



Confidence in a connected world.

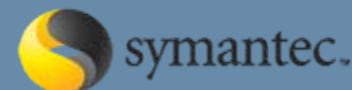


# The role of Information Sharing in Threat and Vulnerability Management

Andrea Rigoni

EMEA Strategic Team – Head of Critical Infrastructure  
Protection

# Why I am here today?



- Head of the Critical Infrastructure Protection
- Advisor to the Italian Prime Minister Cabinet Office
- Member of many european Expert Groups
- I am leading RA/RM projects
  - Air Control sector
  - Energy Sector
  - EU Information Sharing initiative



Confidence in a connected world.

# Information Sharing Setting the Scene

- People share information all the time, all along
- Older than history
- At the very beginning “Information and Knowledge Sharing” was verbal (ancient Greece)
- Information Sharing has gained popularity after 9/11
- Information Sharing is a key element of Intelligence
  - 22-Feb-2008 US Intelligence Community published the new “**Information Sharing Strategy**”
- Why to share
  - You know something – you have a solution
  - You need something – you have a problem

- Formal Framework
  - Parties Involved
  - Standards
  - Privacy and data protection
- Sharing is about Trust
  - People
  - Trust is a feeling and an emotion
  - Not different from perspective of Risk
  
  - Many good examples in daily life...

# What is shared



- Raw Data
- Vulnerabilities
  - Software vulnerabilities
  - System/Process vulnerabilities
- Threats
  - Physical vs Logical
  - Global vs Local
- Incidents
- Good and Best Practices
  - case studies
  - lessons learned
- News and Updates
- Early Warning

# With who?



- Private Companies
  - SME
  - Large Companies
- Critical Infrastructures
  - Interdependent Infrastructures
  - National Infrastructure
  - European Critical Infrastructure
- National Organizations
  - ISACs
  - CERTs
- Government Organizations
  - Law Enforcement
  - Critical Infrastructure/Antiterrorism Coordination Centers
  - Defense and Cyberdefense
  - Regulators
- International Organizations
  - European Agencies
  - Sector specific Associations and Councils

- Availability and Robustness of European Communications Infrastructures: a study prepared by Bell Labs (Alcatel Lucent)
- Recommendation n. 4
  - Recommendation
  - Member States and the Private Sector should establish formal means for sharing information that can improve the protection and rapid restoration of infrastructure critical to the reliability of communications within and throughout Europe.
- Initiatives promoting information sharing must proceed **carefully**. Member State governments, while committed to the European Union, are also firm regarding their primary role in the **sovereign defence** of their nation-state and thus their critical infrastructure. In addition, the European community is a large one. Since trust is ultimately based on **individuals trusting other individuals**, there are practical limitations on how many trusted relationships can be maintained by any given person.

- Industry stakeholders sharing only with selected partners . . . resulting in **fragmented sharing** and response to attacks, and various providers of critical infrastructure being left uninformed.
- Critical government **information kept within government** . . . reduces industry's ability to prepare and respond to attacks.
- Industry threat and outage information shared only within industry . . . Leaves **government interests under-protected** and eliminates potential benefits of government assistance during a crisis.
- **Information sharing kept within a Member State** . . . weakens the ability of other Members States to prepare and respond, and negatively impacts the reliability and security of all networks connected to those of the uninformed Members States.
- A **mandated environment** for information sharing not built on mutual trust . . . results in sharing only to the extent of the mandate, potential unintended consequences, and lost opportunity to benefit from a common body of knowledge.
- Establishment of a **European Institution level program** . . . resulting in loss of Member State control and less effective “star” architecture

# ARECI Proposed model

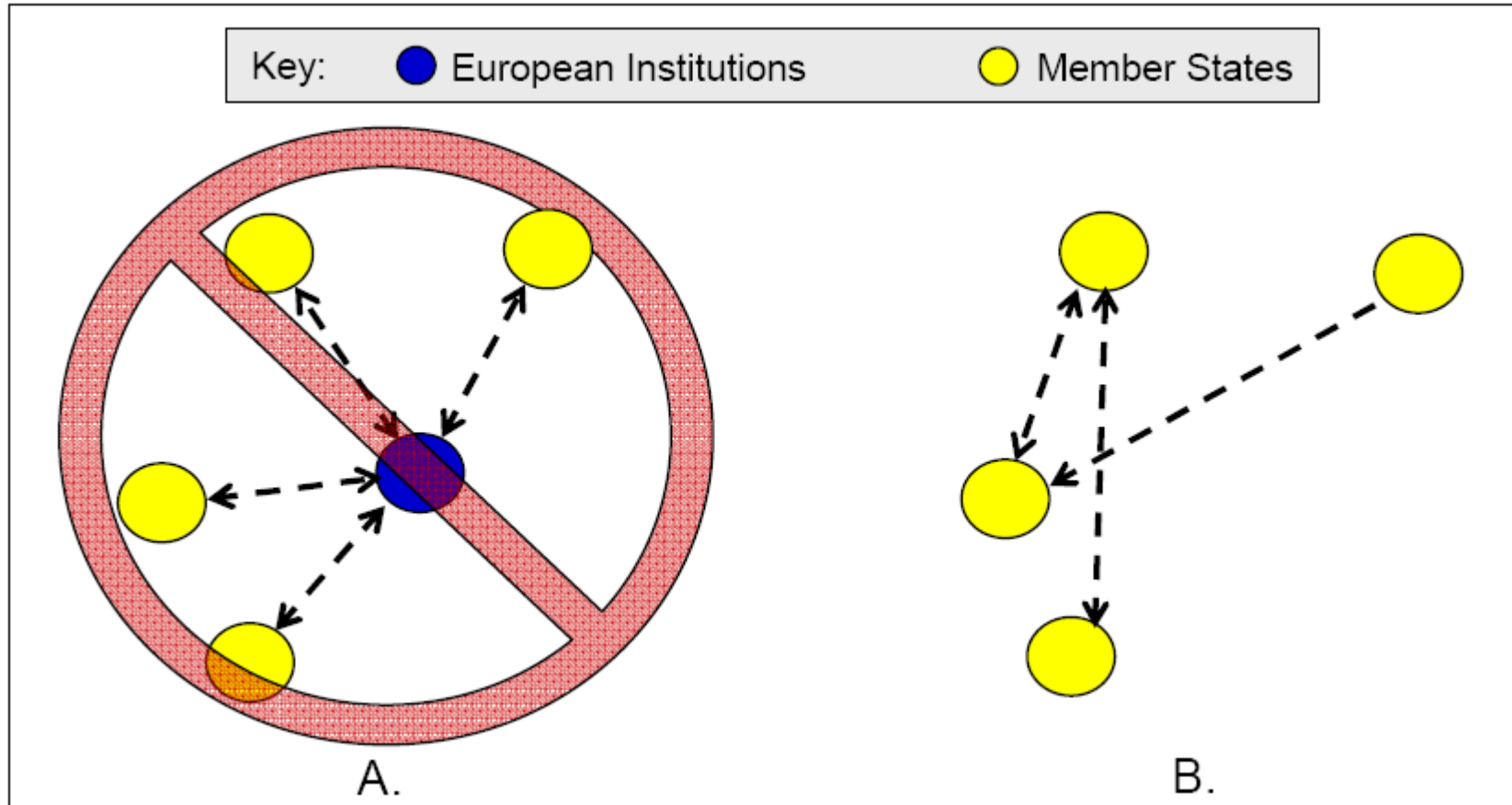


Figure 15: Star (A) and Mesh (B) Architecture Models



Confidence in a connected world.

# Why Information Sharing has become so important? An example from the ICT Sector

# Symantec™ Global Intelligence Network

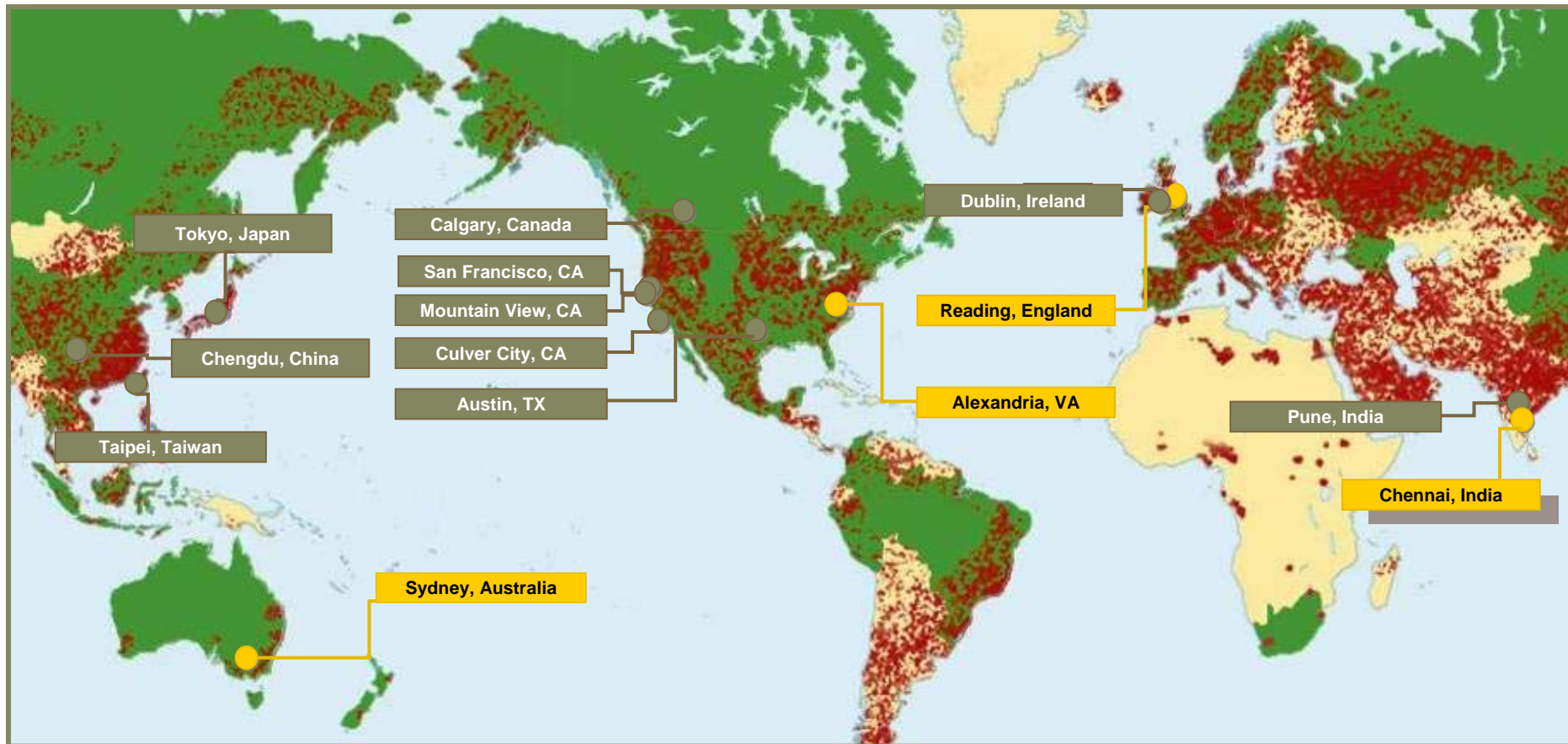
4 Symantec SOCs

80 Symantec Monitored Countries

40,000+ Registered Sensors in 180+ Countries

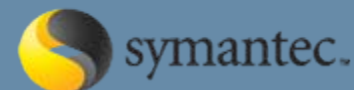
11 Symantec Security Response Centers

> 7,000 Managed Security Devices + 120 Million Systems Worldwide + 2 Million Probe Network + Advanced Honeypot Network

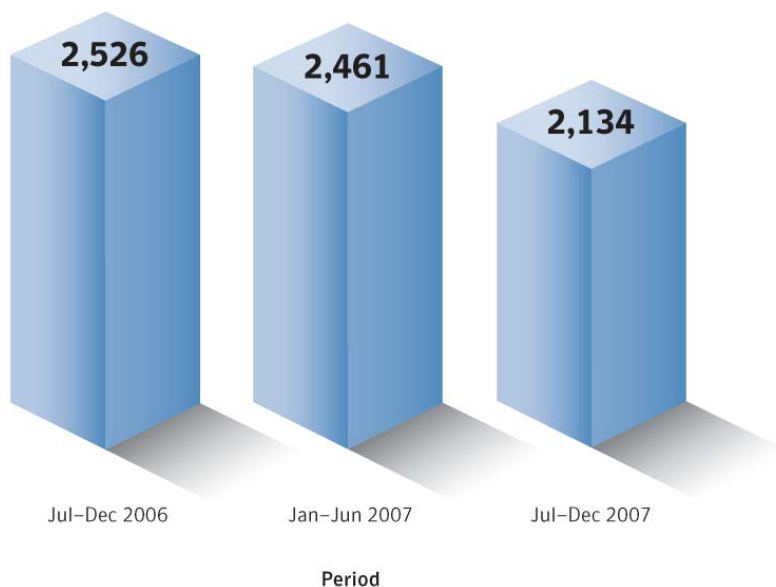


- Most Critical Infrastructures rely on ICT to deliver and support Critical Services
  - Energy Transmission and Distribution
  - Nuclear Plants and Dams
  - Financial
  - Telcos
  - Water Management System
  - Mass Transportation
  - Air Control
  - Etc.
- ICT Security is not mature in every sector
- Analysis of Interdependencies

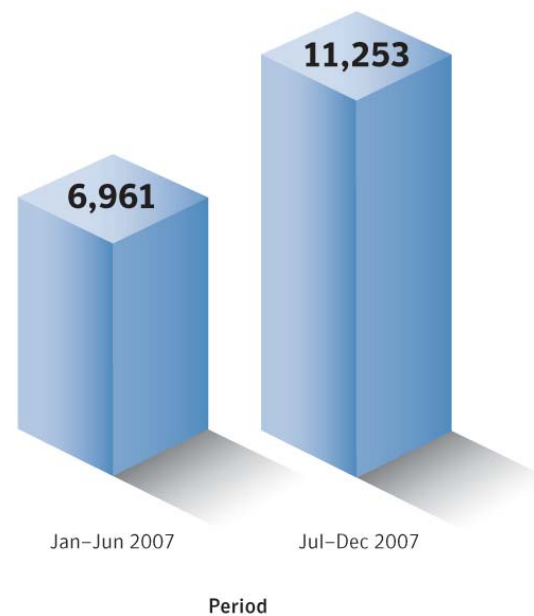
# The Web as the Focal Point



- Vulnerabilities in websites are more popular because they allow for more sophisticated and multi-staged attacks.
- Site-specific vulnerabilities outnumber traditional vulnerabilities nearly 5 to 1 with much lower patch rates – only 473 of the site-specific vulnerabilities had been patched at the time of reporting.



Vulnerabilities - Traditional

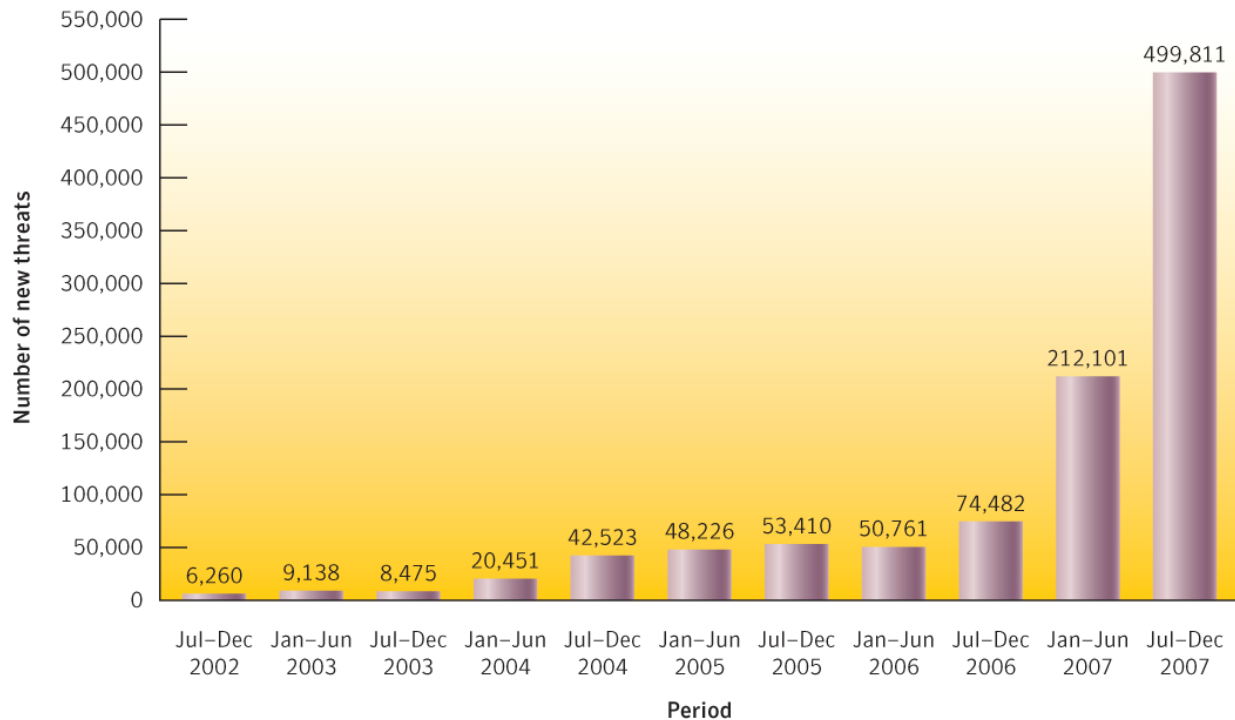


Site-specific vulnerabilities

# Underground Economy Specialization



- The significant increase in new threats over the past year is indicative of the work of specialized malicious code authors and the existence of organizations that employ programmers dedicated to the production of these threats.



Source: Symantec Internet Security Threat Report Vol. XIII



Confidence in a connected world.

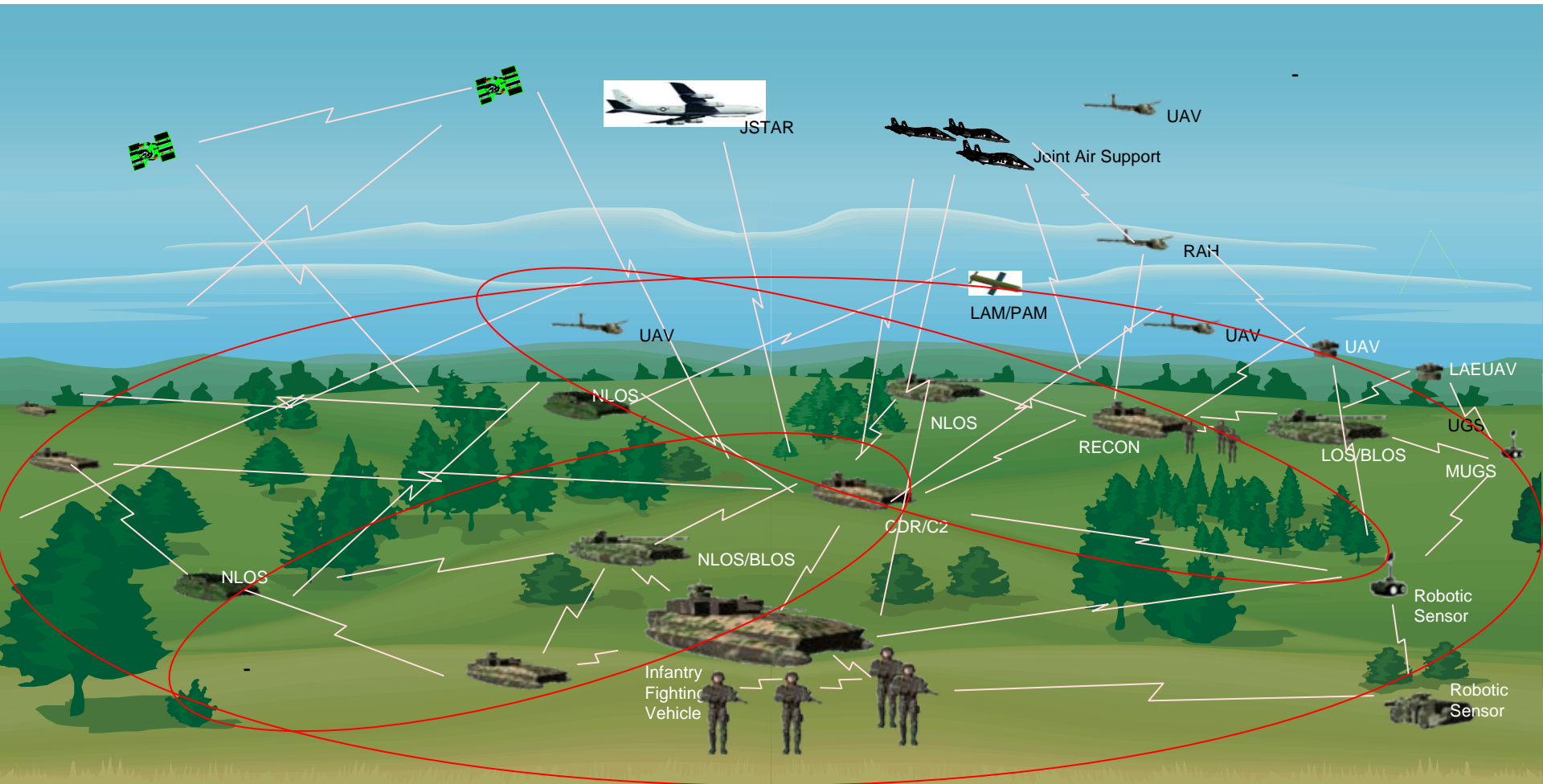
# Why Information Sharing is so critical for Cyberdefense?

- New warfare doctrines provides valid and modern models for IT Security
  - Network Centric Warfare (NCW) or Network Enabled Capability (NEC)
  - C2 Command & Control Doctrine
- NCW
  - Introduced for the first time in 1999 by Alberts, Garstak, Stein
- Key Principles
  - Achieving Shared Awareness
  - Leveraging Shared Awareness
    - Self-synchronization
    - Increase in agility and effectiveness

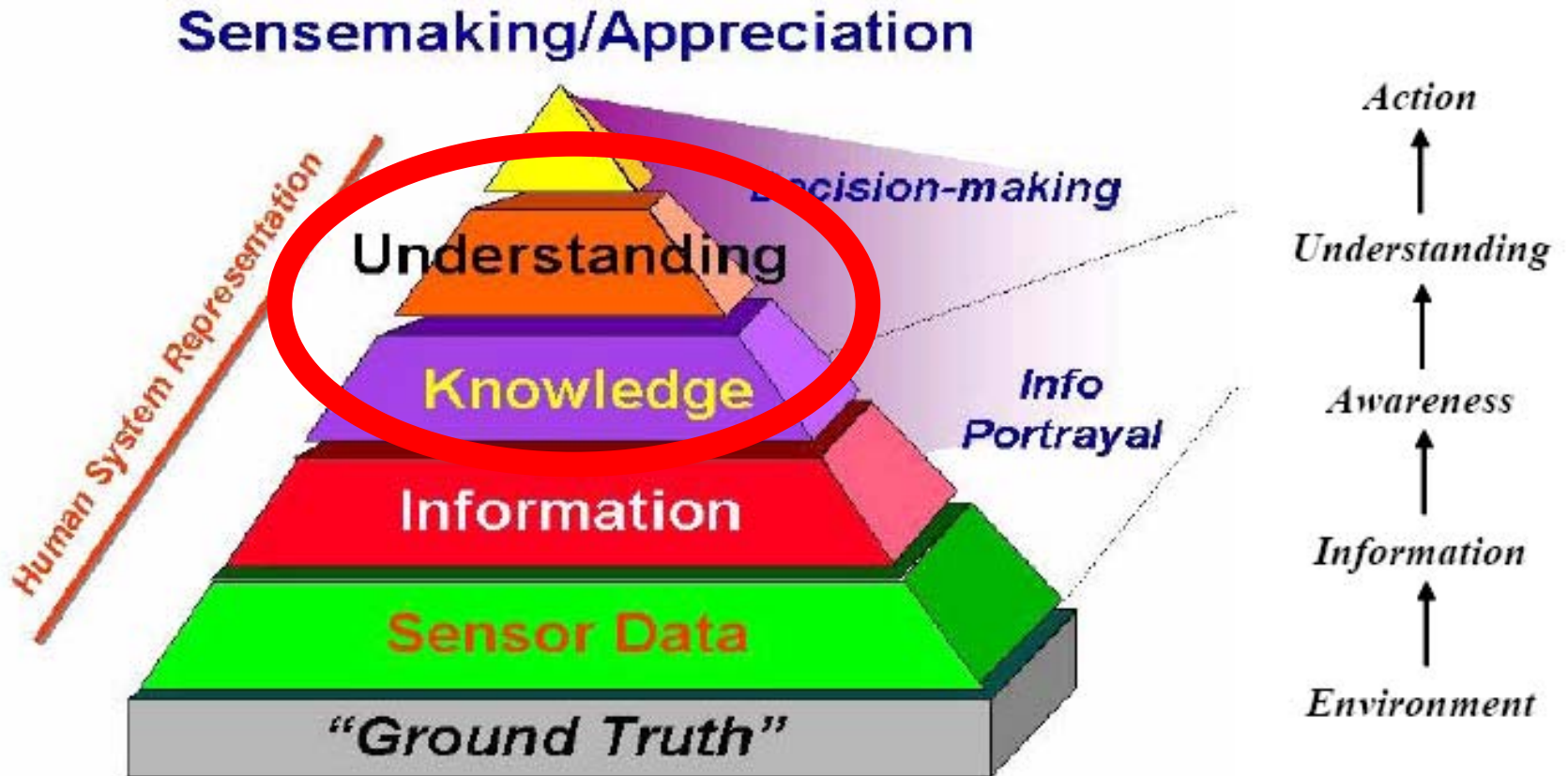


- Information
  - Data
  - Information
  - Understanding
  - Knowledge
  - Wisdom
- Information becomes Awareness when it passes from information systems into the cognitive domain (**human brain**)
- Humans, as individuals, actually hold awareness of situational information

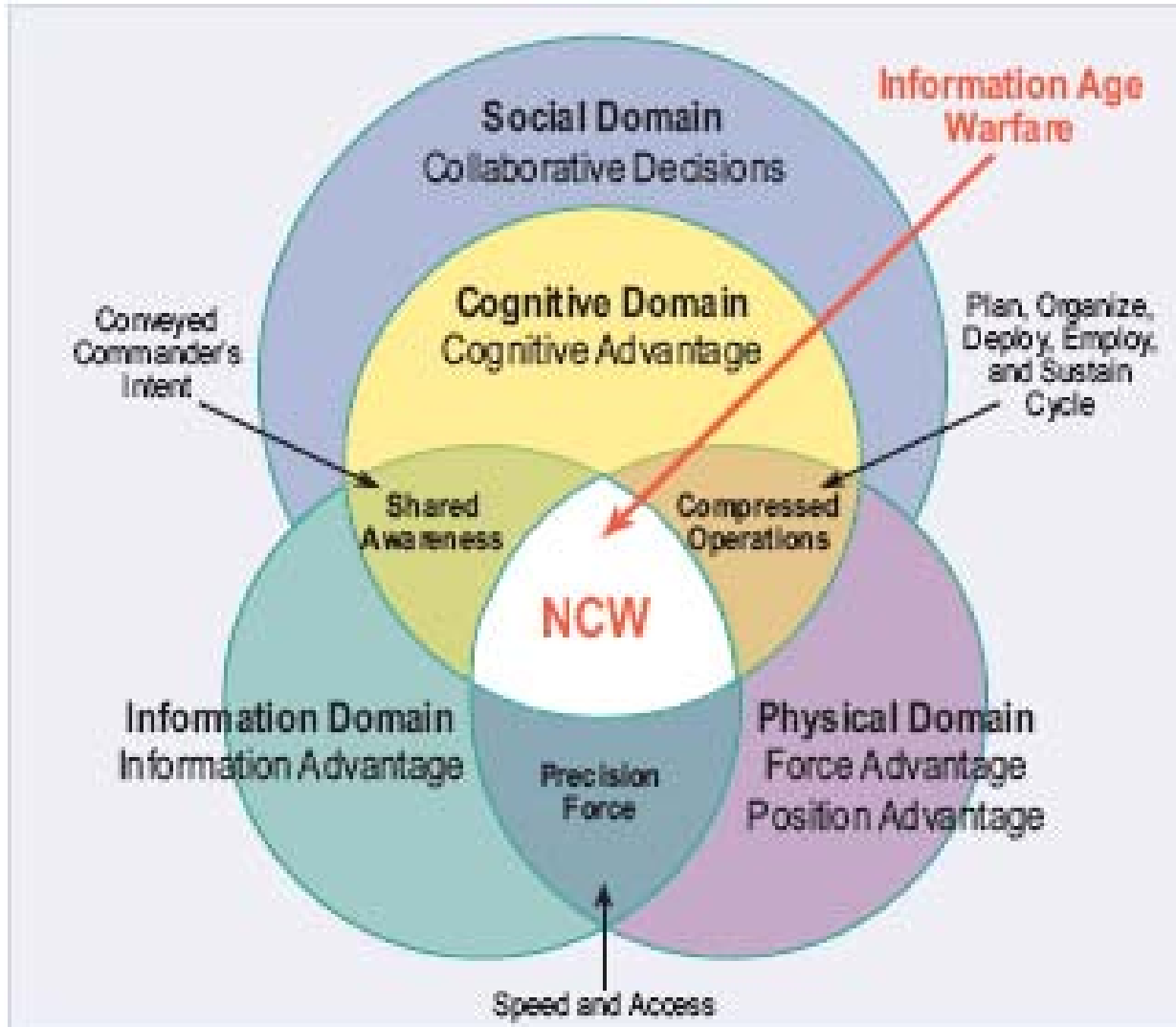
# Digital Battlefield



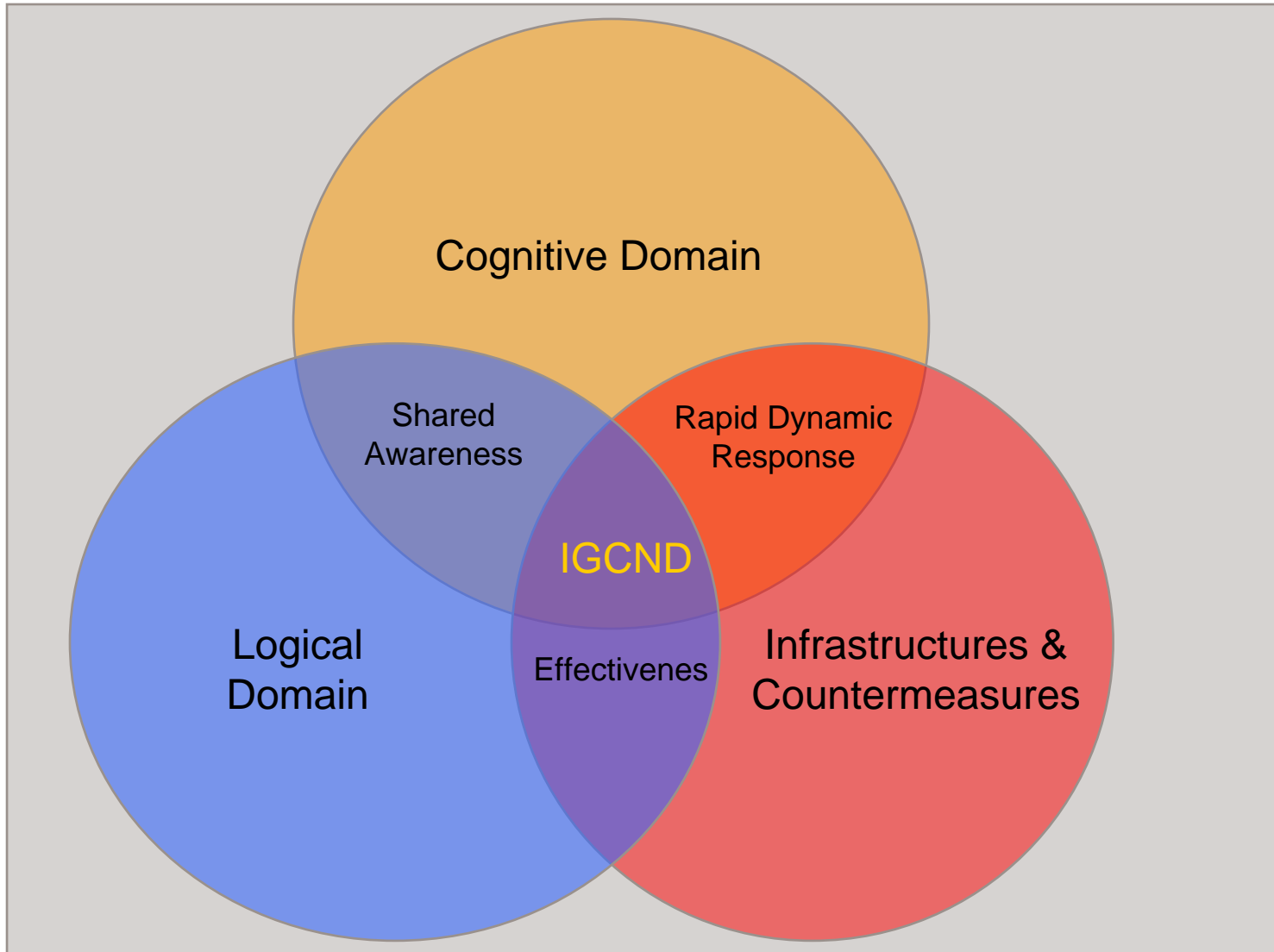
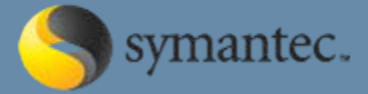
# Cognitive Pyramid



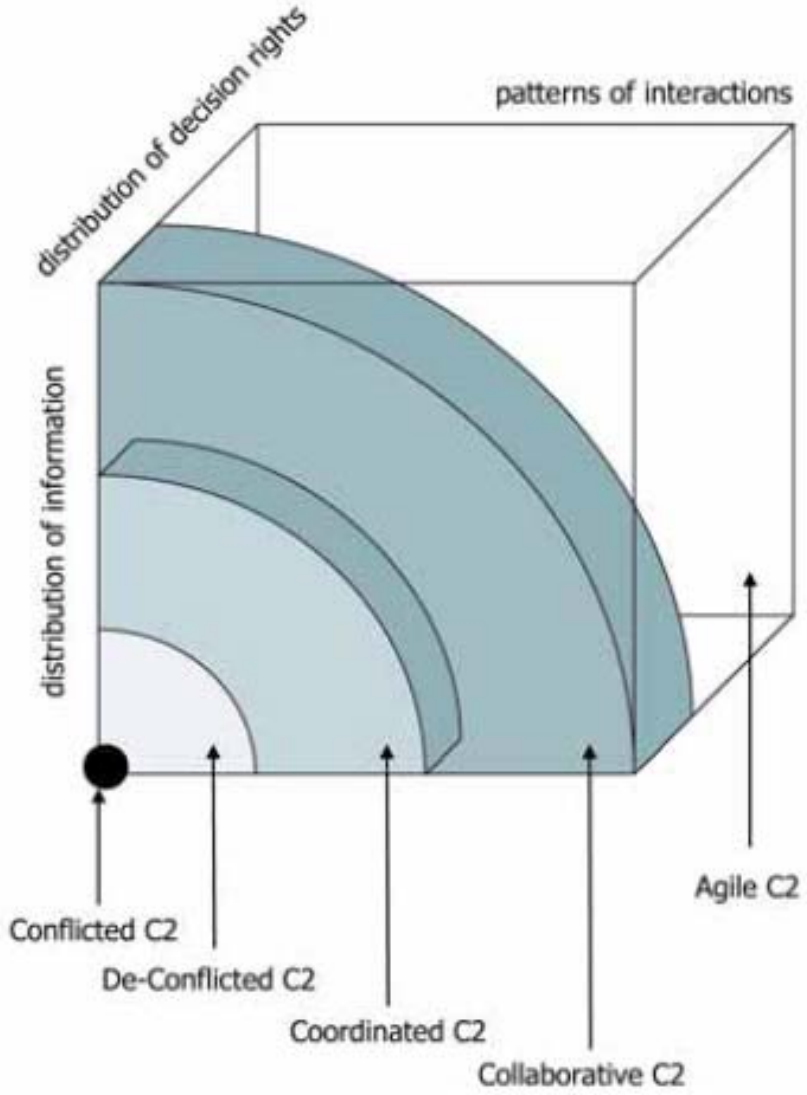
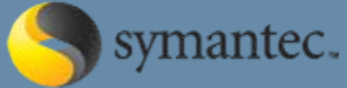
# NCW Model



# IGCND Model



# C2 Maturity Level based on Distribution of Information





Confidence in a connected world.

# The UK Experience: The WARP Trusted Information Sharing model

# What does a WARP look like?



- WARP: Warning, Advice, Reporting Point
- A typical WARP will consist of an operator who knows a little bit about IT security, but is mainly good at communicating with a group of WARP members.
- There will usually be between 20 and 100 members, otherwise it can lose that personal touch.
- The operator uses a website, email, telephone, SMS, and occasional meetings to send a *personalised* service of warnings and advice to the members.
- This will be mainly IT security advice, but can include other material (other threats, e-crime, contingency planning etc) as well.
- The Operator also taps into the knowledge of the members themselves using a bulletin board, meetings and general communication skills.
- A successful WARP will build up enough *Trust* to encourage members to talk about their own incidents & problems, anonymously, for the benefit of the rest (a bit like the 'Neighbourhood Watch' idea).
- WARPs are small, personal and 'Not-for-Profit'.



# WARPs – A development model



## Stage 1: Filtered Warnings

Show the benefits of the WARP to the community through tailored **warning** service, so that everyone feels they are getting a personalised and valuable service.

## Stage 2: Advice brokering

Develop trust through encouraging members to help each other by sharing best practice and giving **advice** to each other through WARP facilities.

## Stage 3: Trusted Sharing

Encourage members to **report** their experiences of otherwise embarrassing attacks or problems (anonymously if necessary, through the operator) within the WARP collective learning.



A feedback circuit of perceived expectations



**Trust** in the person with whom you are sharing;  
**Value** of the information you are sharing;  
**Effort** you need to expend to share;  
**Reward** you would expect from sharing.

To find more: <http://www.warp.gov.uk/TrustedSharing.htm#S4>



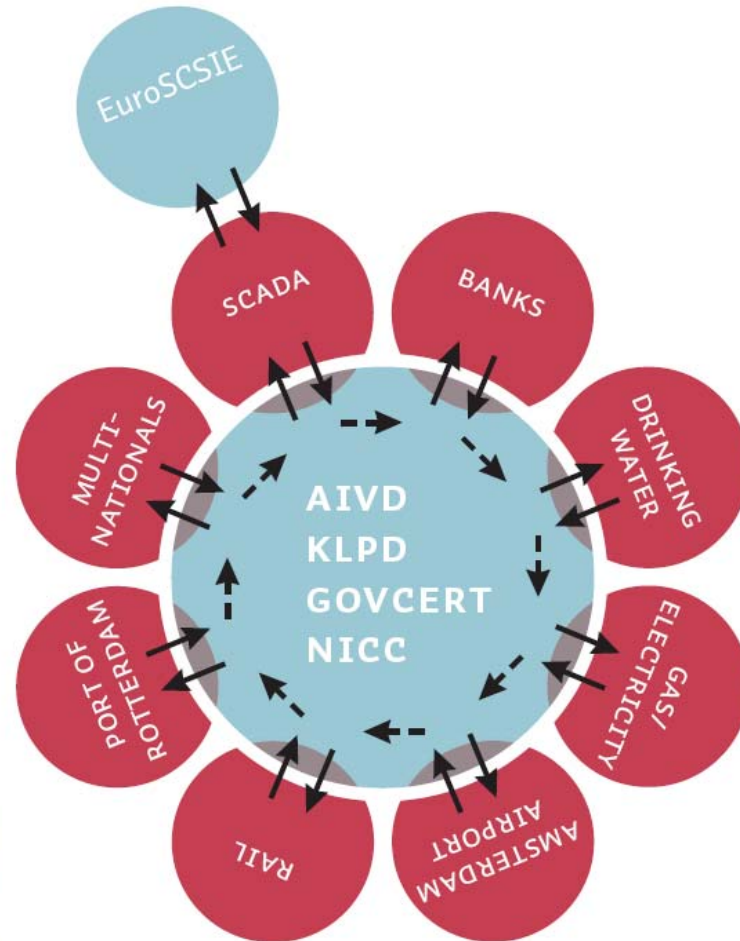
Confidence in a connected world.

# The Netherlands Experience The NICC

# NICC – National Infrastructure Cyber Crime Program



- Government Project
- Public-Private Approach
- Based on CPNI model
- CyberCrime Information Exchange
- Sensitive but unclassified: Traffic Light Protocol
- Information Exchange
  - Face to Face meetings
  - 8 Sectors





Confidence in a connected world.

# European Initiatives and Information Assurance Messaging Framework

Communication, the EPCIP framework will consist of:

- The Directive
- An EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), CIP expert groups at EU level, CIP information sharing processes and the identification and analysis of interdependencies
- Support for Member States concerning National Critical Infrastructures (NCI) which may optionally be used by a particular Member State. A basic approach to protecting NCI is set out in this Communication
- Contingency planning
- An external dimension: cooperation, BP exchanges
- Accompanying financial measures and in particular the proposed EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013

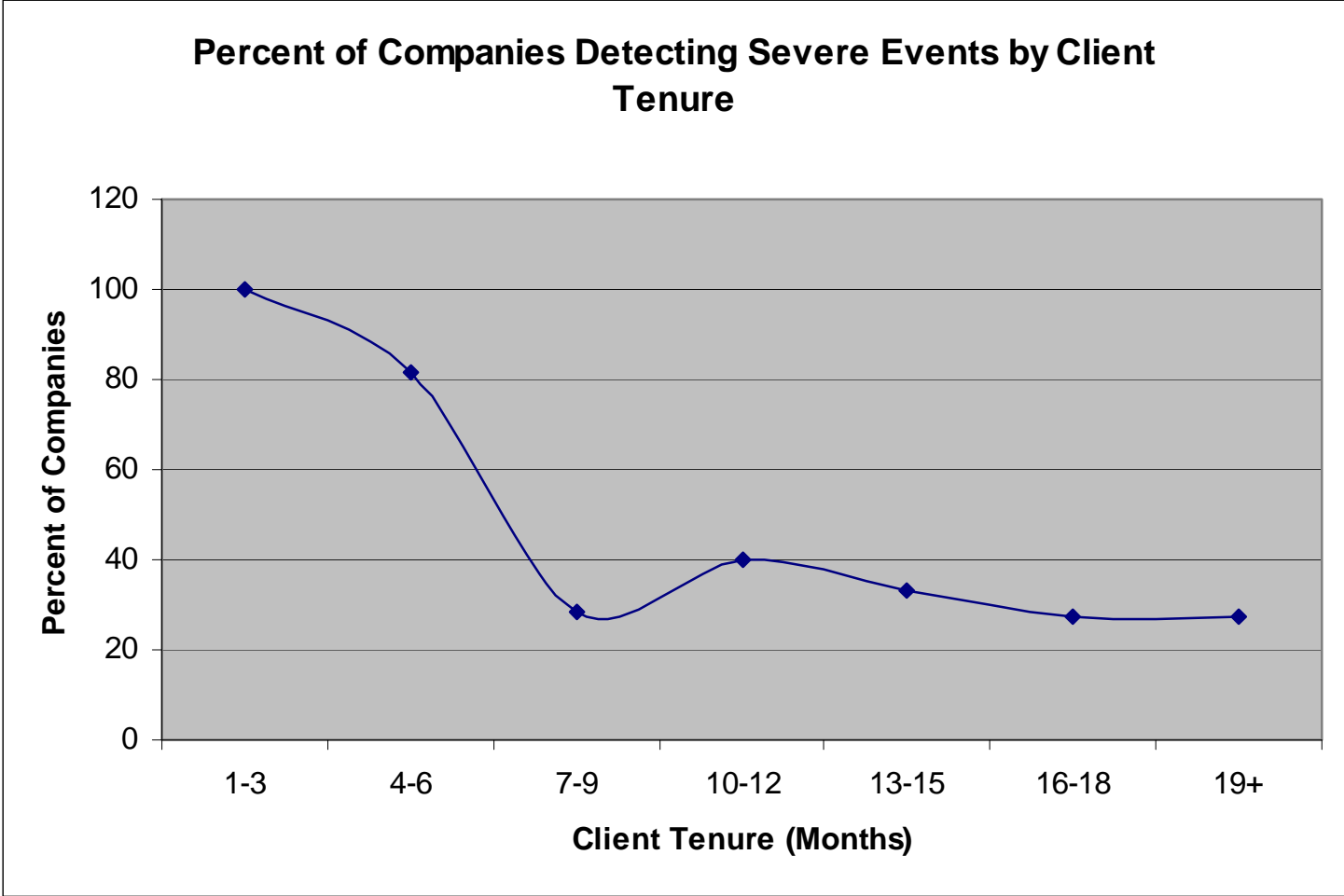
# Information Assurance Messaging Framework



- Awarded in 2007
- 12 months projects
- Definition of a Messaging Framework to allow Critical Infrastructures, National Center, National Authorities and European Agencies to exchange secure messages
  - Vulnerabilities
  - Threats
  - Incidents
  - Practices
- Project started in December 2007

- Hierarchical vs Peer to Peer
  - Blended Approach
- Issues
  - Raw Data vs Data vs Information vs Knowledge vs Awareness
  - Classification and categorization of unstructured data
  - Anonymization
  - Language
  - Define the correct role of Governments, Law Enforcements, National Agencies and European Institutions
  - Common interfaces

# Increased Shared Situational Awareness symantec.



Source: Symantec Managed Security Services

- Information Sharing at the international level is still underdeveloped
- Development of Standards and Frameworks
- Public-Private partnerships must be further developed
  - Balanced relationship – Information shared on both sides
  - New role for governments: from promoter to active party involved in the Information Sharing
- Building Trust is key
- Foster a culture of Propension to Share
- Protection of Privacy and other legal rights



Confidence in a connected world.

# Thank You!

Andrea Rigoni

EMEA Strategic Team – Head of Critical Infrastructure Protection

[Andrea\\_Rigoni \(at\) Symantec.com](mailto:Andrea_Rigoni@Symantec.com)

GSM +39 335 6954784

© 2008 Symantec Corporation. All rights reserved.

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED AS ADVERTISING. ALL WARRANTIES RELATING TO THE INFORMATION IN THIS DOCUMENT, EITHER EXPRESS OR IMPLIED, ARE DISCLAIMED TO THE MAXIMUM EXTENT ALLOWED BY LAW. THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.