Million People

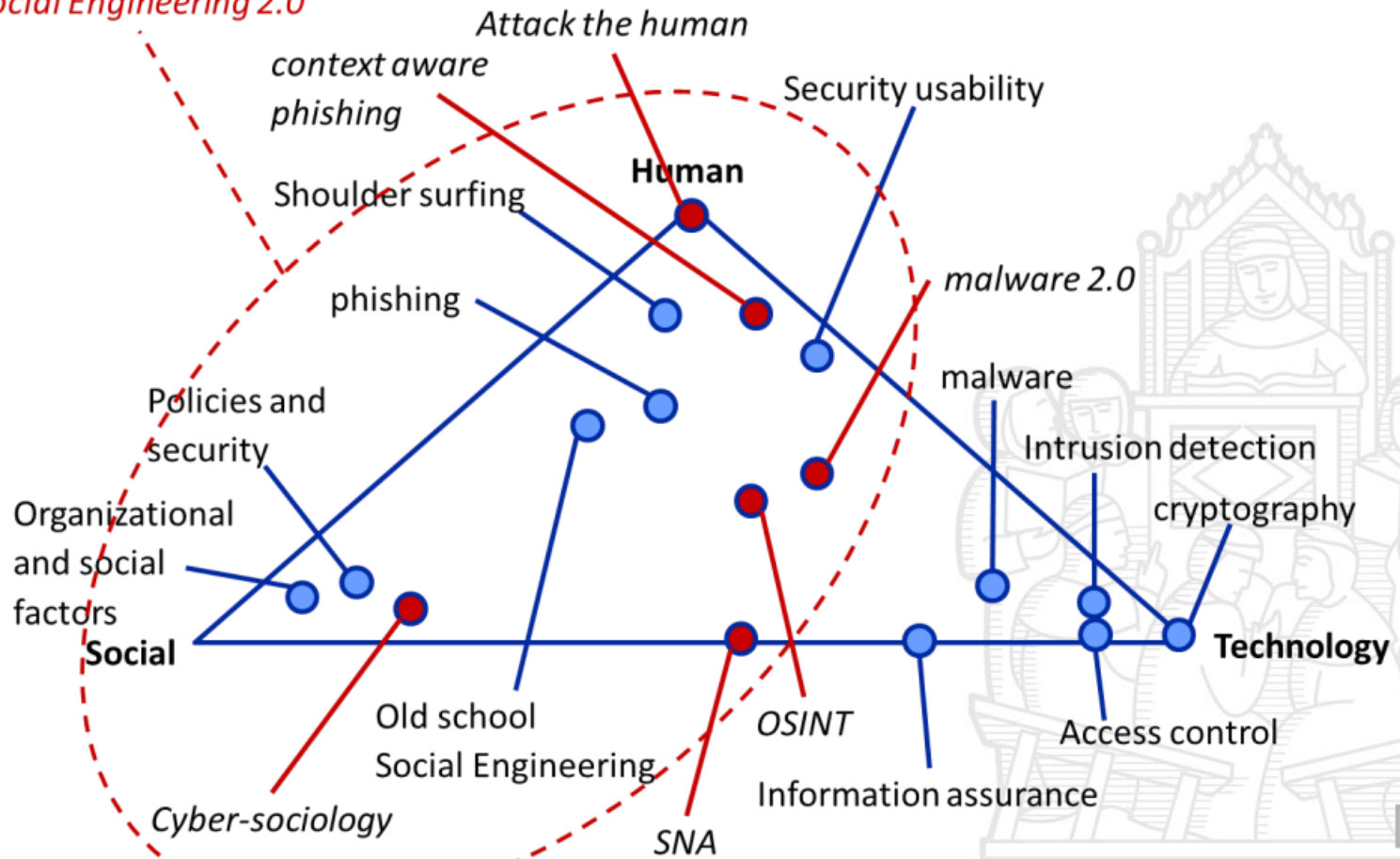
Health insurer says data breach affected up to 70 million Anthem members

Triangle of Security

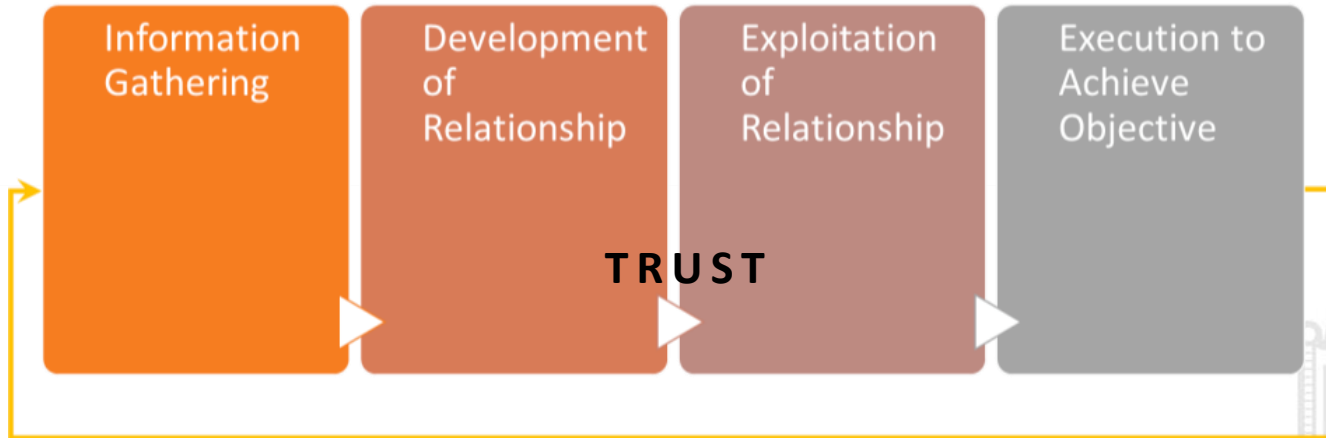


Security Engineering

Social Engineering 2.0

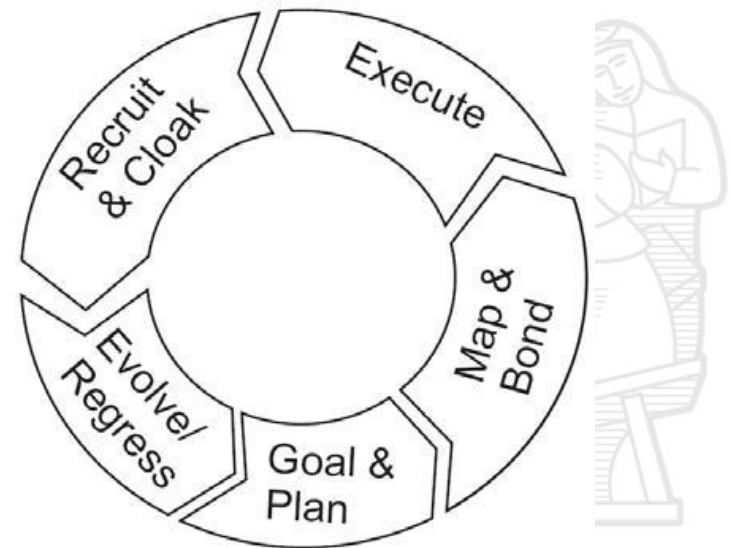


Social Engineering Attack Cycle

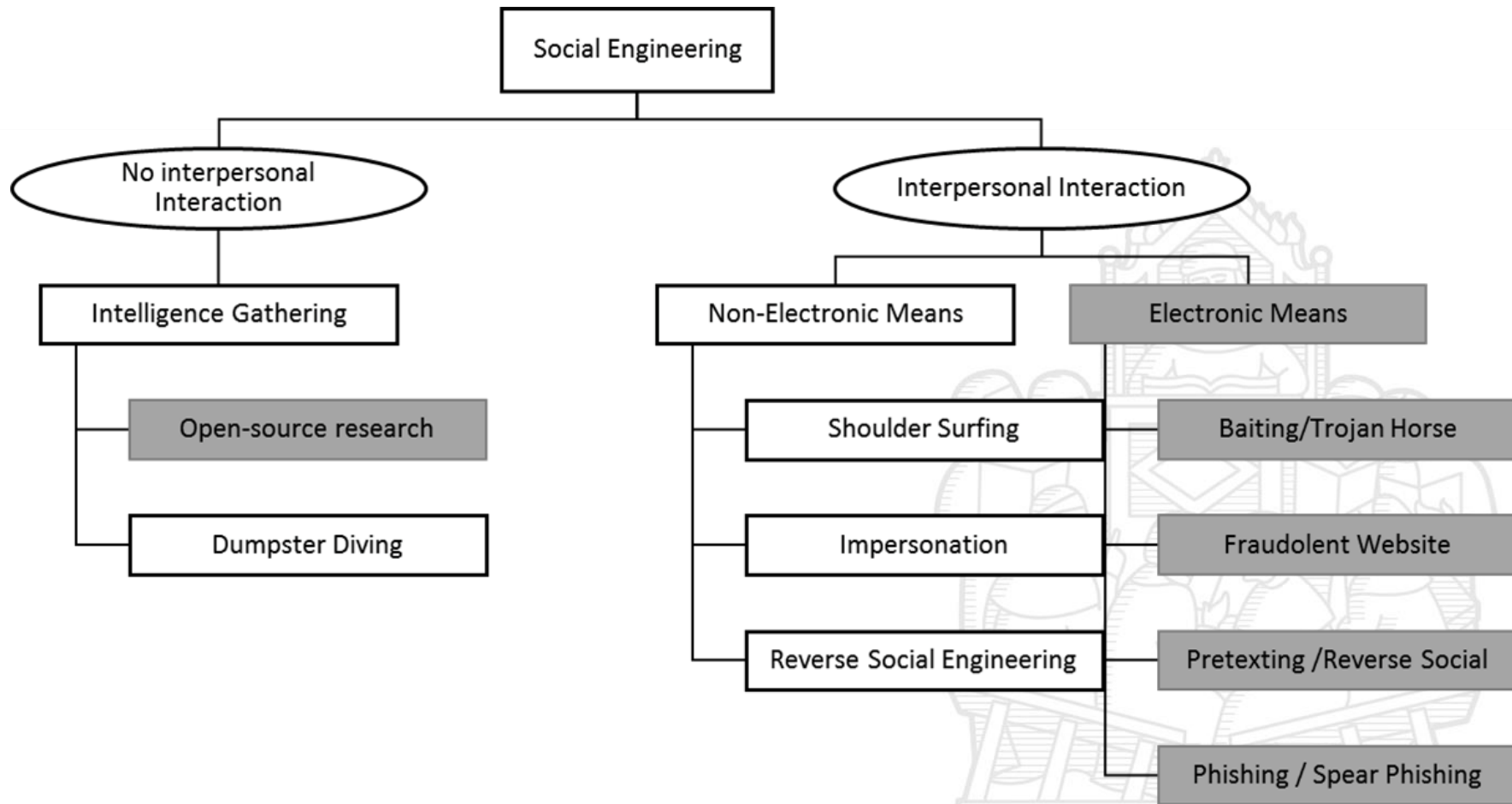


*Mitnick and Simon,
The art of deception:
Controlling the human
element of security.
John Wiley & Sons, 2001*

*Nohlberg and Kowalski
The cycle of deception – a model of social engineering
attacks, defenses and victims.
Proceedings of HAISA 2008.*



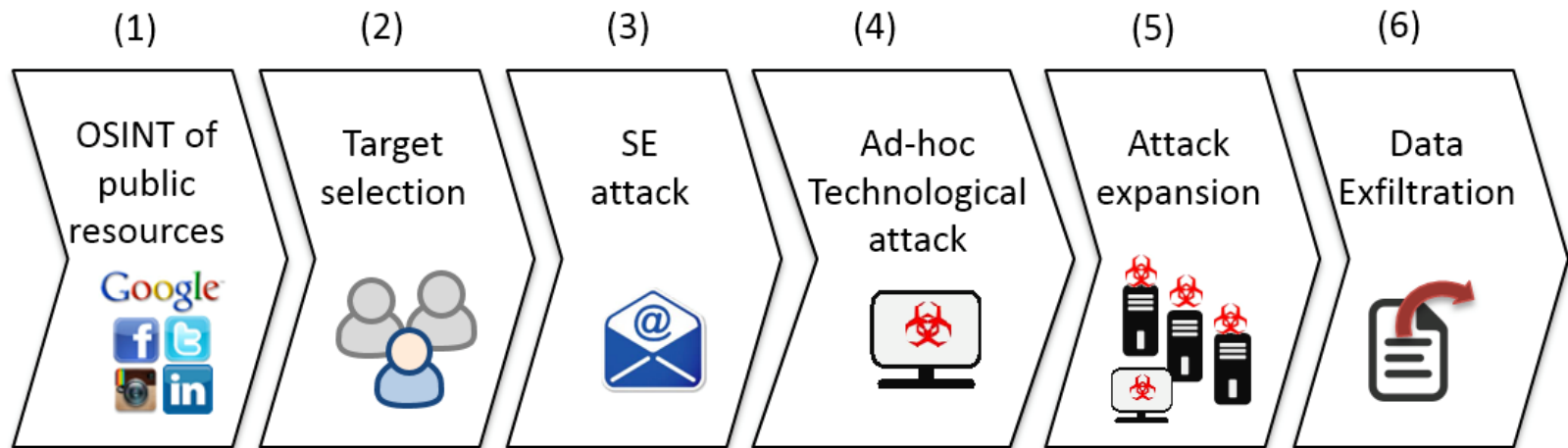
Social Engineering Taxonomy

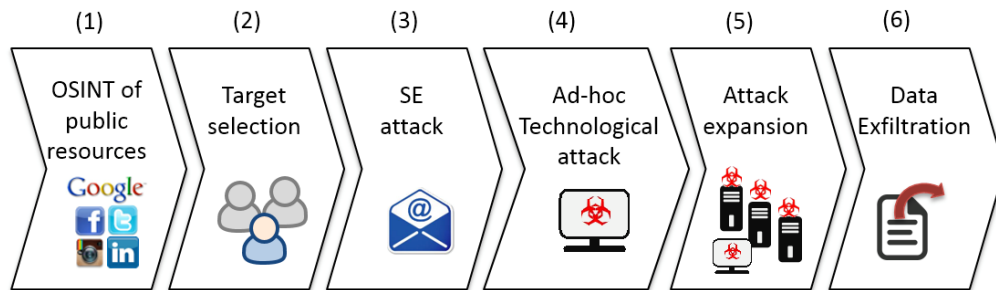


Greitzer et al., "Analysis of unintentional insider threats deriving from social engineering exploits," *IEEE S&P*, 2014



Advanced Persistent Threats





Social Engineering

OSINT



Intelligence Defined*

- Simply defined, intelligence is information that has been analyzed and refined so that it is useful to policymakers in making decisions—specifically, decisions about potential threats to national security.
 1. Intelligence is a product that consists of information that has been refined to meet the needs of policymakers.
 2. Intelligence is also a process through which that information is identified, collected, and analyzed.
 3. And intelligence refers to both the individual organizations that shape raw data into a finished intelligence product for the benefit of decision makers and the larger community of these organizations.

*<https://www.fbi.gov/about-us/intelligence/defined>



OSINT – Origins - 1

- Term Originates from Security Services
- The practice of using open source information to build intelligence is indeed not new:
 - **In Italy OVRA (Organizzazione per la Vigilanza e la Repressione dell'Antifascismo) reported to use OSINT since 1930**
“Gli anonimi informatori, secondo l'ex-prefetto di Brescia Arturo Bocchini (capo indiscusso sia dell'OVRA che della Polizia sino al 1940, anno della sua morte) dovevano fornire elementi per “...sondare con ogni mezzo e continuamente la pubblica opinione”, in modo che Mussolini potesse “...rendersi conto della temperatura del paese”.
 - **During the cold war, american and german secret services heavily analysed the russian press to gather information about their russian enemies**
- Nevertheless, open source information has been traditionally considered definitely less valuable than classified information



* “Anonymous Informer Report”, OVRA Region 1 – Milano, 1939 - <http://gnosis.aisi.gov.it/Gnosis/Rivista2.nsf/ServNavig/15>

OSINT – Origins - 2

- Paradigm change after 9/11 (shock to the system of old style intelligence)
 - Pre 9/11 intelligence services were closed and relied on HUMINT, SIGINT and classified information
 - Realisation that open source could have foreseen attacks -> **“Failure to connect the dots”** → reassessment in use of OS, & in sharing intel between agencies.
 - **Terrorists skilled use of internet was an eye opener.**
- The fast growth of the Internet and the appearance of Social Networks have further pushed the paradigm change
- **“The need to restructure the intelligence community grows out of six problems that have become apparent before and after 9/11:**
 - **Structural barriers to performing joint intelligence work**
 - **Lack of common standards and practice across the foreign-domestic divide**
 - **Divided management of national intelligence capabilities**
 - **Weak capacity to set priorities and to move resources**
 - **Too many jobs**
 - **Too complex and secret”**

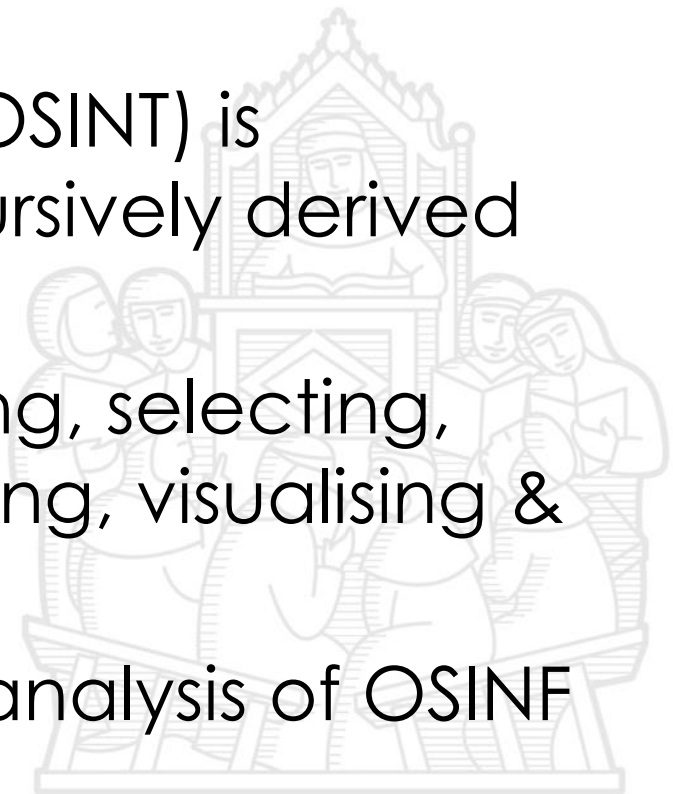


*The 9/11 Commission Report



OSINT - Definitions

- Open Source Information (OSINF) is data which is available publicly – **not necessarily free**
- Open Source Intelligence (OSINT) is proprietary intelligence recursively derived from OSINF
- OSINF Collection is monitoring, selecting, retrieving, tagging, cataloging, visualising & disseminating data
- OSINT is the result of expert analysis of OSINF



Slide Credit: C.H. Best, JRC - European Commission



OSINT Sources of Information - 1

- Media
 - Newspapers, magazines, radio, television, etc.
- The Internet
 - News, Social Networks, Blogs, Video sharing sites, Thematic sites. etc.
 - DeepWeb (not indexed by traditional search engines)
 - Dynamic Web Pages
 - Sites behind Log-in
 - Sytes with a ROBOT.txt file properly configured
 - Dark Nets/Web (TOR, I2P)
- Subscription Services
 - **LexisNexis** (<http://www.lexisnexis.com>) is a corporation providing computer-assisted legal research as well as business research and risk management services. During the 1970s, LexisNexis pioneered the electronic accessibility of legal and journalistic documents.
 - **Factiva** (<http://www.dowjones.com/products/product-factiva/>) is the world's leading source of premium news, data and insight, with access to thousands of premium news and information sources on more than 22 million public and private companies
 - **Jane's** (www.janes.com) Information Group is a British publishing company specialising in military, aerospace and transportation topics.
 - **BBC Monitoring** (<http://www.bbc.co.uk/monitoring>) includes news, information and comment gathered from the mass media around the world for service subscribers.

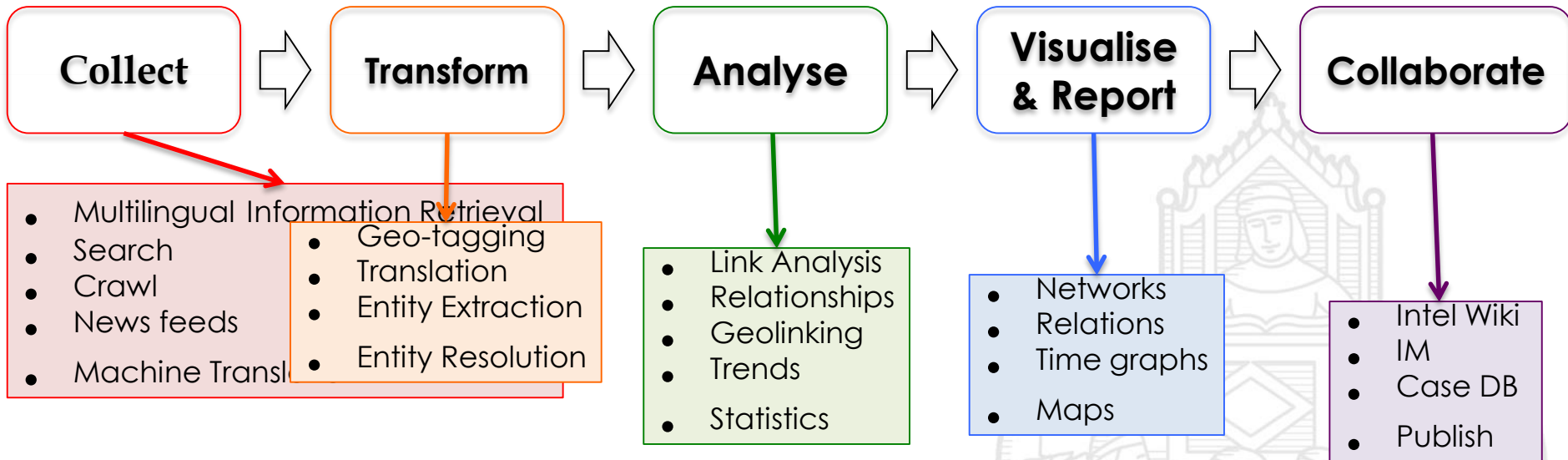


OSINT Sources of Information - 2

- Commercial Satellites
 - <http://www.euspaceimaging.com/applications/fields/security-defense-intelligence>
 - <https://www.digitalglobe.com/industries/defense-and-intelligence>
- Public Data
 - government reports, budgets, demographics, hearings, legislative debates, press conferences, speeches, marine and aeronautical safety warnings, environmental impact statements and contract awards.
- Professional and Academic
 - conferences, professional associations, academic papers, and subject matter experts.
- Open Data
 - <https://open-data.europa.eu/en/data>
 - <http://www.dati.gov.it>
 - <http://www.datiopen.it>
 - Geospatial Data Providers
 - An exhaustive list is available here https://en.wikipedia.org/wiki/List_of_GIS_data_sources



OSINT Processes



“Connecting the dots”

“Generating actionable intelligence”

Slide Credit: C.H. Best, JRC - European Commission

Information Collection – Issues (1)

- Information may be either textual or non-textual
- Textual Information
 - How can I search it?
 - Search Engines
 - General Search Engines: Google, Yahoo, Bing, Baidu (Chinese, Japanese), Sogou (Chinese), Soso.com (Chinese)
 - Thematic Search Engines:
 - » Computers and Devices - Shodan
 - » Maps – Bing, Google, Nokia, Yahoo! Maps
 - » People - Spokeo
 - » Source Code – Koders, Krugle, Google Code Search
 - Libraries
 - E.g. Lexis Nexis
 - E.g. IEEE Xplore, ACM Digital Library
 - How can I extract it?
 - API – constraints on the information which can be accessed; subject to change; specific for each platform
 - Scraping (ad-hoc source code for each platform; noise shall be removed; open solutions exist → need to merge results)



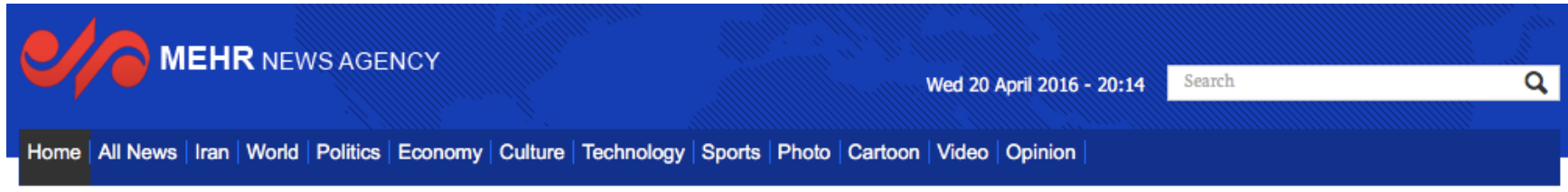
Information Collection – Issues (2)

- Non-Textual Information
 - Images
 - People (who)? Places? Texts? Objects?
 - Videos
 - People (who)? Places? Text? Objects? (as for images)
 - Video contains audio?
 - Transcription
 - Translation
 - Who are the speakers?
 - Audio Traces
 - Transcription
 - Translation
 - Other files
 - E.g. Executables files; files in proprietary formats
- Extraction of Non-Textual information is usually not easy to automate...



Language Issues (1)

Information Collection



MEHR NEWS AGENCY

Wed 20 April 2016 - 20:14

Search

Home | All News | Iran | World | Politics | Economy | Culture | Technology | Sports | Photo | Cartoon | Video | Opinion



English | Türkçe | کوردی | اردو

چهارشنبه ۱ اردیبهشت ۱۳۹۵ - ۲۰:۱۴

طلوع خورشید تهران: 06:25

اوقات شرعی

MEHR NEWS AGENCY

خانه | عناوین اخبار | فرهنگ | هنر | دین و | حوزه و | دانش و | سلامت | جامعه | اقتصاد | بازار | ورزش | سیاست | بین الملل | استانها | عکس | فیلم | مجله مهر | اخبار

- Culture
- Art
- Religion-Thought
- University
- Howzeh
- Hi-Tech
- Health-Environment
- Society
- Economy
- Markets
- Sport
- Politic
- International
- Provinces
- Photo
- Video
- Magazine
- Short news

Language Issues (2)

Information Collection

<http://www.mehrnews.com/en/>

Slide Credit: C.H. Best, JRC – European Commission

- News
- Culture
- Literature
- Religion
- University
- Social
- Economic
- Political
- International
- Sport
- Nuclear
- Photo

<http://www.mehrnews.com/fa/>

Language Issues (3)

Information Collection

The screenshot shows a news article on a Persian website. The main headline is "گزارش تصویری / بازدید اعضای کمیسیون انرژی مجلس از کارخانه فراوری اورانیوم (1)". Below the headline is a sub-headline: "اعضای کمیسیون انرژی مجلس شورای اسلامی عصر امروز از کارخانه فراوری اورانیوم اسفهان UCF بازدید کردند و از نزدیک با واحدهای مختلف این کارخانه آشنا شدند." The main image is a tall, red and white striped industrial chimney against a clear blue sky, with brown hills in the background. The website's navigation menu on the right includes categories like "فرهنگ و هنر", "فرهنگ و ادب", "دین و اندیشه", "خوزه و دانشگاه", "اجتماعی", "اقتصادی", "سیاسی", "بین الملل", "ورزشی", "انرژی هسته ای", and "عکس". There is also a section for "کتابخانه مهر" with a book cover titled "کتابخانه مهر".



Slide Credit: C.H. Best, JRC – European Commission

Entity Resolution

Information Transformation

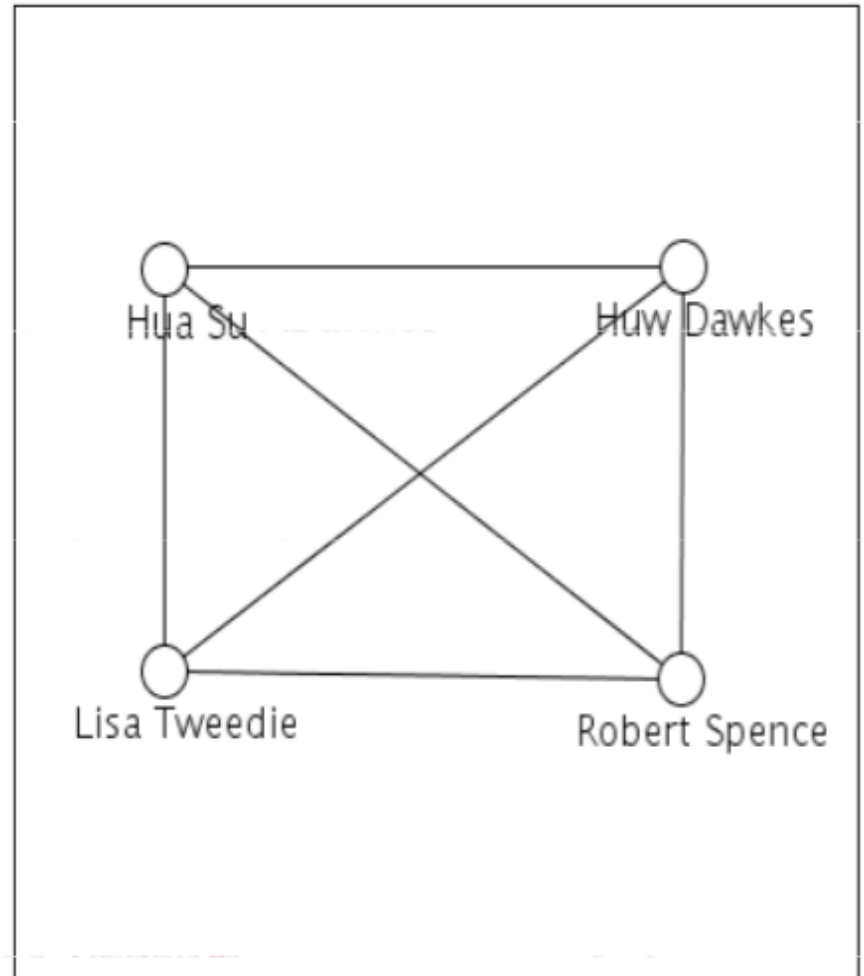
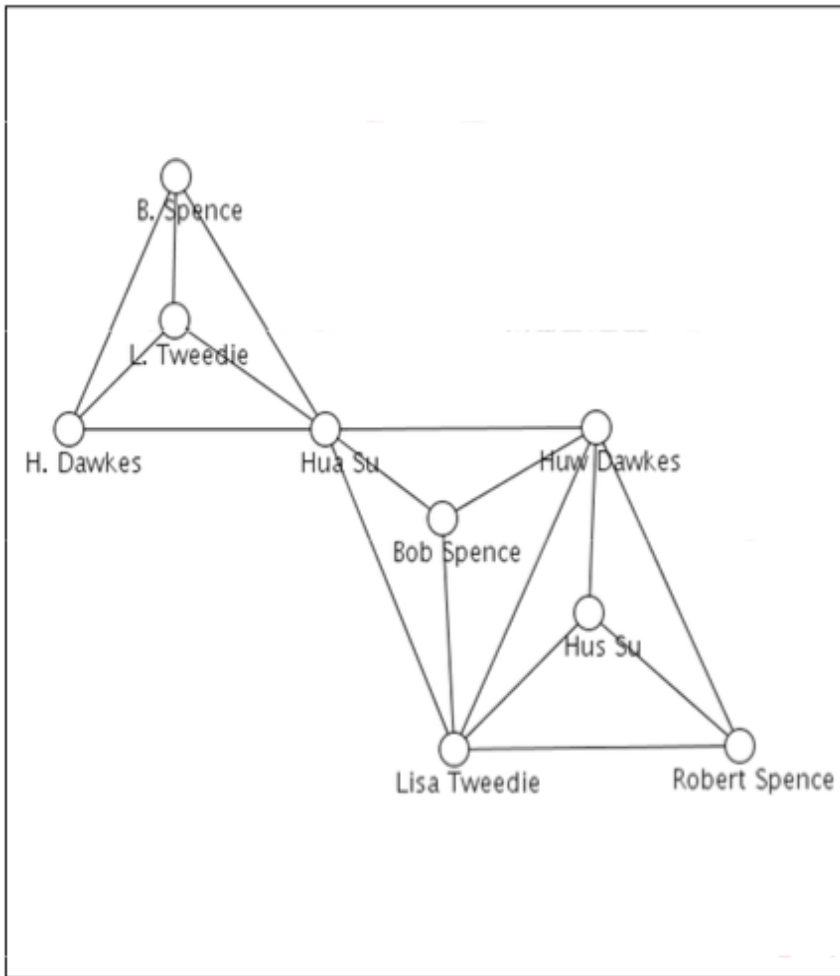
- *Problem of identifying and linking/grouping different manifestations of the same real world object.*
- Examples of manifestations and objects:
 - Different ways of addressing (names, email addresses, FaceBook accounts) the same person in text.
 - Web pages with differing descriptions of the same business.
 - Different photos of the same object.

Source: L. Getoor, A. Machanavajjhala - Entity Resolution Tutorial



Entity Resolution

Information Transformation



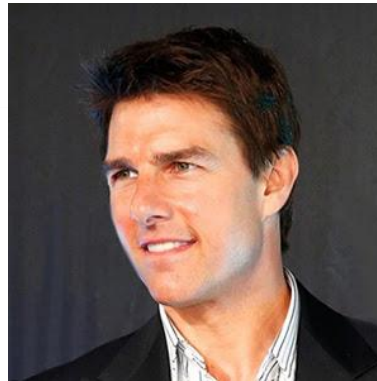
Slide Credit: L. Getoor, A. Machanavajhala - Entity Resolution Tutorial

Traditional Challenges in Entity Resolution

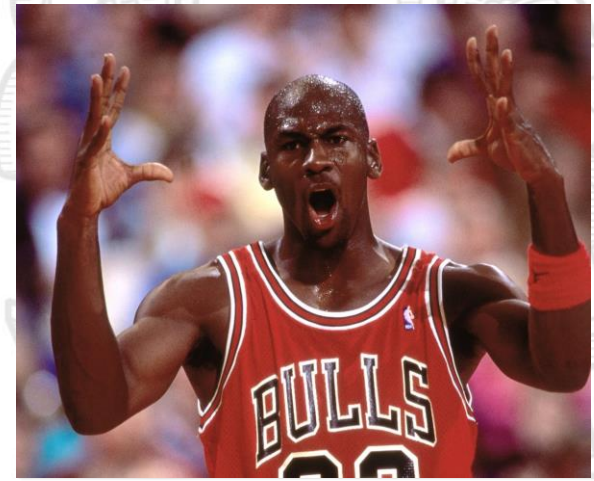
Information Transformation

- Name/Attribute Ambiguity

Tom Cruise



Michael Jordan



Slide Credit: L. Getoor, A. Machanavajhala - Entity Resolution Tutorial



Entity Resolution

Enzo Ferrari e i suoi piloti

«Un padrone delle ferriere». Era questo il modo singolare, ma per certi versi affettuoso, con cui Clay Regazzoni amava definire Enzo Ferrari. E che il Drake fosse un vero padrone, e fatto che nessuno dei piloti che hanno fatto tappa a Maranello puo mettere in discussione. Era lui, Ferrari, che stabiliva simpatie e antipatie, ordini e concessioni, stipendi e provvigioni. Su una cosa soltanto non concedeva margini neppure a se stesso: il valore di chi correva per lui. A patto, pero, che il nome del pilota non avesse il sopravvento, nella popolarita, sul nome delle macchine.

Arrivando a tempi piu recenti, il pilota che piu affascinò Enzo Ferrari fu Niki Lauda. Fortemente parsimonioso e terribilmente abile nella trattativa economica, in cui eccelleva peraltro anche il Drake, Niki racconta che Ferrari ad un certo punto gli affibbio un curioso soprannome: «Mi chiamava ebreo, probabilmente perche mi riteneva anche un buon commerciante della mia professionalità.

A fine luglio 1977, quando l'ex campione del mondo aveva gia firmato per la Brabham Alfa Romeo, Ferrari rivelo un'ammissione di Lauda. «Fino a quando lei sara vivo io guidero per lei», questo disse Niki al Drake, nel frattempo da dieci anni ingegnere honoris causa. Ma alla fine di agosto, Lauda si recò a Maranello e disse a Ferrari che non avrebbe guidato piu le sue macchine. «Se Lauda fosse restato con noi avrebbe almeno eguagliato il record di Fangio di cinque titoli mondiali vinti», confesso Ferrari tempo dopo. Non perdonò mai Lauda e non lo rivolse in Ferrari quando l'austriaco si offerse. Il perdono arrivò anni dopo, poco prima della morte del Drake.

L'ultimo pilota, nella classifica degli amori tecnici di Enzo Ferrari, fu Gilles Villeneuve. Il Grande Vecchio era un umorale, quando Lauda lo lasciò fece una scommessa con se stesso: prender un signor nessuno e portarlo al titolo mondiale.

Entity Resolution

Enzo Ferrari e i suoi piloti

«**Un padrone delle ferriere**». Era questo il modo singolare, ma per certi versi affettuoso, con cui Clay Regazzoni amava definire **Enzo Ferrari**. E che il **Drake** fosse un vero padrone, e fatto che nessuno dei piloti che hanno fatto tappa a Maranello puo mettere in discussione. Era lui, **Ferrari**, che stabiliva simpatie e antipatie, ordini e concessioni, stipendi e provvigioni. Su una cosa soltanto non concedeva margini neppure a se stesso: il valore di chi correva per lui. A patto, pero, che il nome del pilota non avesse il sopravvento, nella popolarita, sul nome delle macchine.

Arrivando a tempi piu recenti, il pilota che piu affascinò **Enzo Ferrari** fu Niki Lauda. Fortemente parsimonioso e terribilmente abile nella trattativa economica, in cui eccelleva peraltro anche il **Drake**, Niki racconta che Ferrari ad un certo punto gli affibbio un curioso soprannome: «Mi chiamava ebreo, probabilmente perche mi riteneva anche un buon commerciante della mia professionalità».

A fine luglio 1977, quando l'ex campione del mondo aveva gia firmato per la Brabham Alfa Romeo, Ferrari rivelo un'ammissione di Lauda. «Fino a quando lei sara vivo io guidero per lei», questo disse Niki al Drake, nel frattempo da dieci anni **ingegnere** honoris causa. Ma alla fine di agosto, Lauda si recò a Maranello e disse a Ferrari che non avrebbe guidato piu le sue macchine. «Se Lauda fosse restato con noi avrebbe almeno eguagliato il record di Fangio di cinque titoli mondiali vinti», confesso Ferrari tempo dopo. Non perdonò mai Lauda e non lo rivolse in Ferrari quando l'austriaco si offerse. Il perdono arrivò anni dopo, poco prima della morte del Drake.

L'ultimo pilota, nella classifica degli amori tecnici di Enzo Ferrari, fu Gilles Villeneuve. Il **Grande Vecchio** era un umorale, quando Lauda lo lasciò fece una scommessa con se stesso: prender un signor nessuno e portarlo al titolo mondiale.

Entity Resolution

Enzo Ferrari e i suoi piloti

«Un padrone delle ferriere». Era questo il modo singolare, ma per certi versi affettuoso, con cui Clay Regazzoni amava definire Enzo Ferrari. E che il Drake fosse un vero padrone, e fatto che nessuno dei piloti che hanno fatto tappa a Maranello puo mettere in discussione. Era lui, Ferrari, che stabiliva simpatie e antipatie, ordini e concessioni, stipendi e provvigioni. Su una cosa soltanto non concedeva margini neppure a se stesso: il valore di chi correva per lui. A patto, pero, che il nome del pilota non avesse il sopravvento, nella popolarita, sul nome delle macchine.

Arrivando a tempi piu recenti, il pilota che piu affascinò Enzo Ferrari fu **Niki Lauda**. Fortemente parsimonioso e terribilmente abile nella trattativa economica, in cui eccelleva peraltro anche il Drake, **Niki** racconta che Ferrari ad un certo punto gli affibbio un curioso soprannome: «Mi chiamava ebreo, probabilmente perche mi riteneva anche un buon commerciante della mia professionalità.

A fine luglio 1977, quando **l'ex campione del mondo** aveva gia firmato per la Brabham Alfa Romeo, Ferrari rivelo un'ammissione di **Lauda**. «Fino a quando lei sara vivo io guidero per lei», questo disse **Niki** al Drake, nel frattempo da dieci anni ingegnere honoris causa. Ma alla fine di agosto, Lauda si recò a Maranello e disse a Ferrari che non avrebbe guidato piu le sue macchine. «Se Lauda fosse restato con noi avrebbe almeno eguagliato il record di Fangio di cinque titoli mondiali vinti», confesso Ferrari tempo dopo. Non perdonò mai Lauda e non lo rivolse in Ferrari quando l'austriaco si offerse. Il perdono arrivò anni dopo, poco prima della morte del Drake.

L'ultimo pilota, nella classifica degli amori tecnici di Enzo Ferrari, fu Gilles Villeneuve. Il Grande Vecchio era un umorale, quando Lauda lo lasciò fece una scommessa con se stesso: prender un signor nessuno e portarlo al titolo mondiale.

Entity Resolution – Other Challenges

- Errors due to data entry
- Changing Attributes
- Abbreviations/Data Truncation



V. Rossi



Valentino Rossi

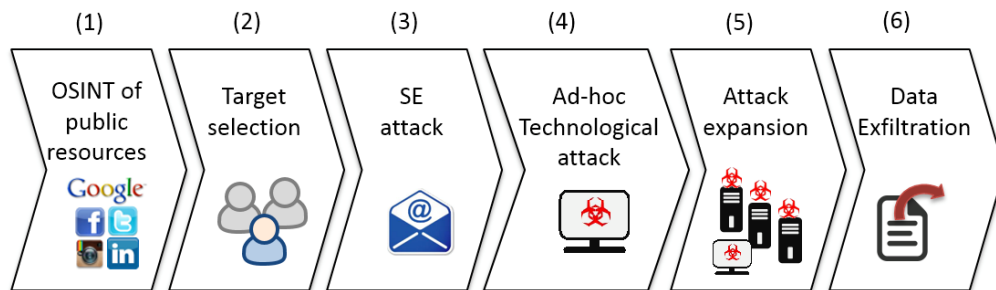


Vasco Rossi



Valeria Rossi





Social Engineering

SE ATTACK



Psychological Foundations

The *Theory of Gullibility*

- The susceptibility to **persuasion** as an extension of credulity: the victim has a willingness to believe someone or something even in the total absence of reasonable proof.

The *Theory of Optimistic Bias*

- People believe that positive events are more likely to occur to them than to other people
The inverse is also true: people believe that negative events are more likely to occur to other people than to themselves.

As a consequence, people think that

- a. they will not be selected as a social engineering target
- b. and are more likely to resist than others



Social Influence

- Social Influence
 - Compliance
 - Persuasion
- The six principles of influence
 - reciprocity
 - conformity(/social validation
 - liking
 - scarcity
 - **consistency/commitment**
 - **authority**

Empirically
examined in online
contexts

E. Guadagno and R. Cialdini, "Online Persuasion and Compliance: Social Influence on the Internet and beyond"



On-line interactions

The following properties characterize Computer Mediated Communications compared to Face-to-Face interactions and provide solid ground for effective social influence techniques

- Anonymity
- Physical appearance
- Physical distance
- Time and Place
- Lack of social cues



Manipulation Techniques

- Pretexting
- Impersonation
- Baiting
- Pressure and solution
- Leveraging authority
- Reverse social engineering
- Chain of authentication
- Gaining credibility
- From innocuous to sensitive
- Priming and loading
- Social proof
- Framing information
- Emotional states
- Selective attention
- Personality types and models
- *Body language*



Pretexting and Impersonation

Pretexting

- The attacker creates a **scenario** to try and convince the victim to give up valuable information
 - Plausible situation
 - Character



Symantec Blocked 100 Million Fake Technical Support Scams in 2015

Cyber scammers now make you call them to hand over your cash

Impersonation

- Need not be of a real individual, instead it will likely be a character specifically designed for the pretext

ISTR 21 (2016) Symantec



Baiting

- e-mails

Hi James,

I don't have time to follow up this lead so do you want it? The client wants to know more about our new services, sounded like a great opportunity.

<http://vulnerableinc.com/contact>"

- Dropped USB drives or CDs / DVDs with enticing labels



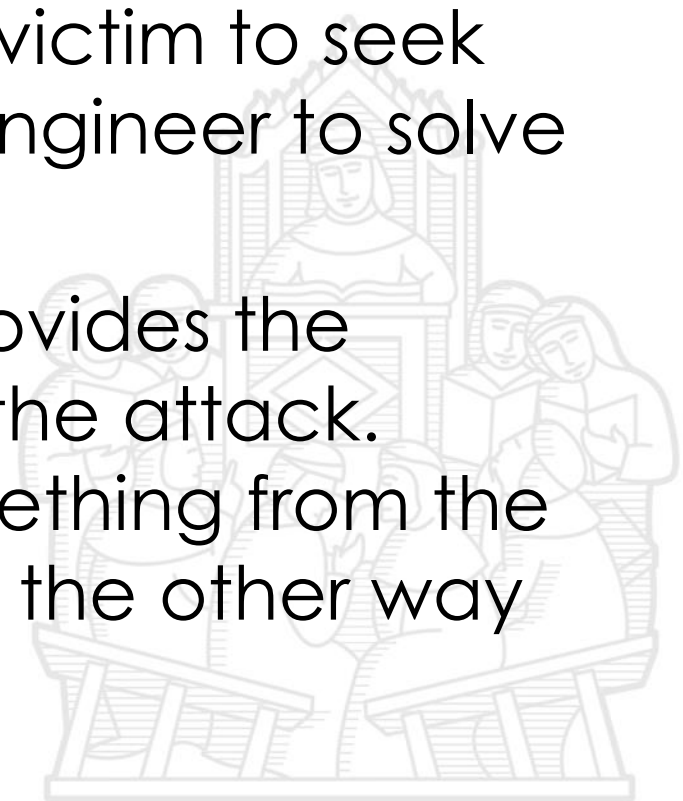
Pressure and solution

- Pressure...
 - Apply pressure to the victim in the form of a negative emotional state such as *fear, anger, indignation, or shame*
 - e.g., by impersonating a supervisor, a chief executive, thus **leveraging authority**
- ...and solution
 - present the victim with a solution that would mitigate or remove the emotion.
 - The solution would of course aid the attacker in achieving their own objective.
- This is similar to baiting as the victim is blinded by the emotion much like they are blinded by the bait



Reverse Social Engineering

- This is a classic technique used to ensure the attacker has solid credibility.
- The basic idea is to get the victim to seek assistance from the social engineer to solve a problem.
- The social engineer then provides the assistance, which also aids the attack. The victim is requesting something from the social engineer, rather than the other way around.



Chain of Authentication

- The concept is to manufacture or orchestrate a situation where the victim “assumes” the social engineer has already been validated.

To gain access to a hospital's server room, a social engineer may approach the reception posing as an air-conditioning repair engineer. The social engineer explains to one of the receptionists that *I'm here to perform a maintenance check of the air conditioning units in the server room, the IT department sent me here as apparently you have keys*

The receptionist replies

Sorry we don't have them, the only person with keys is the porter, his office is just down the hall

The social engineers leave and then return a few minutes later saying *Sorry but no one is answering at the door, I'll try again a little later*

They could continue pretending to try the door and telling reception that they're not answering, until the receptionist agrees to investigate herself. When the receptionist tries the door, the porter answers and the receptionist explains

Ah you are in after all, this gentleman is here to do some stuff with the air conditioning in the server room, can you take him up there

The porter will then very likely assume that the receptionist has already validated the engineer, creating the chain of authentication



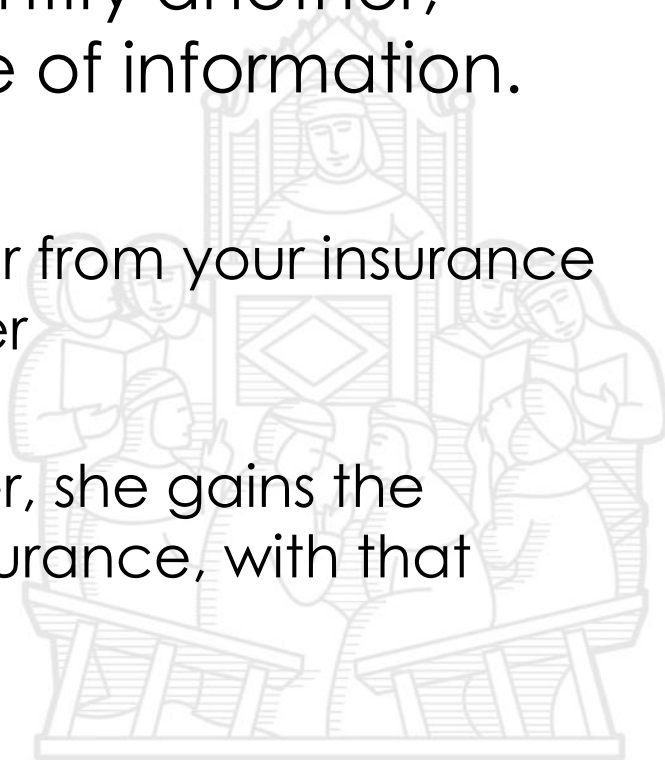
Gaining credibility

- While an employee might be suspicious by receiving a call asking
 - *“Hello, could you tell me what version of Web browser you’re using?”*
- a more credible call would be
 - *“Hello, I’m calling from the IT department, we’re performing some remote patching, can you tell if your Web browser has been updated to version 7.0?”*
- better
 - *“Hi James, it’s Simon from the Service Desk, have you got 2 seconds or are you guys still busy with the xyz project? ...Ah well listen, we’re performing some remote patching, can you tell me if your Web browser has been updated to version 7.0? If not I’ll need to send Dave down to sort it out there.”*



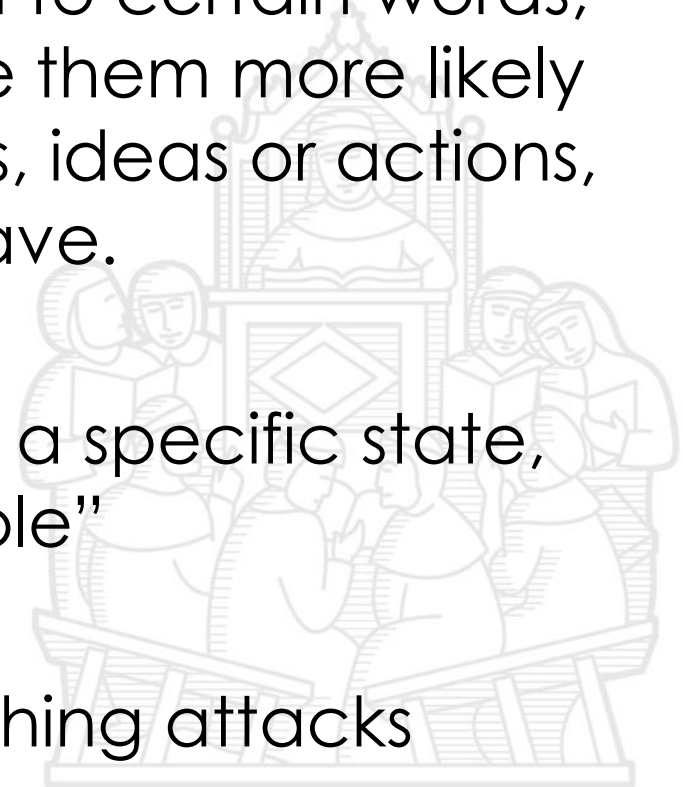
From innocuous to sensitive

- To a social engineer any piece of “innocuous” information is a piece of a jigsaw puzzle, one that could be used to identify another, possibly more significant piece of information.
- Example
 - You throw in the garbage a letter from your insurance company with an additional offer
 - No sensitive data is present, but...
 - if a *social engineer* finds this letter, she gains the knowledge that you have an insurance, with that company...
 - impersonation, pretexting, etc.



Priming and loading

- *Priming* is a fascinating psychological phenomenon.
An individual can be exposed to certain words, ideas or actions that will make them more likely to “choose” associated words, ideas or actions, even without knowing they have.
- A victim could be *primed* into a specific state, such as being more “agreeable”
- Phishing can also support phishing attacks



Social proof

- People follows the crowd. It is human nature to seek the comfort that comes with fitting in with everyone else
- Compare the following messages

All,

We're trying to push our social media presence. Unfortunately, the vast majority of staff haven't liked our corporate page. Please could you follow the link to remedy this.

<http://www.somesocialmediawebsite.com/>

IT Support

All,

Thank you for the great positive response to our social media push. The vast majority of your department have responded with a 'like' and we're really pleased. Join the rest of us if you haven't already using the following link.

<http://www.somesocialmediawebsite.com/>

IT Support

- Which of the two will be the most successful?



Emotional states

- The social engineer tries to invoke a certain emotional state in the victim
 - pity
 - kindness
 - fear
 - trust
- This is not an easy task, as emotions are unpredictable



Selective attention

- Sometimes referred to as the “cocktail party effect”
 - We are able to almost filter out the unwanted sounds, and single out and understand a single voice among the many others
- All that social engineer needs to do is ensure the victim’s attention is focused on something complicated enough to prevent any other information from being processed.
- The “anything else” would be the element that achieves the objective.



Personality types and models

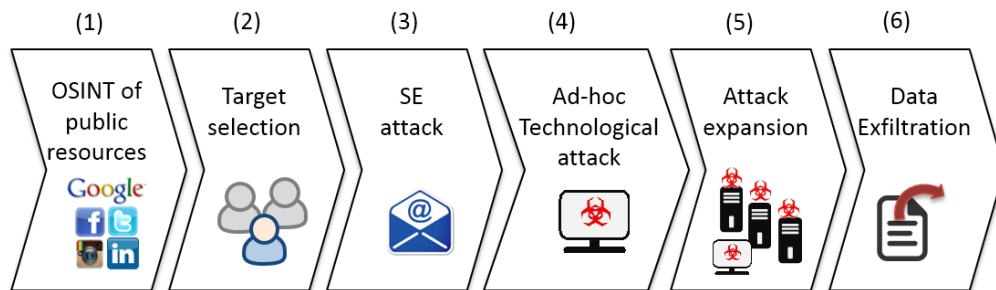
- The idea of placing individuals into specific groups and then using those groups to predict their behavior.
 - If you can accurately and consistently predict your own actions based on your own personality type, then you can use that knowledge to maximize your strengths and reduce your weaknesses.
- From a social engineering perspective, you could adjust your approach based on the target's personality type to maximize the chances of affecting their decisions.
- Unfortunately, as with many areas concerning human nature, personality typing is far from an exact science.



Framing information

- *framing* is about presenting information in such a way as to steer the viewer's subjective perception in a certain direction
 - Sales advertisement: “Up to 50% off”
- Compare the following messages
 - *Hay Susan, I have already spoken to David and Simon in your department. They were really helpful and answered most of my questions, send my thanks. However, there were a couple of questions they said you'd be the best person to answer, have you got a couple of minutes to help me out?*
 - *Hay Susan, [...] However, they couldn't answer a couple of questions, can you help?*
- Which of the two will be most effective in getting the help?





Social Engineering

AD-HOC TECHNOLOGICAL ATTACK



Attack Vectors

Technical

- Spam e-mails
- Phishing
- Spear Phishing
- Context Aware Phishing (Whaling)
- Vishing (voice phishing)
- Popup window
- Interesting software

Non Technical

- Pretexting/Impersonation
- Dumpster Diving
- Spying and Eavesdropping
- Acting as a technical expert
- Support Staff



Spear Phishing

Добрый День!
Высылаю Вам наши реквизиты
Сумма депозита 32 000 000 руб 00 коп, сроком на 366 дней, , % в конце года, вклад срочный
С Уважением, Сергей Кузнецов;
+ 7(953) 3413178
f205f@mail.ru

Translated:

Good Day!
I send you our contact details
The amount of deposit 32 million rubles and 00 kopecks, for a period of 366 days,% year---end contribution term
Sincerely, Sergey Kuznetsov;
+ 7 (953) 3413178
f205f @ mail.ru



Malware 2.0

- SE 2.0 is nowadays the most efficient and economically relevant instrument used in cybercrime. Malware has been particularly affected and it has become extremely different compared to the malware that was identified in recent past.

The main Malware 2.0 characteristics are the followings :

- Lack of a single control centre and ability to adapt the infection to the attacked machine
- Extensive use of methods to fight AV systems
- Victim machines take the role of servants and attacks get more discrete
- Intense production on syntactic – not logical – variations
- Short and targeted attacks from many directions
- Intense and advanced use of SE techniques¹⁰
- Modularity and complexity of infections
- Malwares and SE follow the markets laws governed by supply and demand (MaaS)



DOGANA

Advanced Social Engineering and Vulnerability Assessment Framework

- **Goal:** To develop a framework to mitigate the (cyber) risk arising from Social Engineering



ADVANCED SOCIAL ENGINEERING AND
VULNERABILITY ASSESSMENT FRAMEWORK

**Project Funded by the European Commission under the
Framework Programme Horizon 2020 (2014-2020) – Grant
Agreement N° 653618**

DOGANA Partners

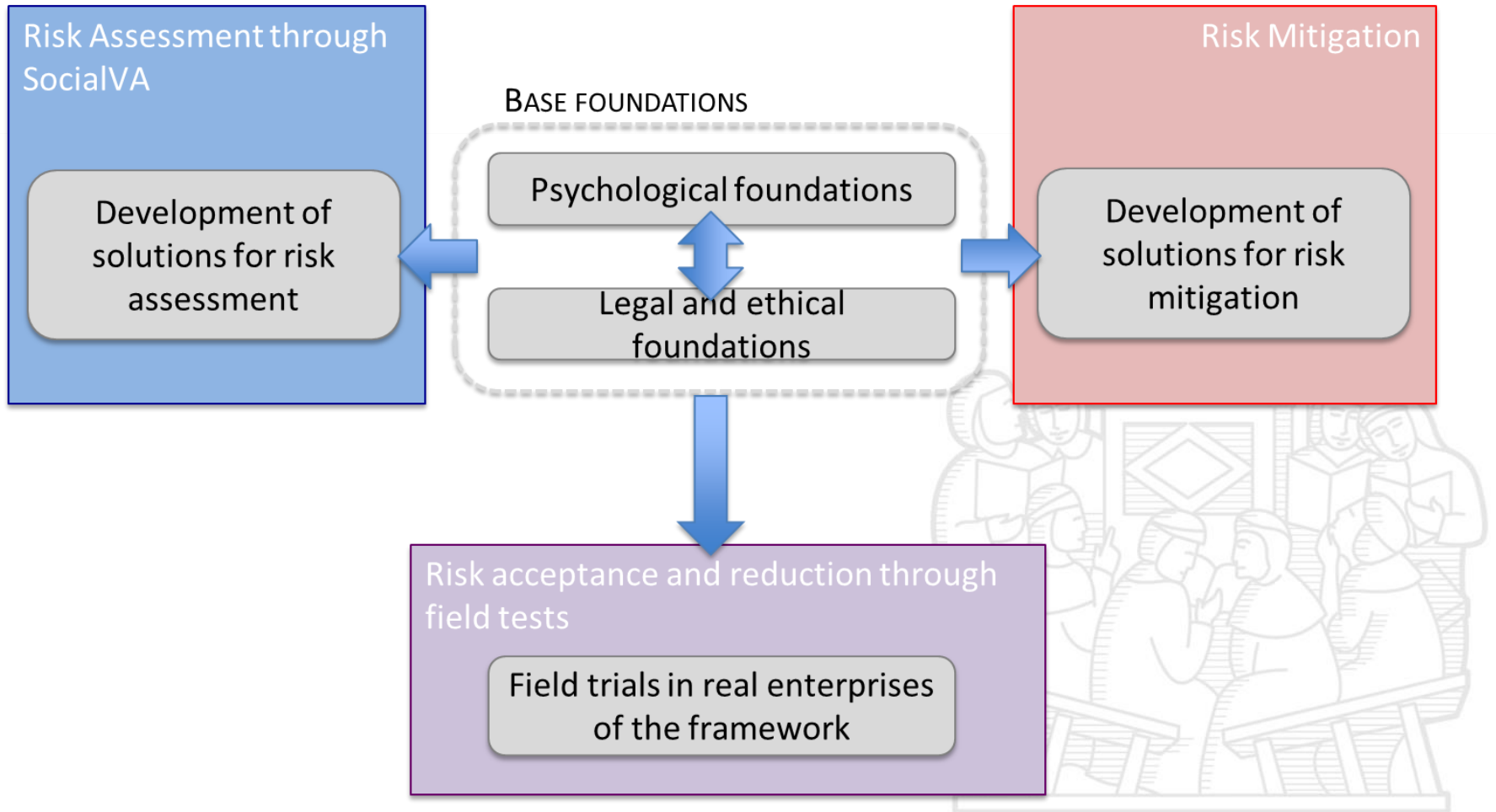


Scuola universitaria professionale della Svizzera italiana



Sant'Anna
Scuola Universitaria Superiore Pisa

The DOGANA Approach



DAVIDE.ARIU@DIEE.UNICA.IT

GRAZIE PER L'ATTENZIONE

