Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI

The Swiss National Cyber-Strategy

Marc Henauer
ENISA Workshop
27. 9. 2012, Brussels

Agenda

- The Mandate and the Challenges
- The Different Notions of Cyber
- The Logic Framework of the National Strategy for the Protection of Switzerland against Cyber-Risks
- Conclusion

The Political Mandate

Establish a national strategy on cyber-defense and analyse:

- The threat in the cyberspace,
- Protective and safety measures of Switzerland and our critical infrastructures in particular,
- Vulnerabilities,
- Possible countermeasures.

Challenges

- Switzerland: a small country?
- Swiss political structure (federalism, direct democracy, neutrality)
- national versus economic interests
- Incentives
- mandatory versus voluntary cooperation
- responsibility and liability
- law and standards

Cyber Defense vs. Cyber Risk

- The term „Cyber Defense“ suggests and entails the following notions and concepts:
  - Cyber is kind of a mono-thematic topic
  - A defense of cyber attacks seems feasible, within a certain space.
  - (Technical) Security Concepts are in the foreground, such as standardization, certification, etc…
  - Analogies to existing concepts, such as Deterrence, Credible Defense Posture, Retaliation, etc… seem appropriate and are used frequently when discussing the concepts of „Cyber Defense“
  - Certain centralistic steering and coordination capabilities are necessary and possible on a strategic level

Cyber Defense vs. Cyber Risk

- The term „Cyber Risk“ suggests and entails the following notions and concepts:
  - Cyber is first and foremost an extension of existing risk-sets
  - A thorough and a as specific threat-analysis as possible is necessary to asses cyber risks
  - Security concepts are only a part of a holistic and integral risk-management-process
  - There is no territorial or similar limitation to cyber
  - Concepts from the realm of defense and immunization cannot be applied, since risks can neither be fought, nor be defended against. Risks can only be reduced and minimized.

The fundamental principles

In part delegation of strategic and operational responsibilities

vs.

Development of structures and processes to obtain a sustainable security culture

Compliance

vs.

Risk Management

The Logic Framework of the Swiss Cyber Strategy

If the strategic handling of risks lays within the responsibility of the management, hence management is also responsible for cyber-risks.

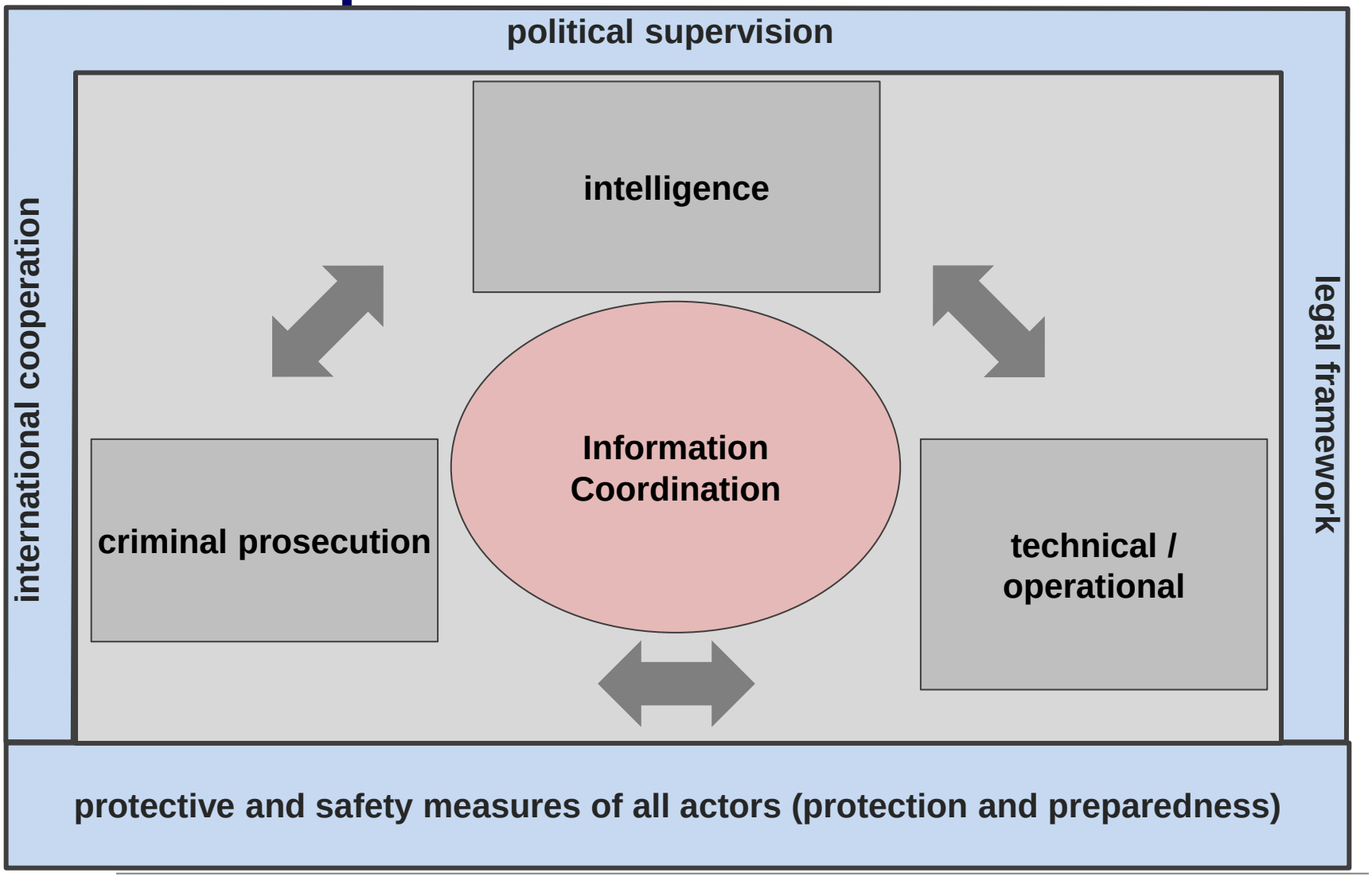
This leads to:

The better and the more complete management is able to identify cyber-risks, the more informed management can take risk-management-decisions.

Ergo:

Establishing the necessary means, resources and processes for a central information gathering, analysis and dissemination is the National Strategy's core demands, in order to enable the responsible stake-holders, to asses occurrences based on the real threat-landscape. This must be the base for specific implementation of the proposed 16 measures within 7 spheres of action, ranging from competence building to continuity management and a heightened international presence.

Capabilities for an Integral Threat Landscape



Conclusion – What the Strategy does

- The core principles are based on self-responsibility. Cyber-risks are understood as an extension of existing responsibilities, means and mandates.
- The focus of the strategy lays on existing processes and structures. These have to be further strengthened, enabled and merged on an operative level to support the strategic decision-making-process.
- The strategy postulates a set of measures reaching from competence-building measures, risk and vulnerability analysis to business continuity planing and crisis management.
- Switzerland shall use its advantages in the field of PPP by consequently strengthening its already established cooperation models in the field of managing cyber-risks.
- Responsible stake-holders within administration (MFA, Regulators etc…) and private economy are required to further work together and implement the measures by 2017.

Conclusion – What the Strategy does not do

- The National Cyber-Strategy does not establish a „Cyber Defense Center“, neither a „Cyber-Tsar“ nor any kind of „Cyber-Ghostbusters-Troop“ as other strategies in other countries do. Switzerland is therefore taking a different approach, by implementing the handling of cyber-risks within existing processes and responsibilities.

- The National Cyber Strategy explicitly excludes war or war-like situations. The Swiss Army is tasked with establishing its own strategy or concept, as well as the implementation thereof, including military doctrine et al.

- The Strategy is not excluding the possibility of active measures even within peace-times. The necessary legal framework for such actions will have to be subjected to the political process.

- The 16 measures of the National Strategy are not meant to solve the whole issue of critical infrastructure protection. They are designed to correspond with overarching measures, stipulated in the National Strategy for the Protection of the Critical Infrastructure.