CyberROAD
FP7 SEC-2013.2.5-1
Developing a Cyber Crime and Cyber Terrorism Research Agenda

Giorgio Giacinto
University of Cagliari, Italy
The CyberROAD project proposal was admitted to the negotiation phase.

The negotiation phase has been closed, and the Grant Agreement between the Consortium and the EC should be signed soon.

At present the project has not yet officially started, and the grant has not yet been officially assigned to the project.
It has 18 years experience on the development of next generation pattern recognition systems for:

- biometric authentication
- computer security
- video surveillance
- multimedia document categorization and retrieval
OBJECTIVES
extracted from the FP7-SEC-2013-1 call

- Development of a research agenda which provides concrete answers to the following issues:
  - In what categories can we subdivide Cyber Crime and Cyber Terrorism?
  - What are the major research gaps?
  - What are the challenges that must be addressed?
  - What approaches might be desirable?
  - What needs to be in place for test and evaluation?
  - To what extent can we test real solutions?
The prefix **cyber** has a long history. **Cybernetics** is the science of communications and automatic control systems in **both machines and living things**.

Recently, the prefix has come to define an **object**, **person** or **activity** present **in the virtual world**, as opposed to the real world (or non-virtual) **cyber-war, cyber-cop or cyber-terrorism**.

But this new use of **cyber** is not correct: **Virtual entities** are not opposed to **real entities**... they are closely related.
IDENTITIES IN THE DIGITAL ERA

- Evolution of the concept of identity for individuals, companies, and governments in the digital era


- Security issues more often related to badly handled virtual identities and assets

The effects in the real world of what is done virtually (and vice versa) are not correctly understood

CYBERROAD aims at Intercepting the evolution of identities to define the research agenda for cybercrime and cyberterrorism
VIRTUAL IDENTITIES

- A projection of the real identity of individuals, companies, governments
  - Pictures, locations, relationships, official documents, etc.

This information can be misused

- But they can also be brand new virtual identities specifically crafted for the virtual world,
  - They can be loosely related to real individuals, companies and governments

This information may have a huge impact on the real and virtual behaviour of individuals, companies and governments
The main purpose of a criminal organization in the physical world is to generate wealth for its members (ethnic groups, hierarchical gangs, etc.)

In the cyberspace, cybercrime has taken an entrepreneurial form
- defined roles
- established margins
- international collaborations to operate in several jurisdictions.
- people involved don’t know the partners with whom they are working.

Partners of cyber criminal organizations come from different countries
- This creates a market of comparative advantage challenges for law enforcement
Targets are not directly related to citizens, but to essential **services** provided by **national critical infrastructures**

*those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic wellbeing of citizens or the effective functioning of governments*

- **New attack surfaces** can be exploited by terrorists to achieve their aims, as the **evolution of technology** expose essential services in new ways.
The **technology** used for creating, exposing, sharing identities does not actually take into account all these implications.

People need to elaborate **new abilities** to cope with the complex environment they live in
- the 6 senses are not enough to cope with the real and virtual world

These abilities should be **empowered by new technologies** that will help individuals **manage trust** either at the personal, corporate or government levels.
CyberROAD GOALS

- To provide **solid definitions** of the concepts of cyber-crime, cyber-terrorism, cyber-security

- To go beyond **current misconceptions** and oversimplifications

- To take into account the **multiple bidirectional links** between the real and the virtual world, links that are exploited by criminals
METHODOLOGY

- **Social, Economic, Political, and Legal Scenario**
  Technical solutions alone does not provide a solution to Cybercrime and cyber-terrorism problems

- **The scientific analysis of legal, ethical, and political scenarios** is an essential component in the fight against cybercrime and cyber-terrorism...

- ...as well as the analysis of the **vulnerabilities and misconfigurations** of the electronic building blocks of the cyber space.
Unifying the Global Response to Cybercrime

CyberROAD ACTIVITIES

- Cyber Terrorism
- Economic, Legal, Political, and Social Scenario
- Cyber Crime
- Technological Scenario
- Scientific Coordination
BUILDING THE CONSORTIUM

- Wide coverage of EU countries
- Wide coverage of expertise
  - Scientific (Universities)
    - economic, social and political scenarios
    - technological issues
  - Industrial
    - malware analysis and detection
    - critical infrastructures
  - Government
    - national defence
    - law enforcement
THE CONSORTIUM

10 countries

AUSTRIA
GERMANY
GREECE
ITALY
NETHERLANDS
POLAND
PORTUGAL
SPAIN
SWITZERLAND
UK
THE CONSORTIUM
20 partners

- ITALY
  - UNIVERSITY OF CAGLIARI (coordinator)
  - POSTE ITALIANE
  - VITROCISET
  - CEFRIEL

- AUSTRIA
  - SBA Research

- GERMANY
  - TECHNISCHE UNIVERSITAET DARMSTADT

- GREECE
  - FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS (FORTH)
  - NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS" (NCSRDN)
  - MINISTRY OF NATIONAL DEFENCE GREECE
THE CONSORTIUM
20 partners

- NETHERLANDS
  - SECURITY MATTERS
- POLAND
  - NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA (NASK)
- PORTUGAL
  - INOV INESC INOVACAO - INSTITUTO DE NOVAS TECNOLOGIAS
    MINISTÉRIO DA JUSTIÇA - POLICIA JUDICIÁRIA
- SPAIN
  - INDRA SISTEMAS S.A.
- SWITZERLAND
  - SCUOLA UNIVERSITARIA PROFESSIONALE DELLA SVIZZERA ITALIANA
    INFORMATIKSTEUERUNGSORGAN DES BUNDES ISB (MELANI)
- UK
  - PROPRS
  - IVARX LIMITED (CYBERDEFCON, CDF)
  - ROYAL HOLLOWAY AND BEDFORD NEW COLLEGE (RHUL)
  - McAfee UK
Unifying the Global Response to Cybercrime

ADVISORY BOARD

- Dr. Marco Morana (UK) – OWASP
- Prof. François Géré (France) – IFAS (Institut français d'analyse stratégique)
- Dr. Richard Nolan (USA) – CERT® Coordination Center
- Junko Hayakashi (Japan) – JPCERT/CC
- Yurie Ito (Japan) – JPCERT/CC
- Etay Maor (Israel) – RSA
- Leonardo Fiocchetti (Italy) – SELEX Sistemi Integrati
- Giuseppe Vaciago (Italy) – Tech and Law Center
EXPECTED PRODUCTS

- The project length is **24 months**
  Expected starting date: **May 2014**

- **Products**
  - Public website
  - Public documents
  - Workshops and Scientific Publications
  - Generalized Awareness and Training Campaigns

- Some joint events will be organised with the other two consortiums that have passed the negotiation phase.
CONTACTS

- The website of the project will be opened after the contract is signed
- You can refer to the UniCA – PRA Lab website
  http://pralab.diee.unica.it

- **CyberROAD** project management office
  Fabio ROLI  roli@diee.unica.it
  Giorgio GIACINTO  giacinto@diee.unica.it
  Davide ARIU  davide.ariu@diee.unica.it