Distr.: General
25 August 2020

English only

Economic Commission for Europe

Inland Transport Committee

Working Party on Transport Trends and Economics

Thirty-third session
Geneva, 7–9 September 2020
Item 6 of the provisional agenda
Inland transport security

2020 Inland Transport Security Discussion Forum

Round Table on Intelligent Transport Systems and Cyber Security

Note by the secretariat

2020 INLAND TRANSPORT SECURITY DISCUSSION FORUM

Round Table on Intelligent Transport Systems and Cyber Security

Held in conjunction with the 33rd Session of the Working Party on Transport Trends and Economics (WP.5)

Geneva, 8 September 2020 - 15h00-16h30

Room XXIV, Palais des Nations
via WebEx as well as physical attendance at the venue

I. INTRODUCTION

Background

This round table on Intelligent Transport Systems and Cyber Security is being held as part of a series of events co-organized by the UNECE Sustainable Transport Division, in the framework of its annual Inland Transport Security Discussion Forum, and the Office of the Co-ordinator of OSCE Economic and Environmental Activities (OCEEA). It takes place in conjunction with the 33rd Session of the Working Party on Transport Trends and Economics (WP.5) and is part of the OCEEA's efforts aimed at promoting connectivity and enhancing regional security and stability, by assisting participating States in the development of safe and secure transport and trade facilitation.

Definitions

For the purpose of this round-table, and in the absence of a single harmonized definition, Intelligent Transport Systems (ITS) are understood as "systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport".

In recent years, the ITS sector has benefited significantly from the introduction of a range of new technologies such as Automated Driving Systems and the widespread implementation of Advanced Emergency Call Systems (referred to as eCall in Europe and ERA-GLONASS in the Russian Federation).

It is expected that ITS will continue to expand with the advance of vehicle communication systems described in more detail below.

ITS technologies

Road operators monitor traffic and roadway conditions in real-time and use gathered data to manage traffic flows using various flow-control mechanisms. ITS vary in technologies applied, from basic management systems such as:

- Car navigation.
- Traffic flow control systems.
- Container management systems.
- Variable message signs.
- Automatic plate number recognition.
- The use of cameras and sensors strategically placed along highways and across entire urban centres transmit real-time data to control centres, e.g. bus lane cameras, speed cameras, roadside weather stations, and vehicle detection systems.
- Automated toll collection systems.

To more advanced applications that integrate live data and feedback from several other sources such as:

- Parking guidance and information systems.
- Emergency vehicle notification systems (AECS) such as eCall and ERA-GLONASS.
- Automatic road enforcement.
- Variable speed limits.
- Collision avoidance systems.
- Dynamic traffic light sequence.
- Weather information.

Furthermore, predictive techniques are being developed to allow advance modelling and comparison with historical baseline data.

II. EMERGING RISKS AND THREATS TO INTELLIGENT TRANSPORT SYSTEMS

Defining the threats

The increasingly digitalized and automated transport system functionalities as described above also create a range of new risks and threats.

- *Security risks*, since connected cars, autonomous vehicles, traffic flow control systems and smart road infrastructure can be vulnerable to cyber assaults and be exposed to terrorist attacks.
- *Privacy issues*, since no regulations are available now. Tracking and collecting driving habits and information about cars with vehicle to vehicle communication is very easy and disastrous consequences can be generated if the data is hacked.
- *Liability concerns*, since information, which is essential to increasingly digitalized transport networks, needs to be protected.

ITS due to their large-scale architectures and pervasiveness in smart societies become especially vulnerable to the threat of cyberterrorism due to the high impact disruptions they could cause.

As ITS continues to grow and becomes more sophisticated, so does the need for integration among different types and layers of information systems. Different information system interchanges and juncture points are especially vulnerable to acts of cyber terrorism.

There are various general vulnerabilities that ITS share with most other enterprise systems, including:

- Wireless and cellular communication.
- Integration of physical and virtual layers.
- Cohabitation between legacy and new systems and increased automation.

ITS specific vulnerabilities on the other hand include:

- Scale and complexity of transportation networks.
- Applying networked technology across large transport system.
- Multiple interdependent systems.
- Access to real-time data.
- Higher volumes of passengers and freight; and Online passenger services.

Examples of cyber-terrorism and Intelligent Transportation Systems[1]

As cyber-terrorism has emerged with the rise of digitization and interconnectivity, intelligent transport systems of different kinds have also become vulnerable to it.

"In 2016, a prominent case was reported in the San Francisco Municipal Transport System, where hackers aided by ransomware took over more than 2000 computers that operated the public transport system of the municipal agency (Gibbs, 2016; Newcomb, 2016). While the computers were left completely inoperable and showing a ransom message, the agency was forced to open all fare gates in order to minimize the impact on the public and the city itself (Gibbs, 2016). While the attack did not impact customers physically, or their data, the event has the potential to disrupt an entire functioning city (Newcomb, 2016)."

"A similar situation happened in 2017 when the notoriously famous ransomware 'WannaCry' affected several stations in Germany's Rail network. The train company Deutsche Bahn had their computers infected with the virus, leading to the ransomware message appearing on screens at train stations. Deutsche Bahn released a press statement revealing that due to the Trojan attack, the train network experienced system failures in various areas (Graham, 2017)."

"Civil aviation is not exempt from the risk of cyber-terrorism, as it heavily relies on "vehicle-to-vehicle" and "vehicle-to-infrastructure" communication technologies, along with complex system controls. In 2013, the commercial pilot and computer security expert Hugo Teso found that much of the flight plan and cruising altitude information of a plane, amongst other key metrics, were neither secure nor encrypted. Gathering and manipulating information of networks and radars linked to flight plans, he was able to come up with an android application

[1] Examples directly derived from: https://eapj.org/wp-content/uploads/2020/02/The-Threat-of-Cyber-Terrorism-Security-in-Intelligent-Transportation-Systems-Architecture.pdf (Last visited 30 July 2020)

called 'PlaneSploit' to gain control of an aircraft remotely, that he presented in the 'Hack in the box' security conference in Amsterdam that year. By doing this, he proved the possibility of cyber-hijacking an aircraft by manipulating in a remote fashion, flight variables such as speed, altitude, direction, and even cabin lights (Heitner, 2014).

III. ROLE OF UNECE

UNECE is at the centre of the legal and regulatory work needed to realize the vision of new sustainable mobility and support the mass introduction of autonomous vehicles on the roads. It started dedicated work on this issue back in 2014. UNECE strongly contributes to enabling automated driving functionalities as it is hosting and administering the Multilateral Agreements and Conventions ruling the requirements and the use of these technologies.

The relevant fora, e.g. the Working Party on Automated/Autonomous and Connected Vehicles (GRVA), the Global Forum for Road Traffic Safety (WP.1) and the World Forum for the Harmonization of Vehicle Regulations (WP.29) are following the technical progress with the aim of ensuring that the benefits of these new technologies can be captured without compromising safety and other progress achieved during the last decades (e.g. border crossing, interoperability etc.). UNECE liaises with all relevant stakeholders, the automotive sector, IT, telecommunication and insurance industries, Governments and REIOs, consumer organizations as well as other international organizations.

IV. ROUND TABLE OBJECTIVES

Need for integration of cyber resilience measures in ITS

As digitization and interconnectivity become more prominent in many UNECE member States/ OSCE participating States, the rise of cyberterrorism poses a variety of new threats to intelligent transport systems.

This 1,5-hour round table will take stock of the various types of cyber threats experienced by the inland transport sector in view of current automation and digitalization processes. Keynote speakers will shed light on these issues from a variety of perspectives. An overview will be provided of the work already done at UNECE on this matter, especially regarding road vehicles and ideas/ proposals will be formulated as to how the cyber resilience of intelligent transport systems can be further enhanced. The deliberations of this expert round table and the recommendations put forward will be reflected in the report of the 33rd WP.5 session, including a list of possible follow-up actions for UNECE, OSCE and other relevant partners.

V. ROUND TABLE AGENDA

15h00-15h10 – Welcoming Remarks

- **Mr. Konstantinos Alexopoulos**, Chief, Transport Facilitation and Economics Section, UNECE Sustainable Transport Division

- **Mrs. Eni Gjergji**, Economic Adviser, Office of the Co-ordinator of OSCE Economic and Environmental Activities, OSCE Secretariat

15h10-15h30 – Mr. François E. Guichard, Secretary of the Working Party on Automated/ Autonomous and Connected Vehicles, UNECE Sustainable Transport Division

15h30-15h45 – Mr. Rosen Naydenov, European Union Agency for Cybersecurity (ENISA)

15h45-16h00 – Dr. Darren Handley, Co-Chair of the GRVA Informal Working Group on Cyber Security and Over-The-Air Issues, Head of Office, Department for Transport, United Kingdom of Great Britain and Northern Ireland

16h00-16h15 – **Dr. Gundbert Scherf**, Partner, McKinsey & Company, Germany

16h15-16h30 – Dr. Guido Gluschke, Director, Institute for Security and Safety (ISS), Brandenburg University

16h30 – Round table wrap up & conclusions