CSS
ETH Zurich

EARLY WARNING & INFORMATION SHARING

INSIGHTS FROM CRITICAL INFRASTRUCTURE PROTECTION (CIP)

JENNIFER GIROUX

SENIOR RESEARCHER | PROJECT MANAGER
RISK & RESILIENCE RESEARCH GROUP
CENTER FOR SECURITY STUDIES (CSS), ETH ZURICH

Discussion Trajectory

- Quick Backgrounder: Info sharing in CIP
- Definitions
  - Early Warning
  - Types of Info sharing
- Analytical framework
  - Strategic, preparedness, response
- Wrap Up
  - Challenges

Info Sharing & CIP

- Role of PPP in CIP
  - Challenges: variance in how CIP is viewed; ownership of info and releasing info
- PPP increase in value: age of complexity, uncertainty & regularized black swans
  - Platforms bring CI stakeholders together to share info so to have adequate time to prepare for and prevent failures and/or respond in timely, resource-efficient, and strategically adequate manner
  - = info sharing in CIP is about creating space & mechanism for the early warning of threats

Information Sharing in CIP

Types of Info Sharing

- Between public and private sectors
- Within and between private sector (companies)
- Within and between public sector (governments)

Early Warning

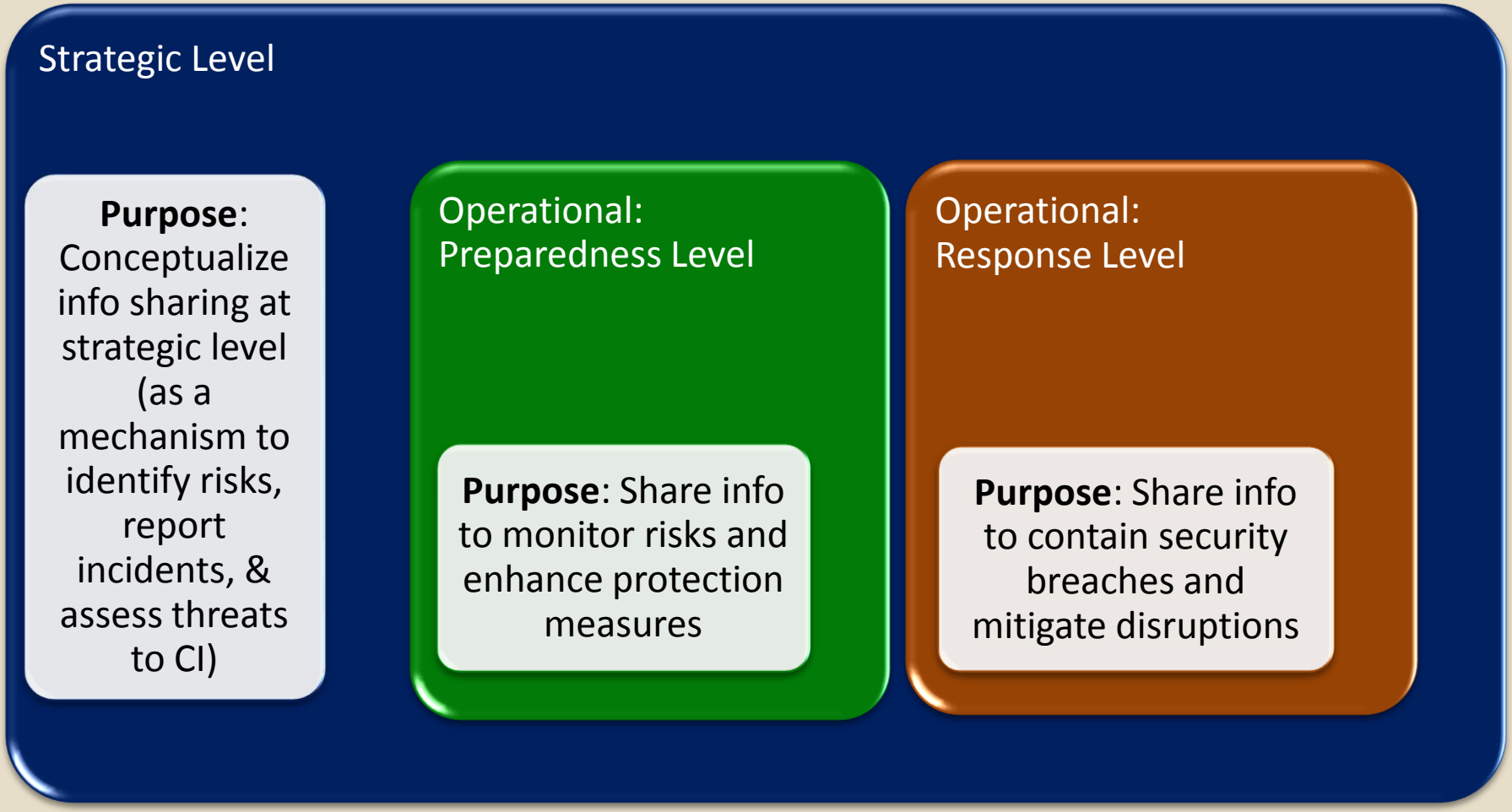
Definitions

In general, EW is the advanced warning of hazards (i.e. events)

Pre-event: EW is about protection - preventing incidents & enhancing preparedness (prevention paradigm)

During event: EW is about resilience - containing disruptions & mitigating effects (resilience paradigm)

Analytical Framework



Public & Private Partnerships

Strategic	Preparedness	Response
Purpose: ✓ (State) Strategic documents; outline role of PPP & info sharing in CIP ✓ Can either make a direct or indirect connection to EW.	**Purpose:** ✓ PPPs exchange Info on CI risks & threats (Threat assess., Intel, etc.) ✓ Enhance situational awareness & preparedness	**Purpose:** ✓ PPPs serve as platform for reporting & response to CI incidents ✓ Members report incidents = early warning for others
Ex.: CIP Strategies; stand alone info sharing strategies	Ex.: (US) DHS HITRAC; (CH) MELANI; (AU) TISN CIP; (UK) CPNI Information Exchanges	Ex.: (CH) MELANI; (Multi-nation) CERTs; (CH) National Emergency Operations Centre (NEOC)

Within & Between Companies

Strategic	Preparedness	Response
Purpose: ✓ Private sector strategic documents ✓ Outline purpose & role of info sharing	**Purpose:** ✓Privately-led CIP partnerships ✓Exchange info on CI related risks, protection strategies, etc.	**Purpose:** ✓ Privately-led CIP partnerships ✓ Platform to report CI incidents & alert members to intrusions (mitigate & contain disruptions)
Ex.: Microsoft's CIPP – "Critical Infrastructure Protection Concepts and Continuum"	Ex.: (US) ISACs (2nd role preparedness; (UK) WARPs (2nd role preparedness)	Ex.: (US) ISACs (primary role report & response; (UK) WARPs (primary role report & response)

Within & between governments

Strategic	Preparedness	Response
Purpose: ✓ Info sharing strategies that outline full vision of info sharing environment ✓Can be within CIP or at national security level	**Purpose:** ✓ Btwn agencies or other states to share info on CI risks & threats ✓Enhance situational awareness & preparedness	**Purpose:** ✓Provide a platform for reporting & response to CI incidents ✓ Members report incidents = early warning to others in the network
Ex.: (US) Info Sharing Environment; (AU) Info Sharing Strategy; (DE) Info Sharing National Strategy	Ex.: (US) DHS HITRAC; (US) Fusion Centers	Ex.: (EU) Secure General Rapid Alert System (ARGUS); (EU) RAS-BICHAT; (CH) NEOC

Wrap Up

CHALLENGES AT THE DIFFERENT LEVELS

Strategic

- Conceptualize to fit early warning pre-event & event
  - Adapt to resilience/risk paradigm
- Political hurdles & competing agenda's
- Legal considerations (privacy or anti-trust)
- Identify network of stakeholders to factor into info sharing exchanges = complex

Operational

Preparedness	Response
• Know your network • Info quality management: accuracy, timeliness, consistency, completeness, relevancy, & fitness for use • Virtual vs. F2F platforms	• Demand & supply of info during event • Info quality: Provide reliable info during event to mitigate disruption • Post-event review & lessons learned

Many Thanks!

STAY IN TOUCH ☺

JENNIFER GIROUX
GIROUX@SIPO.GESS.ETHZ.CH
TWITTER: GIROUXX