IN THE NAME OF GOD

Sharing Analytics of Data Monitored and Analysed

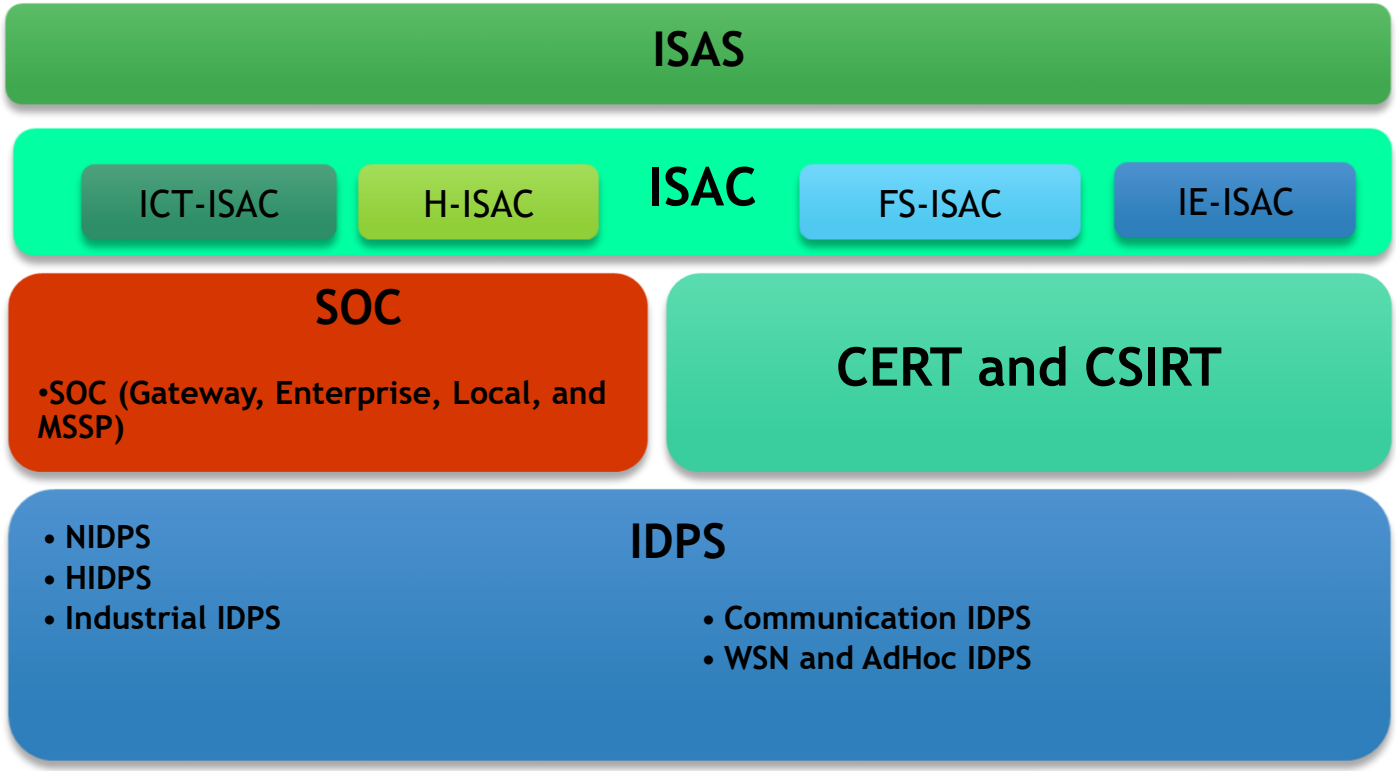
Hossein Gharaee

IRAN Telecom Research Center (ITRC)

Agenda

- Security Operations Technologies
- Information Sharing
- ISAC
- Architecture For Cyber Sharing System
- ISAS

Security Operations Technologies



Information Sharing

- Closed Community. Unless authorized for public disclosure, information is shared only within the trust community. Strict rules are enforced. This:
  - prevents information regarding methods of intelligence gathering and response from being exposed to blackhats,
  - reduces the contribution to evolutionary pressure on malware, trojans, etc.,
  - prevents unauthorized or unintended disclosure concerning institutions involved in incidents, and
  - protects identities of individuals involved in response
- Protected Identities: Unless otherwise necessary, the identities of machines, institutions, or people involved in incidents are shared only to the sites involved.

Information Sharing

National Cybersecurity and Communications Integration Center

- DHS NCCIC is a 24x7 cyber situational awareness, incident response, and management center and a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement

- The NCCIC leads the protection of the federal civilian agencies in cyberspace, provides support and expertise to critical infrastructure owners and operators, and works with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide information to SLTT governments

Incident Response

Multi-State Information Sharing and Analysis Center (MS-ISAC)

- Membership includes all 50 States and over 1000 local government organizations, U.S. territories and tribal nations
- Supports CS&C's efforts to secure cyberspace by disseminating early warnings of cyber threats to SLTT governments
- Shares security incident information and analysis
- Runs a 24-hour watch and warning security operations center
- Provides Albert II Intrusion Detection

- If there is a suspected or confirmed cyber incident that:
  - Affects core government functions;
  - Affects critical infrastructure functions;
  - Results in the loss of data, system availability; or control of systems; or
  - Indicates malicious software is present on critical systems.

Information Sources

- Network instrumentation and sensors
  - Abilene netflow
  - Arbor Networks Peakflow SP
  - Darknet, honeypots
  - Global NOC operational monitoring systems
- Direct reconnaissance
- Information sharing relationships
  - Private network security collaborations
  - Members
  - Daily security status calls with ISACs and US-CERT
  - Backbone network and security engineers
  - Vendors, relationships and monthly ISAC conferences
  - Relationships to national CERTs

Information Products

- The **Daily Weather Report** provides an aggregate-level analysis aimed to help situational awareness and to provide actionable protection information.
- **Alerts** provide critical, timely, actionable protection information concerning new or increasing threat.
- **Notifications** identify specific sources and targets of active threat or incident involving member networks.
- **Threat Information Resources** provide information regarding known active sources of threat.
- **Advisories** inform regarding specific practices or approaches that can improve security posture.
- **Monitoring** views provide aggregate information for situational awareness.

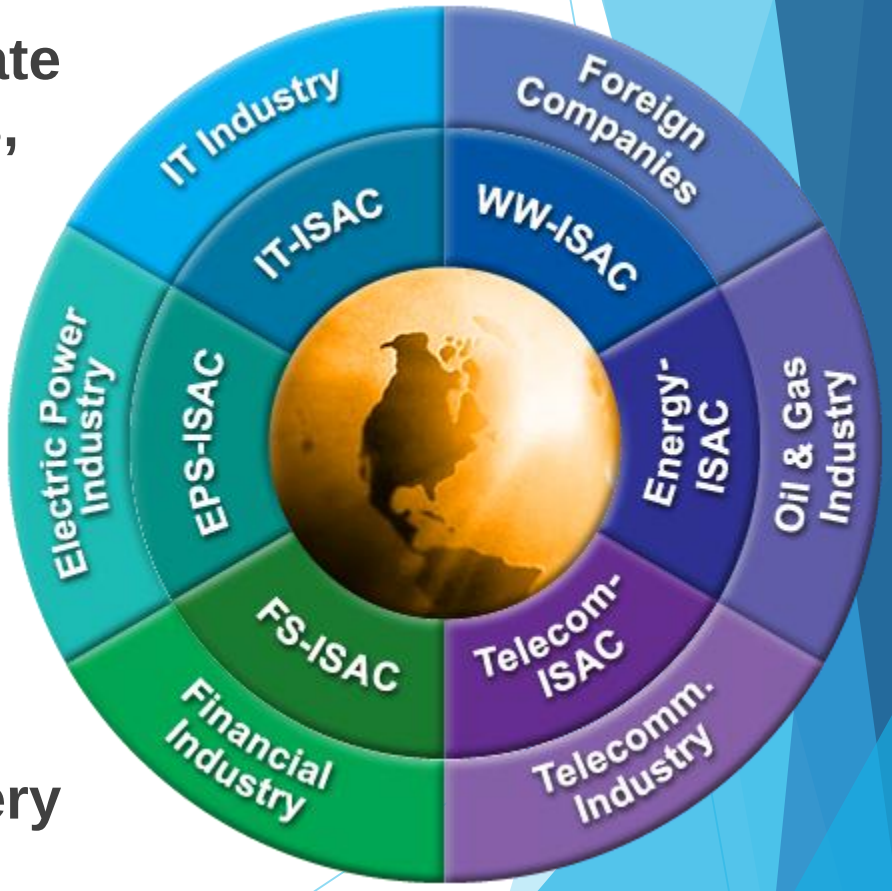
What is ISAC?

- ISACs are trusted entities established by Critical Infrastructure Key Resource (CI/KR) owners and operators to provide comprehensive sector analysis, which is shared within the sector, with other sectors, and with government.
- ISACs take an all-hazards approach and have strong reach into their respective sectors, with many reaching over 90 percent penetration. Services provided by ISACs include risk mitigation, incident response, alert and information sharing.
- The goal is to provide users with accurate, actionable, and relevant information. Member benefits vary across the ISACs and can include: access to a 24/7 security operations center, briefings, white papers, threat calls, webinars, and anonymous CIKR Owner/Operator reporting.
- *NIPP 2013:* Operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure.
- ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders.

Information Sharing and Analysis Centers (ISACs)

Vital part of Critical Infrastructure Protection (CIP)

- **Gather, analyze, and disseminate information on security threats, vulnerabilities, incidents, countermeasures, and best practices**
- **Early and trusted advance notification of member threats and attacks**
- **Organized by industry: cross-sector awareness, outreach, response and recovery**



ISAC Futures

- A Higher Education ISAC with a broader service set is needed, to deal with other campus security issues (system, virus, assessment, etc.)
- REN-ISAC may be/could be expanded to encompass these services

Critical Infrastructure Protection Challenges

- **Government in transition/turmoil**
- **New sectors**
- **Physical and cyber strategies to merge**
- **War on terrorism**
- **Balancing budgets/priorities**

Why ISACs?

- Trusted entities established by CI/KR owners and operators.
- Comprehensive sector analysis
- Reach-within their sectors, with other sectors, and with government to share critical information.
- All-hazards approach
- Threat level determination for sector

Why ISACs?

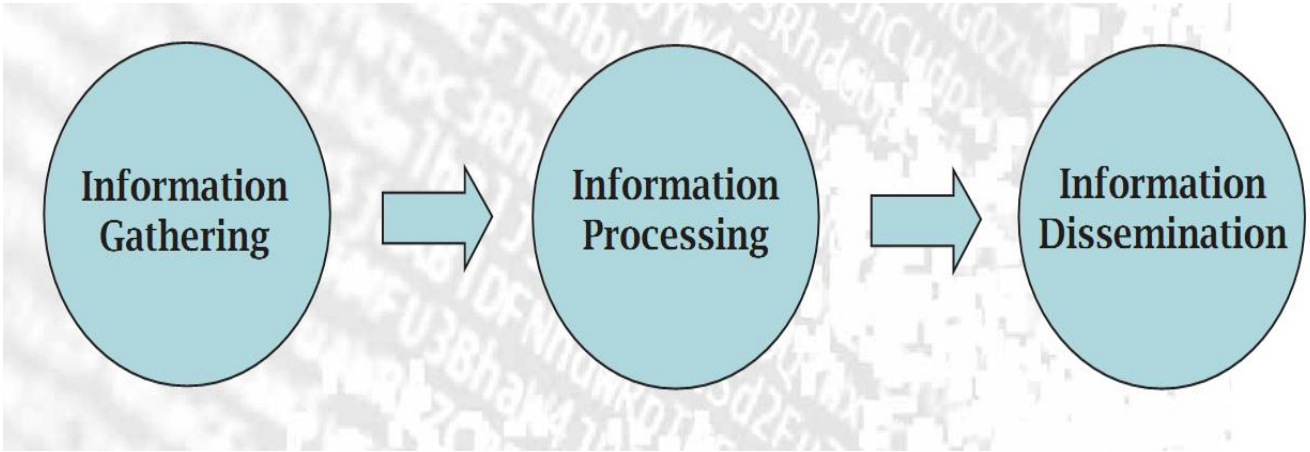
- Operational services such as risk mitigation, incident response, and information sharing
- Fast response on accurate, actionable and relevant information
- Situational awareness
- Empower business resiliency through security planning, disaster response and recovery execution.
- Most ISACs, by definition, have 24/7 threat warning, incident reporting capabilities

Information Types in ISAC

- Threat
- Risk
- Vulnerability
- Attack
- Incident
- Reports (national, International, …)

ISAC Functionalities

Generating, Acquiring, Processing, Analyzing, And Disseminating (DoD)



Beliefs necessary for sharing cyber-security information

- I know that my information is important and urgent
- I know that what I share will help others
- I know I am trusted by my organization
- I know how to get the information to the right people
- I know I can control what happens with what I share.
- I know they will all act with my interests at heart.
- I know others will reciprocate

enisa\Mandy.pdf

Benefits

- Data sharing
  - **Trends:** Retrodictive cyber statistics across the OECD
  - **Anti-crime measures:** Cyber crime targets, vectors, methods, counter-measures
  - **Early warning:** Integrate detection, signatures and anomaly recognition for analysis
  - **Closing defensive gaps:** Comparison of defensive coordination and best practices
  - **IP Protection:** Detection and prevention of industrial espionage
- Expertise integration
  - Focus collective expertise on important cyber data and analysis tasks
- Collaboration and coordination
  - Reduce defensive gaps across the OECD
  - Build crisis response capacity
- Research and development coordination
  - Leverage and combine task-relevant national expertise

The ISACs (Cont.)

- **ISAC Benefits:**
  - **Early notification**
  - **Relevant information**
  - **Industry-wide vigilance**
  - **Subject matter expertise**
  - **Anonymous information sharing**
  - **Trending, metrics, benchmark data**

REN-ISAC Activities

- A vetted trust community for R&E cybersecurity
- Information-sharing and communications channels
- Information products aimed at protection and response
- Participation in mitigation communities
- Incident response
- 24x7 Watch Desk (ren-isac@iu.edu, +1 317 274 6630)
- Improvement of R&E security posture
- Participate in other higher education and national efforts for cyber infrastructure protection

US ISACs

- 18 Defined Sectors:

- Agriculture and Food
- Defense Industrial Base
- Energy
- Healthcare & Public Health
- Banking & Finance
- Water
- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Communications
- Postal & Shipping
- Transportation Systems
- Government Facilities
- Emergency Services
- Nuclear Reactors, Materials & Waste
- Information Technology
- National Monuments & Icons

US ISACs

Communications ISAC (NCC), Electric Sector ISAC (IS-ISAC), Emergency Management & Response ISAC (EMR-ISAC), Financial Services, ISAC, Health ISAC (NH-ISAC), Highway ISAC (First Observer), IT ISAC

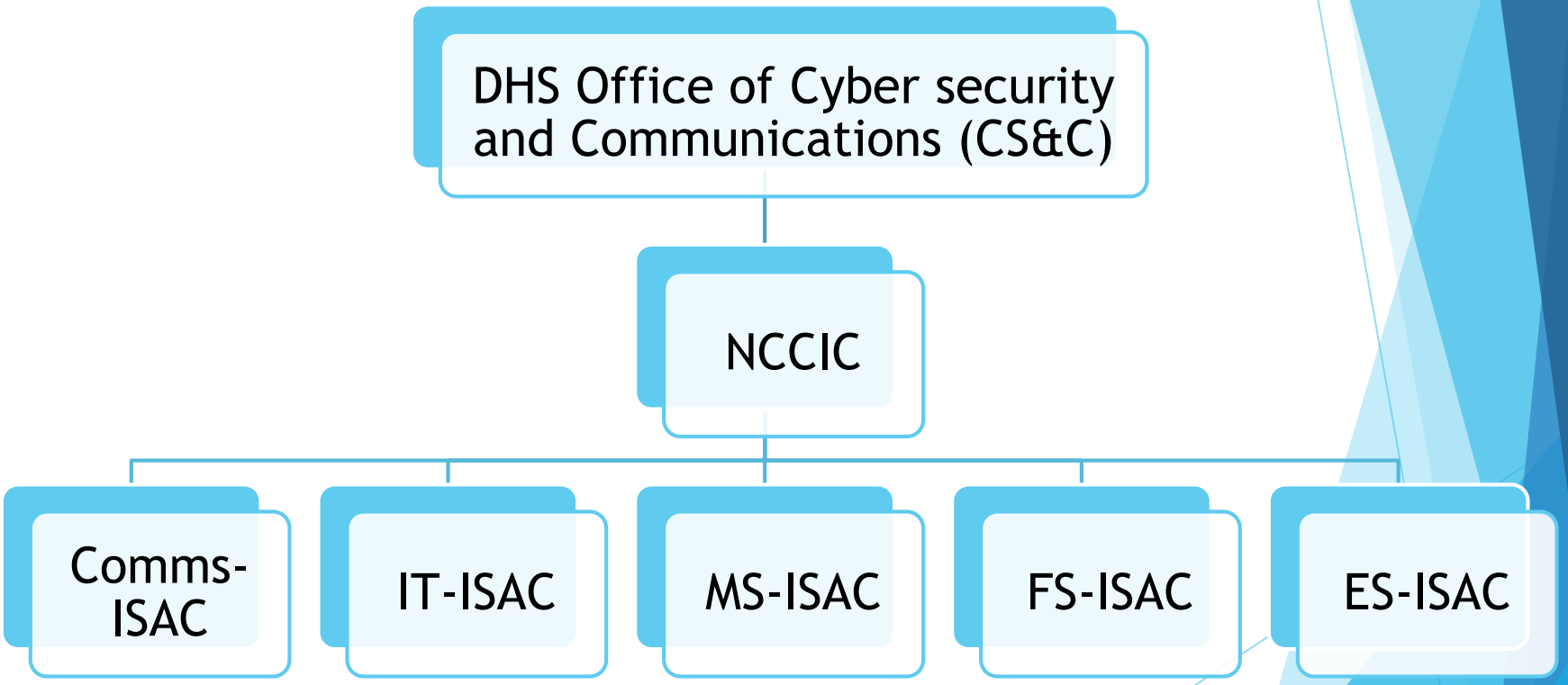
Maritime Security Council ISAC, Multi-State ISAC, Nuclear ISAC (NEI), Public Transportation ISAC (APTA), Real Estate ISAC, Research & Education Networking ISAC (REN-ISAC), Supply Chain ISAC (SC-ISAC)

Surface Transportation ISAC (ST-ISAC), Water ISAC, Chemical Sector Coordinating Council, Defense Security Information Exchange, Oil and Natural Gas Coordinating Council, Partnership for Critical Infrastructure Security, Regional Consortium Coordinating Council

National Council of ISACs

- The National Council of ISACs activities include: drills and exercises, hosting a private sector liaison at the Department of Homeland Security (DHS) National Infrastructure Coordinating Center (NICC) during incidents of national significance, emergency classified briefings, and real-time sector threat level reporting.
- The group also sponsors an annual Critical Infrastructure Protection (CIP) Congress to bring together the critical infrastructure community for networking, learning and addressing issues of concern to CIKR stakeholders.

ISAC Hierarchy



US IT-ISAC members

Organizations	Type
Conagra ، Cargill ،Bunge،.BAE Systems, Inc ،Arrow Electronics ،Intel Corporation ، Informatica ،Hewlett Packard Enterprise ، Oracle Corporation ، NSS Labs ، Mimecast	Basic
CSC, HCA ،Fire Eye ، Cisco Systems ، ،.Afilias USA, Inc ،Monsanto،Netflix ،Juniper Networks، ،Healthcare Jabil Neustar ، Trend Micro, USA	Silver
Cimpress ،.BrandProtect, Inc ،Box.com ،Black Box ،Acquia ،.Fastly, Inc ،Dell Technologies ،Commvault ،AT&T ، ،.USA, Inc , ، ،Foreground Security ، ،InfoReliance ,Nuance ،DocuSign IBM Lockheed Martin Corporation	Bronze

Trust Community for R&E Cybersecurity

- A trusted community for sharing sensitive information regarding cybersecurity threat, incidents, response, and protection, specifically designed to support the unique environment and needs of higher education and research organizations.
- Membership is oriented to permanent staff with organization-wide responsibility for cybersecurity protection or response at an institution of higher education, teaching hospital, research and education network provider, or government-funded research organization.

Recent new member services

- BotNet Tracker service: provides members with a rich list of known botnet command and control domain names and IP addresses.
- Secure IRC: provides a means for members to securely communicate in real time.
- Secure Wiki: provides a controlled access space for members to directly share information and documentation.
- TechBurst Webcasts: 30-minute webcasts on technical topics of concern to the R&E security community. Last month: *Botnet Detection Using DNS Methods*, coming up: *Introduction to NetFlow*, and *Advanced Netflow Topics*

New services in pilot phase

- Pilot/trial of centralized Arbor Networks Peakflow SP service provided to gigapops.
  - Central collector receives netflow from participating gigapop
  - Integrated with the overall Abilene backbone Arbor
  - Segmented, connector-specific views provided to participants through Arbor Customer Portal feature
  - DDoS and worm/malware automated threat feed features
  - Hardware is installed
  - If you're interested and/or want to participate see Doug Pearson < dodpears@ren-isac.net >

New services on immediate horizon

- Shared Darknet Project
  - A wide-aperture darknet sensor
  - Members who run local darknets send their collector data (minus the hits from their own institution) to REN-ISAC. Data is analyzed to identify compromised machines by IP address, destination ports involved, the number of "hits" seen, and timestamps of the activity.
  - The REN-ISAC sends notifications of infected machines to source institutions and develops reports of aggregate activity and trends.
- Warez IRC servers
  - List of known warez IRC servers

New services on immediate horizon

- Passive DNS replication
  - Useful to determine domain name for miscreant servers placed on hacked/infected machines. Similar to RUS-CERT service*, but with a view to what US R&E is experiencing.
  - * http://cert.uni-stuttgart.de/stats/dns-replication.php
- Vendor relationships
  - Representative relationship with Microsoft Security Resource Center.
- Regional Security Groups
  - Facilitate organizational interactions of regional security working groups, particularly aimed to assist new/developing groups.

Summary of Services

Needs	DHS Services	Summary
Identifying and Limiting Vulnerabilities	Cyber Hygiene Scanning	Automated, recurring scans of internet facing systems that provide the perspective of the vulnerabilities and configuration errors that a potential adversary could see
	Risk and Vulnerability Assessment	• Penetration testing • Social engineering • Wireless access discovery • Database scanning • Operating system scanning
Assessing Threats and Sharing Information	NCCIC Tips and Alerts	Provides alerts, analysis reports, bulletins, best practices, cyber threat indicators, guidance, points-of-contact, security tips, and technical documents to stakeholders
	MS-ISAC Security Tips	
Applying security expertise and best practices	Cyber Security Advisors & Protective Security Advisors	Regionally located personnel who engage state and local governments, election crime coordinators, and vendors to offer immediate and sustained assistance, coordination, and outreach to prepare and protect from cyber and physical threats.
Incident Response	NCCIC	24x7 cybersecurity operations centers that maintained close coordination among the private sector, government officials, the intelligence community, and law enforcement to provide situational awareness and incident response, as appropriate.
	MS-ISAC	

Designation of Critical Infrastructure Sectors

situational awareness

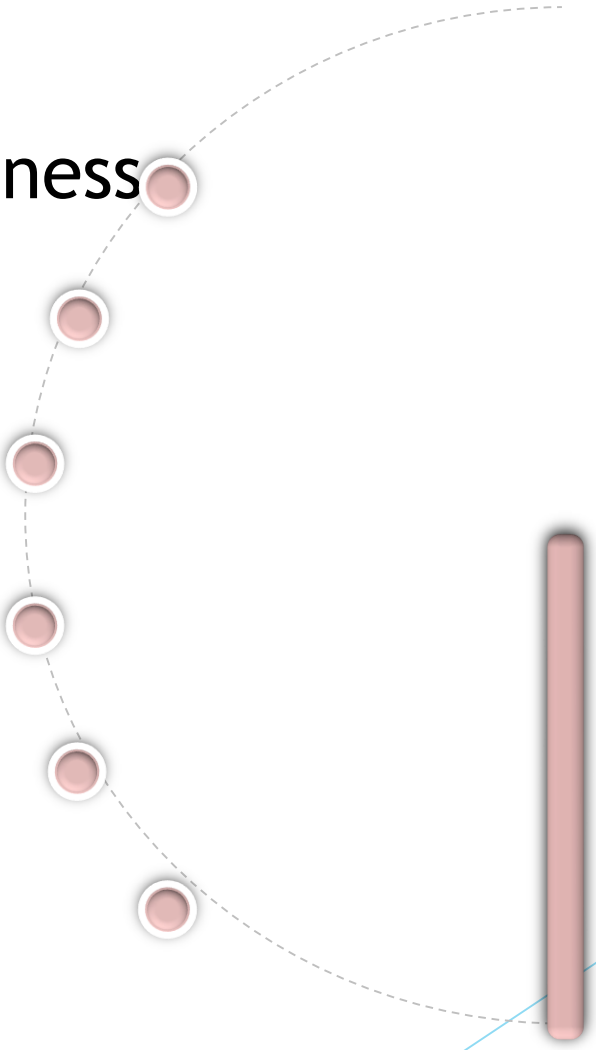
National and International Cybersecurity Strategies

Cybersecurity Centers and Their Responsibilities and Tasks

Situational Awareness Models Supporting Strategic Decision-Making Processes

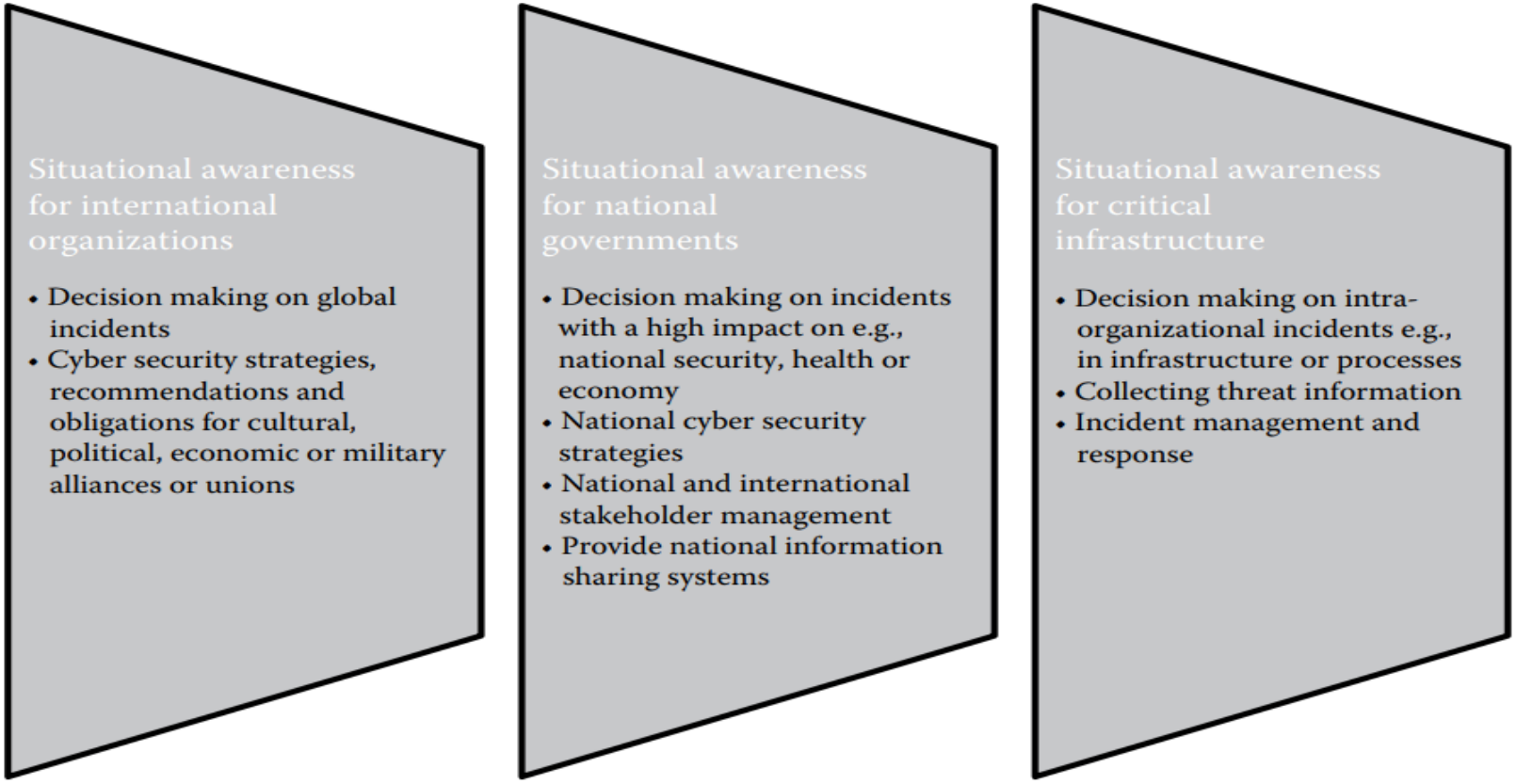
Information and Sources for Situational Awareness at the National Level

Conclusion

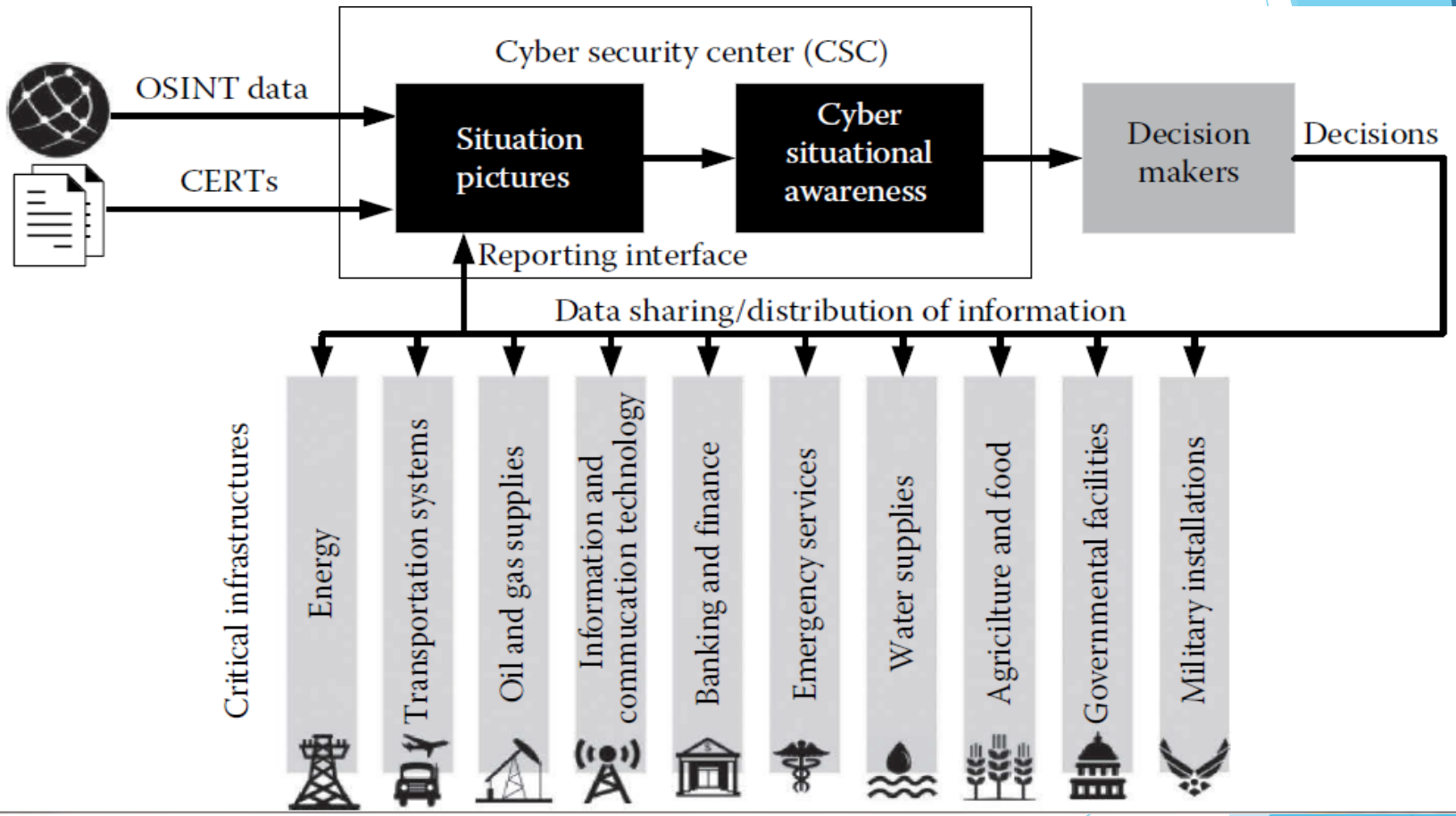


situational awareness

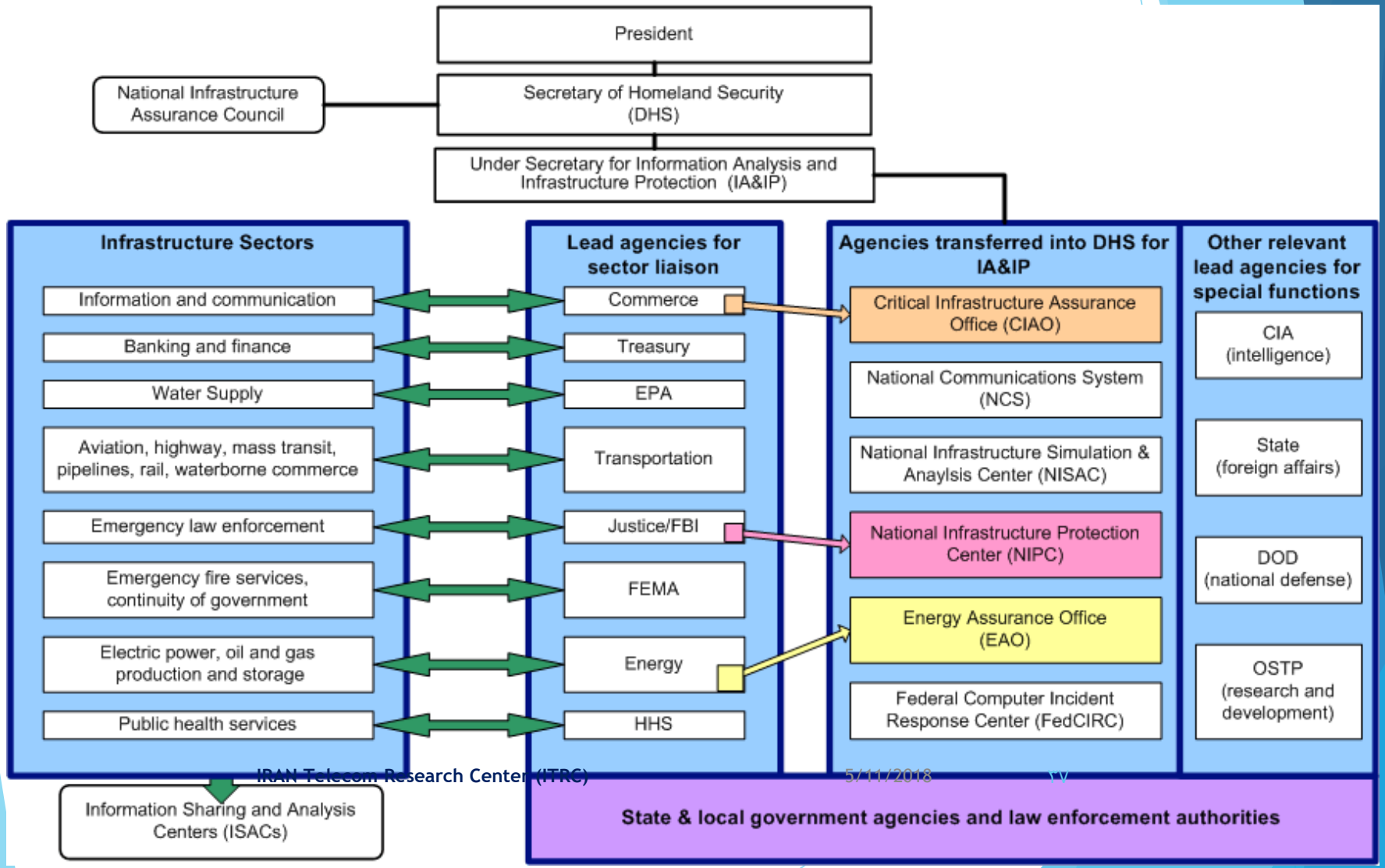
- The perception of the element in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future



- **National cybersecurity centers (CSCs or NCSCs)**
- increase cyber resilience of nations as well as the coordination and provision of information sharing systems between national stakeholders and governments and other related activities.
- CSCs are often called situation centers or IT incident response and management centers.
- **Stakeholders**
- CSCs aim to coordinate (cybersecurity) activities with different stakeholders—from vendors and critical infrastructure providers to political parties and organizations.
- CSCs can enable and provide measures to ensure the information exchange of cyber threat information between stakeholders.
- CSCs interact for example with decision makers that require a certain Cyber Common Operating Picture to make decisions.
- National computer emergency response teams (CERTs) or CSIRTs are often the first contact for organizations about cyber incidents and distribute information on publicly known vulnerabilities.
- **Tasks and Responsibilities**
- Table 6.2 contains recommendations of ENISA for possible services and tasks of national CSIRTs.


Cyber security center (CSC)
OSINT data
CERTs
Situation pictures
Cyber situational awareness
Decision makers
Decisions
Reporting interface
Data sharing/distribution of information
Critical infrastructures
Energy
Transportation systems
Oil and gas supplies
Information and commucation technology
Banking and finance
Emergency services
Water supplies
Agricilture and food
Governmental facilities
Military installations

CIP Relationship Transitions



U.S. CIP Effort: Sector Lead Agencies

- Commerce — Information and Communications
- Treasury — Banking and Finance
- EPA — Water Supply
- Transportation — Aviation
- Highways (including trucking and intelligent transportation systems)
- Mass Transit
- Pipelines
- Rail
- Waterborne Commerce
- Justice/FBI — Emergency Law Enforcement Services
- FEMA — Emergency Fire Service
- Continuity of Government Service
- HHS Lab Services — Public Health Services, including Prevention, Surveillance and Personal Health Services
- Energy — Electric Power
- Oil and Gas Production and Storage
- ---

- *CIAO — Critical Infrastructure Assurance Office*
- *NIPC — National Infrastructure Protection Center*

New Sector Lead Agencies

- DHS — Information & Communications
  Transportation (aviation, rail, mass transit, waterborne commerce, pipelines, and highways (incl. Trucking & intelligent transportation systems)
  Postal and Shipping
  Emergency Services
  Continuity of Government
- Treasury — Banking and Finance
- HHS — Public Health
  Food (all except for meat and poultry)
- Energy — Electric power, oil & gas production and storage
- EPA — Water
  Chemical Industry and Hazardous Materials
- USDA — Agriculture
  Food (meat and poultry)
- DOD — Defense Industrial Base

رویکردهای تبادل اطلاعات امنیت سایبری

- دو رویکرد موجود برای تبادل اطلاعات:
  - H2H (انسان با انسان): ارتباطات سنتی بین اشخاص
  - M2M (ماشین با ماشین): خودکارسازی تبادل اطلاعات

TLP | TRAFFIC LIGHT PROTOCOL

When should it be used?	Color	How may it be shared?
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	RED 	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	AMBER 	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN 	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	WHITE 	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Agenda

- Security Operations Technologies
- Information Sharing
- ISAC
- Architecture For Cyber Sharing System

Concept

- Dramatically improve defensive understanding and coordination
  - Bias work factors for cyber attack and defense in favor of defenders
- Create an international system for sharing data about:
  - Cyber crime
  - Attack patterns
  - Best defense practices
- Motivate relevant research and international collaboration via the technical needs in a data sharing scenario
  - Rather than forward chaining from current cyber research alone (deduce scenario from security capabilities)
  - Backward chain from scenarios to enabling research (abduce technical capabilities from scenario)
- What data makes sense to share?
  - What impacts?
  - What collection issues?
  - What sequence of data domain for ramp up?

Key Questions

- **Data:** What cyber data should be shared?
  - What domains?
  - What purposes?
- **Synergies:** What synergies arise from integrating data and analysis across national boundaries?
- **Impact:** How will data sharing help participating countries?
- **Incentives:** What are the incentives for providing data?
- **Quality:** How can the integrity and quality of data be assured?
- **Availability:** How can data be made available in useful formats and in time to be relevant?
- **Risk:** How should data sharing risks be managed?
  - What risks are involved in assembling and sharing data?
  - How can data be sliced or aggregated to reduce risk?
  - How can access be controlled to reduce risks while enabling benefits? (e.g., incremental revelation)

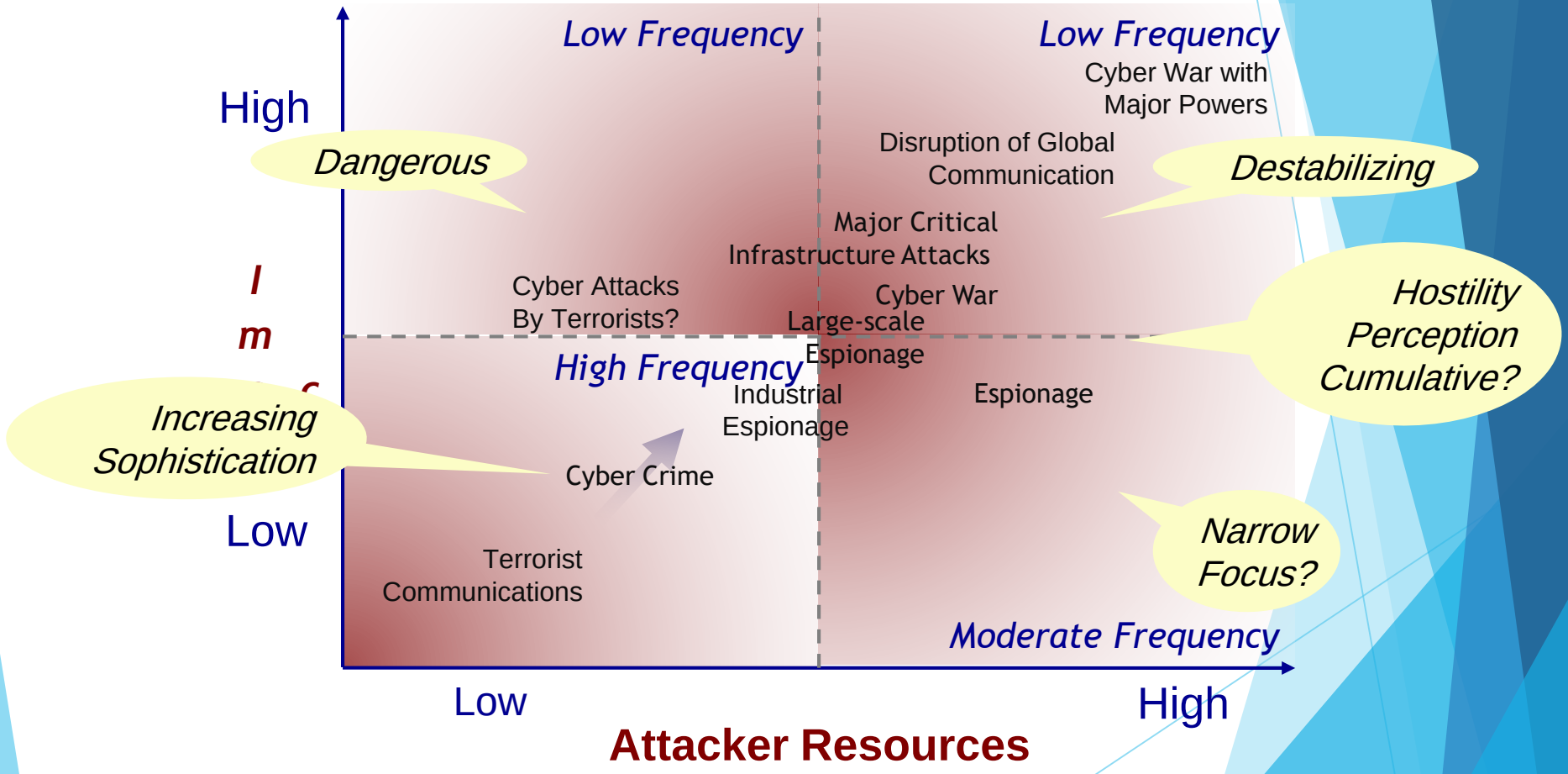
Goals

- Build shared awareness and understanding of cyber phenomena across countries
  - Employ shared data collection methodologies
  - Integrate measurements of phenomena across borders
  - Focus early on cyber crime and cyber economics
- Create comparable transnational data sets
  - Capture cyber breaches, attack patterns, best practices, defensive coordination
  - Include aggregate data on crime, black markets, economics, state-state interactions, long-term cyber-fueled transformations
- Field a cyber data sharing framework that helps countries to:
  - Collect cyber data for compatible sharing
  - Fuse data to create common situational awareness
  - Manage national legal impediments to sharing via derived or aggregate data or by recommending harmonization steps
  - Exchange derived data in real time
  - Provide mechanisms for controlled drill down needed for law enforcement, advanced persistent threats (APT) or cyber emergencies
- Develop shared collection, fusion, analysis, and response capabilities

Threat Actors And Capabilities Suggest Different Cyber Data

Threat Actors	Motive	Targets	Means	Resources
Nation States During War Time	Political	Military, intelligence, infrastructure, espionage, reconnaissance, influence operations	Intelligence, military, broad private sector	Fully mobilized, multi-spectrum
Nation States During Peace Time	Political	Espionage, reconnaissance, influence operations	Intelligence, military, leverages criminal enterprises or black markets	High, multi-spectrum, variable skill sets below major cyber powers
Terrorists, Insurgents	Political	Infrastructure, extortion	Leverage black markets?	Limited, low expertise
Political Activists or Parties	Political	Political outcomes	Outsourcing?	Limited, low expertise
Black Markets For Cyber Crime	Financial	Hijacked resources, fraud, theft, IP theft, illicit content, scams, crime for hire	Tools, exploits, platforms, data, expertise, planning	Mobilizes cyber crime networks
Criminal Enterprises	Financial		Reconnaissance, planning, diverse expertise	Professional, low end multi-spectrum, leverage of black markets
Small Scale Criminals	Financial		Leverages black markets	Low, mostly reliant on black markets
Rogue Enterprises	Financial	IP theft, influence on sectoral issues	Outsourcing to criminal enterprises?	Sectoral expertise, funding, organization

Attacker Resources and Impacts Suggest Different Cyber Data Categories



Precedents Can Inform The Architecture

- Financial Services Information Sharing and Analysis Center (FS-ISAC)
  - Organizations submit information anonymously
  - Data received by members cannot be attributed to any specific organization
  - ISAC was based on the US Center for Disease Control (CDC) model
  - ISAC was created by Global Integrity, part of SAIC
- National Cyber Forensics and Training Alliance (US)
  - Non-profit that integrates information and analysis for the financial services sector across private, public and academic communities
- Symantec Wombat Project
  - Collaborative sensors for Internet malware and attack data
- European Network & Information Security Agency
  - Collects, analyzes, disseminates data on InfoSec in pan European context
- European Public-private Partnership For Resilience
  - Critical information infrastructure protection
- DHS Predict (US)
  - Legal framework for sharing cyber data with US
  - International framework in progress
- Others?

Political and Legal Concepts

- Political and legal barriers
  - Divergent legal requirements
  - Government procedures for handling classified information
  - Export controls
  - Proprietary data
  - Privacy
- How can progress be made quickly before legal and regulatory harmonization is addressed? (10 years or more?)
  - Share derived data
  - Share patterns to be detected in 1st order data
- Create country-level fusion centers
  - Provides governments with control over national data and analysis
  - Manage drill down for exceptional cases

Key Idea: Data Generality vs. Specificity

- Data sensitivity often correlated with specificity
  - Sharing easier: Aggregate data
  - Sharing harder: Specific, identifiable data
- Three Legal frameworks
  - Aggregate data suitable for national accounts statistics
  - Intermediate data provides more structure but no revelation of identities or "private" data
  - Specific data gives full details with PPI obfuscated or not
- Specific data will likely require a PREDICT like legal framework
  - Establish framework for provider-consumer specific agreements for shared data
  - Provide special handling procedures for sensitive data
- Incremental access via general -> specific can reveal whether access is needed
  - Fine-grained security can support precise access
  - New access control model based on abstraction?

Key Idea: Fine-grained Sharing

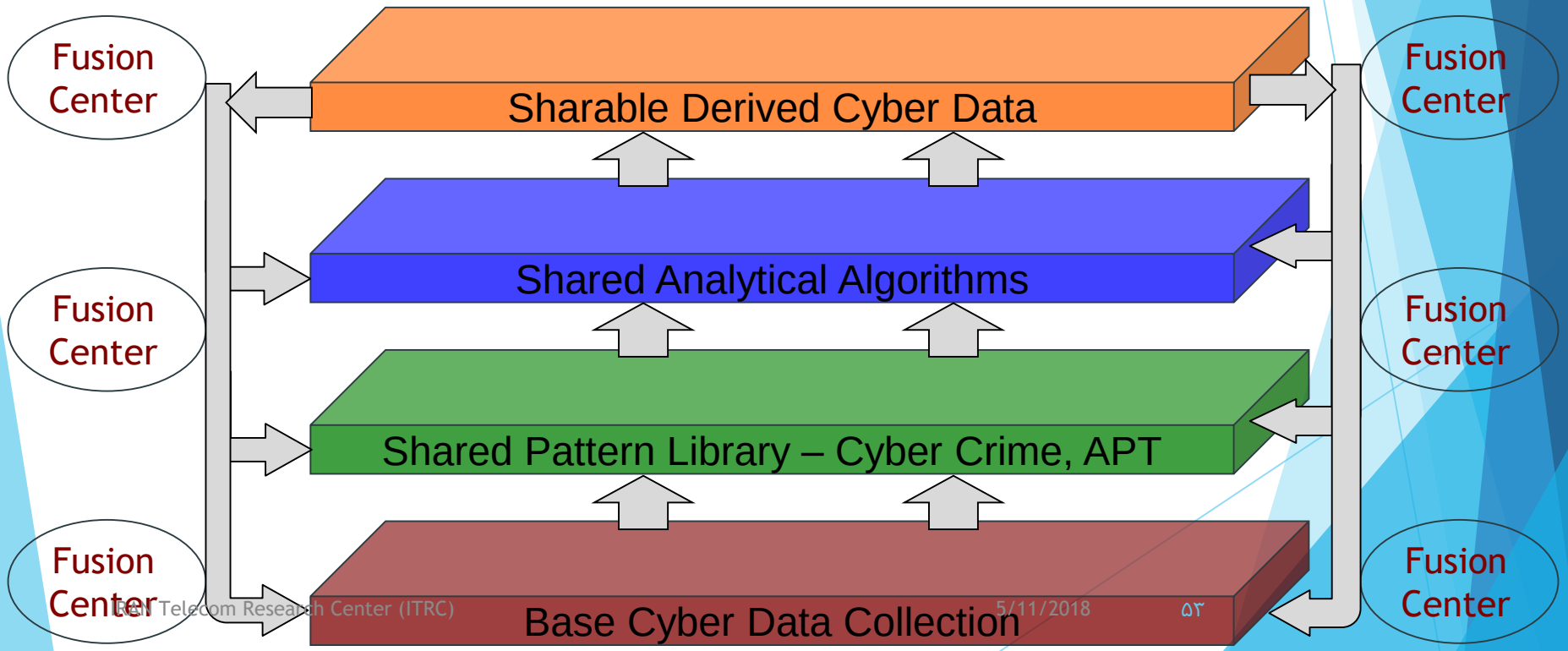
- Dimensions of data slicing
  - Sector
  - Sensitivity
  - Generality-specificity
  - Legal-regulatory rules
- Manage sharing parts of resources
  - Sub-resource labeling and access control
  - Incremental revelation to establish need to share
    - Indexes
    - General slices

Architecture

- Establish national cyber data fusion centers
  - Collect shared base data across public and private sectors
  - Apply shared algorithms for aggregation, pattern matching and creation of derived data
  - Share the derived data
  - Build redundancy into the collection mechanism to enable checking of data validity
- Link these centers together for sharing
  - Provide methods to assure the integrity of data
  - Provide appropriate access control policies
- Make data available to appropriate 3rd parties to perform value-added analysis
- Accept feedback from all participants on improvements to data collection and analysis
  - Track successes, near misses
- Tight integration with key sectors
  - Telcos, ISPs, network & computing infrastructure (implements ICT)
  - Critical infrastructures
  - Financial sector
  - Major online application infrastructure
  - IP-based sectors (industrial espionage)
  - E-business (readily accessed via Internet)

Data Sharing Architecture

Data Integrity	**Information Flow**	**Cryptography**	**Fine-grained Security**
Provenance• Metadata•	Access Control• Monitoring•	Authentication• Obfuscation•	Identifier calculus• Access & integrity control•



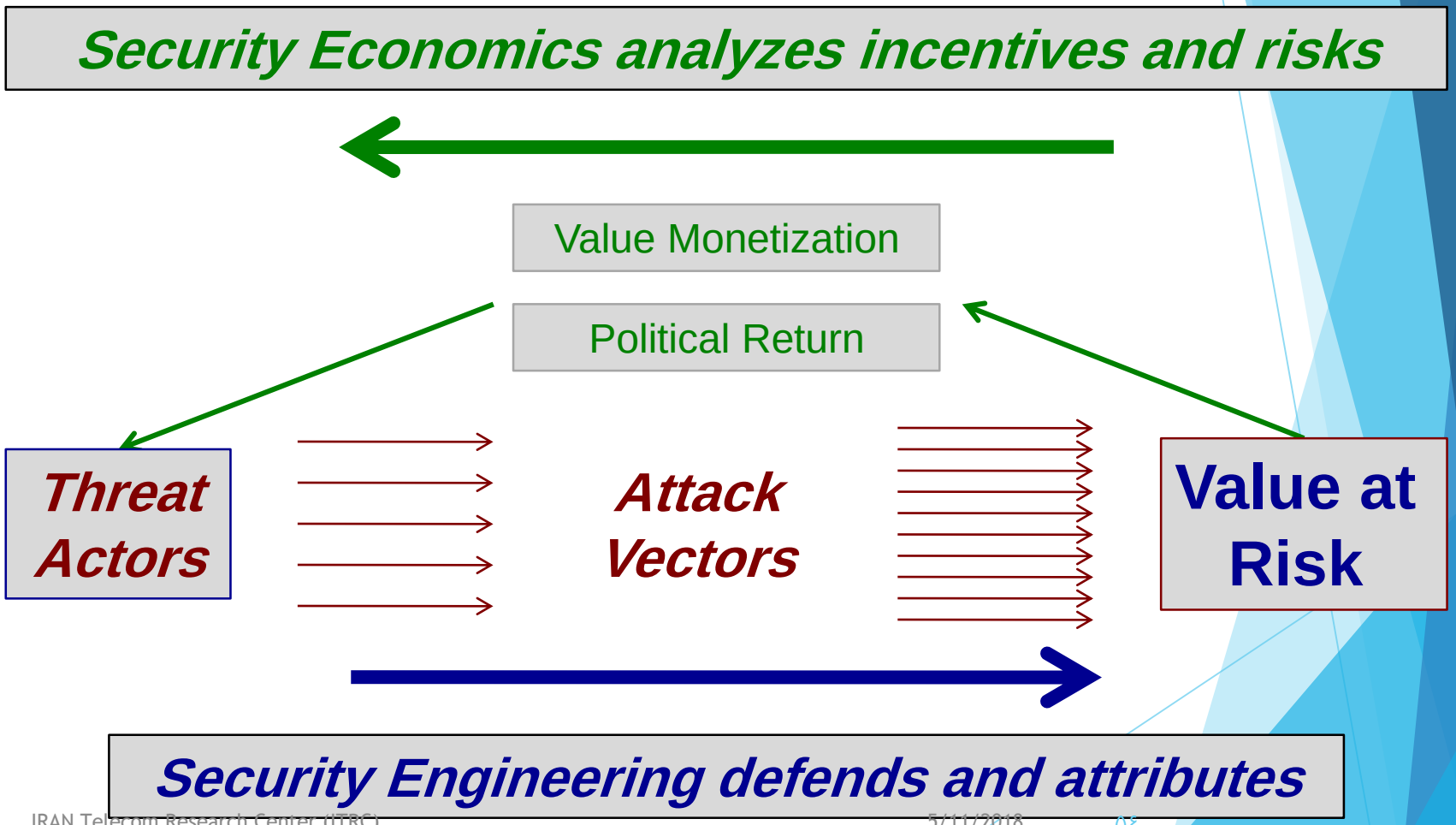
Recursive Architecture

- Create a scalable sharing, fusion and collaboration architecture
- Apply the architecture the the following levels:
  - Sectors
  - Countries
  - Internationally
- Effectiveness will be as good as the engineering and security architecture investment in the systems
  - Trust in the platform will govern how much data is shared
- Field higher standard systems at all levels
- Amortize the cost at multiple levels

Data Considerations

- Comparable characterization of cyber crime across countries by:
  - Sectors targeted
  - Methods of attack & coordination
  - Vulnerabilities exploited (technical and organizational)
  - Nature of criminal organizations (including black markets)
  - Precursor signatures
  - Detection signatures
  - Effectiveness of defensive coordination
  - Countermeasures
- Capture of sufficient time window data to detect APT footprints
  - Retention of ISP and traffic logs
  - Enterprise network sensor data
  - Compression via known patterns
- Layer data by generality
  - Aggregates easier to collect and manage
  - Specifics better for response to criminal or state activities
- Support real-time response to cyber crime or other attacks
  - Higher assurance handling required
  - Need based access
- Measure contribution of data to anti-crime efforts
  - Feedback to improve data and reinforce cooperation

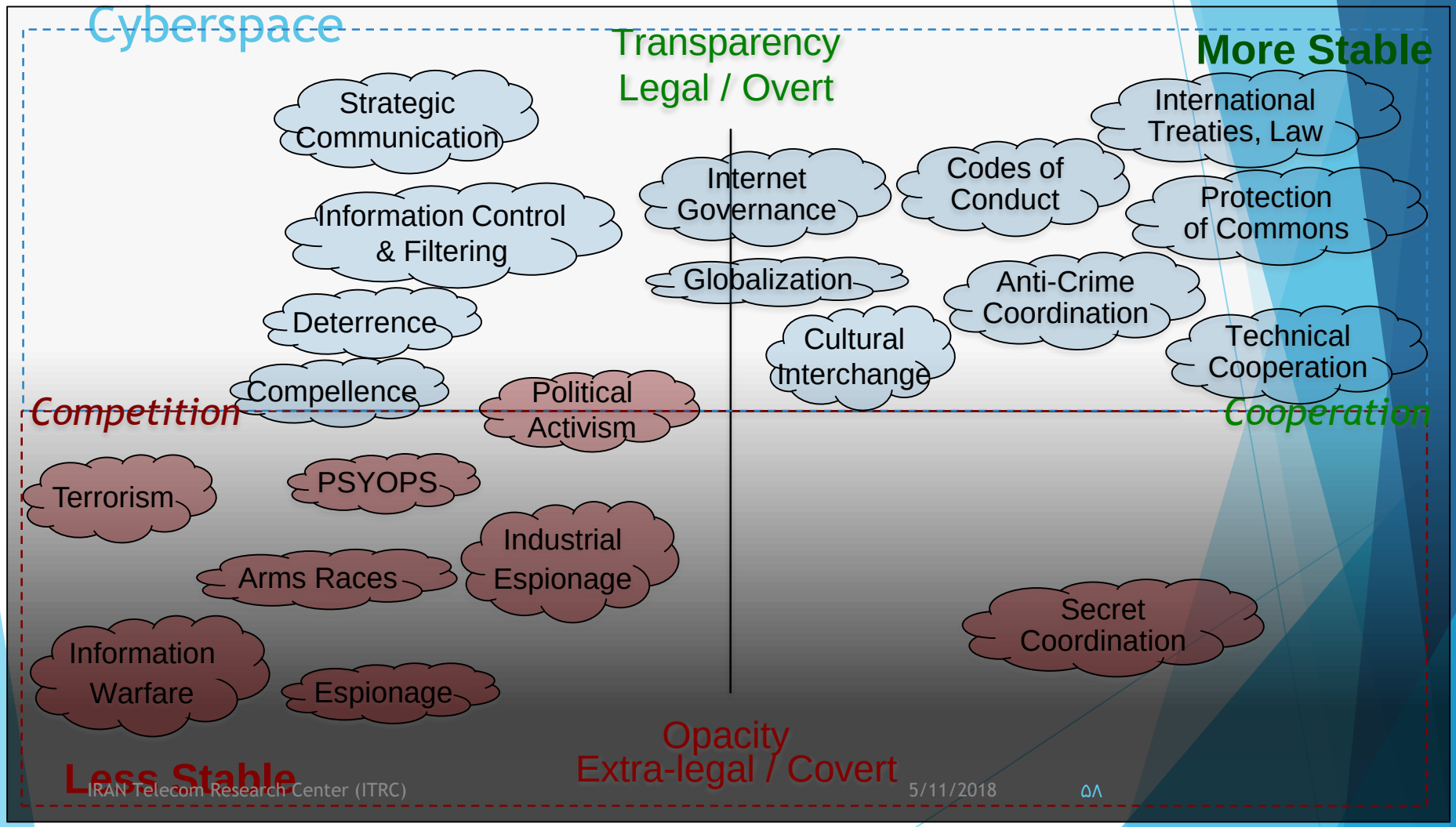
Integrate Technical and Value Data



Data Planes

- Technology Plane
  - Focus on the range of technical vulnerabilities and technical approaches to defense
  - Includes new attack surfaces like cloud computing and mobility, but also improving defensive technologies
- Cyber Crime and Criminal Justice
  - Focus on cyber crime motivated by financial gain, prevention, detection and prosecution
  - Includes economics of cyber crime, forensics, industrial espionage, vigilante activities, international cooperation
- Economic Plane
  - Focus is on data supporting policy moves to improve market response to cyber security
  - Includes industrial organization in the IT capital goods sector, risk management, actuarial data and insurance and analysis of potential government intervention
- Defensive Coordination
  - Focus on sharing of threat, vulnerability, breach and response data as well as best practices within sectors
- State-centric Cyber Interactions
  - Focus is on interstate cyber espionage, sabotage, preparation of the battlefield and cyber attacks
  - Includes indications & warnings, cooperative defense, norm development
- Cyber-fueled Long-term Transformations
  - Focus is on the transformations within modern economies and international systems arising from ubiquitous integration of computation and global networking
  - Includes changing action possibilities for old and new groups, whether economic, political or affinity

Policy-relevant Data for Characterizing Interstate Cooperation and Competition In Cyberspace



Coordination Reduces Search Space for Defenders

- Attacker search leverage
  - Integrated organization
  - Focus on target
  - Choice of attack vector(s)
  - Selection of place and time of attack
  - Black markets for crime ware
- Defender search leverage
  - Shared situational awareness (data, info)
  - Constrain search by linking data across dimensions (attack vectors, value at risk)
  - Shared detection
  - Shared responses
  - Shared best practices
  - Sharing expertise
  - Focused and scalable collaboration
  - Shared R&D

Coordination Reduces Search Space for Defenders

- Amortize effort to establish frameworks for international data sharing
  - Base: Data, information, knowledge, algorithms
  - Expertise: Index expertise around data topics
    - Better ability to understand and use the data
    - Enable focused collaboration
  - Collaboration: Refine the data, practices and responses
    - Sectoral practitioners, stakeholders
    - Cross-sectoral synergies
    - R&D to improve data, practices and responses
  - Architecture: Evolve the sharing and collaboration system
    - Task-driven legal and regulatory harmonization
    - Security & collaboration research

Data Harmonization

- Collaborative processes required for developing:
  - Shared vocabularies for describing cyber data and phenomena
    - Cross human language mappings
  - Domain ontologies data
    - Standardized data formats within domains
    - Approach for data format evolution
    - Cross-ontology linkages
    - Provenance metadata
    - Security policies – appropriate use
  - Derived data definitions
    - Algorithms for computing derivations
    - Metadata for outputs
- Approach
  - Start from existing datasets
  - Work towards integration of base datasets
  - Define generalization planes on datasets
  - Evolve datasets based on experience

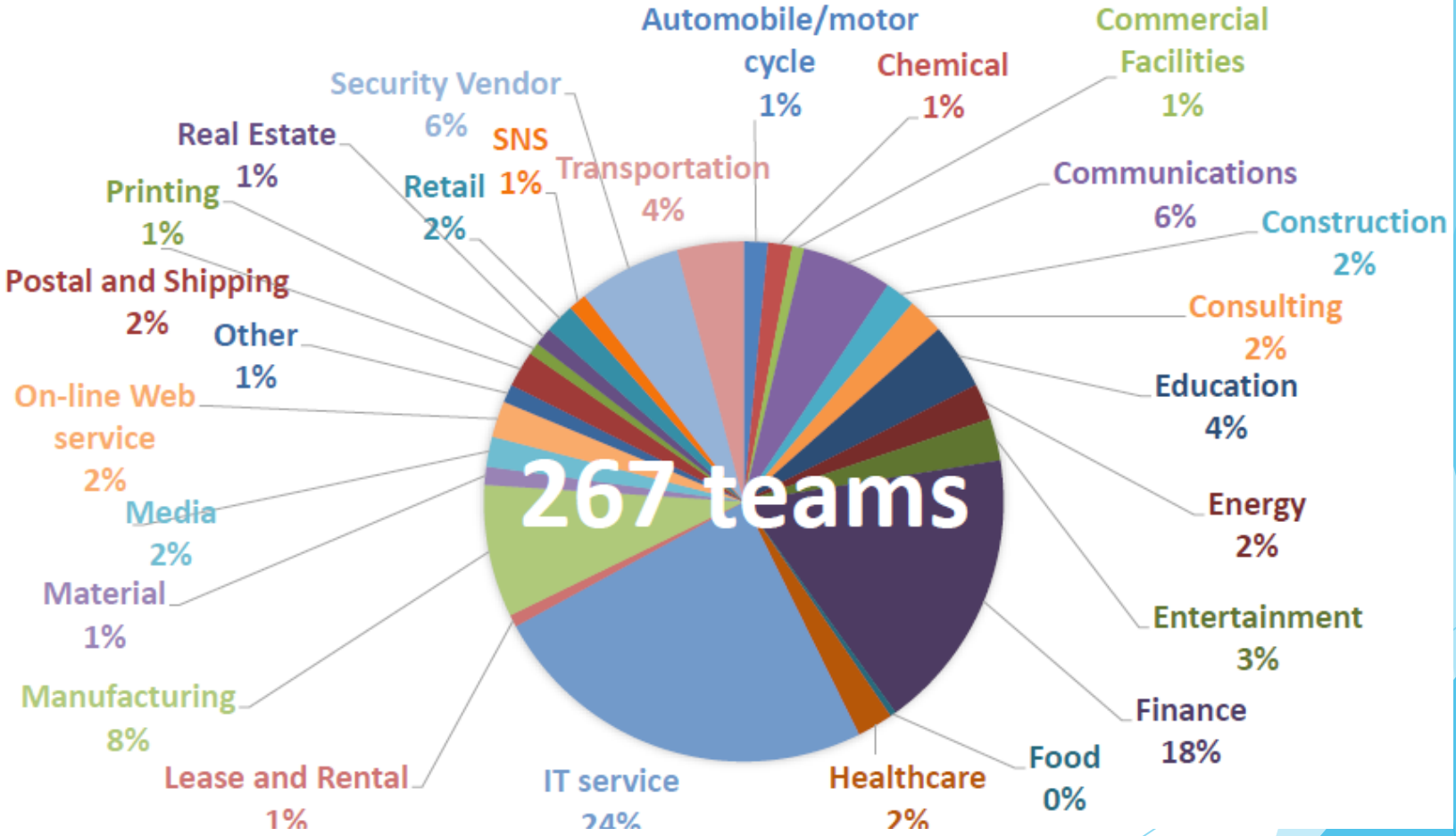
Enabling Technologies

- Core
  - Harmonized data collection strategies
  - Tools for collection, storage and pattern matching
  - Patterns of criminal and APT behavior
  - Data interoperation standards (e.g., semantic data web)
  - Binding of legal and regulatory requirements to process and security architectures
  - Usability
- Security
  - Identifying anomalous behavior
  - Audit and accountability
  - Managing risks (economic analysis)
  - Access control, preventive
  - Approaches to access control across administrative boundaries
  - Compositional enforcement of policies under constraints
  - Remote policy enforcement
  - Integrity of data
  - Undo decisions, provenance, retraction, update
  - Sandboxed computation on sensitive data
- Cryptographic techniques
  - Data splitting
  - Differential privacy
  - Checking the integrity and provenance outputs from computations on the data
  - Private data analysis
  - Watermarking (aggregate information)
  - Arithmetic (+, x) helps elicit data without divulging identity
    - Inputs are encrypted
    - Operation performed on cyber text
    - Outputs decrypted using keys that cannot decrypt the inputs
    - Extra credit: audit system to check the data integrity and reliability

Supporting Technologies

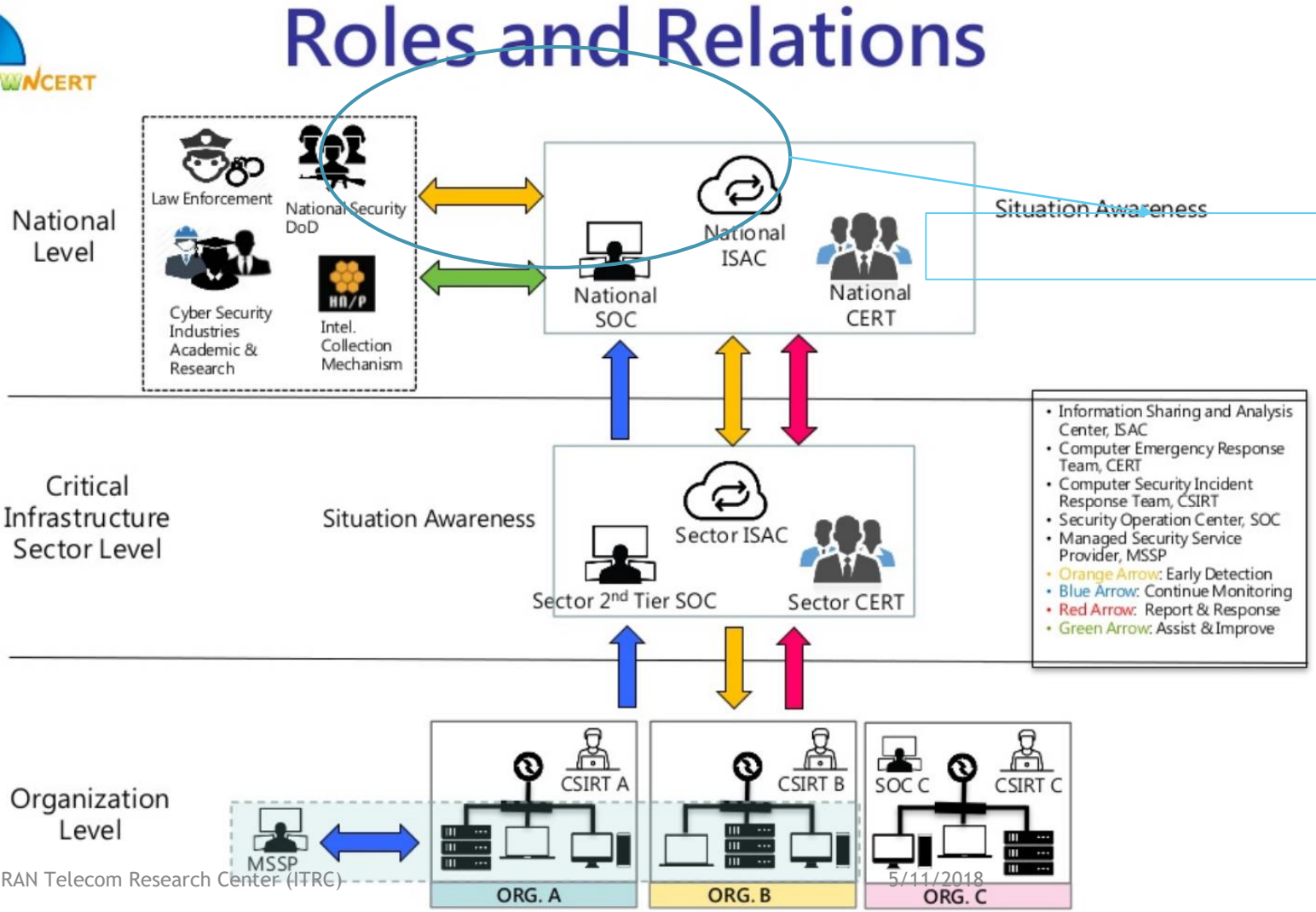
- High integrity storage with fine-grained security
- Pattern-based compression techniques
- Techniques for obfuscation of private information, including identity
- Policy representation and understanding
  - Understanding the law, social norms (higher level concepts, meta-language?)
  - Expressive policy languages
  - Policy analysis and conflict detection
  - Formalization and semi-automated enforcement
  - Usability
- Revocable anonymity
- Technical reinforcement of incentives
  - Resilient mechanism design
  - Interdependent risk
  - Game theory

JAPAN ICT ISAC members



ISAS
Information Sharing and Alert System

Taiwan ISAS



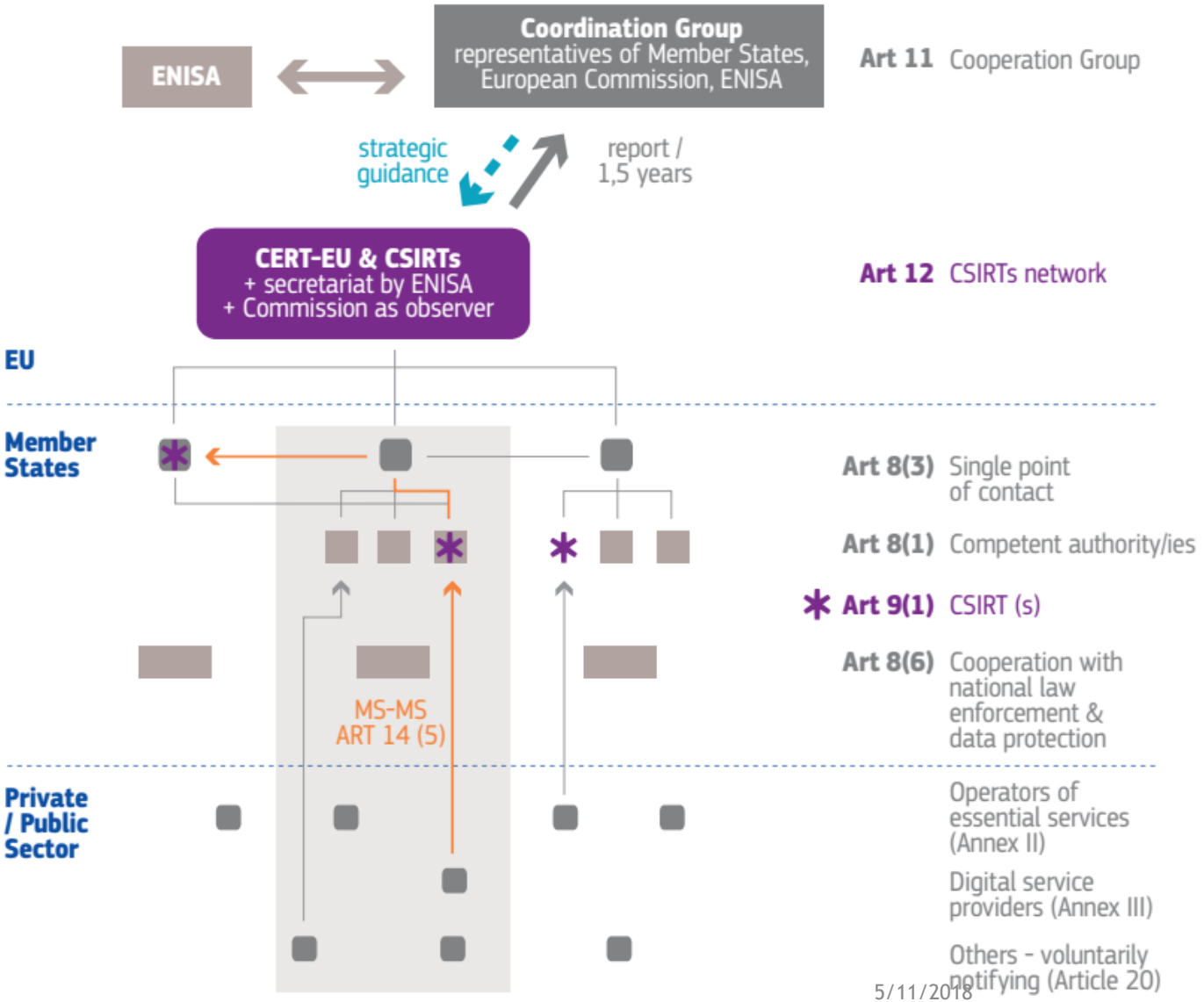
NIS Platform (Created in 2013)

- The expert work of the NIS Platform was divided into Working Groups:
  - WG1 on risk management, including information assurance, risks metrics and awareness raising;
  - WG2 on information exchange and incident coordination, including incident reporting and risks metrics for the purpose of information exchange;
  - WG3 on secure ICT research and innovation.
  - The findings of the Platform will feed into Commission recommendations on cybersecurity to be adopted in 2014

Legal Consideration

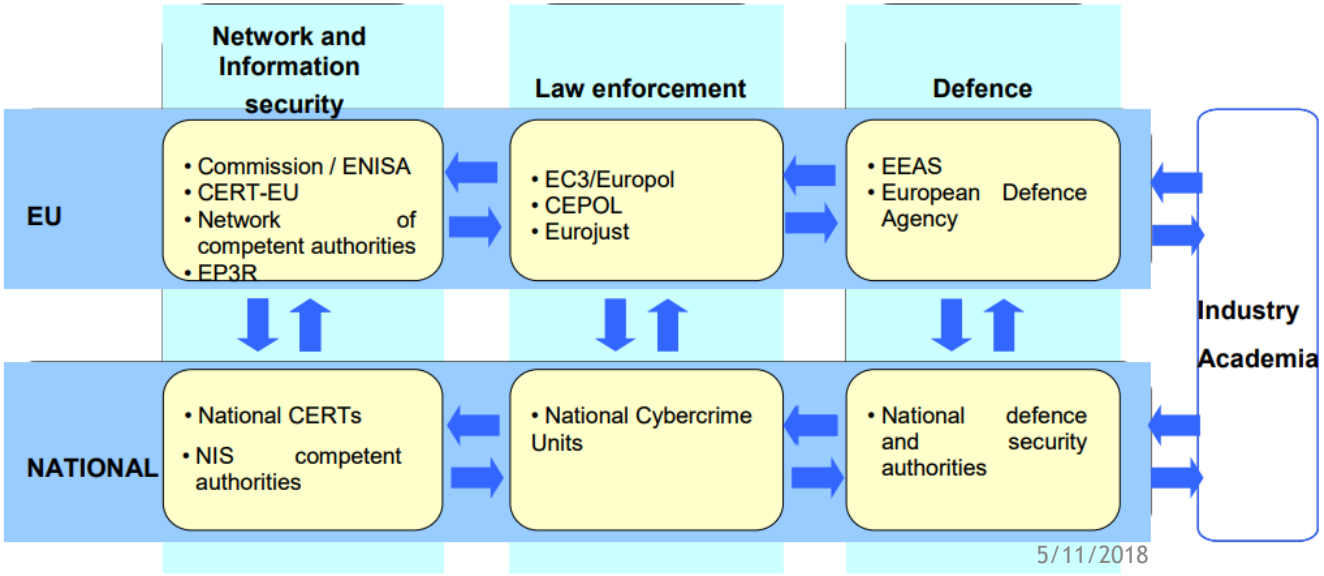
- NIS Directive : directive on security of network and information systems
  - Adopted in July 2016
  - To be implemented in 9 May 2018
    - *TOWARDS AN EFFECTIVE AND GENUINE SECURITY UNION*
  - ***Goals:***
    - to bring cybersecurity capabilities to the same level of development in all Member States,
    - to reinforce trust and confidence among them and
    - to ensure that information exchange and cooperation are efficient, including at cross-border level.
  - **To achieve this golas:**
    - Establishing a **new, multi-level governance structure for European cyber protection**

ENISA Structure



ENISA


IT Security
Law enforcement
Intelligence
Diplomacy and Defense


Network and Information security
Law enforcement
Defence
EU
• Commission / ENISA
• CERT-EU
• Network of competent authorities
• EP3R
• EC3/Europol
• CEPOL
• Eurojust
• EEAS
• European Defence Agency
NATIONAL
• National CERTs
• NIS competent authorities
• National Cybercrime Units
• National defence and security authorities
Industry
Academia

European Cybersecurity Coordination Platform

- **ENISA could be transformed into an established European Cybersecurity Coordination Platform** with responsibility of improving capabilities in areas:

Detection
- Focal point of authorized bringing together the information and oversight (dot connections)
- Joint Information Sharing mechanism and taxonomy is needed (developed for CSIRTs and law enforcement)

Prevention
- Strategic risk assessment of cyber threats
- Developing European deterrence and counter-strategies
- Monitoring current and future legislation at MS level
- Mapping and monitoring the development of cybersecurity capabilities against benchmarks
- Conducting stress tests and friendly hacking exercises to assess CI resilience

Cooperation
- Facilitating synergies between internal and external security
- a **highly-secured network among relevant EU institutions**

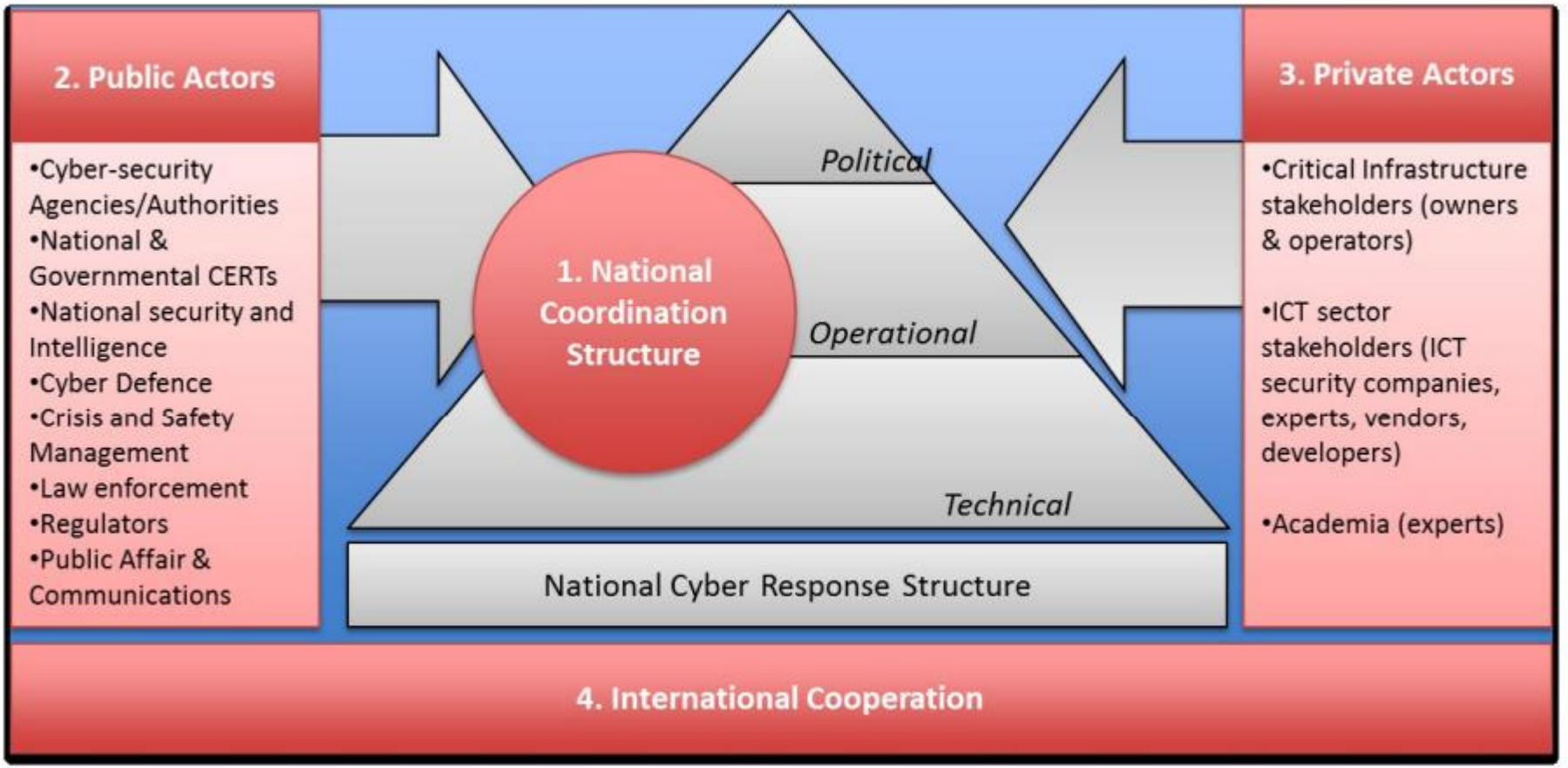
Protection
- To enable coordinated responses to large-scale EU cyberattacks and hybrid threats
- outlining specific steps to be followed
- to pool resources and skills at European level to provide assistance to overwhelmed Member States, or in cases of attacks against critical European infrastructures

Prosecution
- **Could contribute in prosecution**
- *This should remain within the remit of the Member States and Europol*

ENISA

- **Article 5.2 of the proposal for a NIS Directive** articulates the way a risk assessment should fit into an supreme strategy and plan, namely that:
  - The national NIS strategy shall include a national NIS cooperation plan complying at least with the following requirements
    - A risk assessment plan to identify risks and assess the impacts of potential incidents;
    - The definition of the roles and responsibilities of the various actors involved in the implementation of the plan;
    - The definition of cooperation and communication processes ensuring prevention, detection, response, repair and recovery, and modulated according to the alert level;
    - A roadmap for NIS exercises and training to reinforce, validate, and test the plan.
  - Lessons learned to be documented and incorporated into updates to the plan.

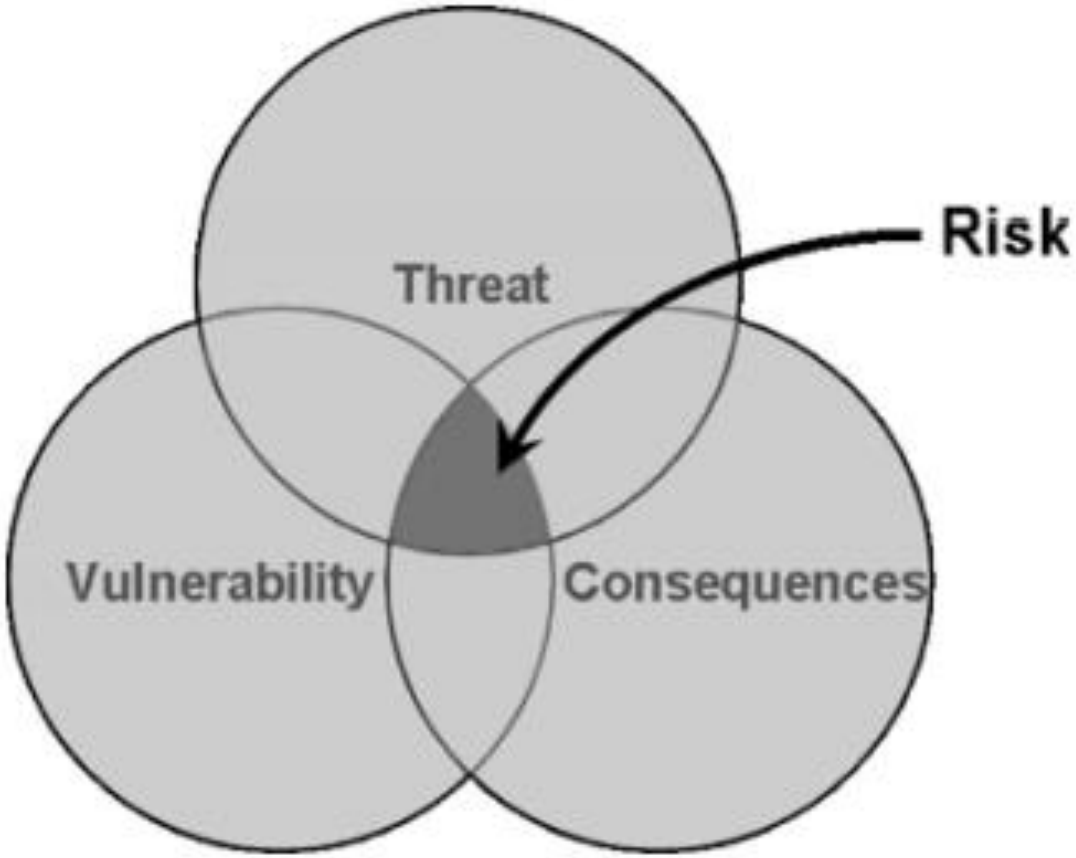
National NIS Cooperation Plan Structures



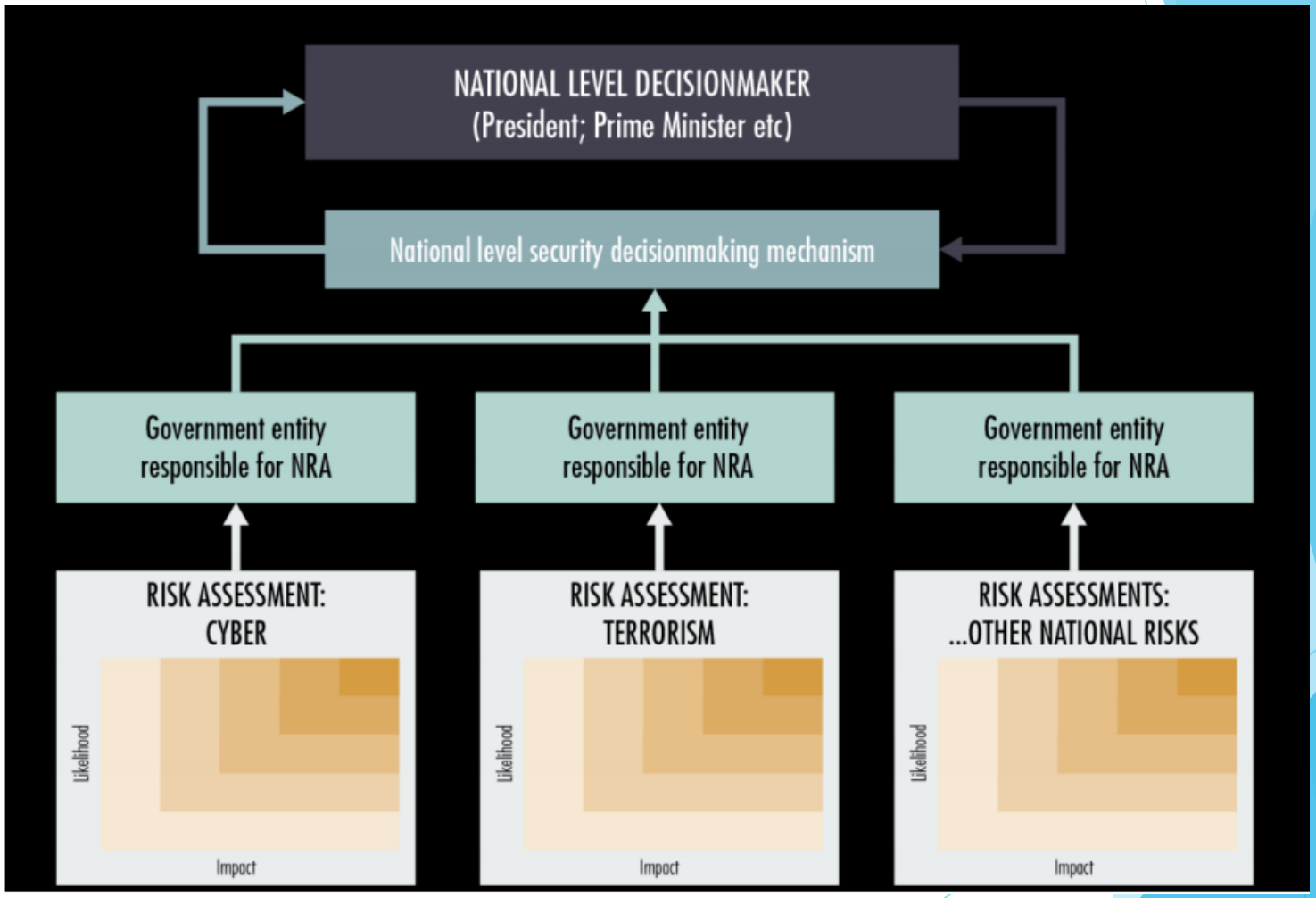
National-level risk assessment and threat modelling for cyber security

- To contribute to the wider objective of improving ***national contingency planning***
  - To reduce or eliminate vulnerabilities of critical information and communication Technology (ICT) services and infrastructures
    - Stated in European Cyber Security Strategy and thus sits within broader EU-wide efforts to **improve crisis cooperation activities**
- Current priorities of National-level Risk Assessment programs:
  - Improving understanding of threats and their effects upon society;
  - Better incident management;
  - Greater stakeholder involvement and information sharing;
  - Improved national CIIP frameworks;
  - Seeking further EU guidance and support

Risk definition



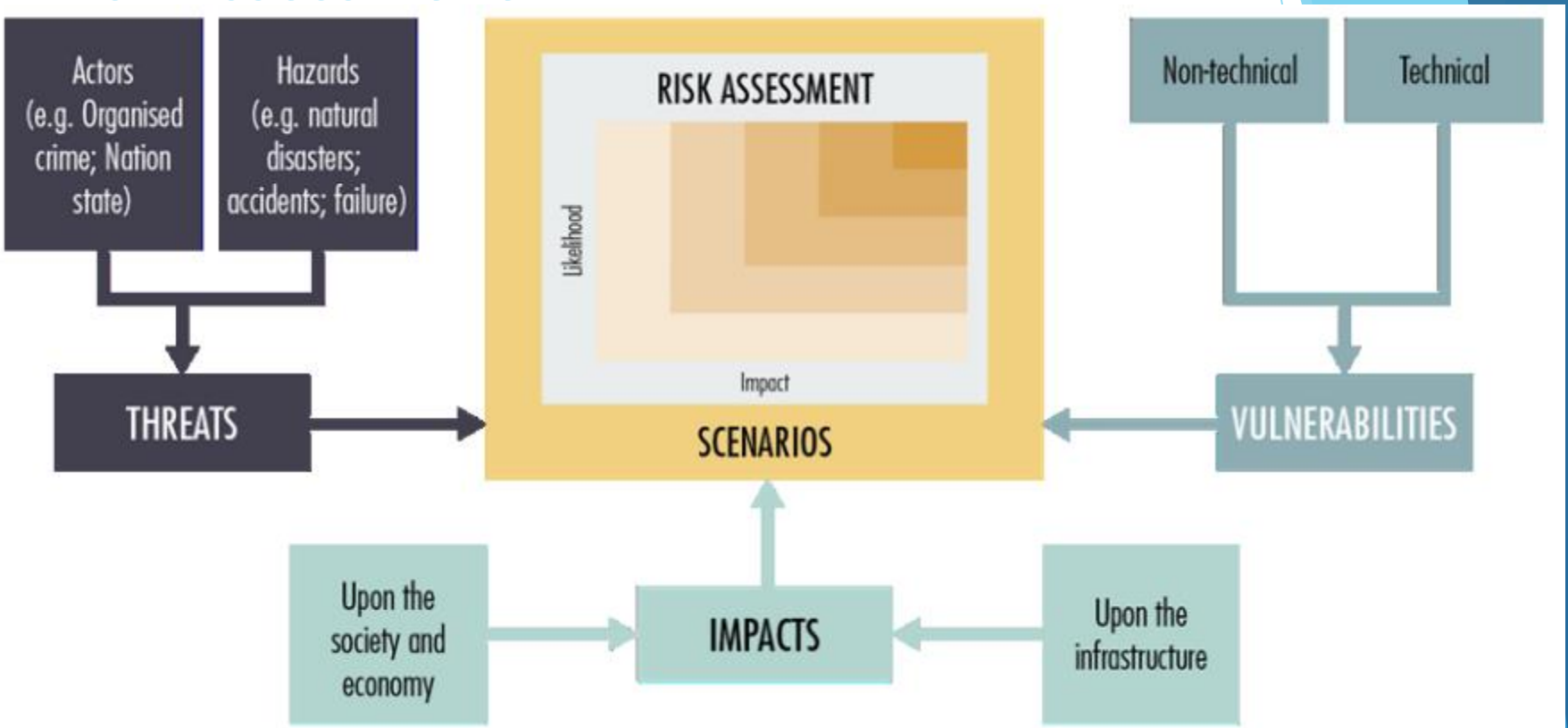
Risk inputs to senior decision-makers



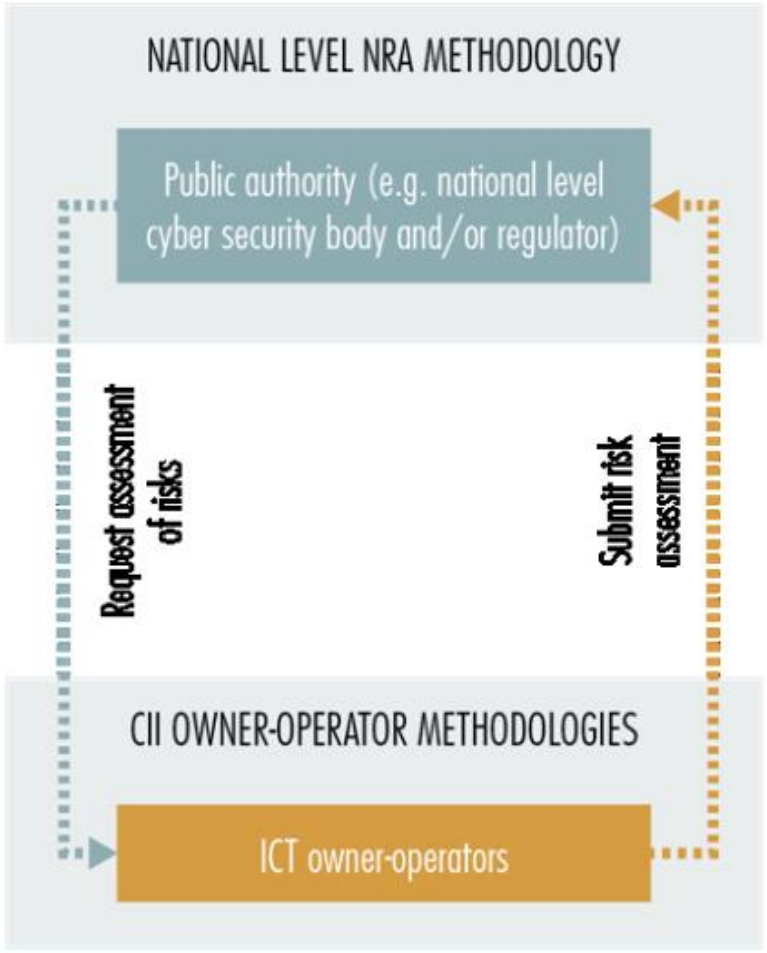
Involved entities at national level

- Government bodies responsible for cyber security
- Government bodies performing NRA(s)
- Civilian crisis management bodies
- Telecommunications regulators
- Law enforcement agencies
- National/government CERT
- Interior Ministry
- Other regulators
- Cabinet level bodies supporting national decisionmakers
- Regional or local administrators
- CII owner-operators
- National Intelligence Agency(s)
- ICT users

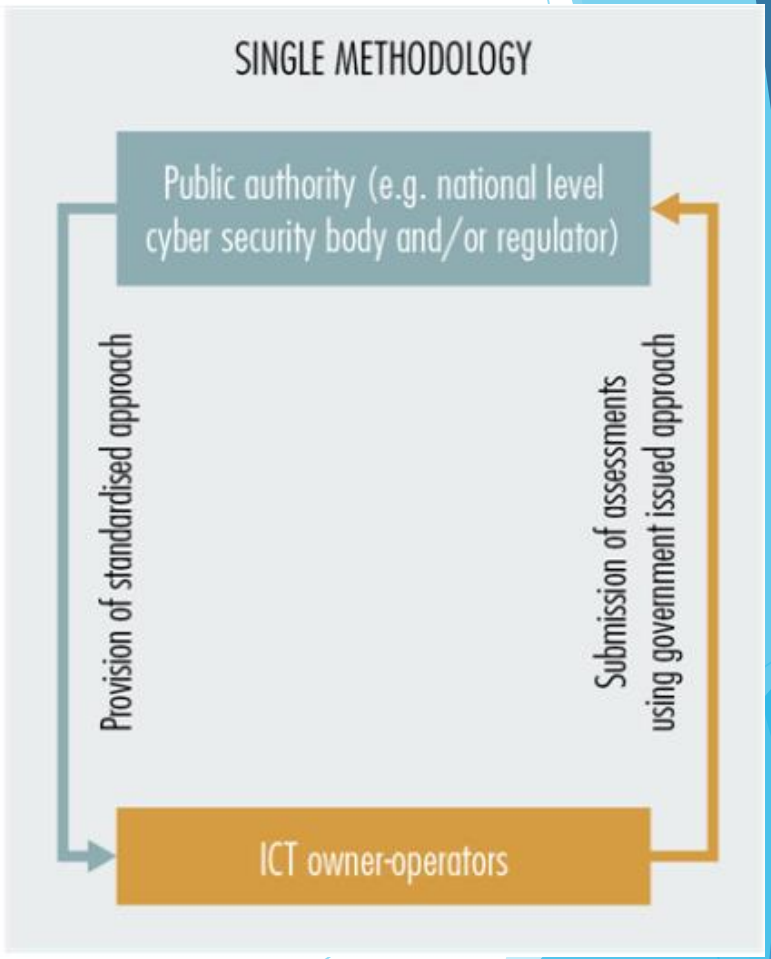
Possible inputs to the National-level Risk Assessment



Approaches



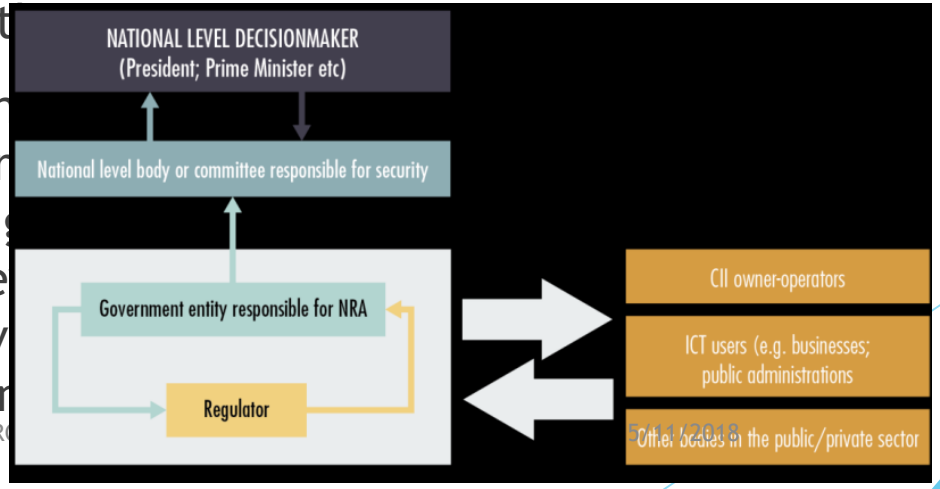
Decentralized



centralized

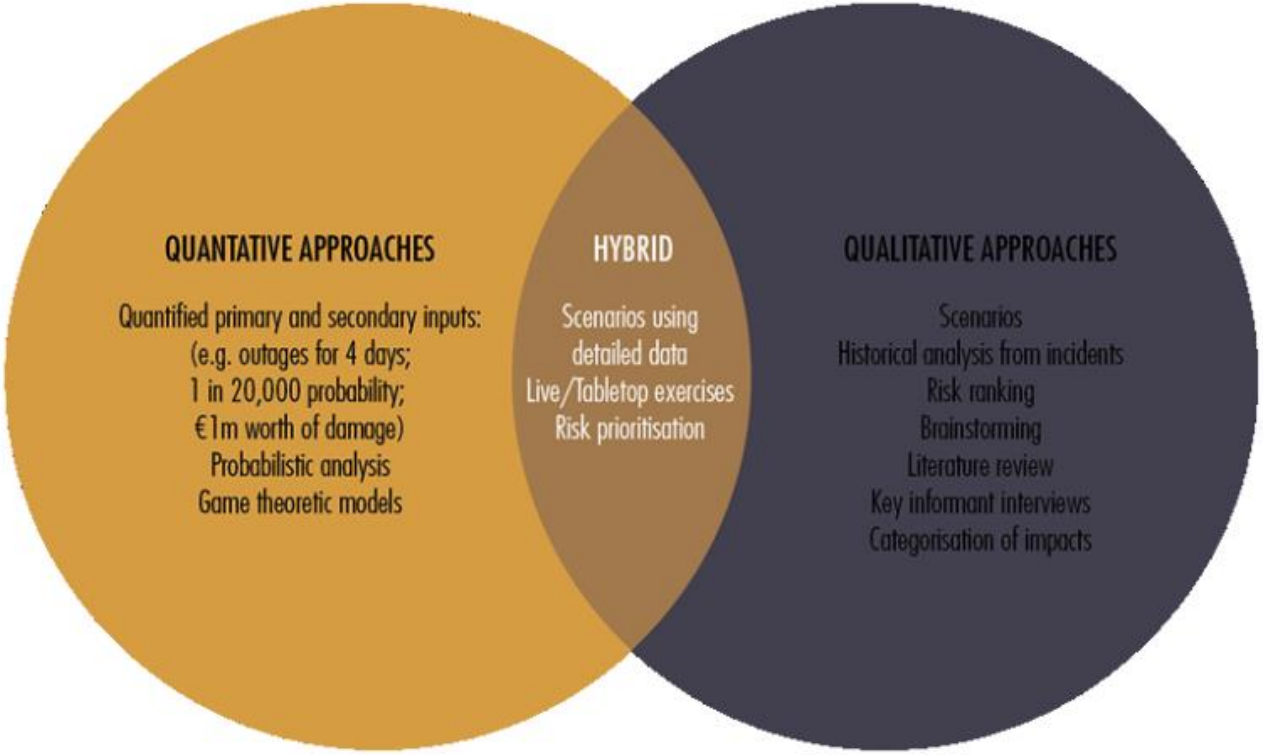
Critical Information Infrastructures Protection approaches in EU (Key findings 2015)

1. Governance of the CII Action Plans in national level also varies in the Member States: in some cases the National Security Authority has full supervision of specific activities and stakeholders involved, in other cases a decentralized model is followed. This depends on the already setup framework in national level, of the budget and resources and of course on the priorities of t
2. Collaboration through a for like working some cases e that all relev critical inform

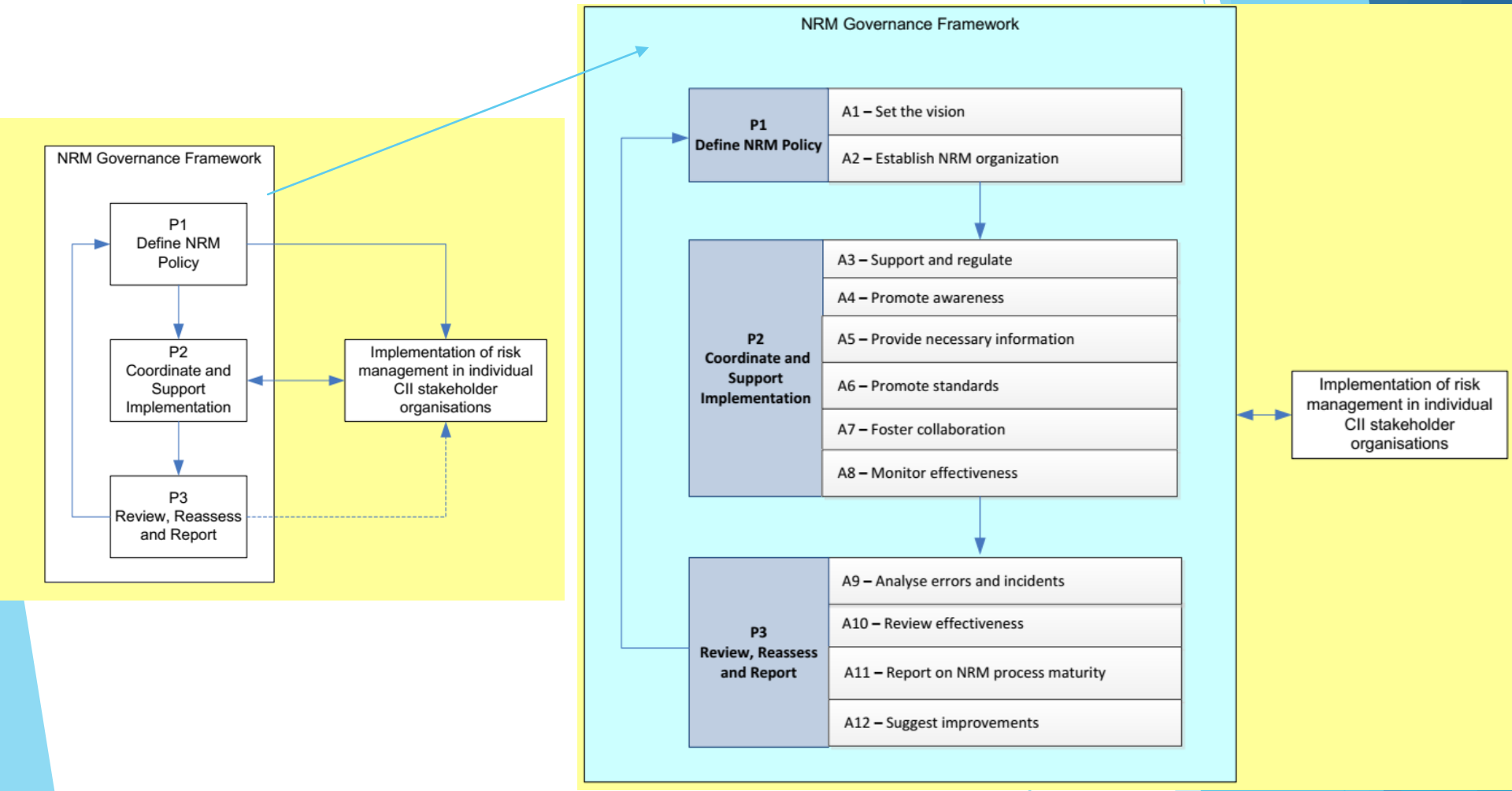


Methodologies

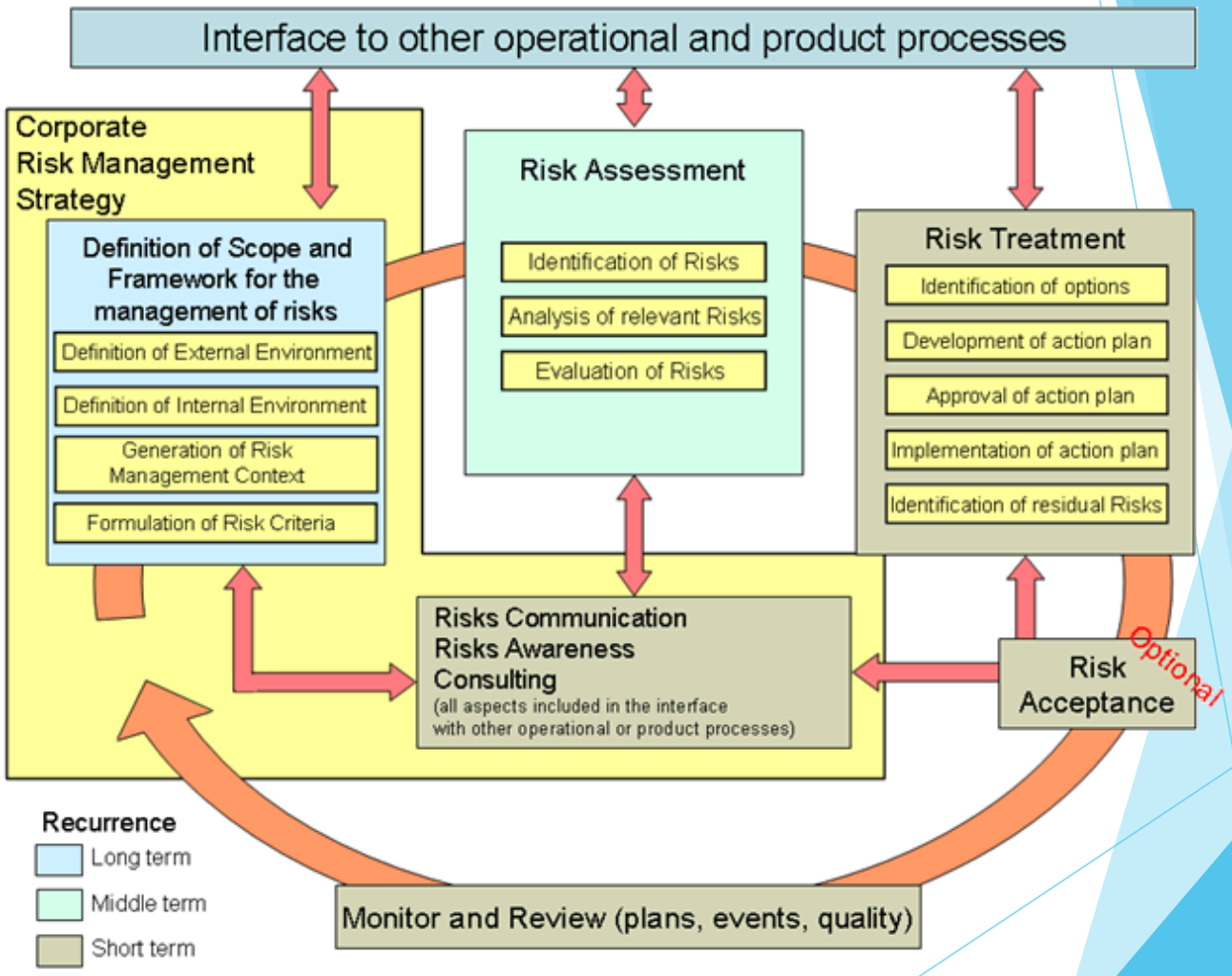
- **Scenario-based**
  - UK
  - Germany
- **Qualitative or quantitative**
  - Japan
  - Sweden
  - Netherland
- **Combined**
  - Switzerland
  - France
  - Estonia



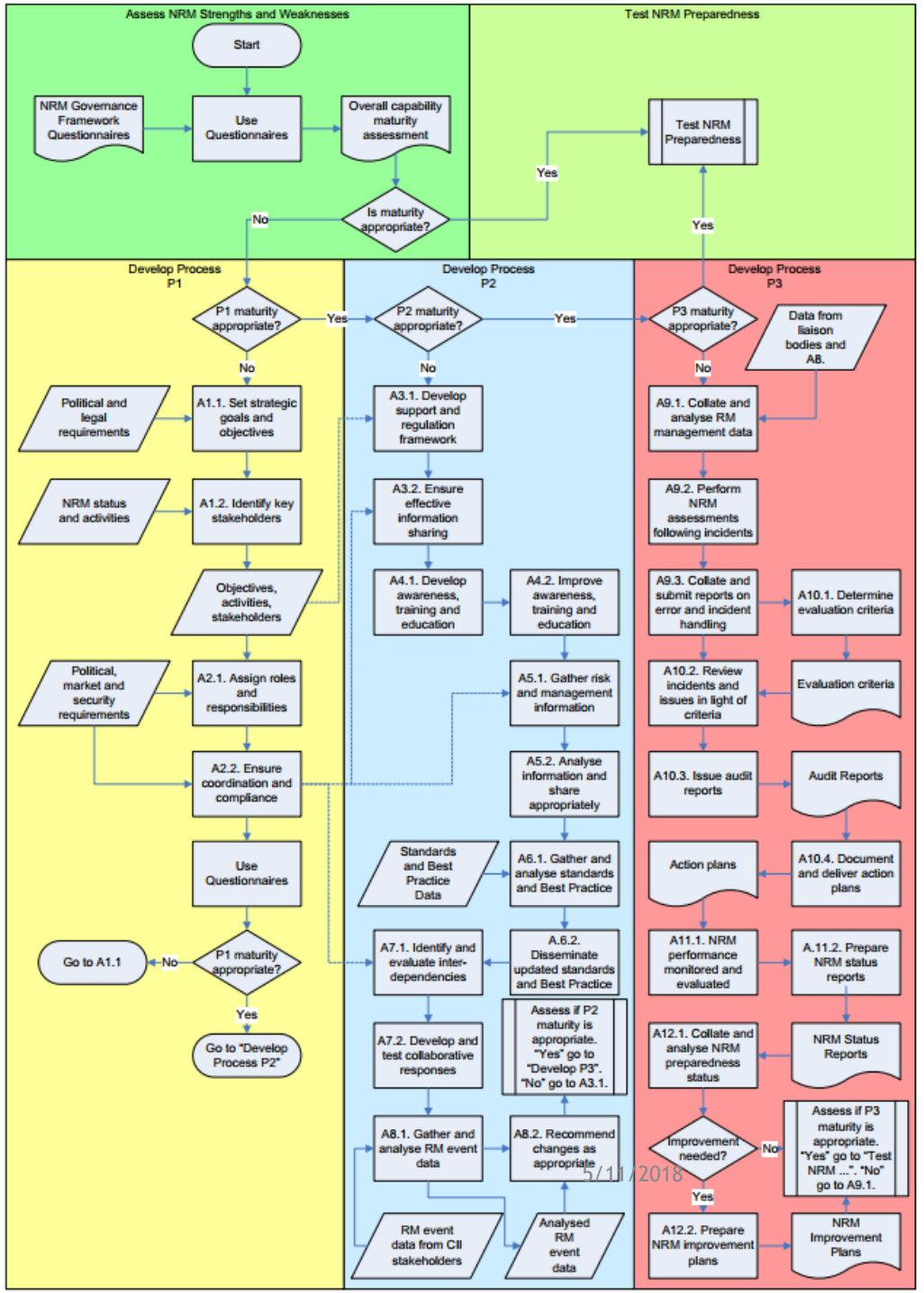
NRM Governance Framework



RM PROCESS


Interface to other operational and product processes
Corporate Risk Management Strategy
Definition of Scope and Framework for the management of risks
Definition of External Environment
Definition of Internal Environment
Generation of Risk Management Context
Formulation of Risk Criteria
Risk Assessment
Identification of Risks
Analysis of relevant Risks
Evaluation of Risks
Risk Treatment
Identification of options
Development of action plan
Approval of action plan
Implementation of action plan
Identification of residual Risks
Risks Communication
Risks Awareness
Consulting
(all aspects included in the interface with other operational or product processes)
Risk Acceptance
Optional
Recurrence
Long term
Middle term
Short term
Monitor and Review (plans, events, quality)

Developing the framework



Cyber crisis

- A ‘crisis’ can be defined as ‘an extraordinary event that differs from the normal and **involves serious disturbance or risk for disturbance of vital societal functions**’.
- A ‘crisis’ can be defined respectively as an **abnormal and unstable situation** that threatens an organization's strategic objectives, reputation or viability.

Management Levels of crisis

Strategic

- is automatically involved when an incident escalates into a crisis with potential socio-economic impacts
- heads of departments, cyber security councils, national defence councils, national crisis management boards

Operational

- focuses on threat analysis, situational assessment and mitigation action measures.
- Actors at this level are cyber security agencies or authorities, governmental CSIRTs,
  national communication authorities, and operational crisis management bodies

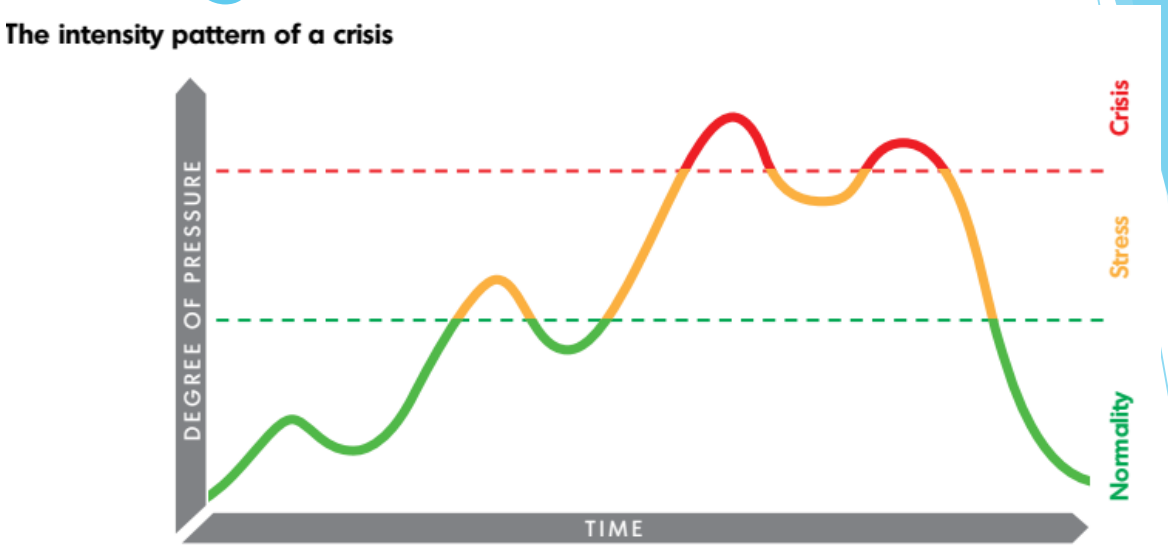
Technical

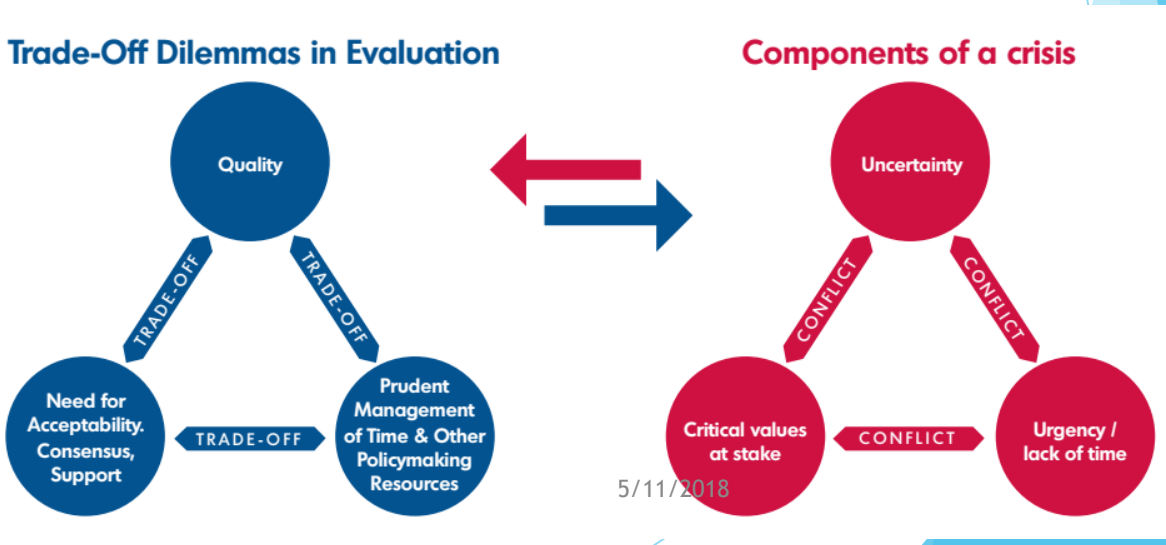
- The **technical level** involves incident handling by monitoring, detecting and handling the incidents, and alerting and informing the operational level with the appropriate raw technical information.
- CSIRTs and abuse teams operating at information systems

	EU and national	Academia	Best practice
Cyber-incident	A (cyber) incident is a disruption of IT services where the expected availability of the service disappears completely or in part. It can also be the unlawful publication, obtaining and/or modification of information stored on IT services.[30]	Violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.[31]	A malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, • Disrupts, or was an attempt to disrupt, the operation of a Cyber System.[32]
Cyber Crisis	An abnormal and unstable situation that threatens an organisation's strategic objectives, reputation or viability. An event that strikes at the heart of the organization.[33]	A serious threat to the basic structures or the fundamental values and norms of a system (in cyber space), which, under time pressure and highly uncertain circumstances, necessitates making vital decisions.[34]	Situation where the equilibrium among the basic components of the system on the one hand, and approach of the environment on the other hand, is disrupted in a serious way.[35]

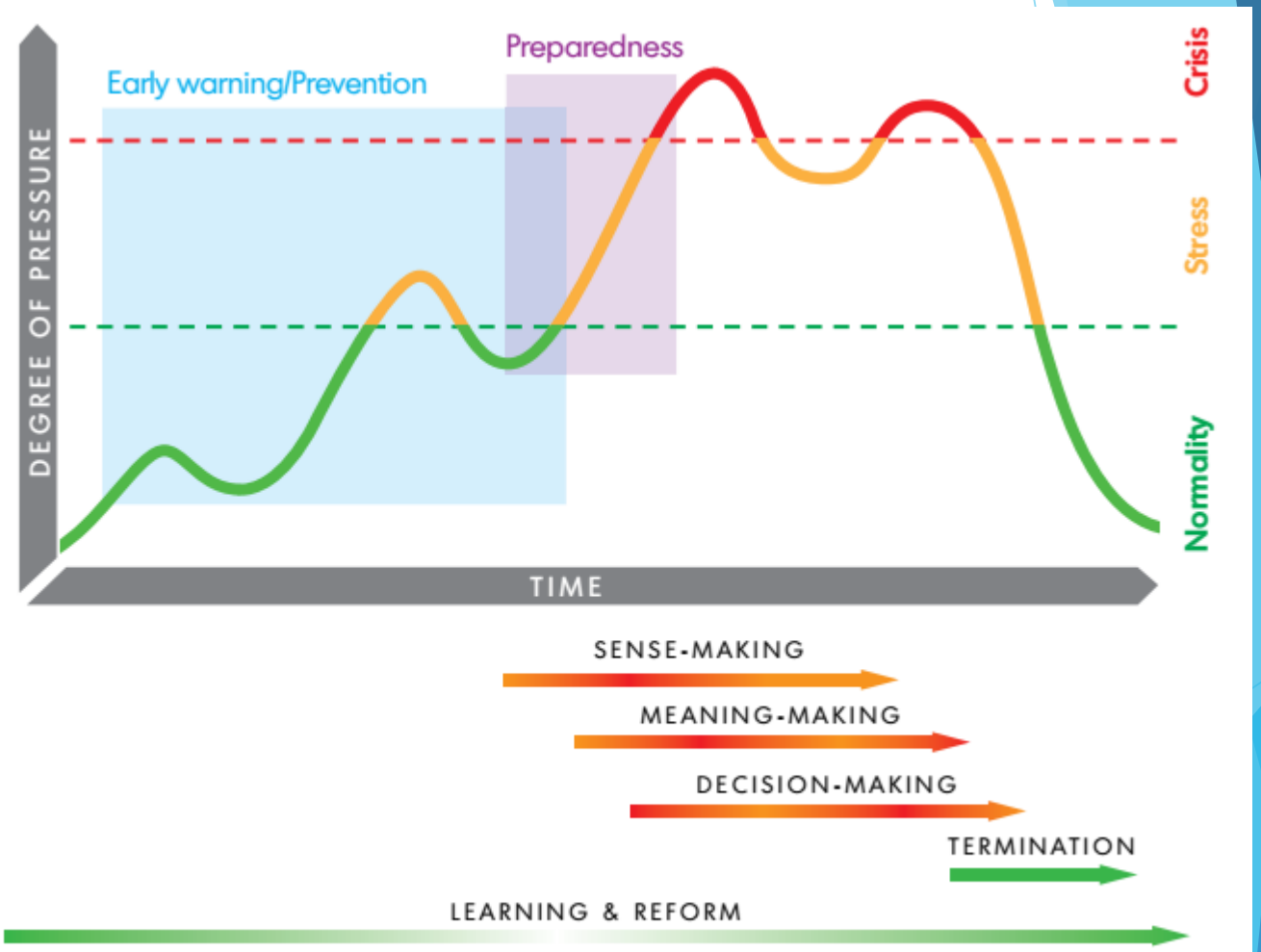
Crisis escalation model based in the EU

Crisis Management models



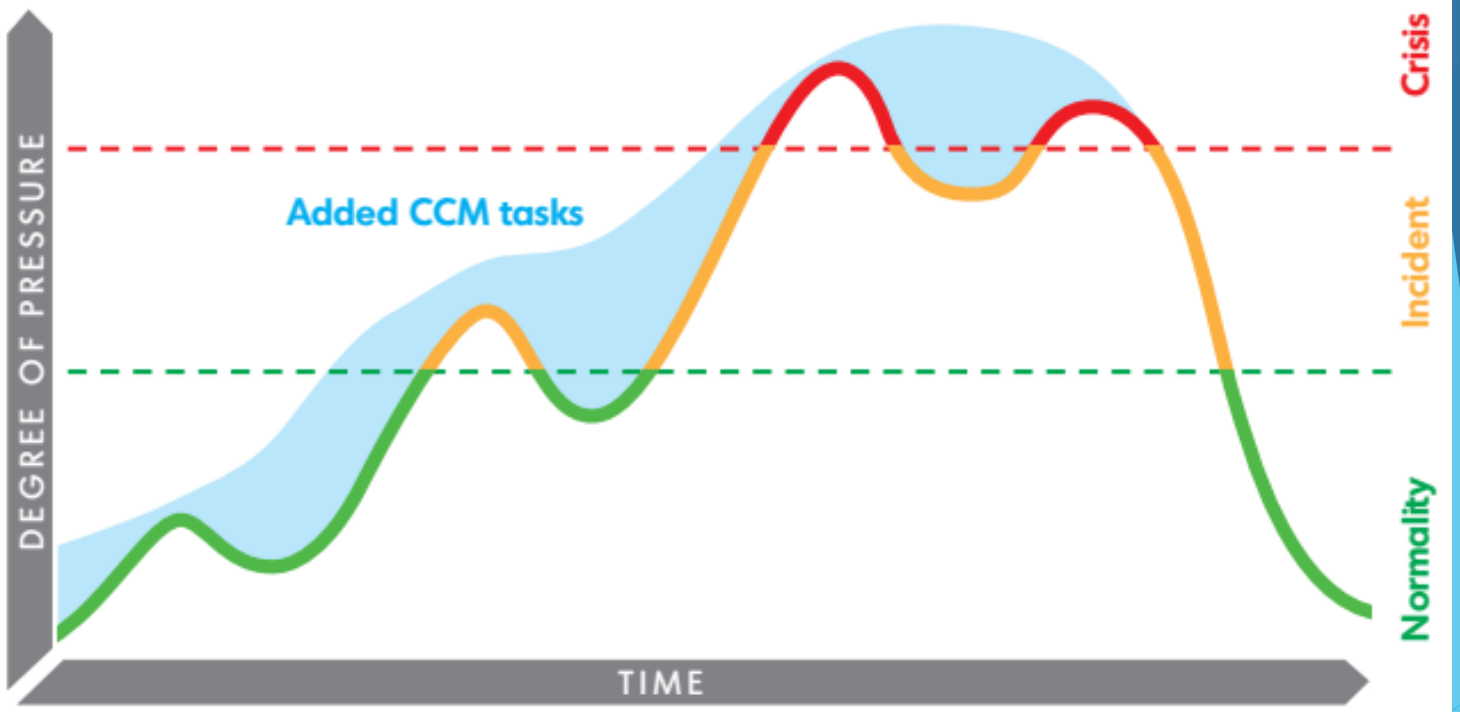


CRISIS Management Tasks



Timing and intensity of crisis management tasks

Cyber crisis is escalated from incident

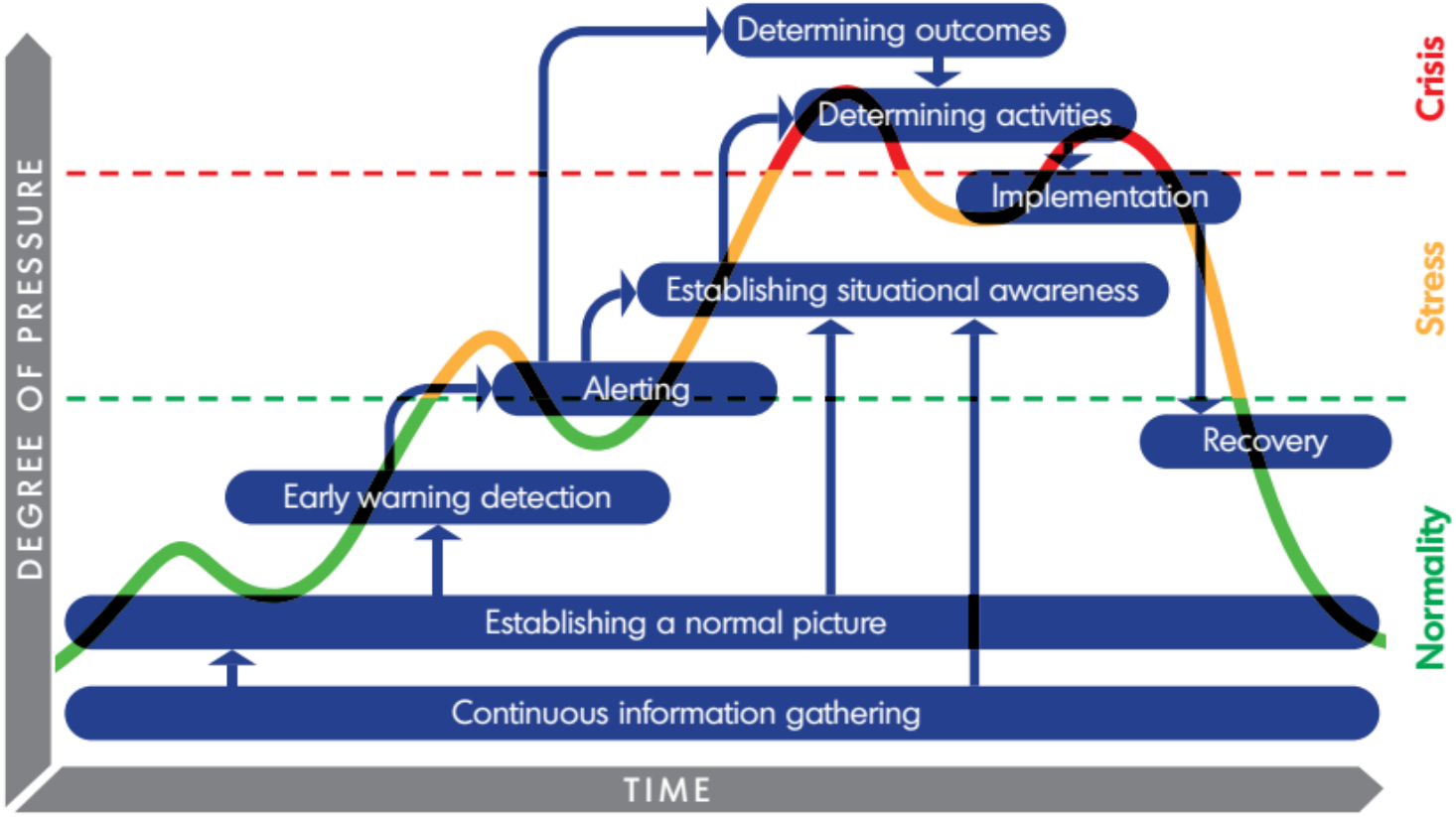


The intensity pattern of a cyber crisis

- the severity of a crisis tends to be measured by the severity of its impacts.
- the effective mitigation of any sectorial crisis induced by severe cyber incidents, will depend on the effective mitigation of the causes of the incidents (A paradigm shift crisis management

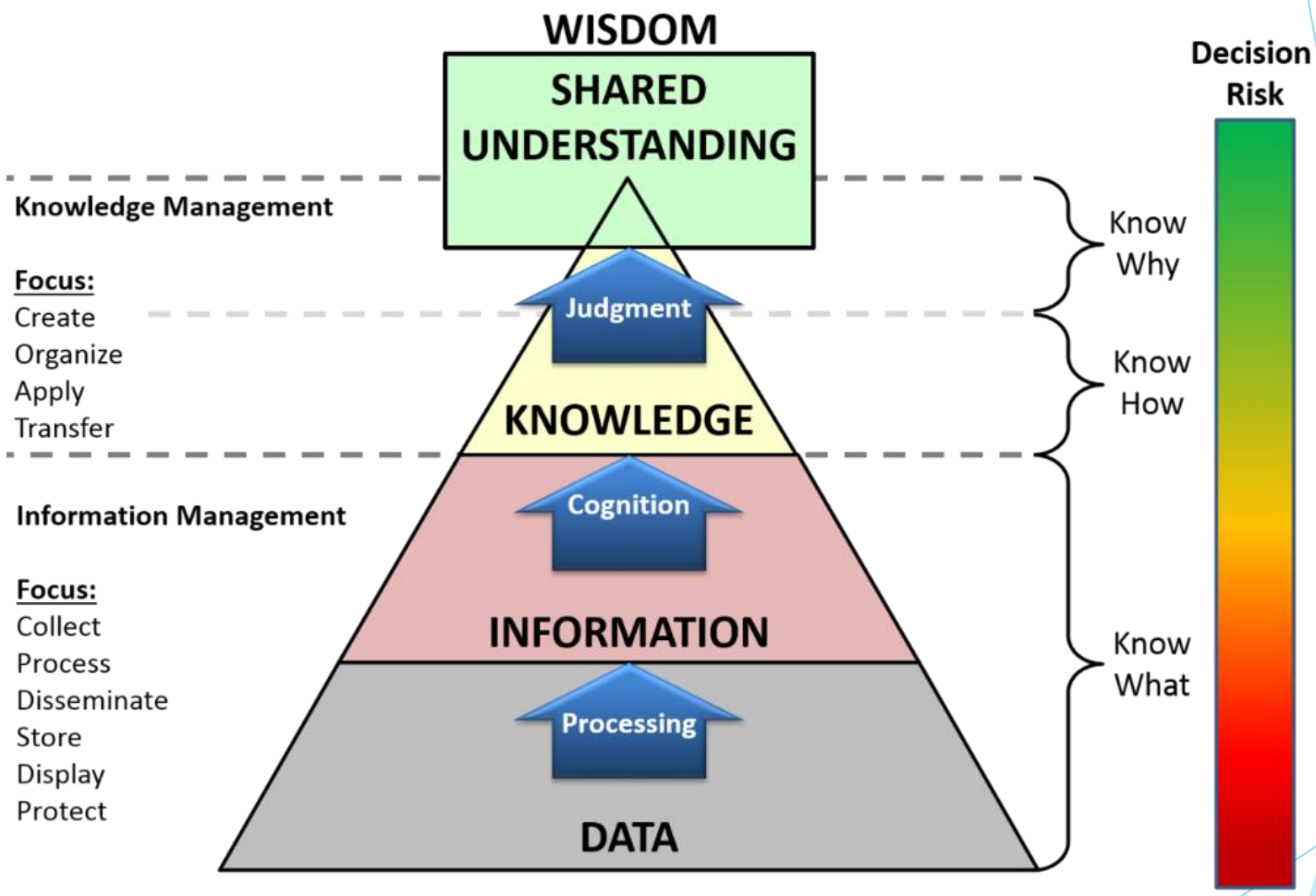
NIS Directive is to fill the legislative gap

Practical activities

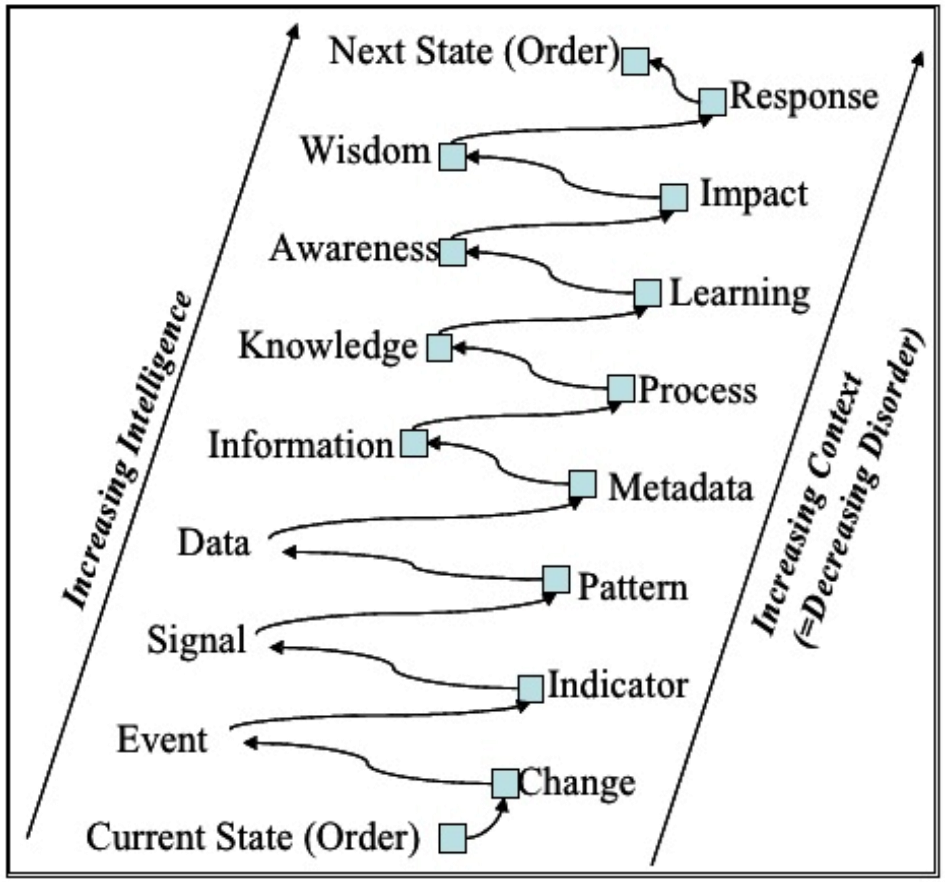


Practical crisis management activities

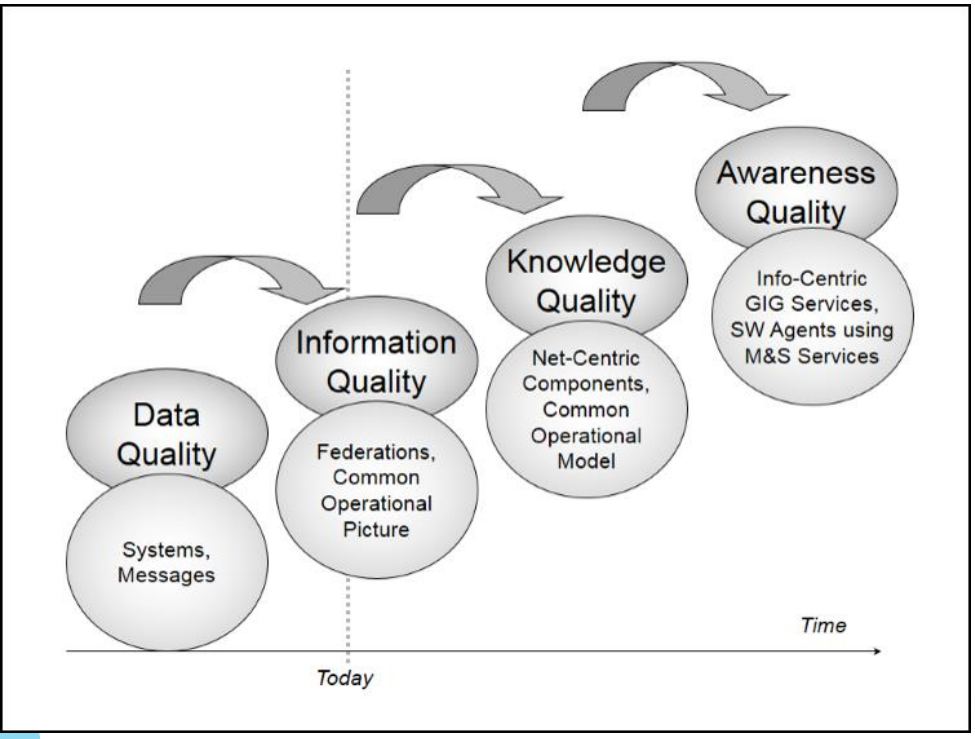
Knowledge Management Cognitive Pyramid



A Model of Intelligence



Organized intelligence identifies the basis for responses to change, and their subsequent impacts


Awareness Quality
Info-Centric GIG Services, SW Agents using M&S Services
Knowledge Quality
Net-Centric Components, Common Operational Model
Information Quality
Federations, Common Operational Picture
Data Quality
Systems, Messages
Time
Today

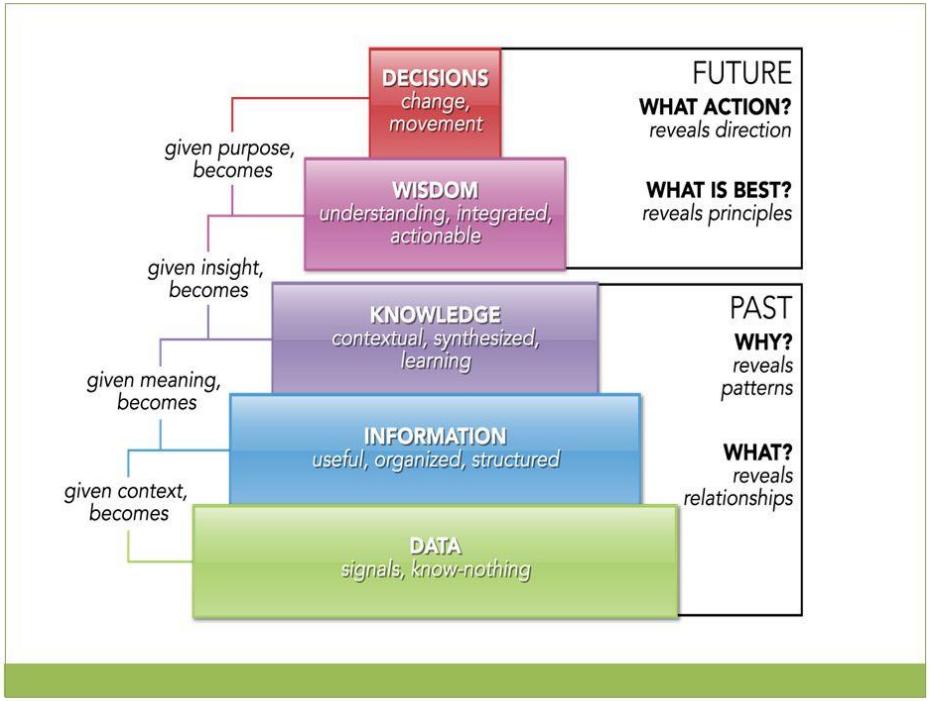
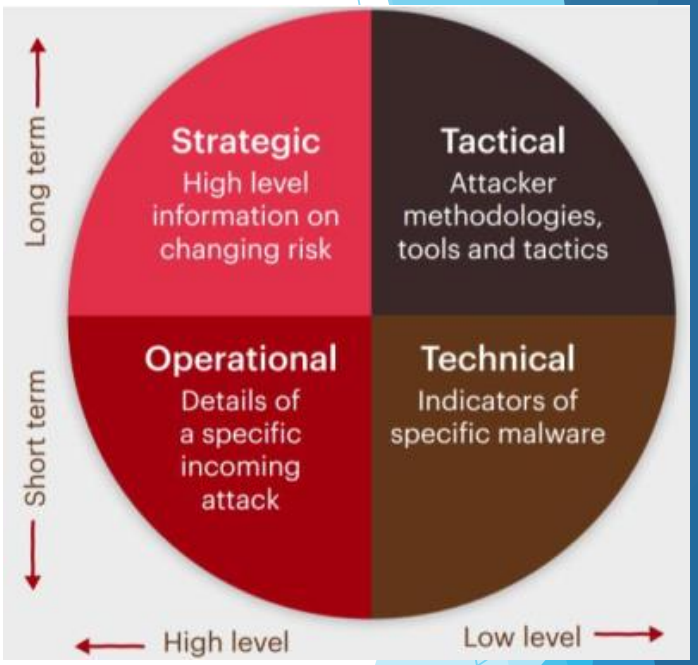
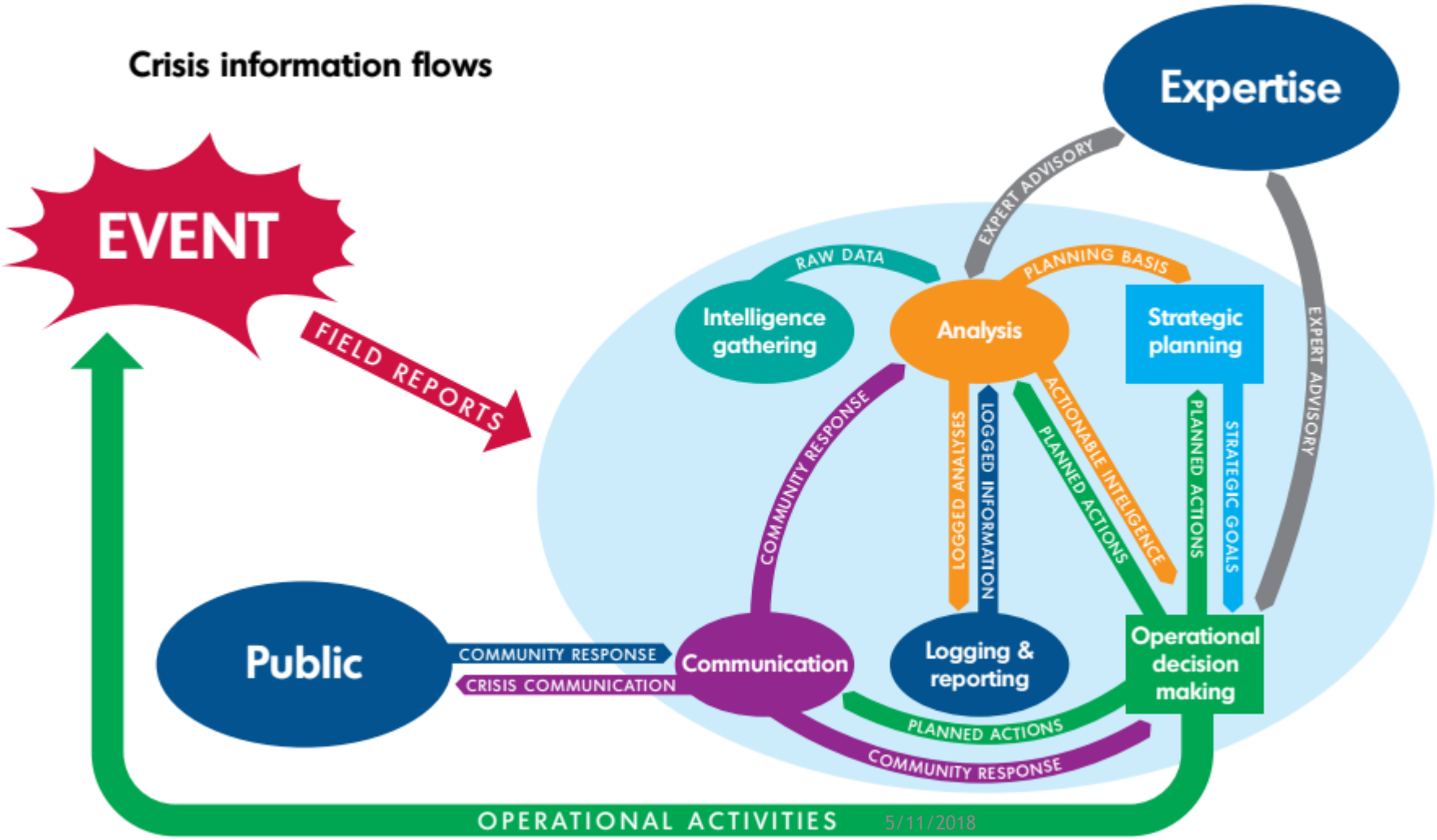

DECISIONS
change, movement
FUTURE
WHAT ACTION?
reveals direction
given purpose, becomes
WISDOM
understanding, integrated, actionable
WHAT IS BEST?
reveals principles
given insight, becomes
KNOWLEDGE
contextual, synthesized, learning
PAST
WHY?
reveals patterns
given meaning, becomes
INFORMATION
useful, organized, structured
WHAT?
reveals relationships
given context, becomes
DATA
signals, know-nothing

Figure 5: Processes involved in generating TI. Image courtesy CERT-UK (CERT-UK, 2015)



CPNI's categorisation of cyber intelligence.

Crisis Information flow



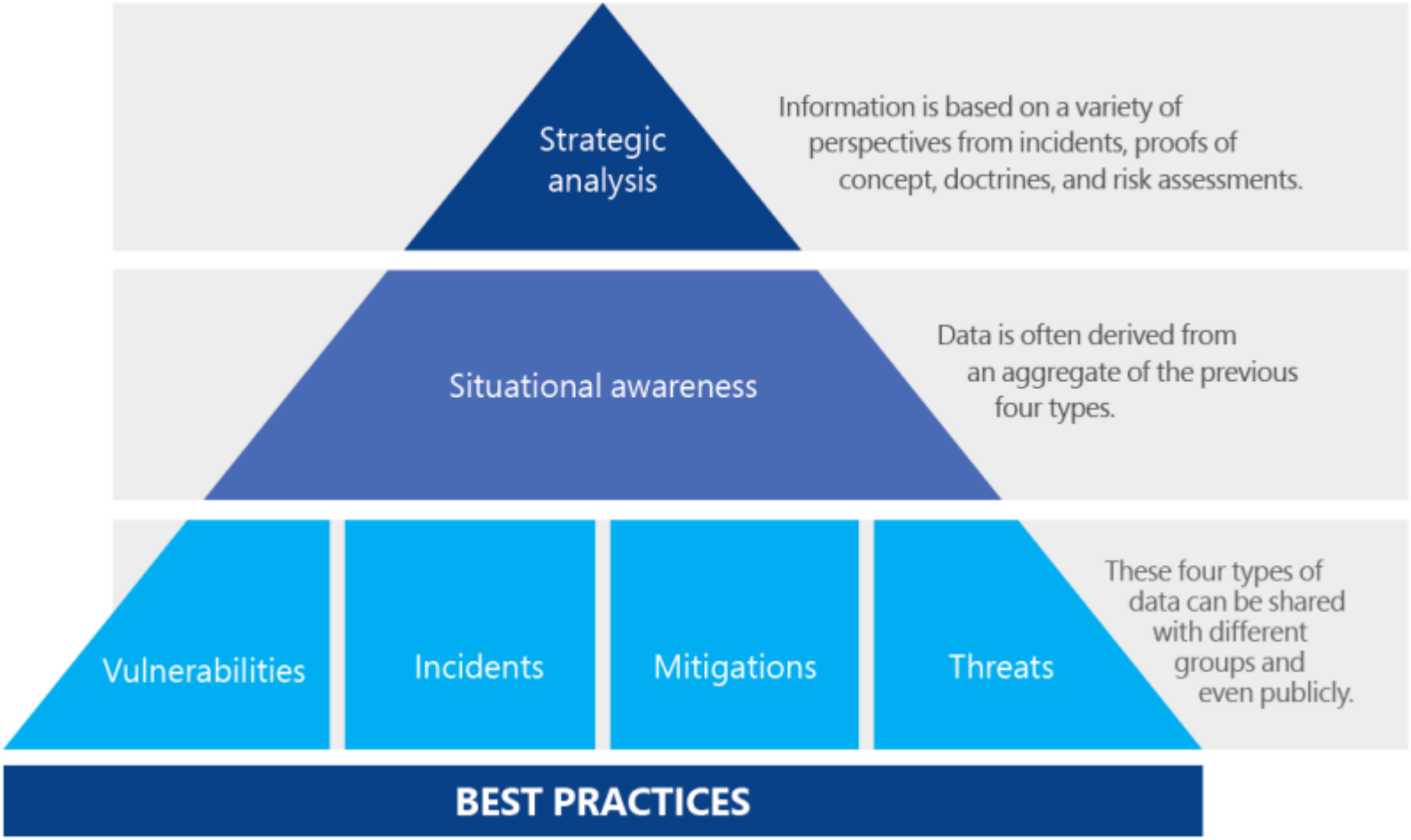
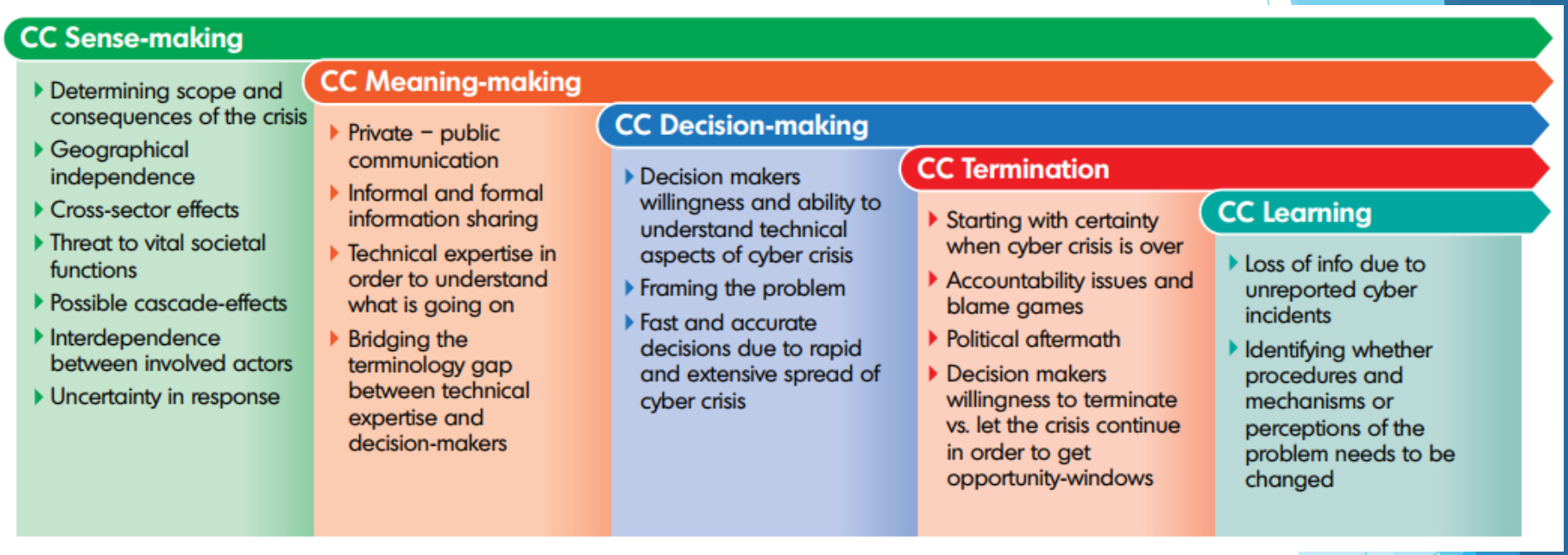


Figure 11: Types of cyber-security information. Image courtesy of Microsoft (Goodwin, et al., 2015)

Challenges of tasks



Needed! ➡ **a harmonized and trusted framework and standard operating procedures to effectively respond to large-scale incidents causing crisis and to hub of experts and a EU-level coordination platform**