Cyber-Security Strategy and Regulatory Context

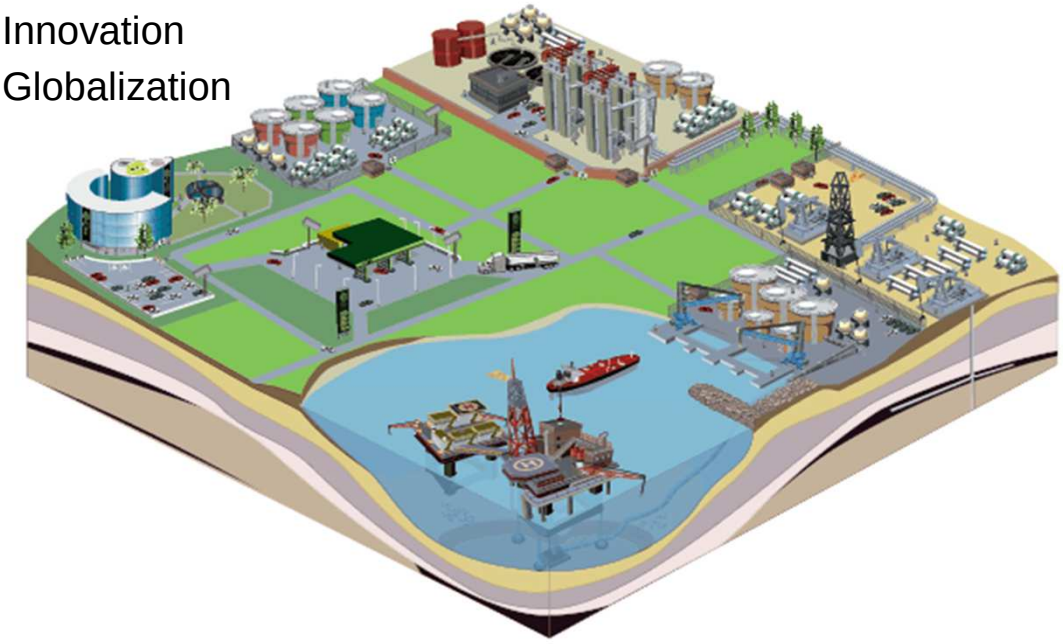
Paul Reither, OMV AG

Chamber of Commerce and Industry of the Russian Federation
Moscow, 30. March 2018

Moving more. Moving the future. OMV

THE HYDROCARBON VALUE CHAIN CHALLENGES DRIVES DIGITIZING THE HYDOCARBON NETWORK…

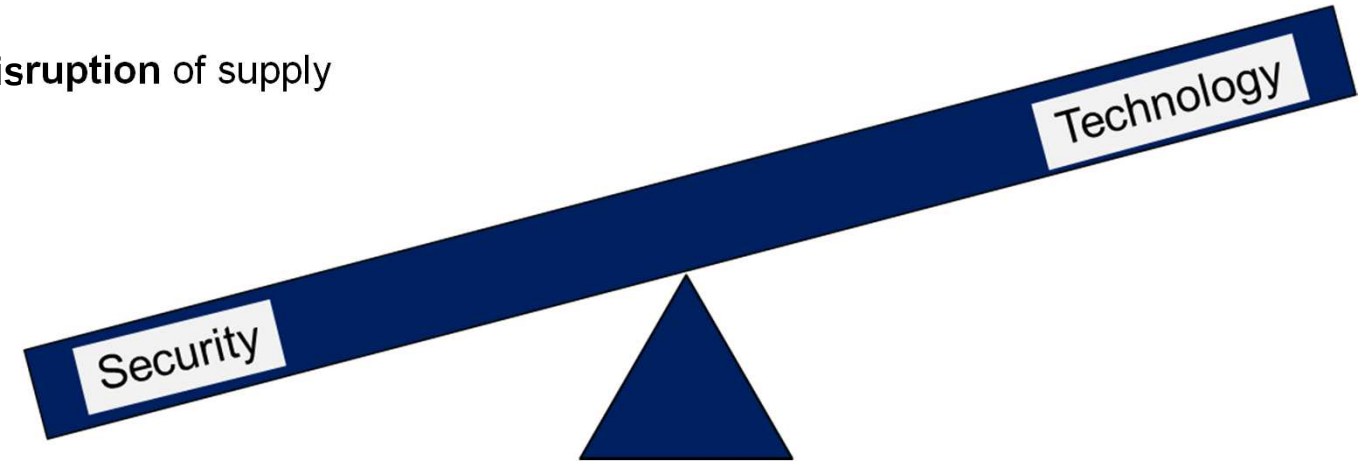
- Competition for reserves
- Pressure on cost
- Innovation
- Globalization



- Real time production and reservoir monitoring
- Collaborative production operations across teams and technologies
- Production optimization and real time asset monitoring
- Automated issue detection and response, predictive asset maintenance

..WHICH MIGHT COMPROMISE SECURITY AND SAFETY

- Compromising the oil field and refining networks can create **physical impact** on safety and environment
- Potential for **compromise of information** flow might impact competitive advantage
- **Disruption** of supply

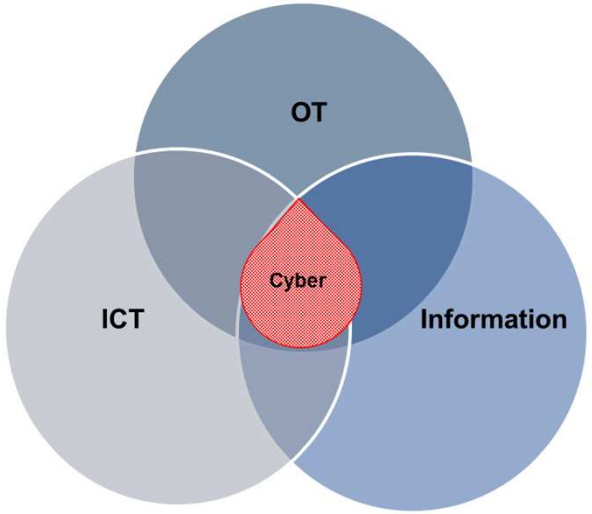


A THREAT BASED, HOLISTIC APPROACH IS REQUIRED

Homogenous Threats (random)

- Vulnerabilities
- Actors unknown
- Random

„IT Security“ – compliance driven, baseline measures



Insider Threats

Heterogeneous Threats (targeted)

- Attractiveness
- Actors known
- Targeted

Direct threat, physical or digital threat based measures

Regulatory framework of Cyber-Security (example EU and A)

EU-Directive on security of network and information systems (NIS)	▶ Aims at acquiring a high level of security of network and information systems across the EU (harmonization) and to improve the security of critical infrastructure against disruptions and attacks
	▶ Key aspects
	  ▶ national strategy for security of network and information systems
	  ▶ definition of operators of essential services and digital service providers
	  ▶ national organizational and coordinating structures
	  ▶ data protection and sanctions
	▶ Sectors affected (Annex II): energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructure

National implementation	▶ The EU-Directive has to be implemented into national law until May 2018
	▶ Operators of essential services have to be defined by November 2018.
	▶ Discussions with Federal Chancellery and Ministry for Interior ongoing – draft expected in upcoming weeks
	▶ Austrian Strategy for Cyber-Security (ÖSCS)
	  ▶ Adopted by the Austrian Government in March 2013
	  ▶ Key aspect is the establishment of a coordination structure at operational level with the aim of securing a regular exchange between cyber-security stakeholders in Austria and to continuously monitor and analyze the situation in the cyber-field
	  ▶ Concrete measures were defined to improve cyber-security in Austria and to secure high resilience of critical infrastructure against cyber-attacks

Operators of essential services

- **Member States shall identify operators of essential services which will be obliged to**

- Comply with security requirements at technical and organizational level
  - State of the art; adequacy
  - Usage of international norms, standards and specifications

  ➔Operators need to provide evidence for the effective implementation (e.g. result of authority/qualified auditor)

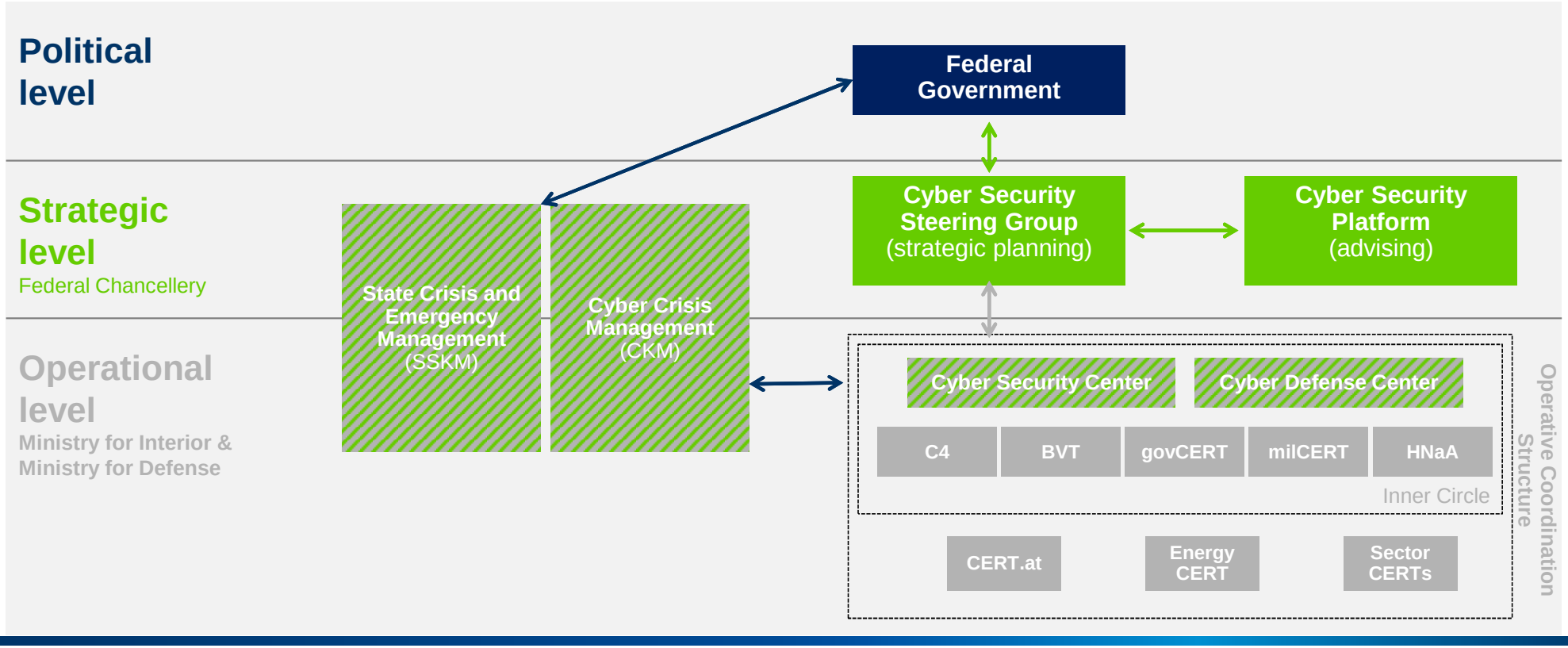
  ➔Authority may issue binding instructions to remedy the deficiencies identified (Art. 15)

- Notification of incidents with significant disruptive effect on the provision of that service (Art. 6), a.o.
  - Number of relying users
  - Dependency of other sectors of Annex II
  - Impact on economic and societal activities or public safety
  - duration
  - geographic spread

  ➔ **Notification without undue delay** to responsible Computer-Emergency Team (CSIRT) - Art. 14

- **Designation of an-house contact point (CISO)**

National actors & structures in the strategy for cyber-security



Source: Federal Chancellery, Ministry for Interior, Ministry of Defense

Summary: Approach from the industry‘s perspective

- **Holistic** approaches and (industry) tailor made security solutions, including physical security, information security, industrial control systems’ security, personnel security thorough cross-disciplinary organizations, strong cross-functional networks
- **Integrated** approach – prevention, reaction, business continuity
- **System approach** – value chain, not single objects/services (dependencies)
- **Governments and companies should have distinct, but cooperative roles:**
  - Governments to be responsible for deterring cyberattacks by nation states and organized criminal elements (highly targeted attacks)
  - Companies retaining autonomy and primary responsibility for protecting their assets against cyber-attacks
  - Governments and companies collaborate and share information of cyber threat indicators and intelligence

Summary: Principles of implementation and co-operation

- **Harmonization** of definitions and criterias laid down for the definition of critical infrastructure; harmonization of threat and risk assessments (common assessment)
- **Collaborative** - cross-border exchange with companies and states
- **Cost neutral** - potential security requirements for critical infrastructure are implemented in a cost neutral way
- **Standards** - globally used security and industry standards companies impose on themselves are recognized (no additional regulation)
- **Audits** - no additional audits shall be necessary; flexibility for companies to prove risk reduction measures implementation
- **Balanced** – sectoral and cross sectoral neutral application (no competitive disadvantage)
- **Reporting** – ensure data sovereignty and confidential business information; no duplication of existing reporting lines; severe cases only
- **Focus**: Performance not compliance

Questions & Answers

Paul Reither

Head Corporate Security & Resilience

+ 43 (1) 40440 23231
+ 43 664 61 22 392
paul.reither@omv.com