WELCOME

CYBER SECURITY RESEARCH @ BELL LABS

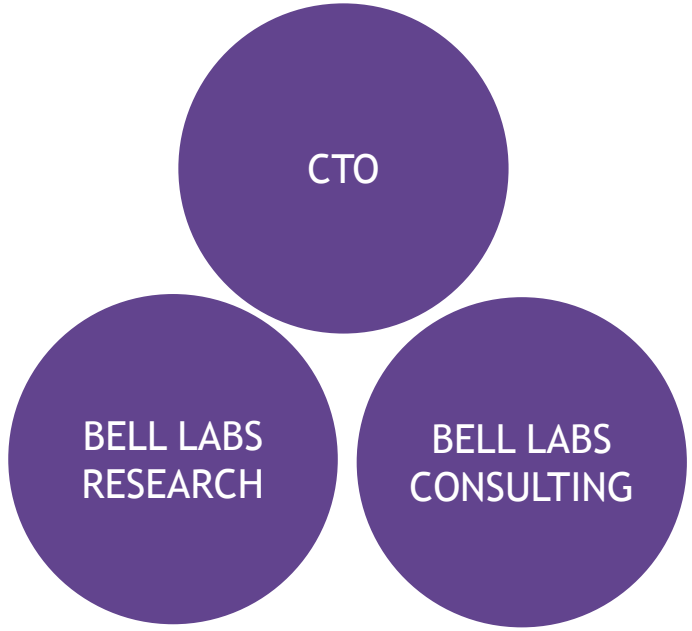
DR. Waël KANOUN

November 2015

Alcatel·Lucent

Our Bell Labs-CTO Organization

Mission
To define the technological and architectural vision for the ICT industry

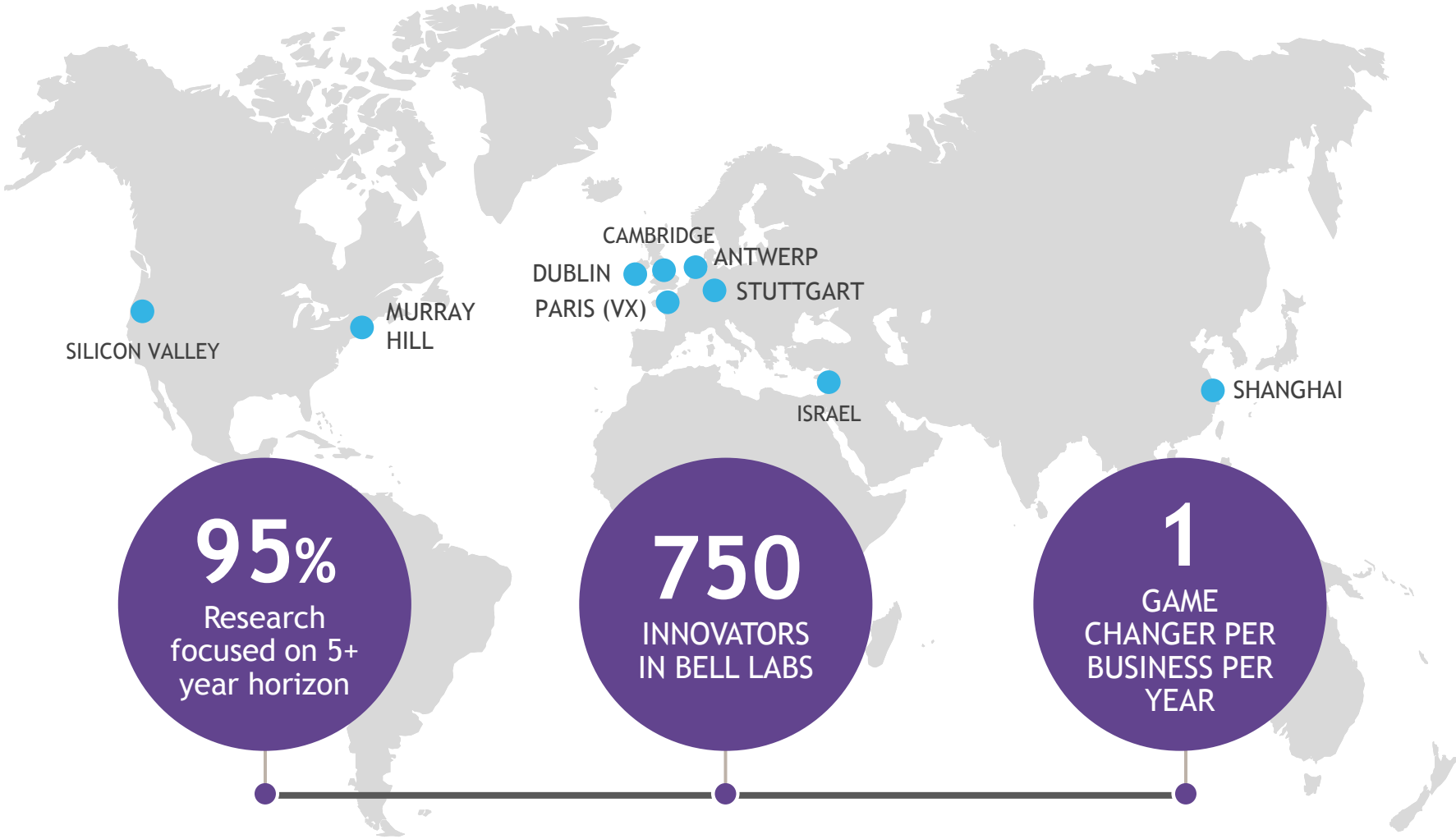


Mission
To understand the key challenges and invent novel solutions

Mission
To advise the industry on the economics of the vision and underlying technologies

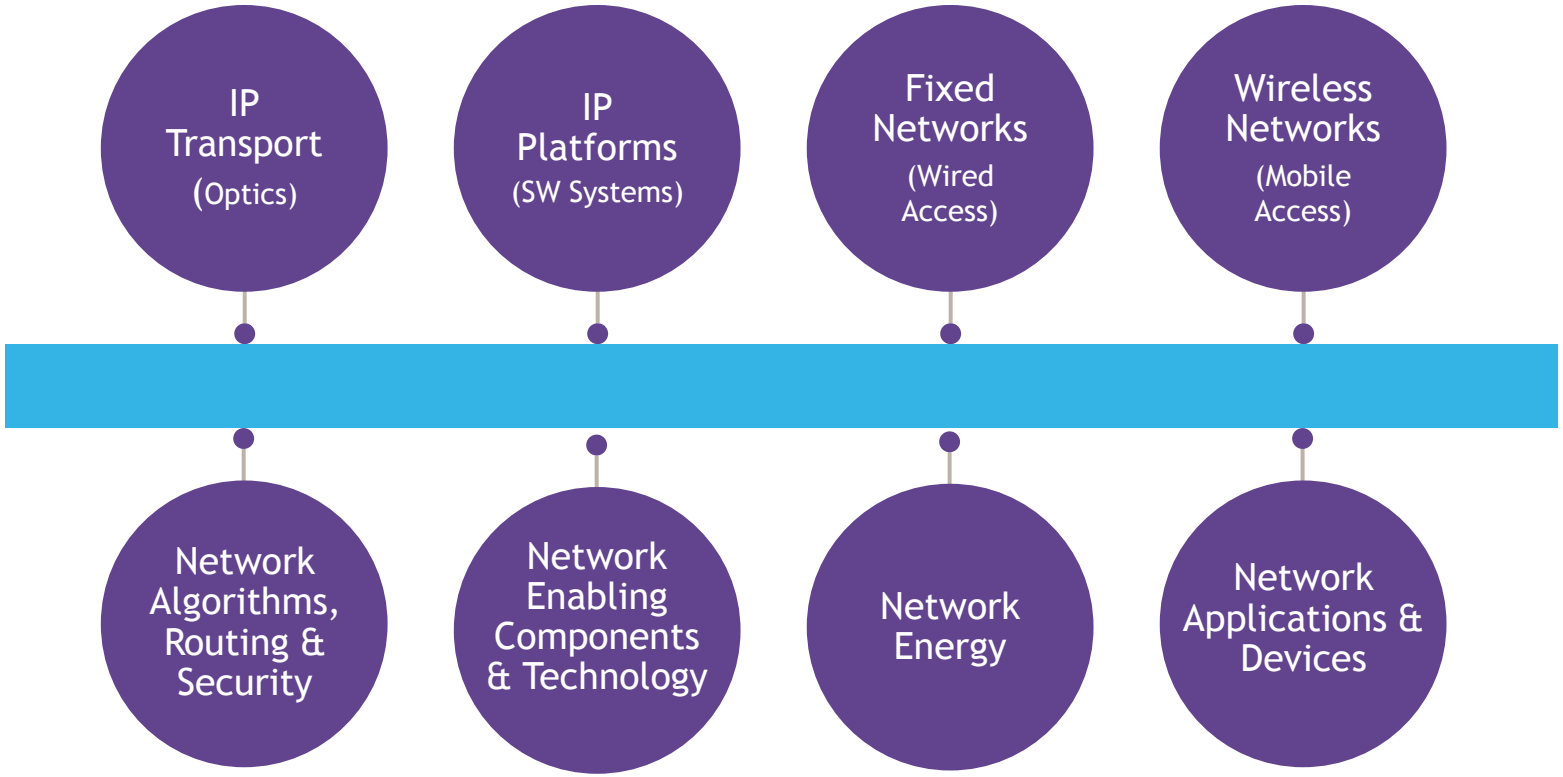
Three Coupled Functions That Define and Invent the Future

The Present: A Global Innovation Leader

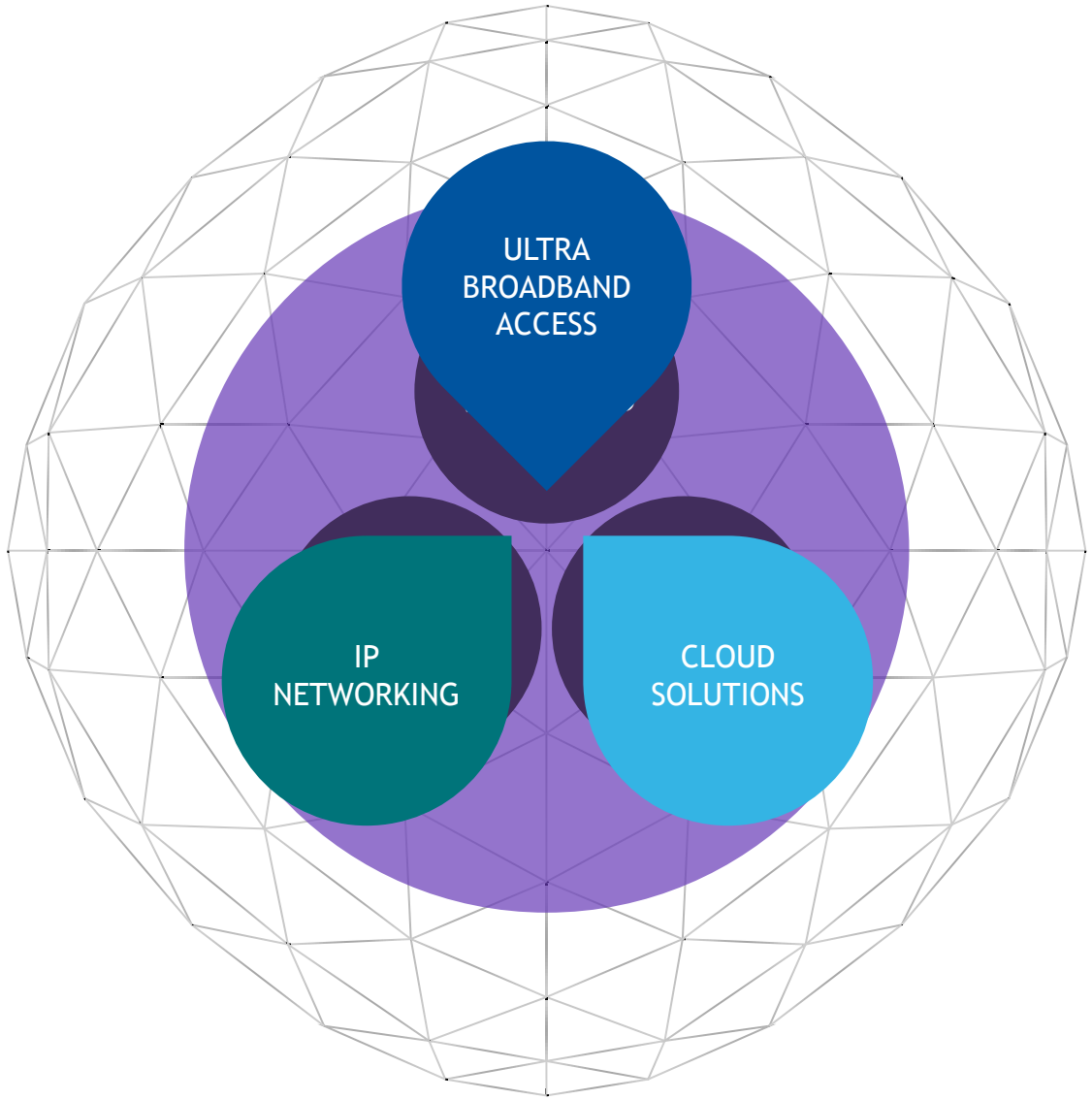


How We Innovate: Structure, Function, Numbers & Goals

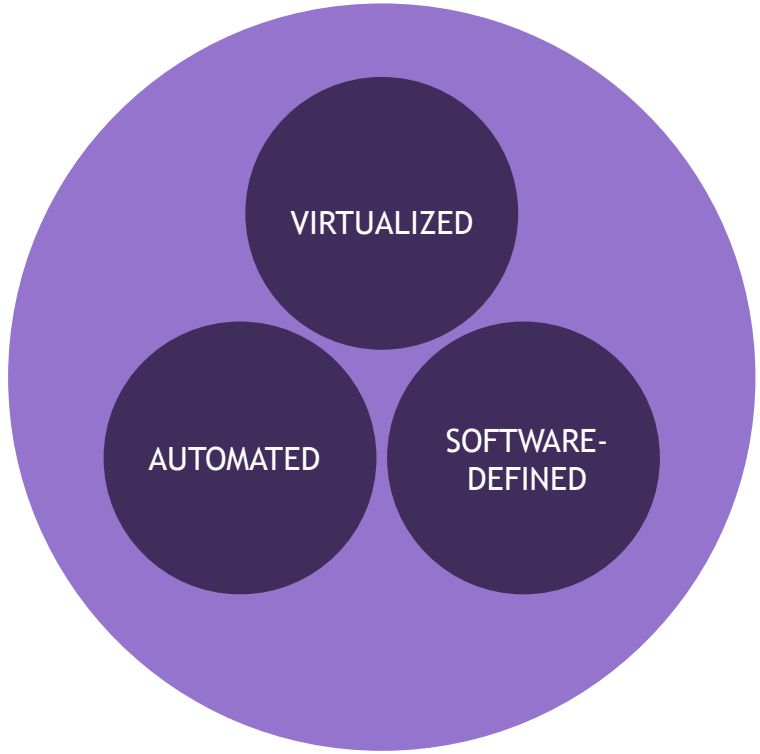
Structure



Cyber Security Research's mission is to provide Scientific excellence, Innovation & Support for Alcatel-lucent's Business Units

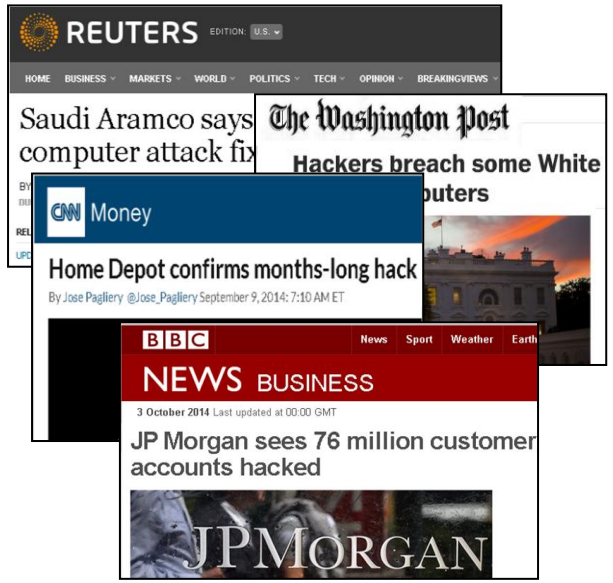


SECURITY IS TRANSVERSE



DYNAMIC RISK MANAGEMENT

Problem Statement



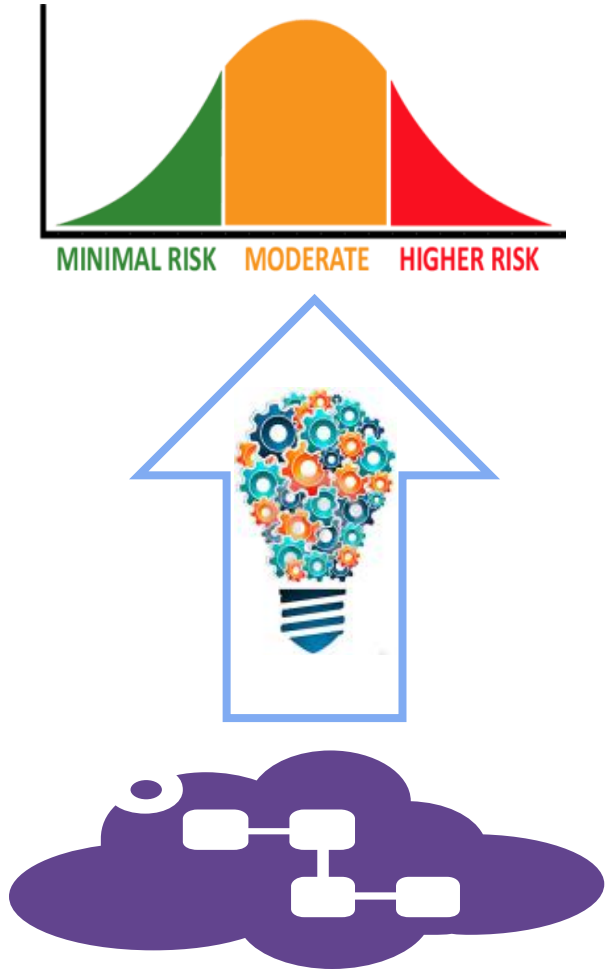
Systems are exposed to plethora of cyber risks with devastating consequences

ICT systems and Cyber threats do not cease to evolve

Today's Security and Risk management models are obsolete

DYNAMIC RISK MANAGEMENT

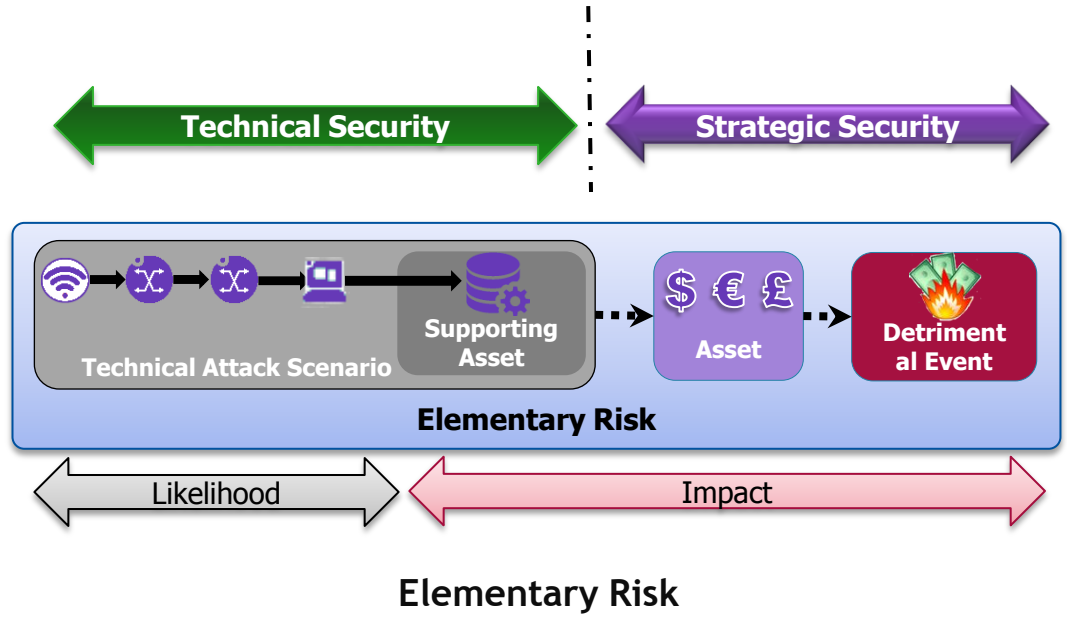
Objective



Dynamic Risk Management bridges the gap between technical and strategic security

DYNAMIC RISK MANAGEMENT

Novel Concept



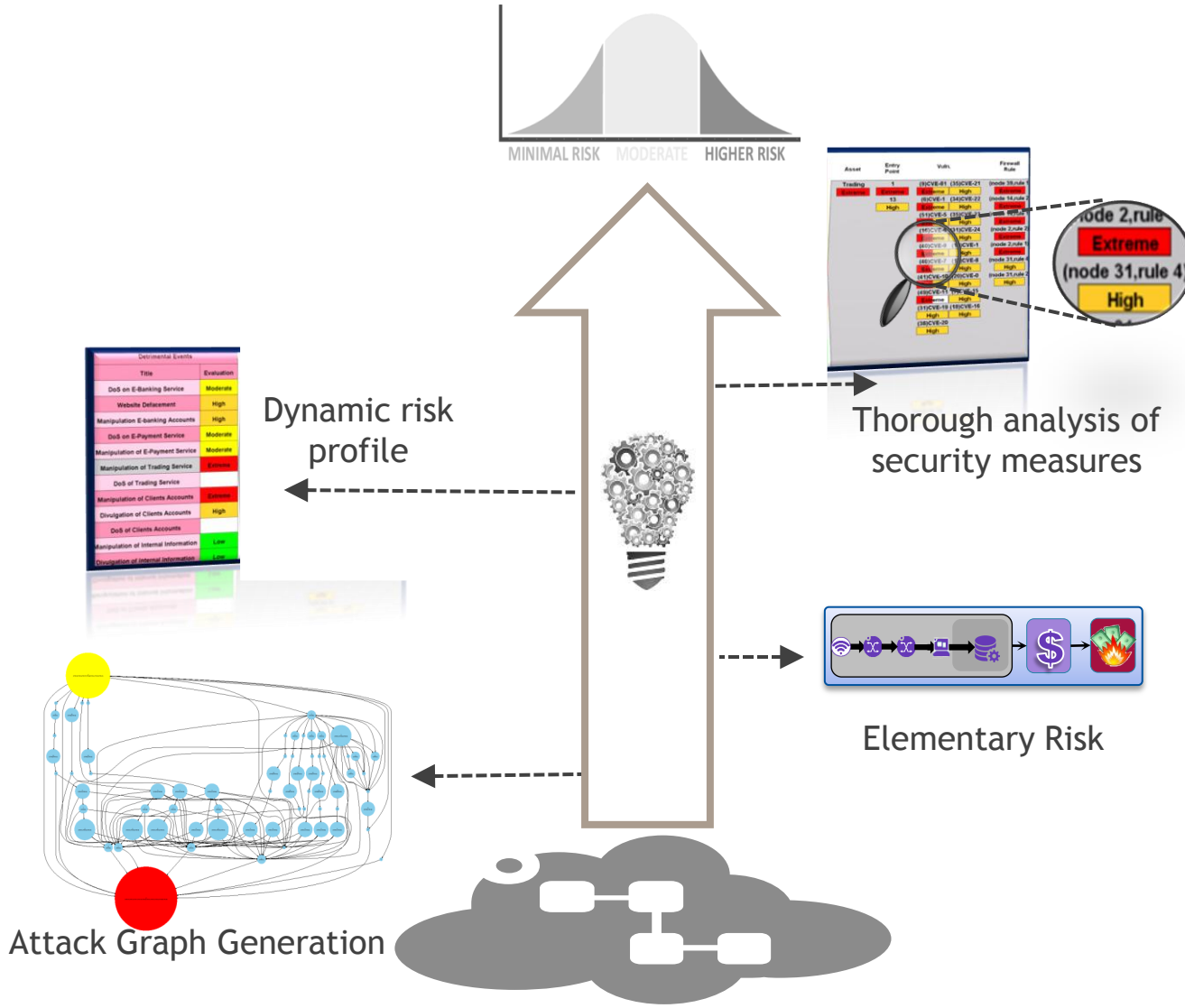
Elementary Risk

- Elementary Risk is risk quantum that can be added or removed for a system
- Algebra to combine Elementary Risks

Elementary Risk bridges the gap between technical and strategic security

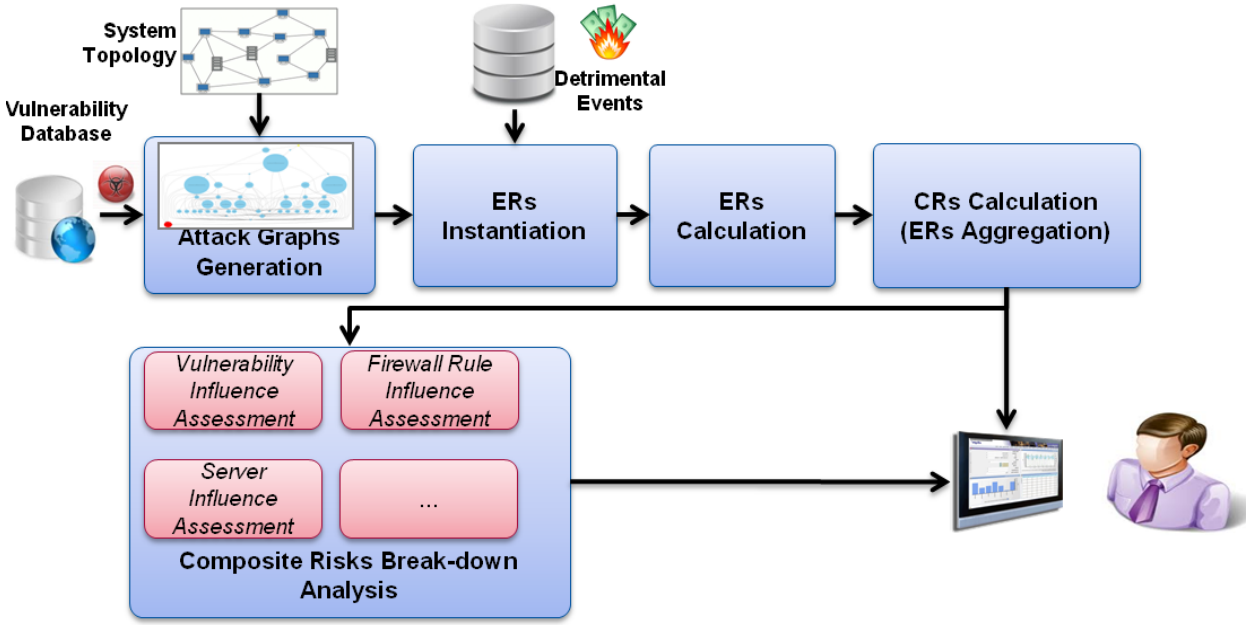
DYNAMIC RISK MANAGEMENT
Technical Roadmap

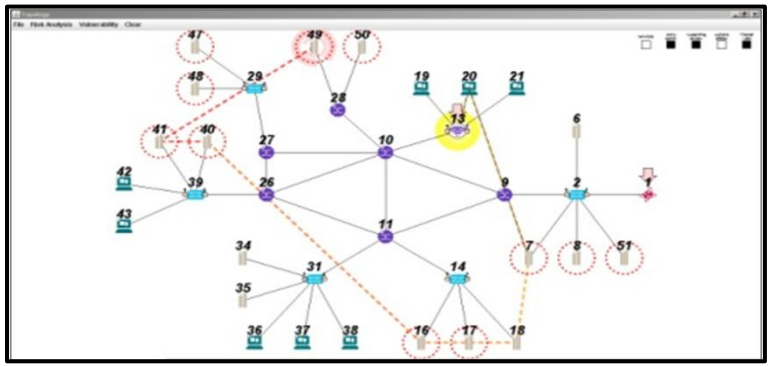
- Devised an attack graph algorithm with enhanced detection (+20%) thanks to the backtracking feature
- Proposed novel Elementary Risk concept as Quantum Risk theory foundation for ICT systems.
- Devised a novel algorithm to dynamically calculate the risk profile of an ICT system. This shifts the risk assessment duration from weeks to minutes (~x500)
- Proposed a break-down analysis framework to evaluate the effect of security measures towards risk profile

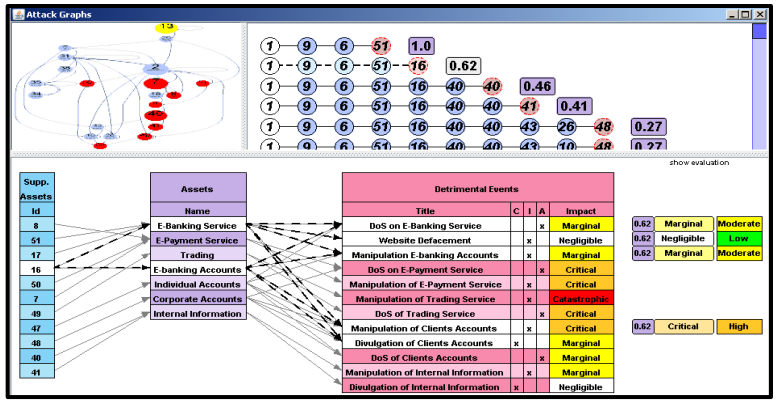


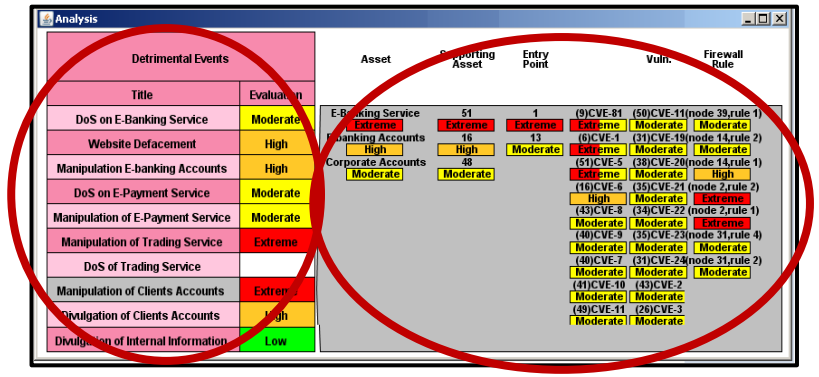
Multiple Breakthroughs towards Dynamic Risk Management

DYNAMIC RISK MANAGEMENT
Architecture









CERES: Composing Elementary Risks to Evaluate Security

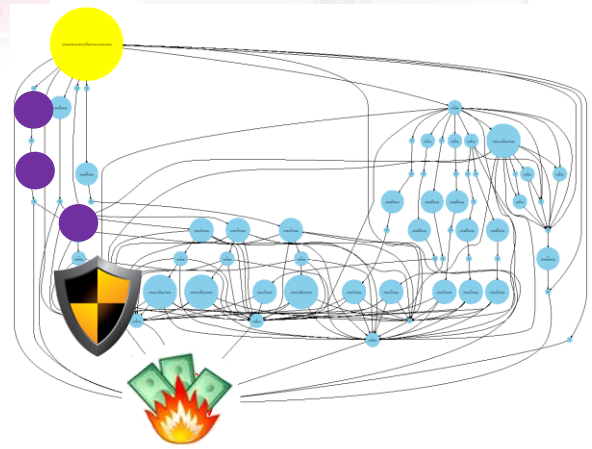
DYNAMIC RISK MANAGEMENT
Exploitation

1. Dynamic Evaluation of security posture

2. Evaluation of security measures
   - Selection
   - Justification by efficiency measurement

3. Track & Respond against ongoing attacks
   - Alert Correlation
   - Response Selection

Detrimental Events	
Title	Evaluation
DoS on E-Banking Service	Moderate
Website Defacement	High
Manipulation E-banking Accounts	High
DoS on E-Payment Service	Moderate
Manipulation of E-Payment Service	Moderate
Manipulation of Trading Service	Extreme
DoS of Trading Service	
Manipulation of Clients Accounts	Extreme
Divulgation of Clients Accounts	High
DoS of Clients Accounts	
Manipulation of Internal Information	Low
Divulgation of Internal Information	Low



CONCLUSION

- Current Dynamic Risk Management are rendered obsolete 
- Concept of quantum risk: Elementary Risk (ER)
  - Calculation of all ERs for a system
  - Algebra to combine ERs
- Dynamic risk Assessment and Treatment
  - Establishing dynamic risk profile 
  - Identifying responsible technical elements 
  - Measuring effectiveness of security measures 
- PANOPTESEC FP7 project *"Dynamic Risk Approaches for Automated Cyber Defence"*
  - Critical infrastructure (SCADA) use case
    - Provided by ACEA – Rome
  - Other partners: Supelec, Telecom SudParis, University of Rome, etc.

over 15 publications, 4 patents, 2 PhD theses, and demos in international events (NATO, Scientific conferences…)

Effective & Continuous Risk Management Enables Us To Fly Further

Wael.Kanoun@alcatel-lucent.com

www.alcatel-lucent.com