UNECE 2020 INLAND TRANSPORT SECURITY DISCUSSION FORUM

Round Table on Intelligent Transport Systems and Cyber Security

Guido Gluschke
8 September 2020
Institute for Security and Safety (ISS)

- Scientific Institute at the Brandenburg University of Applied Sciences in Germany with the following areas of work

  - ISS is in consultative status with the UN
  - ISS is founder and member of the IAEA International Nuclear Security Education Network (INSEN)
  - ISS is a Center of Excellence (CoE) of the ITU Academy
Support of International Organizations and NGOs in terms of cyber security e.g.

Process on Confidence Building Measures (CBMs) in cyber at the OSCE in 2016

DASICON panel on OSCE’s role in the cyber realm at the Diplomatic Academy in Vienna in 2017

ITU GSR conference on cyber security in 2018
Key Topics of Discussion

From our point of view the following aspects are relevant for discussion:

- Holistic View and Scope
- Threats and Nation State’s Dilemma
- Cooperation, Competences, and Terminology
Holistic View and Scope
Autonomous Vehicle Ecosystem

- Manufacturer of vehicle (OEM)
  - Tier 1
- Operator of the vehicle
- Environment in which vehicle is used
- Communication
- 3rd Party Service Provider
- Energy provider for the vehicle

Tier 2
Holistic View and Scope
Autonomous Vehicle Ecosystem

ISO 27001 ISMS
TISAX

Manufacturer of vehicle
OEM
Tier 1
Tier 2

Operator of the vehicle

Environment in which vehicle is used

Privacy/GDPR

Communication

3rd Party
Service Provider

Energy provider for the vehicle

UN ECE WP.29 GRVA CSMS

Cyber Threats
Threats and Nation State’s Dilemma

High Threat Capabilities

*Maximum Threat Capability against which protection will be reasonably ensured*

Design Basis Threat

Low Threat Capabilities

- e.g. particular military attacks
- e.g. terrorist attacks
- e.g. malicious attack by single person

State Responsibility

Operator Responsibility

Cyber Threats
Cooperation, Competences, and Terminology

Successfull Dialogue and Cooperation

→ ISS has experience in implementing such an approach from the work with international organizations, such as the IAEA
Conclusion

• UN ECE WP.29 regulation and OSCE CBMs exist while international legally binding instruments, such as cyber norms, are still lacking

• A strong dialogue and political will is needed in order
  • to come to a common understanding of the battlefield, the threat actors and threat vectors, and
  • to find agreements on a model for cyber defense and its associated responsibilities

• Terminology and competence building is key for a mature dialogue between all relevant stakeholders
Thank you for your attention

g.gluschke@uniss.org
www.uniss.org