Chapter 4
Analysis of Cyber-Attacks against the Transportation Sector

Brett van Niekerk
University of KwaZulu-Natal, South Africa

ABSTRACT
For many countries the physical transport infrastructure is critical to the economy, with ports forming a gateway for the majority of trade, and rail and road used to distribute goods. Airlines are crucial to the tourism industry. Whilst the focus of cyber-defense is on financial networks and the power grid, recent incidents illustrate that the transport infrastructure is also susceptible to cyber-attacks. The chapter provides an overview of cyber-security incidents related to the transportation sector, and analyses the reports of the incidents to illustrate the prevalence of threat types and impact. The chapter then discusses some efforts to mitigate the threats in terms of regulations, threat intelligence and information sharing, and awareness training.

INTRODUCTION
Cyber-defense has focused on the financial and electric power grids due to the potentially catastrophic outcomes should a major cyber-attack on those infrastructures cause widespread damage. More recently, more focus has been applied to the cyber-security of the physical transport sector. Whilst this infrastructure may not be considered as critical as the power or financial systems, international trade and
employees travelling to work depend on the transportation. Military deployments are also dependent on the infrastructure, although it may not be interconnected with the civilian versions. Cyber-attacks on this sector therefore could have severe implications for national economies and international trade.

Hughes, quoted in Stelter (2015), indicates that the threats faced by a nation were different when transport infrastructure was built. Similar to other critical infrastructure, many of the IT systems for the transport sector were designed assuming that the Internet and those online could be trusted, therefore there is a lack of inherent cyber-security. Combining this vulnerability with the fact that the World Economic Forum (2015) listed cyber-attacks and critical infrastructure failure in the top risks, it is evident that there is a need to investigate cyber-attacks targeting the transportation sector.

This study will follow a similar methodology to that of Miller and Rowe (2012). In their study, they classified attacks against industrial control systems (ICS) according to impact and attack vector. For this study, the incidents related to the transportation sector will be assessed according to the threat type (attacker) and the impact. The source of the incident descriptions are from primarily from online news reports and from existing analysis where it is available. A thematic (qualitative) analysis of the reports is used to identify the threat types and impact for each incident. For the purposes of this chapter, the threats types include:

- Individual hackers,
- Disgruntled insiders (and a category for a combination of hackers and insiders),
- State-sponsored attacks, cyber-criminals, and
- Malware.

Researchers are also considered even though they are not necessarily a threat, however they do expose system vulnerabilities. The impact categorizations include:

- Disruption of operations,
- Data loss,
- Financial theft,
- Illegitimate control of networks or systems,
- Unauthorized access to information or systems, and
- Proof of concept of vulnerabilities and/or attack methods that researchers develop.

The incidents under consideration are described in the next section. Thereafter the analysis provides the tabulated number of occurrences for each threat type and
#TerroristFinancing: An Examination of Terrorism Financing via the Internet
[www.igi-global.com/article/terroristfinancing/198315?camid=4v1a](www.igi-global.com/article/terroristfinancing/198315?camid=4v1a)

Toward a U.S. Army Cyber Security Culture
[www.igi-global.com/article/toward-army-cyber-security-culture/69773?camid=4v1a](www.igi-global.com/article/toward-army-cyber-security-culture/69773?camid=4v1a)