The role of Information Sharing in Threat and Vulnerability Management

Andrea Rigoni

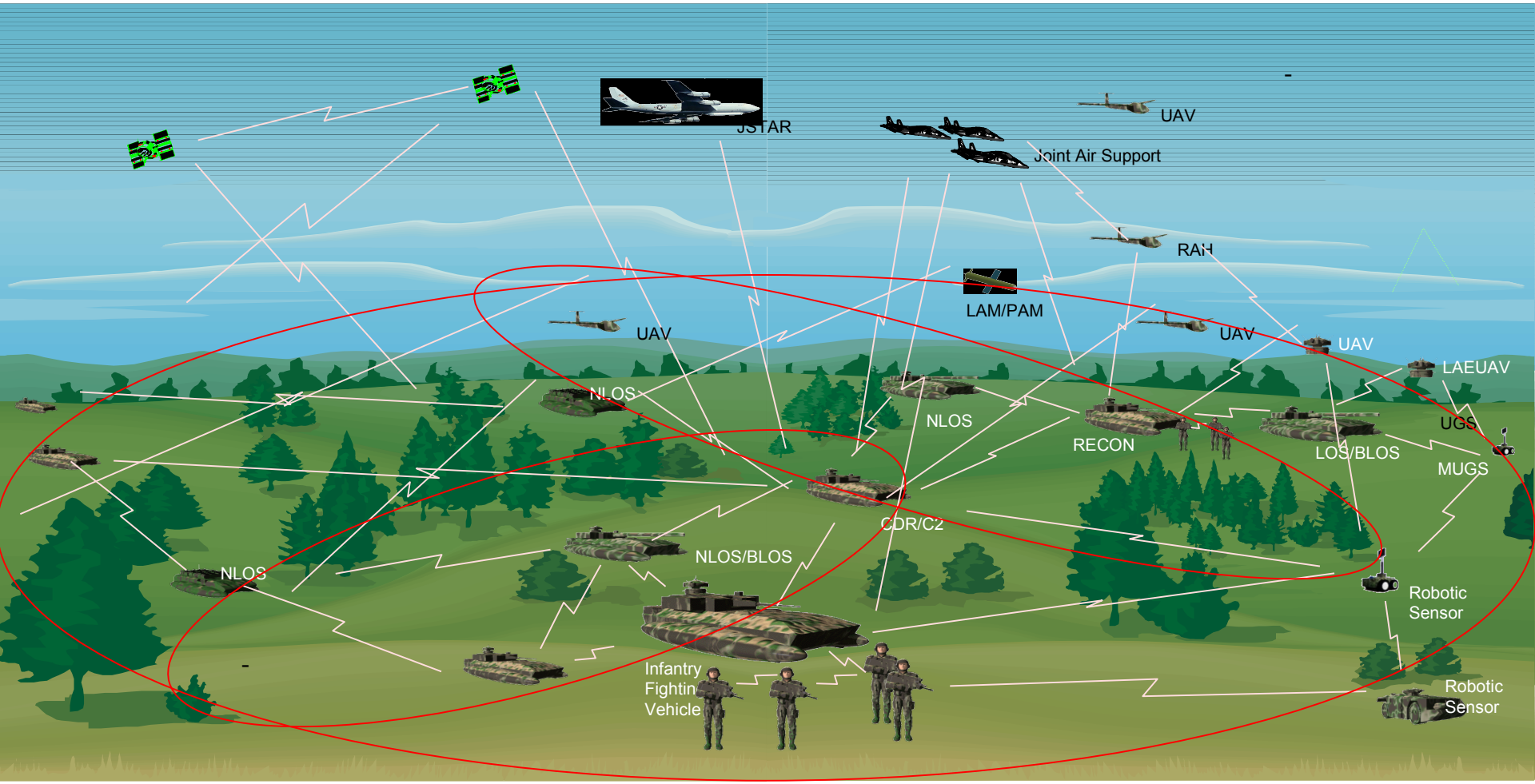
EMEA Strategic Team – Director of Critical Infrastructure Protection

symantec™

Confidence in a connected world.

Information Sharing Setting the Scene

Digital Battlefield



Information Sharing

- 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

Information Sharing to protect

- Formal Framework
  - Parties Involved
  - Standards
  - Privacy and data protection
- Sharing is about Trust
  - People
  - Trust is a feeling and an emotion
  - Not different from perspection of Risk

What is sharded

- 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

ARECI

- 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 primarily 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.

Considerations

- 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

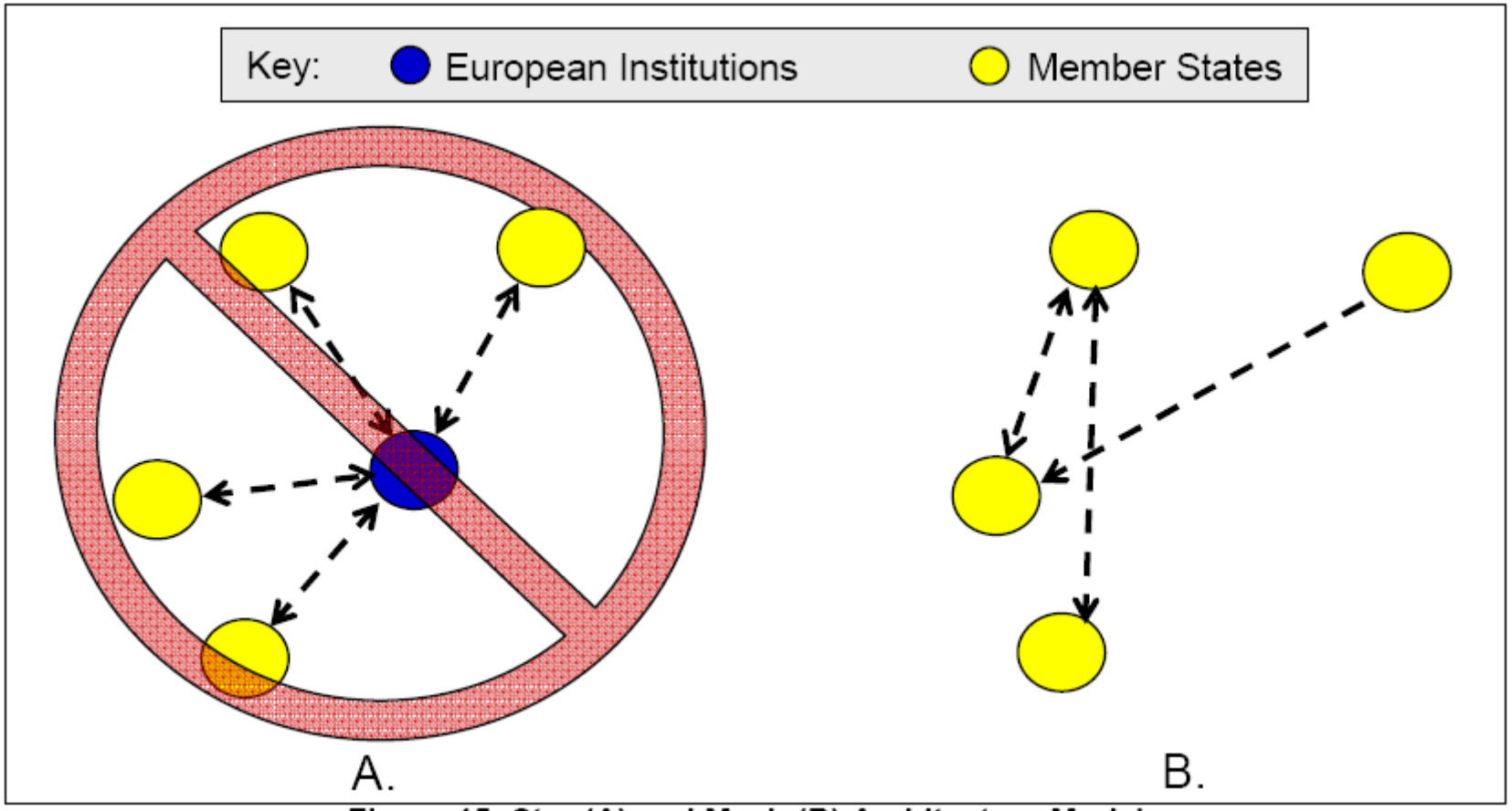


Figure 15: Star (A) and Mesh (B) Architecture Models

symantec™

Confidence in a connected world.

Why Information Sharing is so critical for Cyberdefense?

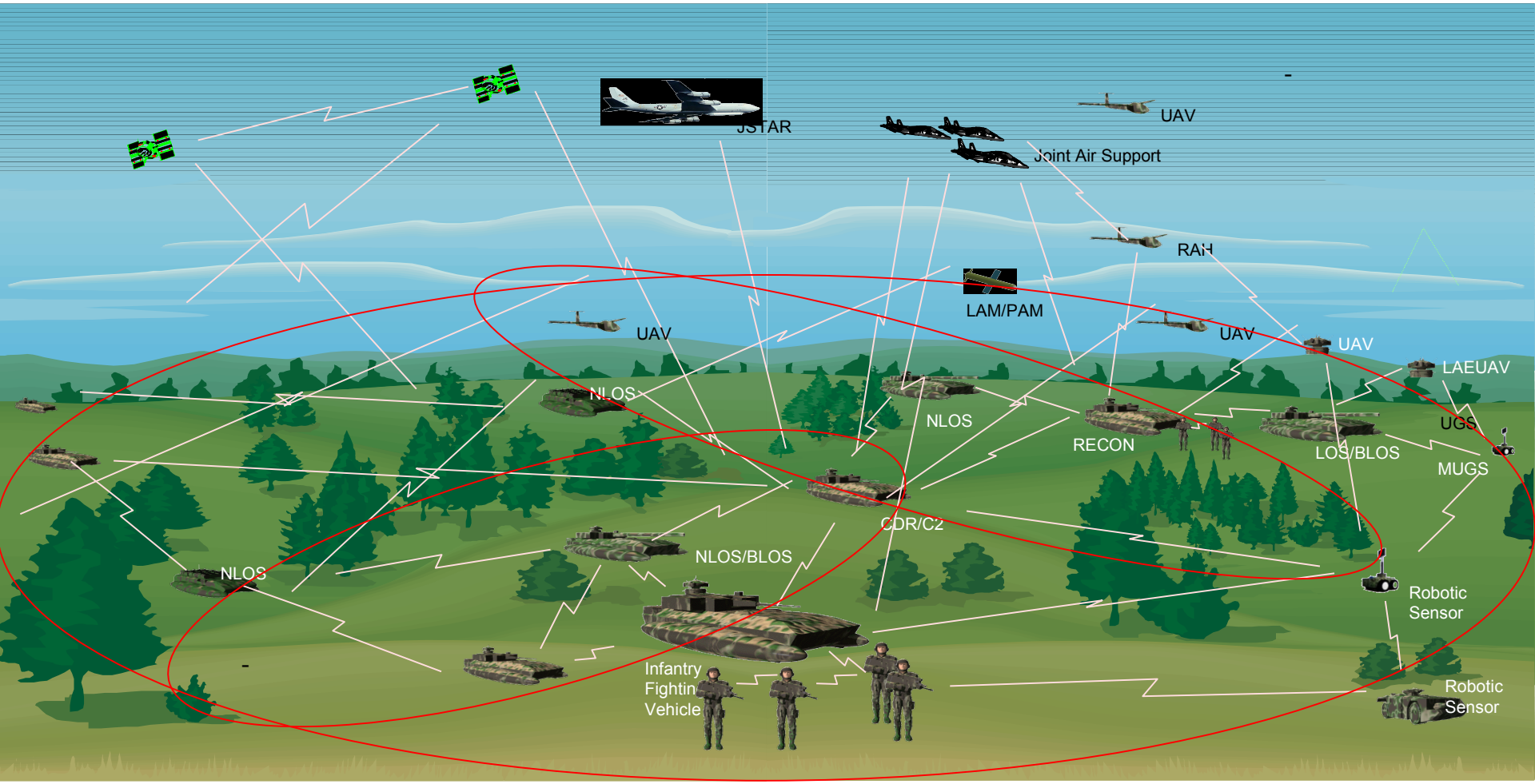
The doctrine

- 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-syncronization
    - Increase in agility and effectiveness

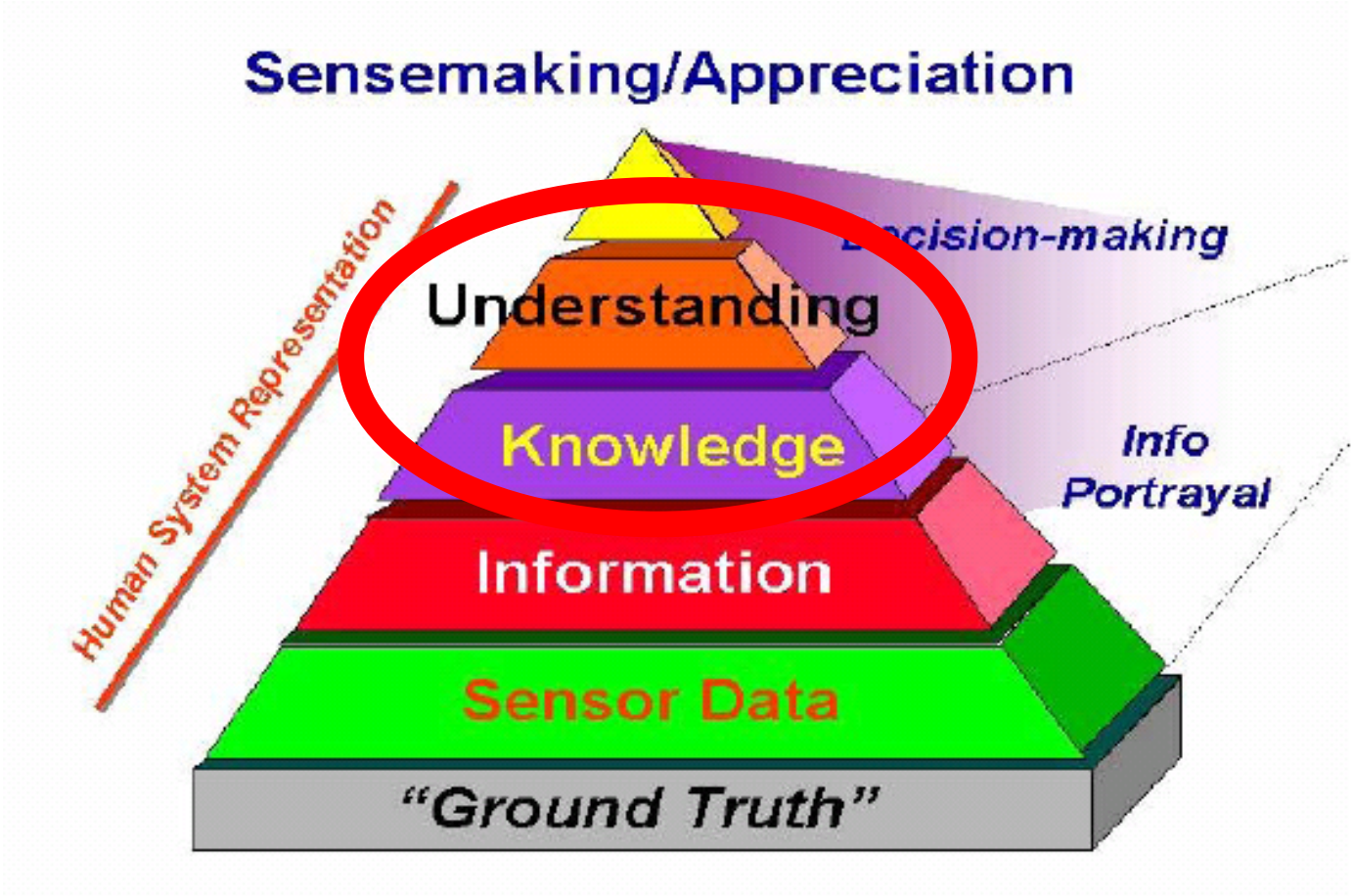
Shared Situational Awareness

- Information
  - Data
  - Information
  - Understading
  - 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

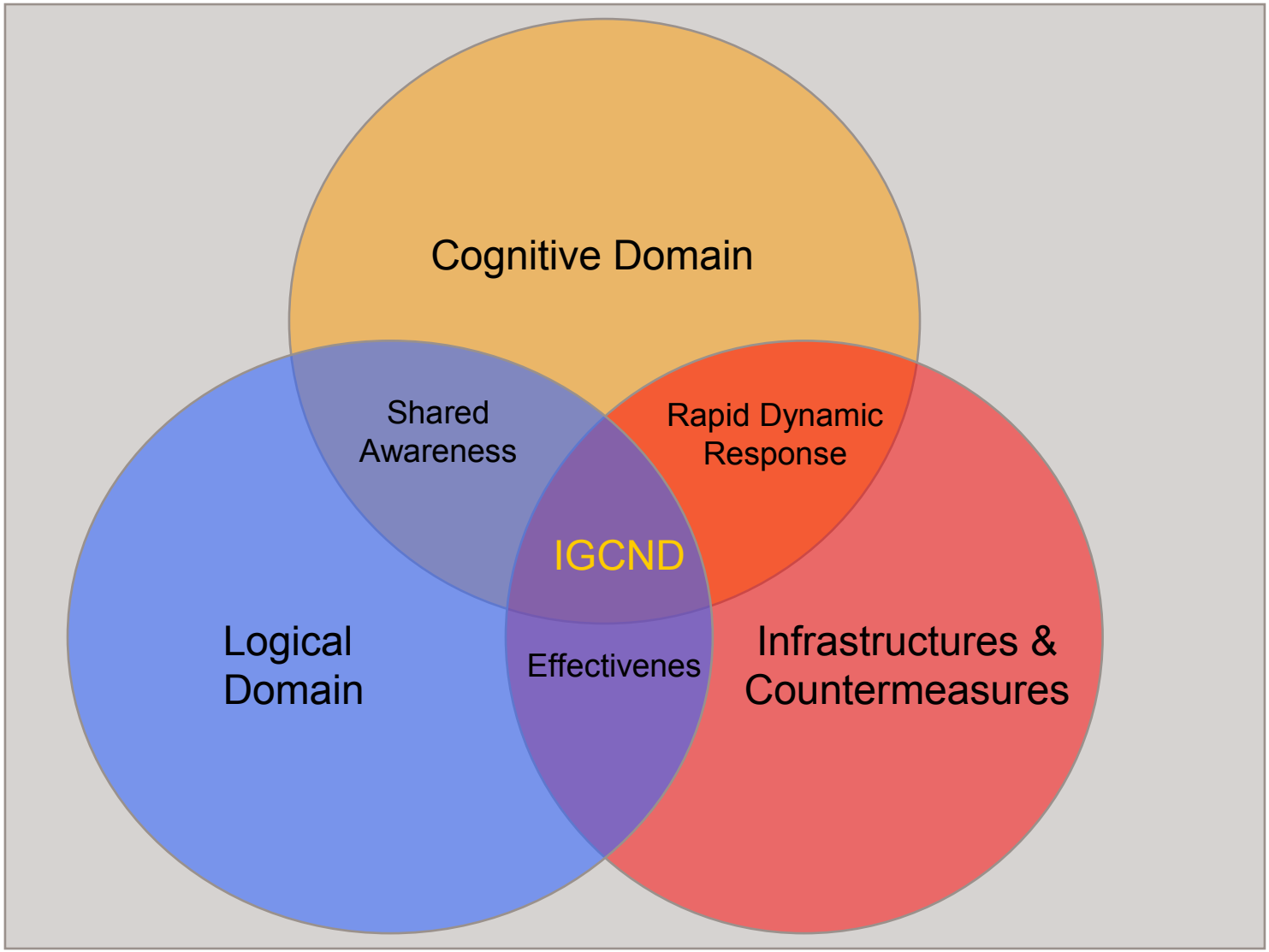
Digital Battlefield



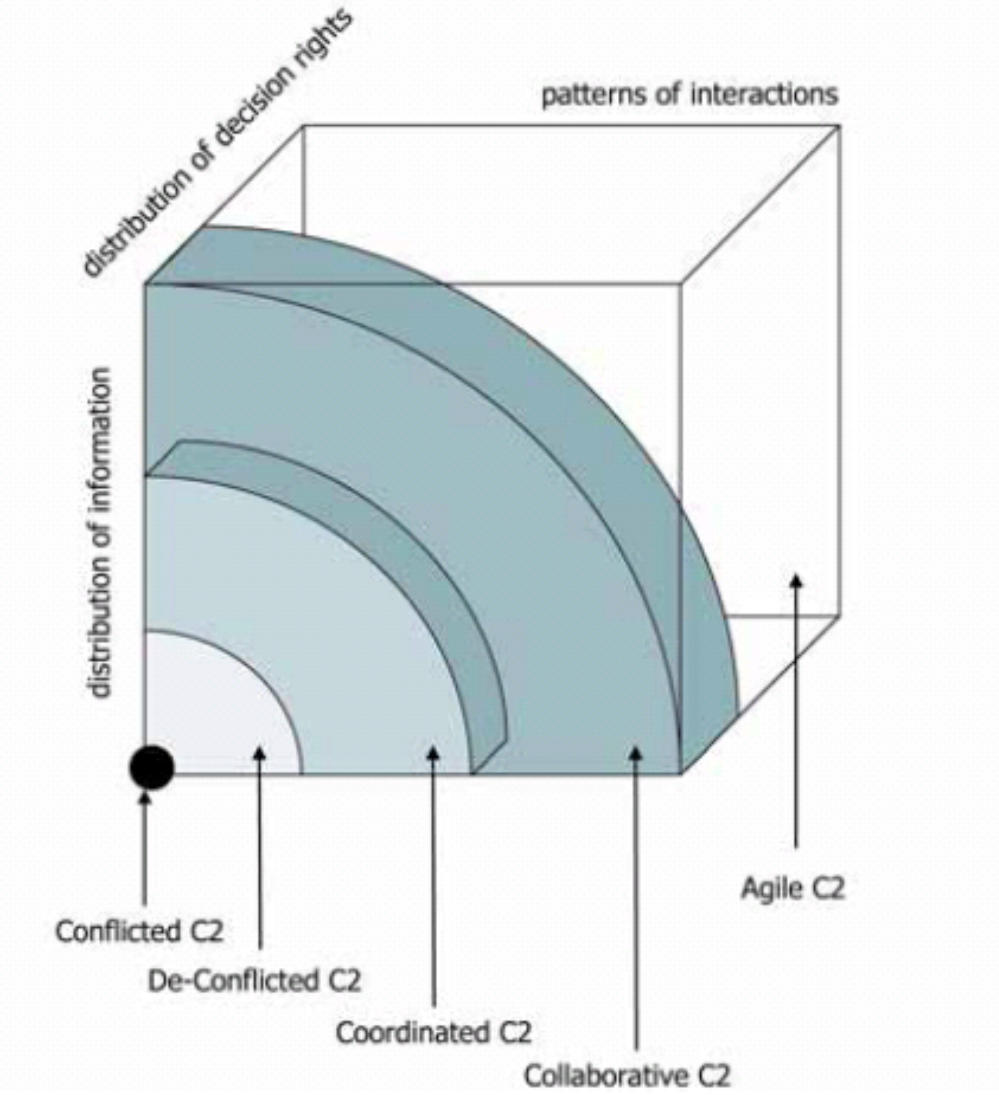
Cognitive Pyramid



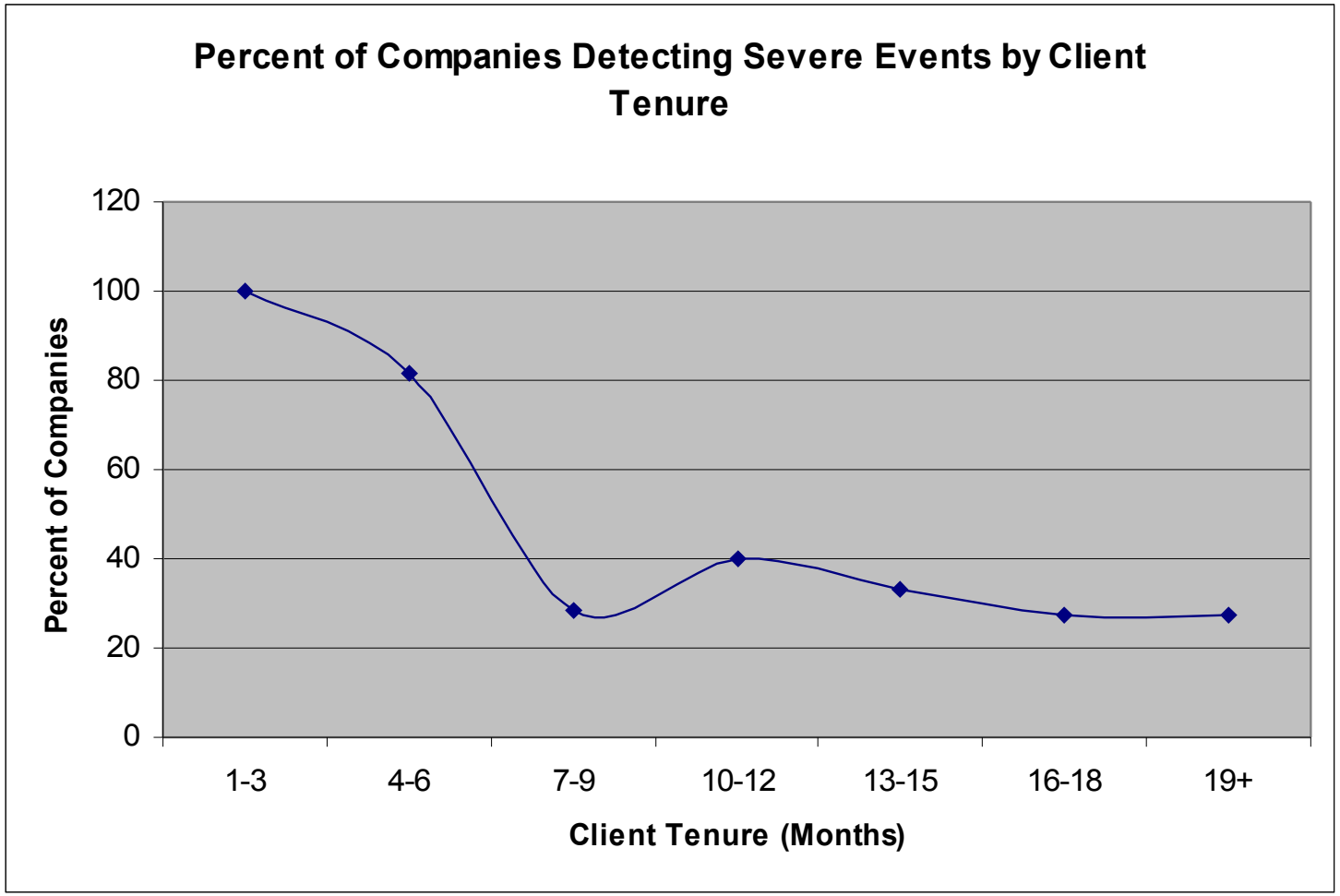
Symantec IGCND Model



C2 Maturity Level based on Distribution of Information



Increased Shared Situational Awareness



Source:Symantec Managed Security Services

Warning, advice & reporting point

symantec™

Confidence in a connected world.

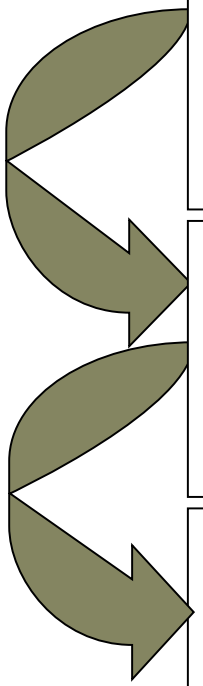
The UK Experience:
The WARP Trusted Information Sharing model

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'.

WARP
Warning, advice & reporting point

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.

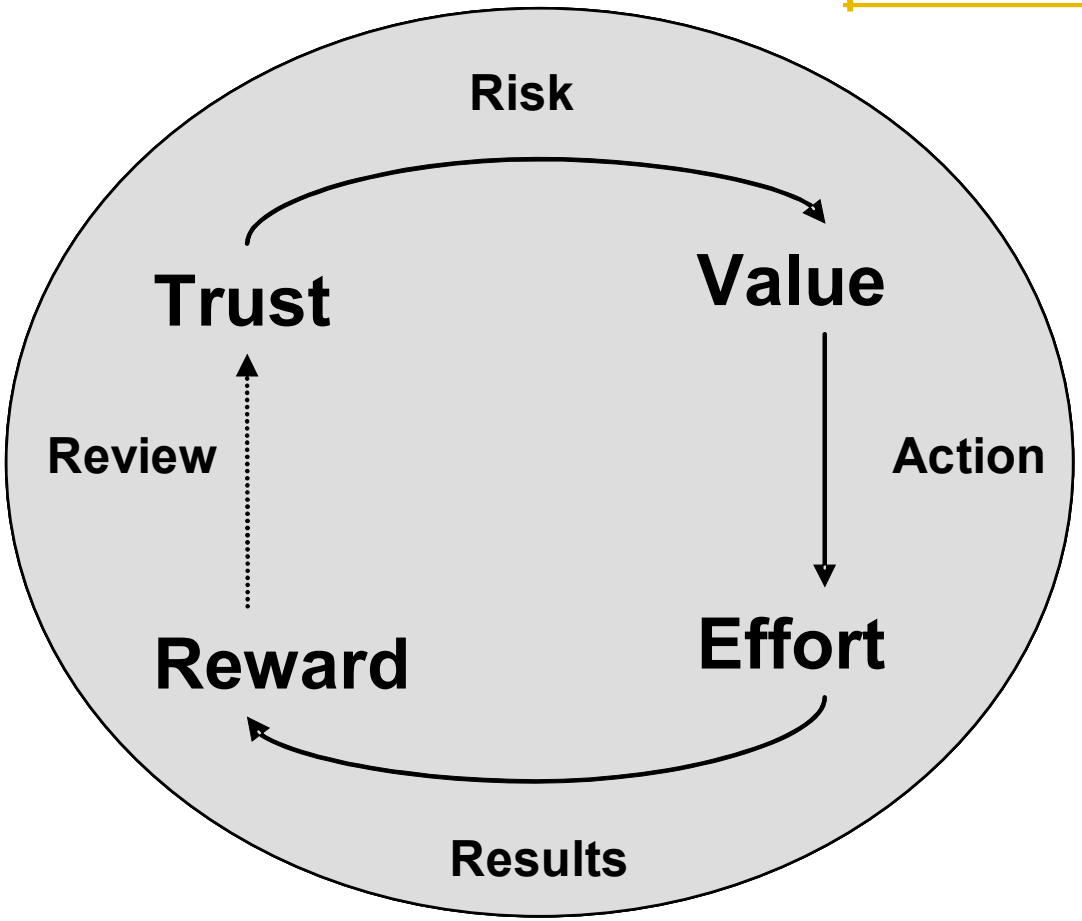
Stage 3: Trusted Sharing

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

WARP
Warning, advice & reporting point

Sharing Model – by Mandy Messenger

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

WARP
Warning, advice & reporting point

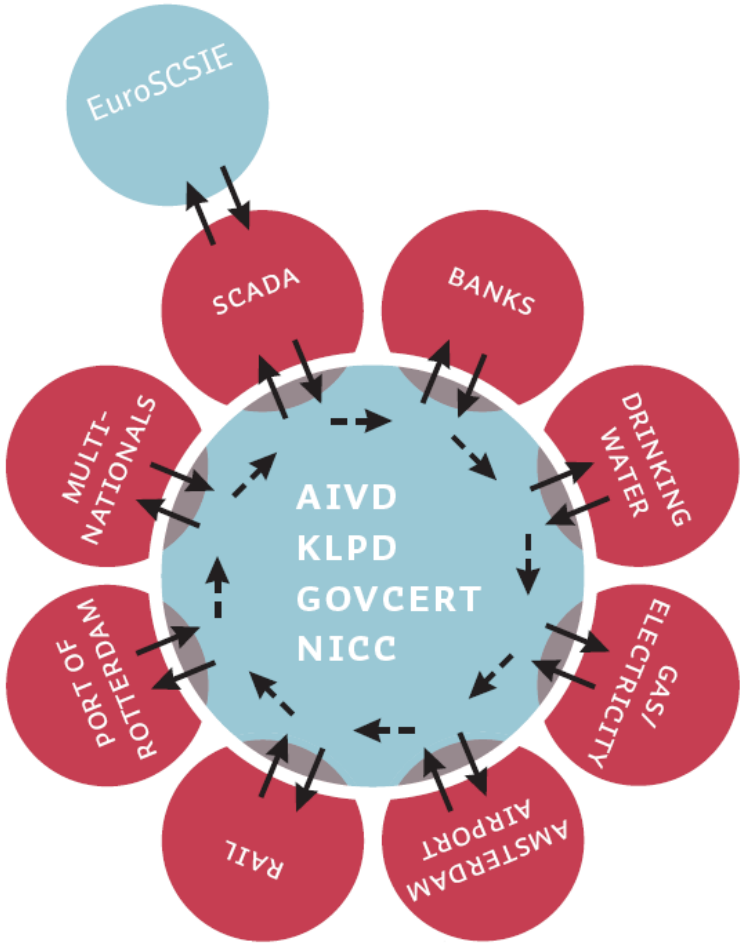
symantec™

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



symantec™

Confidence in a connected world.

European Initiatives and Information Assurance Messaging Framework

European Program for CI Protection

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

Some early results

- 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

Conclusion

- 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

symantec™

Confidence in a connected world.

Information Assurance Messaging Framework

Information Assurance Messaging Framework (IAMF)

- 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

IAMF: Main areas

- Architectures
  - Hierarchical vs Peer to Peer
- Issues
  - Common structures and Metrics
    - Management of Unstructured data
  - Sector Specific requirements
  - How to manage heristic approach
  - Anonymization
  - Language
  - Define the correct role of Governments, Law Enforcements, National Agencies and European Institutions
  - Common interfaces
  - Management of Sensitive Data

IAMF: International Informatin Sharing

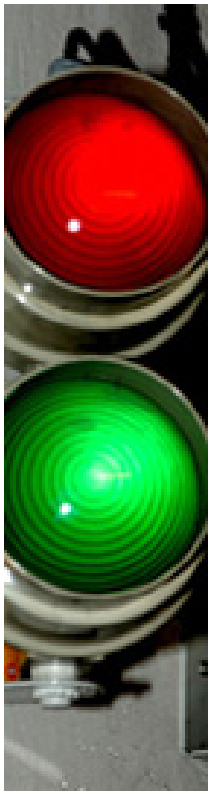
- Actors Involved
  - National and Critical Infrastructures
  - Sector specific organizations/associations/communities
  - Research and Academia
  - EU Member States Organizations
  - European Commission
  - Other Governments
- Issues
  - Communication Standards
  - Trust
  - Classification and Trusted Controlled Distribution
- Advantages: too many!

Managing Sensitive Data

- **Information sharing is top priority for federal CIOs, says Pentagon official**
- Information sharing is the "top imperative" of federal chief information officers, said a top Defense Department IT official on Monday. But progress will be stifled as long as agencies regard **information sharing and security as mutually exclusive**, said the Pentagon's deputy chief information officer

Managing Sensitive Data

- Unclassified but controlled data
  - Sensitive documents, but unclassified
  - Adoption of the Traffic Light Protocol
- Controlled Distribution through the **Traffic Light Protocol**
  - White: Public, can be published on the Internet
  - Green: Public, but not to be published on the Internet
  - Amber: confidential, can be disclosed with other emplyees in the same company/organization of the recitipent
  - Red: confidential, cannot be disclosed



Thank You!

Andrea Rigoni

EMEA Strategic Team – Director of Critical Infrastructure Protection

Andrea_Rigoni (at) Symantec.com

GSM +39 335 6954784