Public and Private Sector Cooperation to Enhance Fraud Investigations

Presentation for:

BANCHE E SICUREZZA 2015

Rome, 4 June 2015

William Boley

VP Security Operations and Investigations

CONCEPTIVITY

Introduction

Public and Private Sector Cooperation to Enhance Fraud Investigations

Year 2020: Seven billion people on the earth and 50 billion devices connected to the Internet.

The IoT is becoming the **Internet of Everything**: We have connected our entire lives to the Internet. That is why, because all of life is there, that is where bad people come who want to hurt children, who want to steal money, who want to take identities, who want to steal corporate secrets, who want to damage critical infrastructure in Europe and elsewhere. It's the way they come at us because that's where life is.

Main Message: Our governments do not have all the answers, nor all the talent, nor enough resources to fight Fraud within the Banking Sector and they need your help. Cybersecurity must be a partnership between government and the private sector and of course Academia. We need each other, and we must work together.

Partnerships through Research

COURAGE

CYBERCRIME and
CYBERTERRORISM
EUROPEAN RESEARCH
AGENDA

www.courage-project.eu

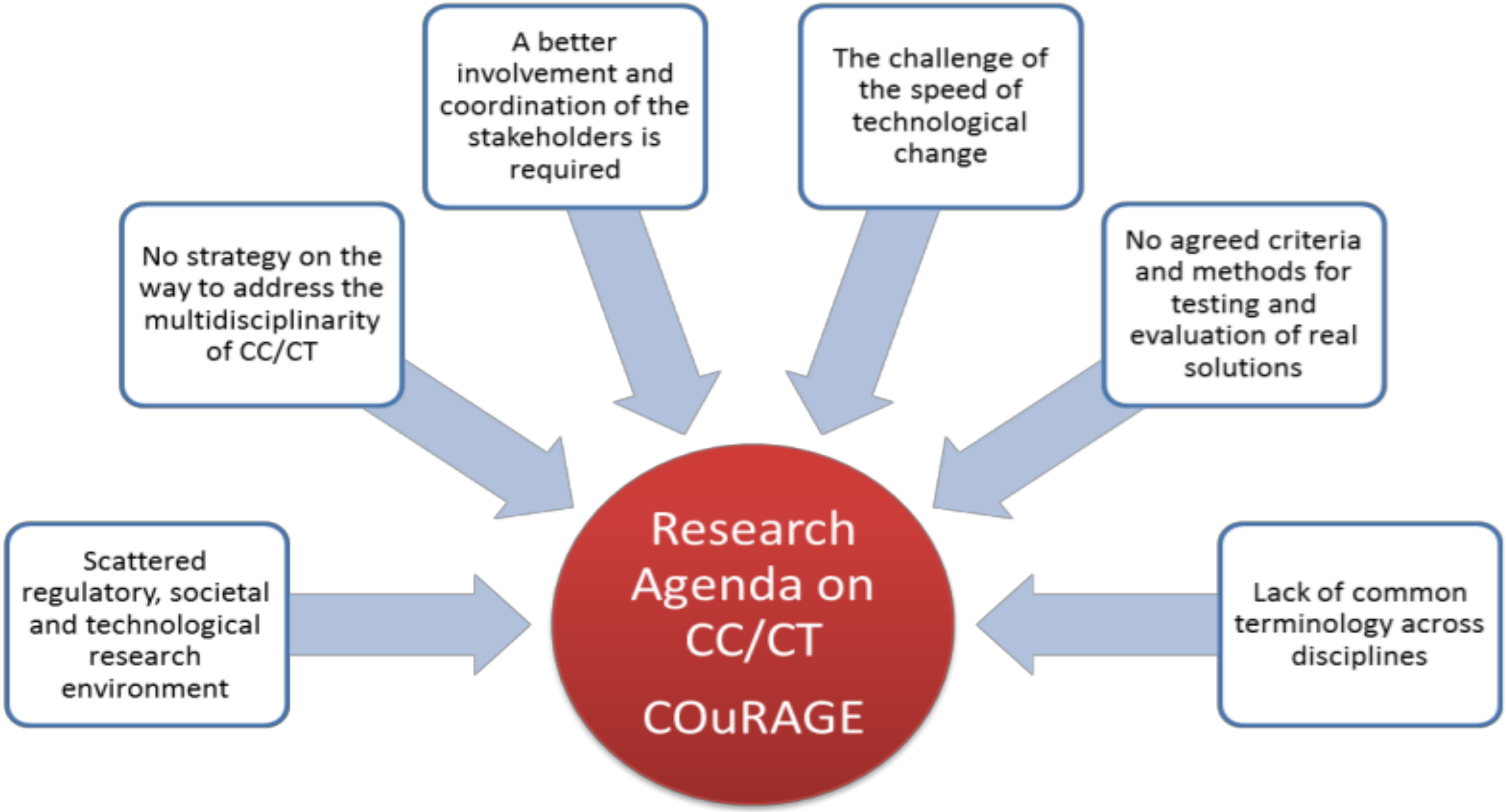
CAPITAL

Cybersecurity research Agenda
for PrIvacy and Technology chALlenges

www.capital-agenda.eu

CONCEPTIVITY

WHY A RESEARCH AGENDA FOR CC/CT?
WHY COuRAGE?



A better involvement and coordination of the stakeholders is required

The challenge of the speed of technological change

No strategy on the way to address the multidisciplinarity of CC/CT

No agreed criteria and methods for testing and evaluation of real solutions

Scattered regulatory, societal and technological research environment

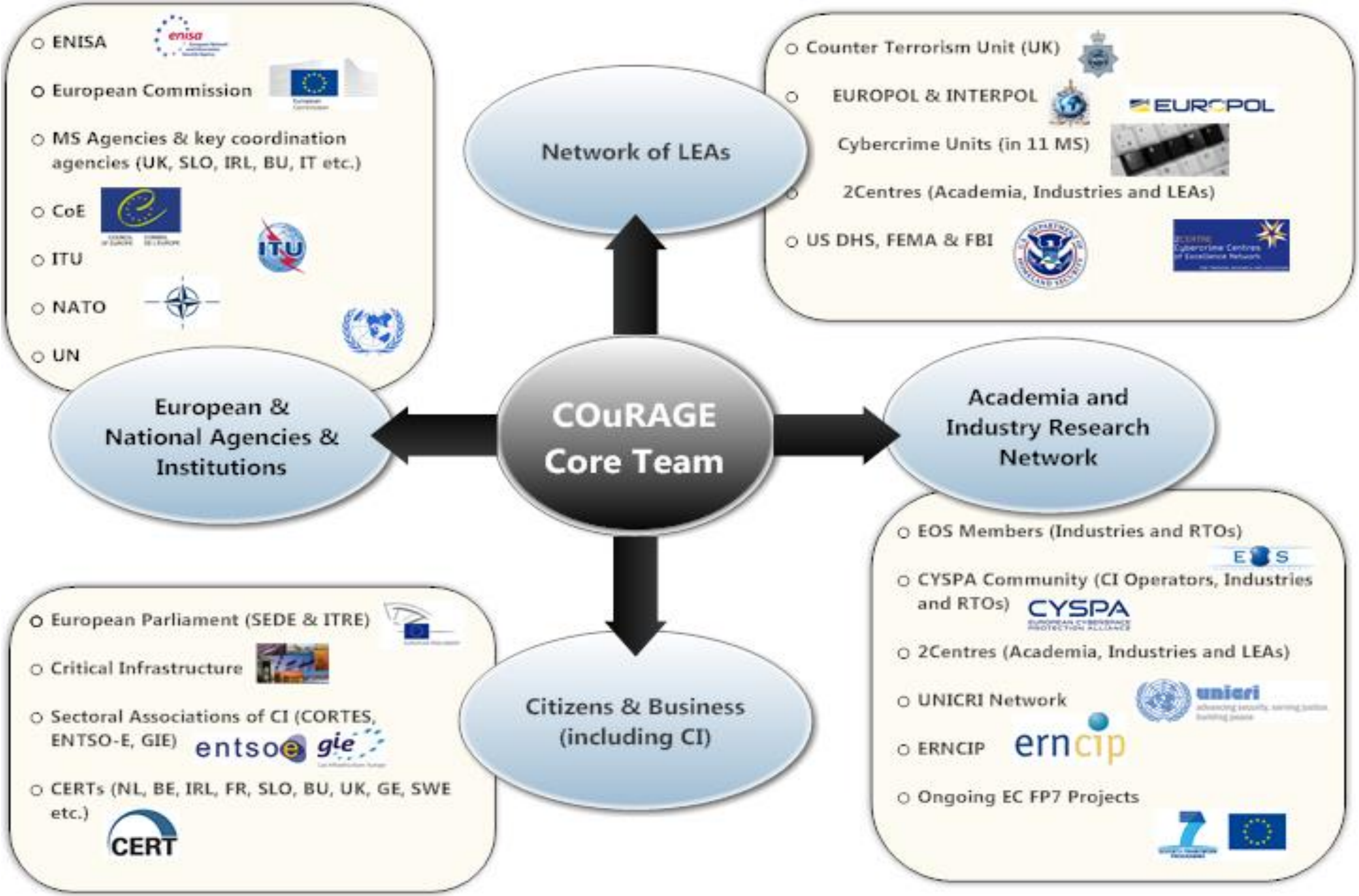
Research Agenda on CC/CT

COuRAGE

Lack of common terminology across disciplines

The purpose of COURAGE is to significantly improve the security of citizens and critical infrastructures and **Support Crime Investigators.**

CONCEPTIVITY



COuRAGE Core Team

Network of LEAs

- Counter Terrorism Unit (UK)
- EUROPOL & INTERPOL
- Cybercrime Units (in 11 MS)
- 2Centres (Academia, Industries and LEAs)
- US DHS, FEMA & FBI

European & National Agencies & Institutions

- ENISA
- European Commission
- MS Agencies & key coordination agencies (UK, SLO, IRL, BU, IT etc.)
- CoE
- ITU
- NATO
- UN

Academia and Industry Research Network

- EOS Members (Industries and RTOs)
- CYSPA Community (CI Operators, Industries and RTOs)
- 2Centres (Academia, Industries and LEAs)
- UNICRI Network
- ERNCIP
- Ongoing EC FP7 Projects

Citizens & Business (including CI)

- European Parliament (SEDE & ITRE)
- Critical Infrastructure
- Sectoral Associations of CI (CORTES, ENTSO-E, GIE)
- CERTs (NL, BE, IRL, FR, SLO, BU, UK, GE, SWE etc.)

Cyber Crime or just “E-nabled”

- Are Cyber Criminals Unique?
- “I rob banks because that is where the money is”
- True Cyber Crimes vs e-enabled
- moving at the speed of light in nothing but my underwear
- The criminals and terrorists have shrunk the world
- Cybercrime is a fundamental shift in the way modern crime works. Modern crime has already reached a point where nearly every crime today involves a cyber component

Mitigation

- Share Information: Many Hurdles

- IoT will need a Bring Your Own Identity Approach (Biometrics/IP addresses/ **analytics** on the backend/ handset codes…

- Containment:
  - Prevent the intruder from entering the system
  - More importantly, prevent the intruder’s ability to leave the system with confidential data
  - Devalue the data so it is meaningless to an intruder who gains access to it. If he cant sell it he won’t steal it…

CAPITAL selects key societal and technological domains whose future is at risk due to potential cyber security and privacy threats

CAPITAL identifies how ICT could address these threats and can contribute to decreasing their impact or completely removing them

CAPITAL works closely with the European Commission Public-Private Platform for Network and Information Security (NIS Platform) WG 3 on Secure ICT Research & Innovation

The Black Market study:

- **Source code for malware**, customizable according to user needs. Security experts have detected numerous variants of Zeus and Carberp malware released in the wild, and designed for specific financial institutions.

- **Managed SMS flooding services** and **DIY DoS tools** to hit the phone of a bank payment service's customers, in an attempt to prevent customers to be reachable when a suspicious real-time withdrawal or transaction takes place.

- **Millions of harvested emails, spam-ready SMTP servers, and DIY spamming tools** are available to target bank customers.

- **Bank information stealing applications** for Android devices (e.g. Android.Bankun.)

- **DIY RDP-based botnet generating tools** with features for collecting information about a payment or banking system.

- **Trained fraud assistants**, speaking multiple languages, to socially engineer a user or their bank or payment processing service.

Vulnerabilities: The Human Factor

- Poor Training/Awareness
- Insider Threat: most incidents were detected through tips and audits while personally identifiable information (PII) is a prominent target of those committing fraud
- Compliance tools = Yesterdays Strategies

Vulnerabilities: The Technology Factor

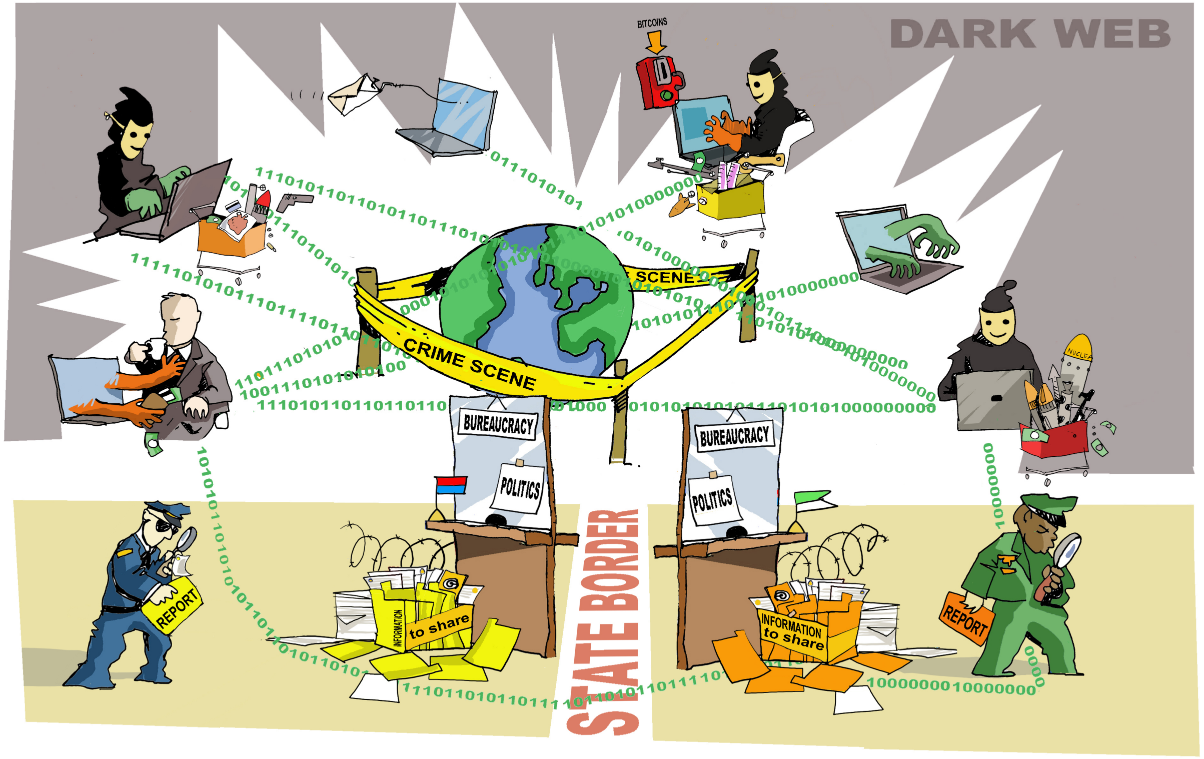
- Third Party reliance on service vendors: This is the nexus of Cyber Security and Supply Chain Security

- Hardware and Software not made in Europe

- Certification and testing issues

- The IoT/IoE is altering the landscape of payment methods and provides a wide and growing variety of entry points for those looking to steal, divert, or disrupt payments

CONCLUSION



Concept: Vladimir Radunović Illustration: Vladimir Veljašević

- Support Research

- Collaborate / Coordinate / Cooperate as it takes a network to defeat a network

CONCEPTIVITY

360 SECURITY

CONCEPTIVITY was created in Geneva in 2010 - we are a leading innovator in risk management for Supply Chain Security and Cyber Security.

CONCEPTIVITY has a 360° approach that is designed to protect your staff, your assets, your brand image and your integrity.

CONCEPTIVITY is a validated SME for European Commission contracts and is registered with EU Transparency. We are a member of the European Organisation for Security with the CEO as the Vice Chairman.

www.conceptivity.ch