

CENTER FOR SECURITY STUDIES

Swiss Federal Institute of Technology (ETH Zurich)

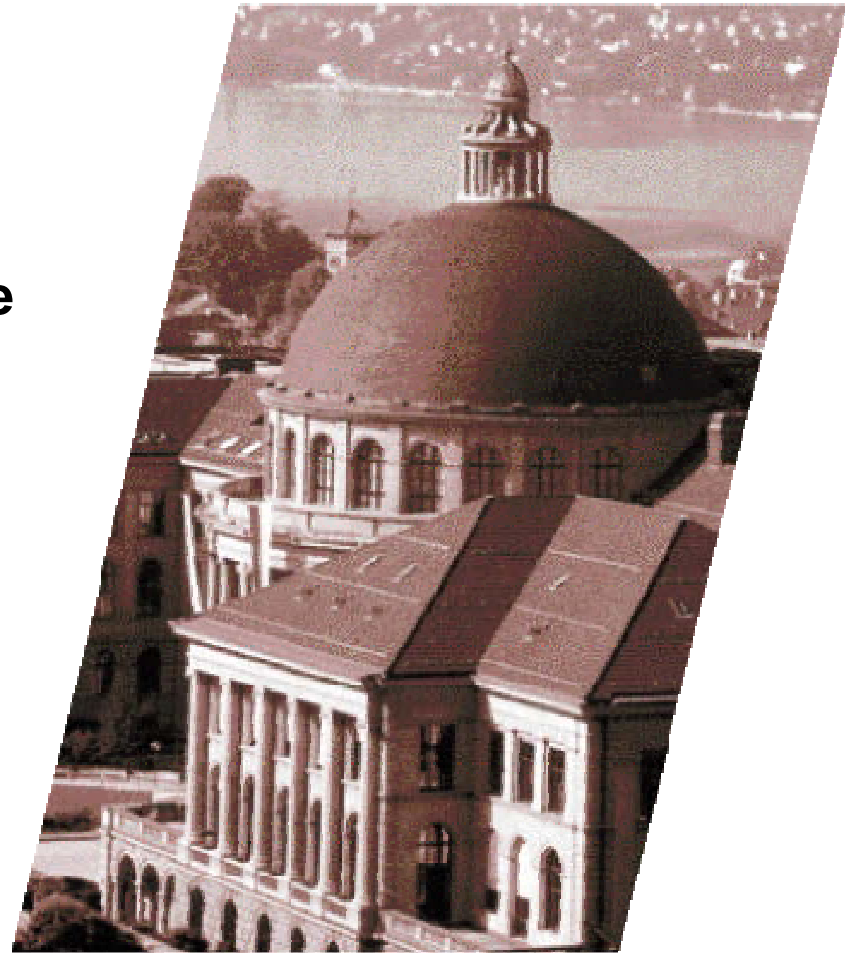
Critical (Information) Infrastructure Protection

History, Trends, and Concepts

Dr. Myriam Dunn Cavelty

ENISA-FORTH NIS School,
Hersonissos, Crete

15 September 2008



Aims of this Presentation

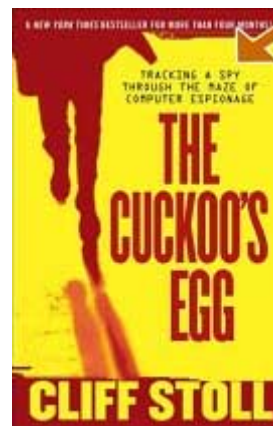
- To show the broader political context of critical (information) infrastructure protection (CIIP)
- To show how the issue evolved into a key national security issue
- To show a Best Practice Model for a CIIP Unit
- To show why many cooperative arrangements between the public and the private sector face difficulties
- To propose a move from Governance to Meta-Governance in CIIP

- A Short History of Cybersecurity Policy Concerns
- The Genealogy of Critical (Information) Infrastructure Protection as a Policy Concern
- Q&A

- A Best Practice Model for CIIP
- The Limits of Public-Private-Partnerships: From Governance to Meta-Governance
- Q&A and Discussion

Short History of Cybersecurity Policy Concerns

- Cybersecurity concerns are not a phenomenon of the 1990s
 - Viruses and Worms since mid-1980s (Morris Worm)
 - Cyber crime (Kevin Mitnick, Captain Crunch)
 - Early Hacker incidents (414s, Operation Sundevil)
 - Culture: „War Games“ (1986); Cyperpunk Novels
 - Espionage: The „Cuckoo’s Egg“ (1988-1989)



- „Hacking“ comes to the attention of the policy community
- *Cyber-crime* interlinked with *foreign intrusion/espionage*
→ elevated to a national security issue!
- Main concern: prevention of damaging disclosures of classified information
- But: Problem rather limited due to nature of the information infrastructure (no mass phenomenon)

Drivers of Change in the 1990s

- Increasingly *networked systems*, rapid technological development
- Quantitative increase in cyber-incidents (*statistics*)
- Gulf War 1991/92, development of *Information Warfare* ideas
- US DoD is target of cyberattacks
 - 1994, Rome Lab
 - 1998, Solar Sunrise
 - 1998, Moonlight Maze
- DoD cyber-exercises
 - 1996, RAND „The Day After“ Exercise
 - 1997, Eligible Receiver

Change in the Security Environment

System:	Bipolar, MAD	→	Change, Complexity
Framework:	Domestic – International	→	Global – Local (Regional)
Space:	Territory = Society = Economy	→	Blurring Boundaries
Power:	Hard Power	→	Soft Power
Actors:	States, IOs	→	States, IOs, NGOs, TNCs, ...
Issues:	Military	→	Military, Economic, Ecological, Cultural, Societal ...

- Information revolution leads to *novel vulnerabilities* (highly interdependent software-based control systems)
- Modern societies rely heavily upon infrastructure, *particularly ICT (dependency)*
- Information infrastructure links other infrastructure systems together
 - inherently insecure
 - “Drivers of change” that aggravate problem in the future (market forces - technological evolution - emerging risks)
- Capabilities* of “new” malicious actors seem enhanced: inexpensive, ever more sophisticated, rapidly proliferating, easy-to-use tools in cyberspace (buzzword: Cyber-terror)
- Asymmetry* as defining feature
- Critical infrastructures* become key focal point

The Genealogy of Critical (Information) Infrastructure Protection as a Policy Concern

- **Critical Infrastructure:** systems whose incapacitation or destruction would have a debilitating impact on the national security and the economic and social well being of a nation
- Interconnected, complex, and increasingly virtual systems
- ‚Soft underbelly‘ of liberal, open, networked societies
- Sectors most often named:
 - banking and finance,
 - government services,
 - telecommunication and information and communication technologies,
 - emergency and rescue services,
 - energy and electricity,
 - health services,
 - transportation,
 - logistics and distribution, and
 - water supply

- CIP as focal point of the current national security debate of Western states
- Confluence of two factors:
 - Modern societies are exposed to potentially catastrophic *vulnerabilites*
 - *Malicious actors* (esp. terrorists) are willing to exploit these vulnerabilities
- Important: CIP as concept and practice has a history
- Current efforts follow „old“ logics ...
- ... but there are „defining moments“

I CIP as security approach is distinguishable by:

1. a concern with the *critical systems* upon which society, economy, and polity depend
2. the identification of the *vulnerabilities* of these systems
3. the identification of the *threats* that might exploit these vulnerabilities
4. the effort to develop *techniques* to mitigate system vulnerabilities

- *Strategic Bombing*: vital nodes of enemy industrial systems could be exploited as vulnerabilities (nodes as ‘vital targets’)
- *Double-edged sword*: assumption that enemy would attack the ‘vital industrial heart’ of the US → First efforts to catalogue the ‘critical infrastructure’ of the US (before WWII)
- *The United States Strategic Bombing Survey* (early CW): a set of techniques grouped together under the term ‘vulnerability mapping’

- 1960s and early 1970s: techniques for analyzing the vulnerability of systems and for planning response are generalized
- '*Total preparedness*' and all-hazards planning in the 1970s
- *Non-deterrable threats*: a sub-group of security thinkers with ties to civil defence became concerned with the rise of threats other than the Soviet Union
- *Vital Systems Security* in place around 1984: a national security problem in its own right

Information Revolution as Defining „Moment“

- Growing concern with information security (1980s/1990s) found *technical vocabulary*, set of *analytical tools*, and practices of intervention in mode of thinking about infrastructures as a security problem
- Shift from a specific emphasis on systems essential for military production *to broader concern* with vital systems essential for the economic and social well-being of the entire nation
- Change of emphasis *from physical* infrastructure *to information* infrastructures
- CIIP as subset and vital part of CIP

A Best Practice Model for CIIP

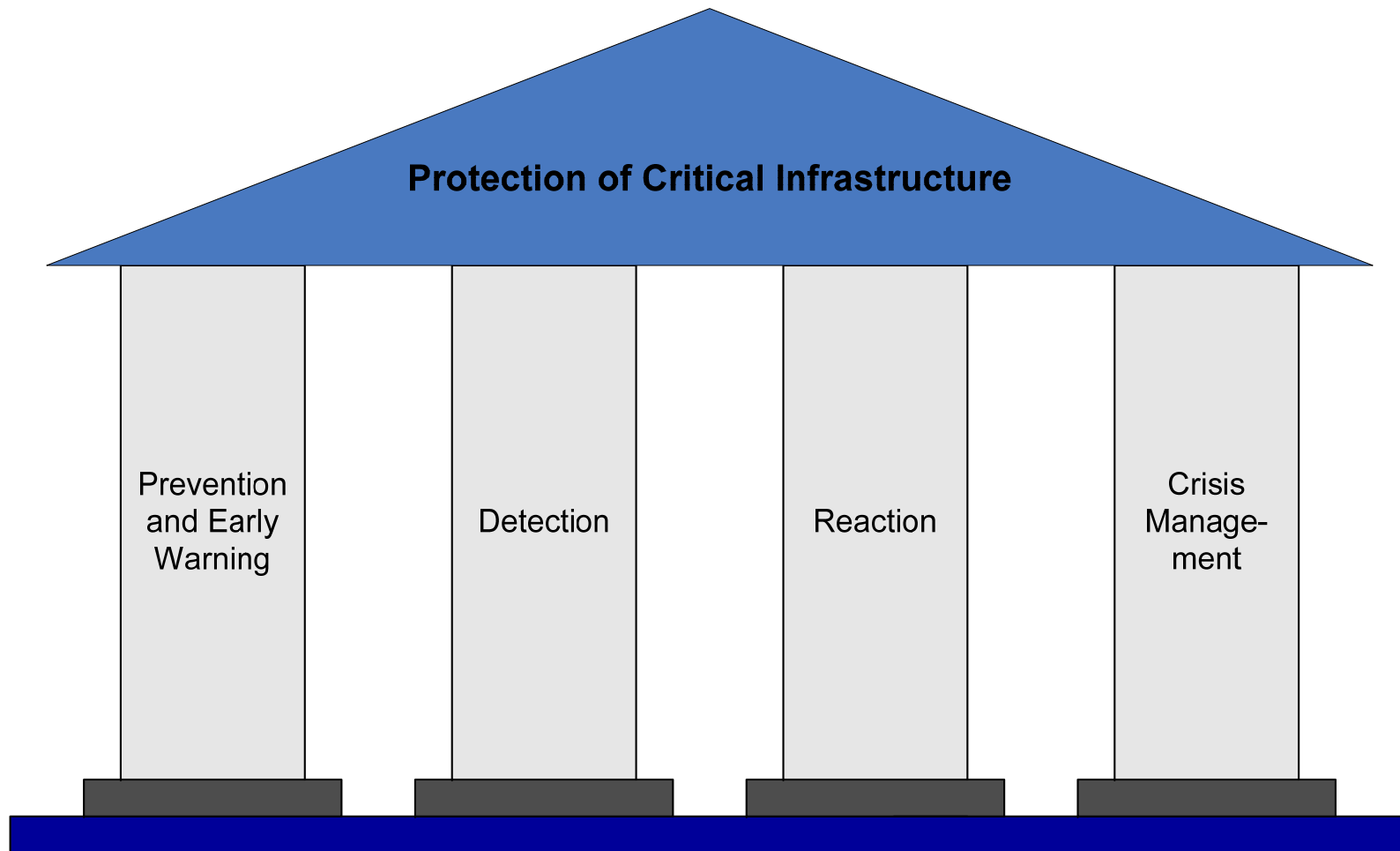
The Dilemma of the State

- Power to *resist* vulnerability disappears *outwards*, to transnational actors and international organisation
- Power to *cause* vulnerability disappears *downwards*, even down to the level of the individual
- State can no longer „go it alone“ – private actors increasingly important
 - Non-state actors threaten
 - Non-state actors directly threatened
 - Non-state actors needed for definition AND enactment of security policy
- Public-Private Partnerships (PPP) are seen as panacea for this problem
- Cooperation programs following the PPP prototype are part of all existing initiatives in the field of CI(I)P

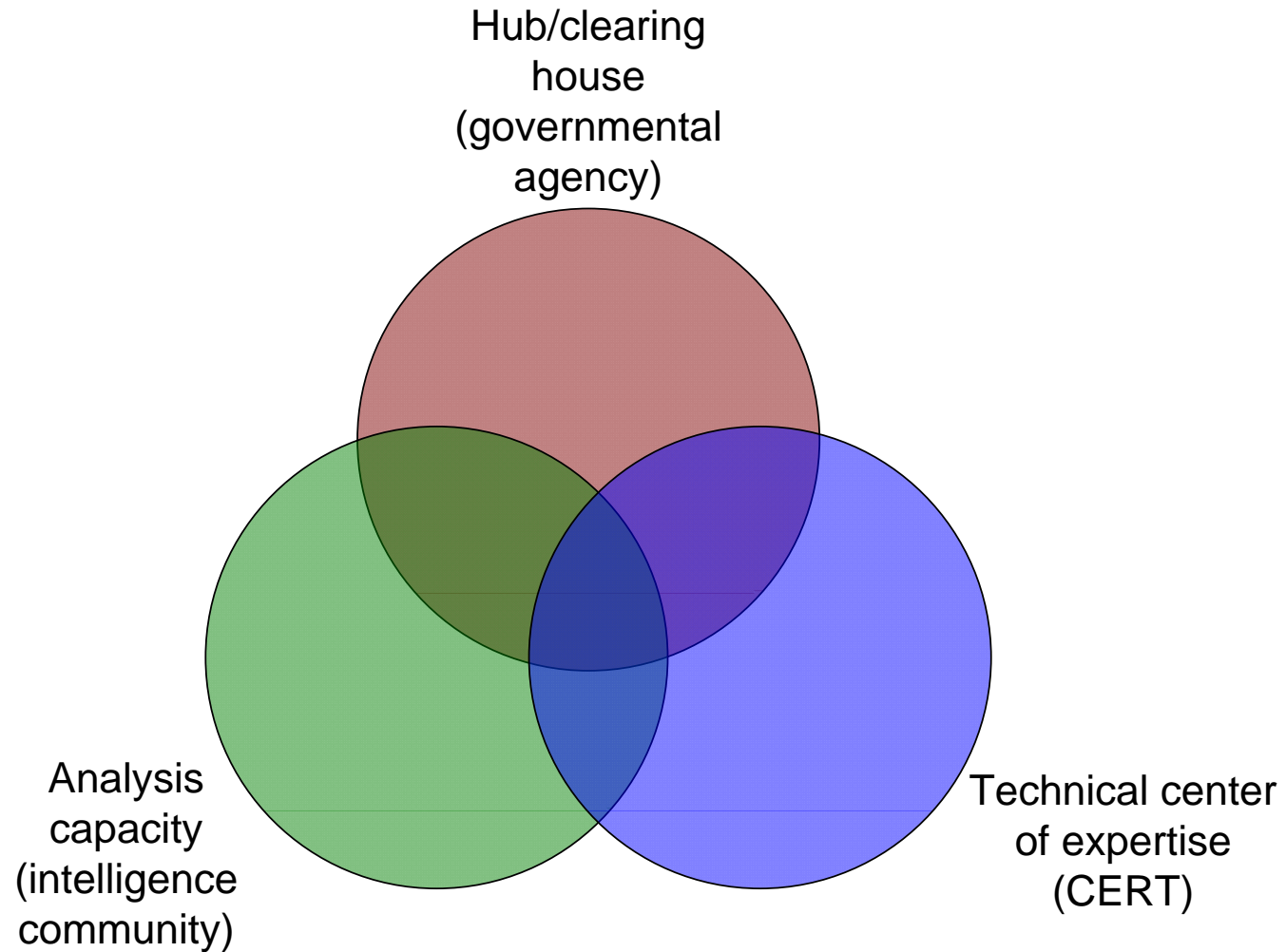
- Critical Information Infrastructure Protection (CIIP) is a *complex and multi-faceted* task:
 - The threat spectrum is very wide and rapidly evolving
 - CIIP involves *various actors*: governmental agencies from different ministries as well as private companies
 - *Different perspectives*: technical, business, law-enforcement, national-security
- National models for CIIP organizations are not necessarily applicable to other countries, because of their complexity and their *country-specific configuration*
- Many of the existing solutions are fairly *resource-intensive*
- What could the “optimal” CIIP Unit look like?

- Design of a relatively inexpensive solution that can be further tailored to country-specific needs
- Key elements for such a unit:
 - Concentration on the *essential tasks*
 - *Cooperation* with all relevant stakeholders
 - *Flexibility* and *adaptability*
 - *Information-sharing* with the private sector
 - *National and international contacts*
- It is *no static solution*: CIIP unit must constantly take into account
 - various interests of its partners
 - that different incidents may demand different alliances

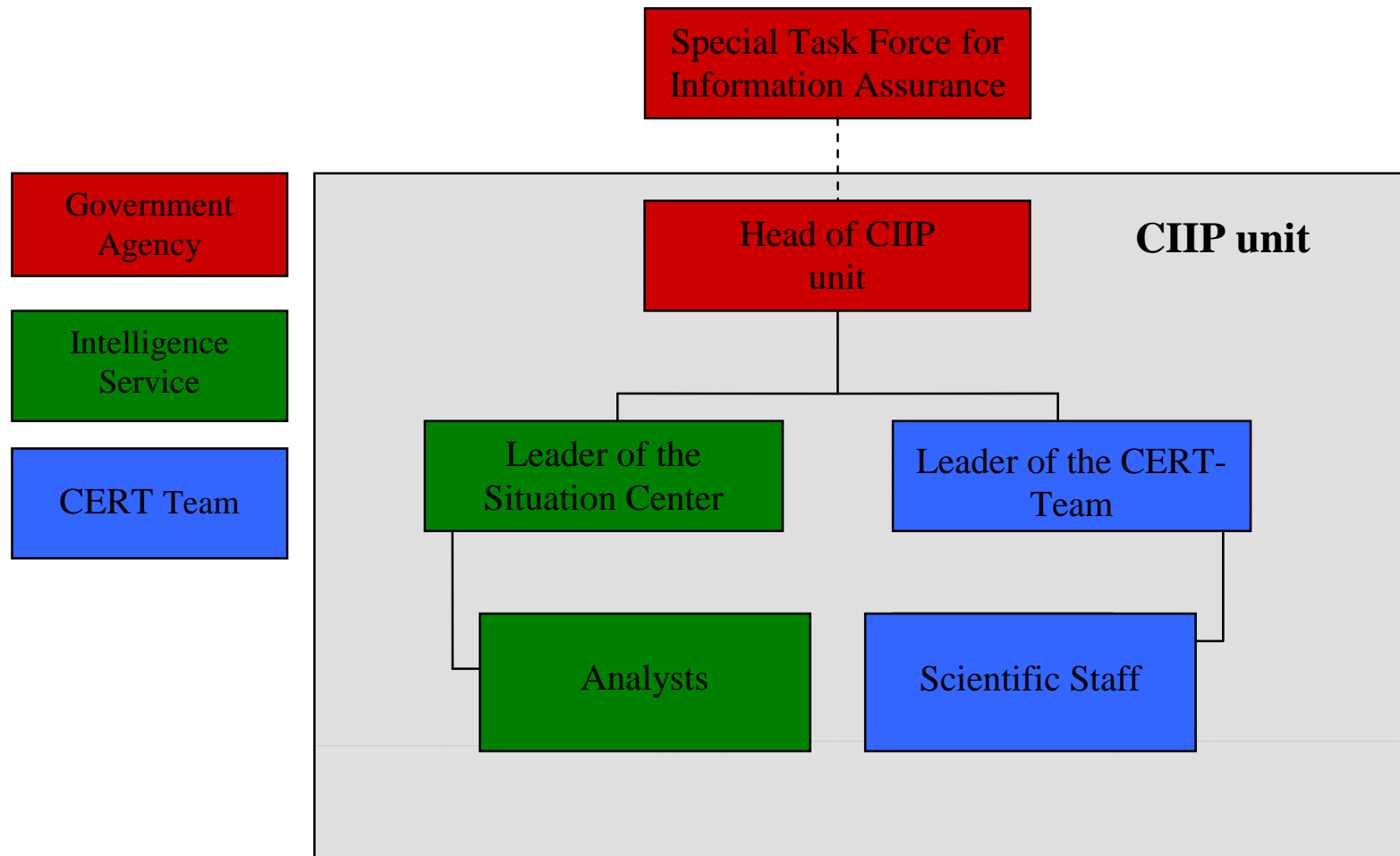
Essential Tasks: The Four Pillars of CIIP



Essential Partners: The Cooperation Model

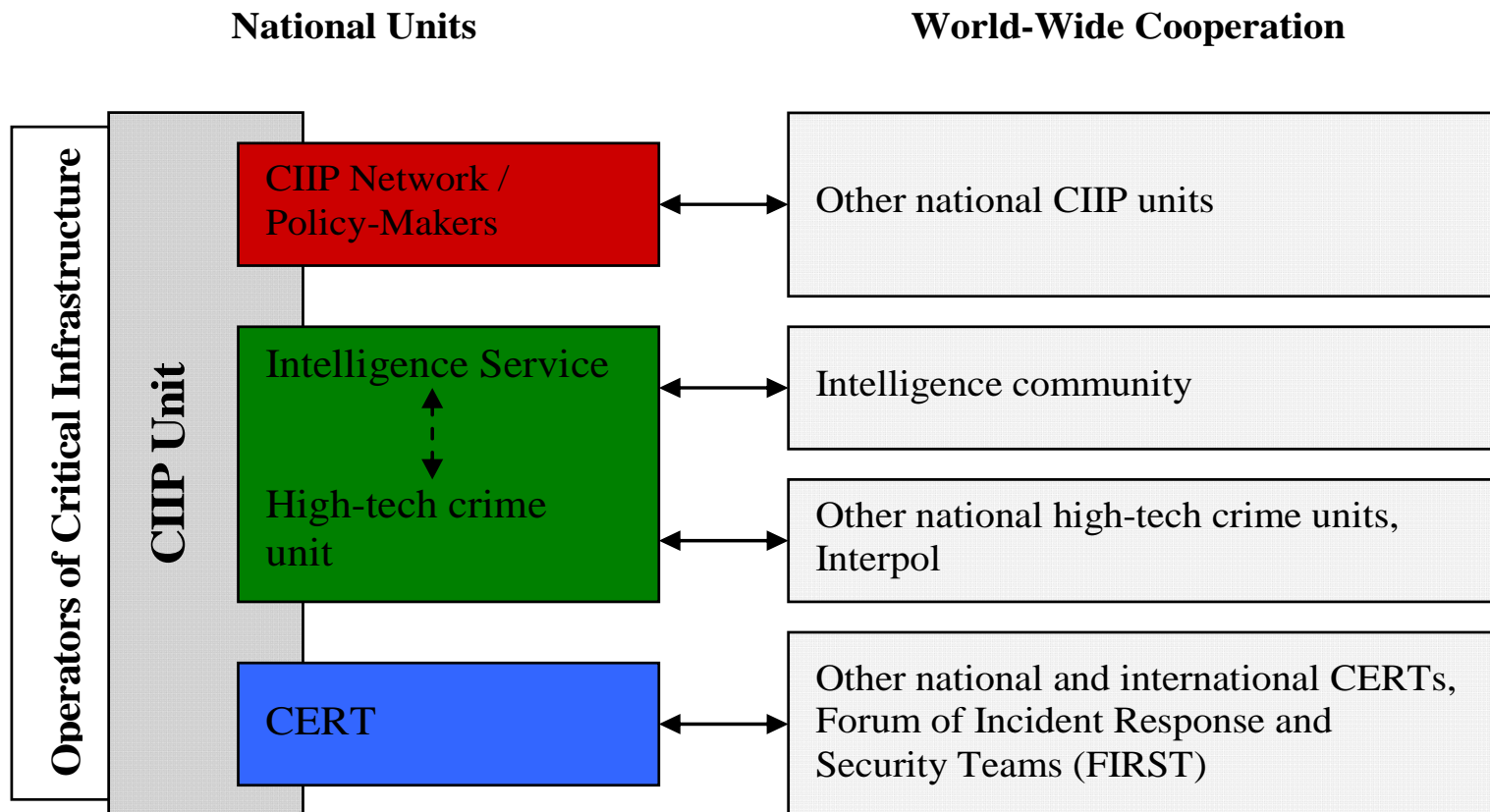


Organization of the CIIP Unit



The Network of the CIIP Unit

- In order for the CIIP unit to be successful, each sub unit needs to be embedded in a broad network of national and international partners.



The Two Customer Bases of the CIIP Unit

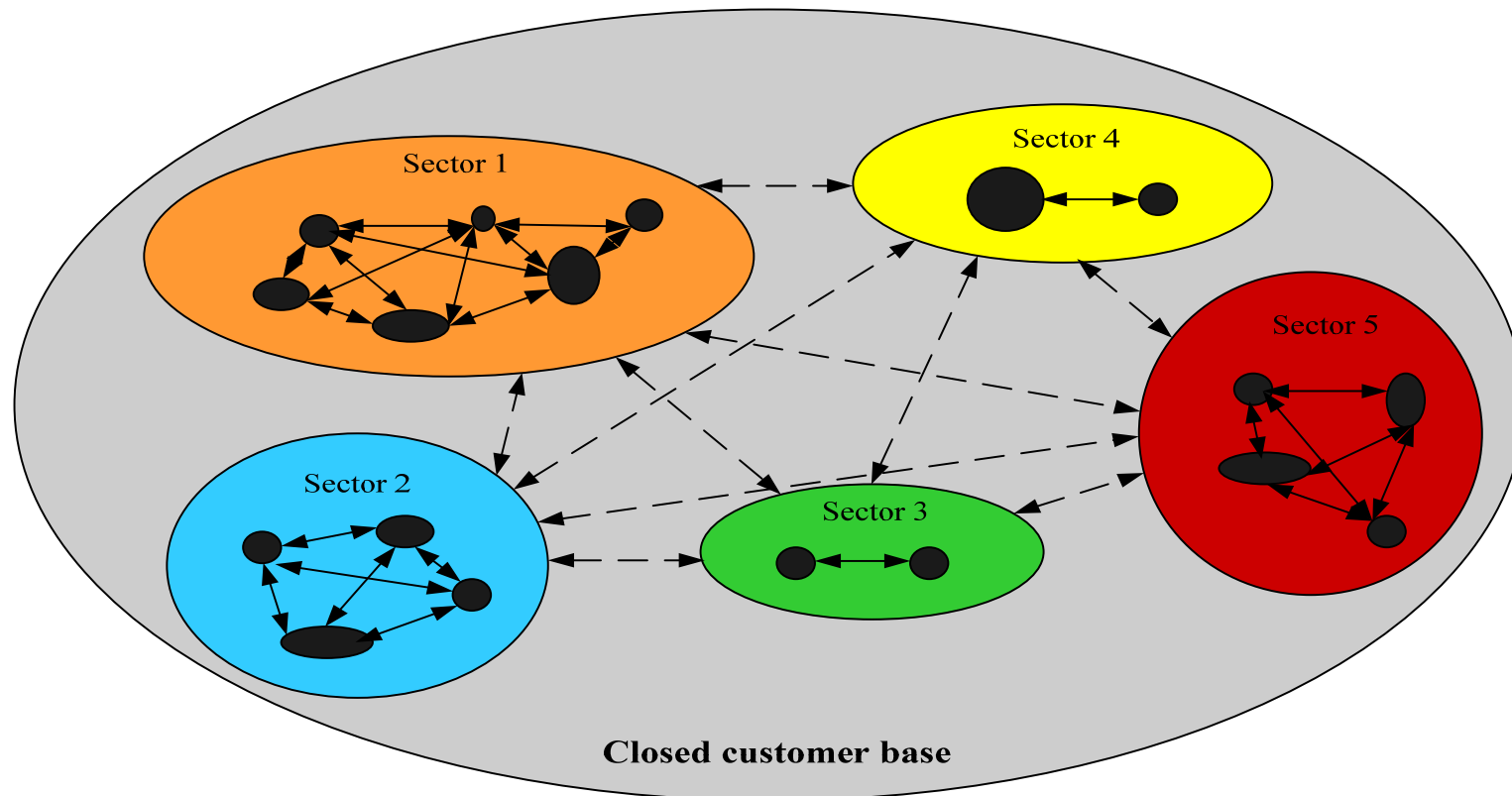
- Most importantly, the CIIP unit must *address the owners and operators of CII*
- However, in the fight against cyber-crime, it is also vital *not to neglect private users, SMEs, and other large businesses* that are not operating CII
- In consequence, the CIIP unit serves two customer groups:
 - the *Closed Customer Base*, which should include the operators of nationally critical infrastructures; and
 - the *Open Customer Base*, which includes all other companies (in particular SMEs), as well as home computer users

The Two Customer Bases of the CIIP Unit

Customer base	Closed	Open
Members	Selected operators of critical infrastructures (limited membership)	SMEs Citizens
Number	2-4 representatives of each member	Open
Trust	Strong Trust	Weak Trust
Build-up of Trust	Within the whole customer base (regular meetings, interactive network), and in particular within each sector.	Media, internet, exhibitions - with the help of partners.

The Closed Customer Base

- Membership of the CCB is restricted to operators of CII.



Products and Services for the Closed Customer Base

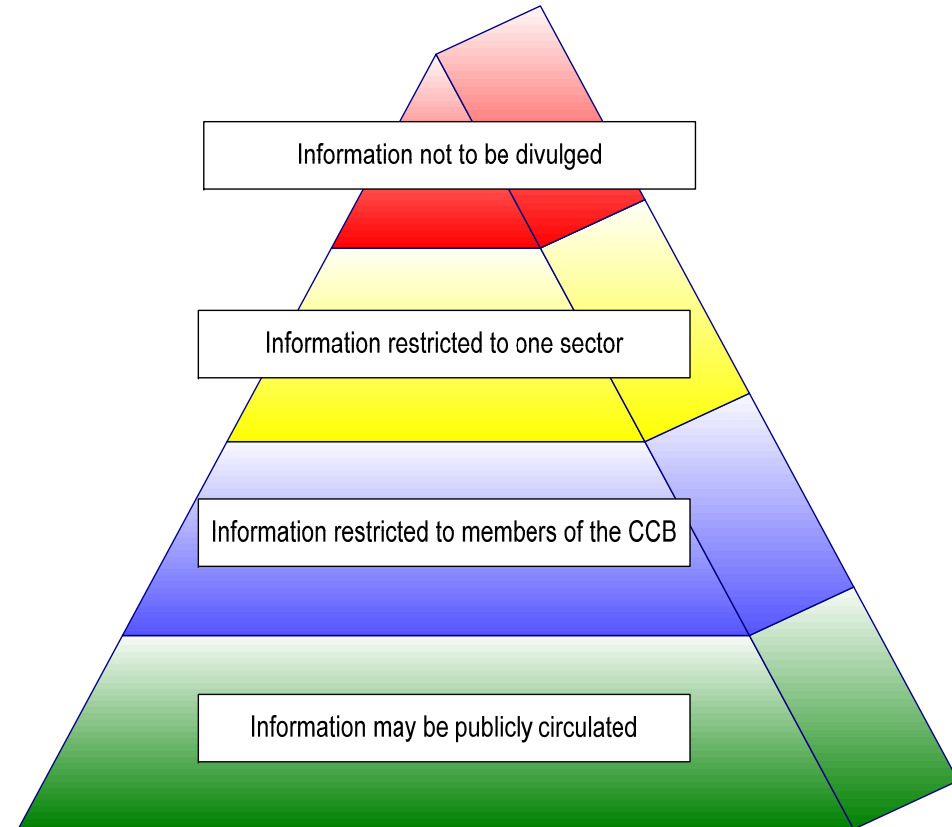
- Assistance in case of incident:
 - 24/7 on-call service
 - One-stop-shop

- Distribution of exclusive information:
 - Early warnings, situation reports, background information, perpetrator profiles
 - Online platform, newsletters

- Workshops, meeting, exercises:
 - Sector-specific workshops: reinforcing knowledge of specific issues
 - Cross-sectoral workshops: increasing awareness of interdependencies

Information-sharing and Classification Levels

- Considerable *know-how can be gained* through exchanges of experiences
- Companies are *competing* with each other
- Information-sharing in the area of information security can be *an extremely sensitive matter* for companies
- ➔ Strong mutual trust is an absolute condition for any information-sharing effort
- ➔ Each company should be able to decide with whom it wants to share information



- The Open Customer Base: private users, SMEs, large businesses that are not operating CII
- Services and products for the Open Customer Base:
 - *Awareness-raising*: increasing basic knowledge on information security
 - *Warnings and advices*: filtering the bulk of warnings
 - *Assistance in case of incident*: providing hints on problem resolution, answering technical questions
- Partnership with other actors (Media, private associations, other governmental agencies)

The Limits of PPP: From Governance to Meta-Governance

- Cooperation programs following the PPP prototype are part of all existing initiatives in the field of CI(I)P
 - Some successfully facilitate the exchange of information between both sides
 - Others, however, have scarcely generated more than joint statements of intent of the actors involved
- Result: *increasing criticism*
 - condemning the lack of efficiency in existing arrangements
 - questioning the validity of the entire cooperation concept

- PPP concept originally developed in a completely *different context*: in the field of administrative reform in the 1980s (New Public Management)
- Subsequently, PPP concept *adopted uncritically* by many governments for CIP policy at the end of the 1990s
- To this day, concept remains *defined vaguely* or not at all, and in particular is devoid of theoretical foundation
- This causes a number of *problems in the implementation* of such forms of cooperation and is main cause for feelings of disillusionment

- *Problem 1:* The state has no way of *monitoring* whether private companies are fulfilling their functions in the area of CIP
- *Problem 2:* Public-private cooperation is often difficult due to *diverging interests*
- *Problem 3:* PPP can only be carried out with selected companies and must be *small* (based on mutual trust). The *number of PPP must remain limited*, since an overly large number would exceed the government's capacities
- *Problem 4:* Due to the intensive involvement of the government, PPP are *not suited for fostering international cooperation*

- Problem: critics of PPP risk throwing the baby out with the bath water
- Fact: cooperation between the state and private enterprise on CIP is not only sensible, but quite simply essential
- *New / expanded models are required:*
 - Direct partnerships between public and private actors are *just one of several instruments* that can be deployed in the field of CIP
 - Need approach that does not reduce cooperation between the state and the private sector to direct partnership (as in the case of PPP), but also takes into account *other forms of interaction*

- **Governance** takes place wherever political power is highly fragmented
- Fragmentation of political power can occur through decentralisation, government tasks and authority are delegated
 - downwards (localisation),
 - upwards (supranationalisation), or
 - sideways (privatisation)
- Older ideas of governance (neoliberal approach, PPP) demands **“less government and more governance”**
 - State precisely defines and contractually stipulate how the tasks it delegates to companies must be fulfilled

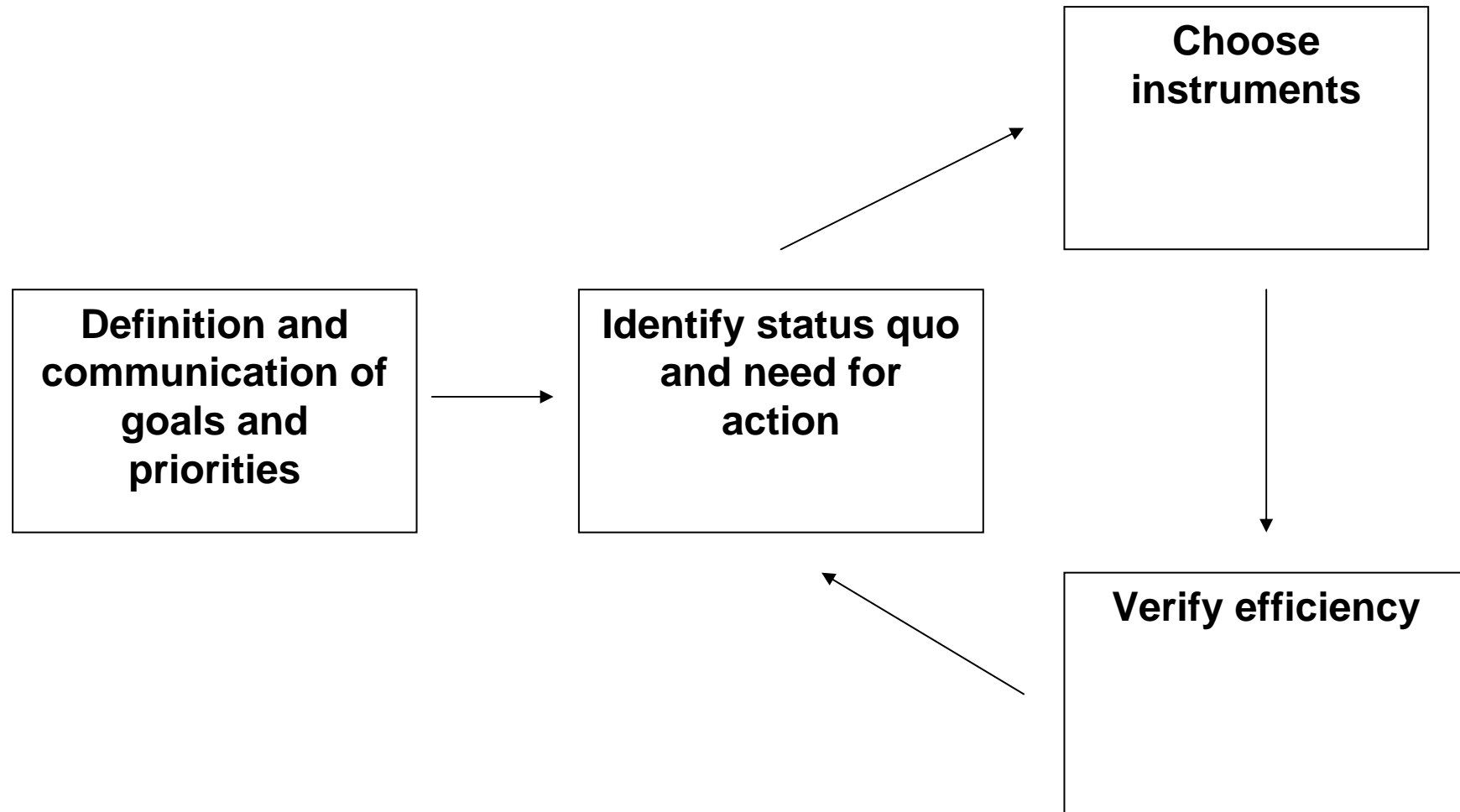
- In conditions of increasing specialisation, *direct control* becomes *increasingly difficult*
 - Governments no longer have required specialised knowledge to ensure appropriate degree of control over outsourced functionalities and services
 - Governments can no longer simply issue instructions and monitor their implementation
- Complex, modern societies require *new forms of public administration*
- Such new forms are called *Network Governance*

- Public services are provided by independent, self-regulating, and *self-organising networks*
 - *Small and relatively homogenous networks* involve all actors who will and can contribute to the fulfilment of a public service in their own interest
 - Such actors, from both the public and the private sectors, then organise themselves *quasi autonomously*
 - They *fix rules* for common action and determine responsibilities and commitments of individual partners
- The various networks monitor themselves, because it is only within the network that sufficient expertise can be found to check whether all parties are meeting their obligations

New Role of Governments

- ▮ Instead of distributing tasks and monitoring fulfilment, governments take on role of *coordinators and stimulators of networks*
- ▮ This indirect control is referred to as “organisation of self-organisation” or “*meta-governance*”
- ▮ Part of this meta-governance consists in *creation of framework conditions* that allow networks to organise themselves
- ▮ Governments must activate new networks *only when necessary* and orchestrate and modulate existing ones
 - ▮ governments first define public tasks and then verify whether they are already being carried out
 - ▮ If a function is not being fulfilled sufficiently, governments must create new networks or convince existing networks to fulfil it
- ▮ Choosing the *right instruments* to promote the specialized networks becomes the most crucial responsibility of governments

The Meta-Governance Process



- *Problem 1: The state has no way of monitoring whether private companies are fulfilling their functions in the area of CIP*
 - Solution: self-regulation (and self-policing) of networks
 - Partners within a network know each other well and are able to assess whether degree of cooperation is sufficient
 - While companies may find it easy to gloss over their weaknesses and vulnerabilities towards government, it is more difficult to embellish performance in communication with other experts
 - Example: ISACs (FS-ISAC)

- *Problem 2: Public-private cooperation is often difficult due to diverging interests*
 - Problem mainly arises when partners are forced to cooperate
 - Networks can only be successful if they are based on a sufficiently large common denominator
 - Self-organisation will partly solve this problem
 - When governments can make a meaningful contribution to the functioning of a network, they can be part of it (as primus inter pares)
 - Example: Swiss Reporting and Analysis Centre for Information Assurance (Melde- und Analysestelle Informationssicherung, MELANI)

- *Problem 3: PPP can only be carried out with selected companies and must be small, The number of PPP must remain limited*
 - Only an issue if one assumes that it is mandatory for the government to work together with private businesses directly (ignores the possibility of self-regulating networks)
 - Businesses themselves have an interest in security, and some of them are already engaged in sub-areas of CIP
 - Government's role can therefore frequently be limited to that of promoting existing networks with similar mandates or supporting the emergence of new networks
 - Example: Warning Advice and Reporting Points (WARPs)

- *Problem 4: Due to the intensive involvement of the government, PPP are not suited for fostering international cooperation.*
 - International cooperation is often obstructed rather than advanced by the direct involvement of governments
 - Large corporations that operate critical infrastructures are frequently well-connected at the international level
 - Cooperation between experts can therefore evolve quite naturally
 - Example: Forum of Incident Response and Security Teams (FIRST)

- The *context/history* of policy issues can help us understand characteristics, peculiarities and path-dependencies
- *Almost all aspects* of an issue are influenced by the context/history of it
- The absolute key issue in the field of CIIP are *public-private partnerships (PPP)*
- Good solutions for PPP exist – but they have their *limitations*
- They can be overcome if *government's role is redefined*
- CIP policy should be based as far as possible on *self-regulating and self-organizing networks*

Thank you!

Dr. Myriam Dunn Cavelty
Center for Security Studies
ETH Zürich WEC
Weinbergstrasse 11
8092 Zurich
Switzerland