Process modelling of physical and cyber terrorist attacks on networks of public transportation infrastructure

Alexander Gabriel
TH Koeln - University of Applied Sciences
Alexander.Gabriel@th-koeln.de

Simon Schleiner
TH Koeln - University of Applied Sciences
Simon.Schleiner@th-koeln.de

Florian Brauner
University of Wuppertal
Brauner@uni-wuppertal.de

Florian Steyer
TH Koeln - University of Applied Sciences
Florian.Steyer@th-koeln.de

Verena Gellenbeck
TH Koeln - University of Applied Sciences
Verena.Gellenbeck@th-koeln.de

Ompe Aimé Mudimu
TH Koeln - University of Applied Sciences
Ompe_Aime.Mudimu@th-koeln.de

ABSTRACT

Recent events have demonstrated the vulnerability of IT-systems of different companies, organisations or even governments to hacker attacks. Simultaneously, information technologies have become increasingly established and important for institutions of various branches. With respect to modern terrorism developments, cyber-attacks may be used to physically harm critical infrastructures. This leads to a new dimension of cyber-attacks called "terrorist cyber-attacks".

This research-in-progress paper aims to develop a process model for data acquisition and support of decision making that seeks to enhance the security of public transportation in the context of counterterrorism. Therefore, a generic process model for terrorist cyber-attacks – produced in the research project RE(H)STRAIN[1] – is introduced as a basis for a decision support system (DSS). In the future, such models could improve the decision process by comparing the effectiveness of different security measures.

Keywords

Cyber-attack, (counter-)terrorism, process modelling, decision support, critical infrastructure

INTRODUCTION AND RESEARCH QUESTION

As a result of increasing interconnection of systems and progressing digitalisation of processes, there is a rising dependence on IT systems across all industrial sectors including public transport. Analogous technology has been replaced by computerised (railway) control centres and in many cases e.g. railway signals and switches are operated automatically and remote-controlled (Tschirner et al. 2014; Kawalec and Rżysko 2016). IT support is used to control complex train systems (Chen et al. 2015), especially for high-speed railway traffic. Future railway developments will make signalling on the tracks obsolete because trains will receive the necessary control commands directly via mobile communication services like GSM-R (cf. European Train Control System). This will enhance the density of train succession, create higher speed possibilities (Stamm 2011), but also lead to an even higher dependence on IT systems and networks.

[1] "Resilience of the Franco-German Highspeed Train Network", Research for Civil Security funded by the German Federal Ministry for Education and Research and the Agence Nationale de la Recherche (France),Grant No. 13N13786 to 13N13790

In addition to IT utilisation, there is an increasing risk through cyber threats. In recent years, cyber-attacks have become more relevant by increased occurrence and induced damages, even such as data theft (World Economic Forum 2012, 2016). This paper discusses the question how basic characteristics of physical terrorist attacks are transferable to the processes of terrorist cyber-attacks.

In particular, the focus will be on high speed traffic, since national high-speed trains are flagships of the national transportation services, technology carriers, and thus are attractive targets for terrorist attacks (Strandberg 2013).

Very recent cyber-attacks were without consequences (McGoogan and Willgress 2016; Boyle 2016), but they showed the general ability of attackers to access IT-systems of transport infrastructure. It can be assumed that it is only a matter of time before cyber-attacks will cause physical damage to certain structural elements – a similar development were the Stuxnet cyber-attacks in 2007 to 2010 (Subhash Lakshminarayana et al. 2016; Bambauer 2014).

In the light of the above, the main idea of this research in progress paper is to create a better understanding of attack sequences through the use of process models. So called points of intervention (POIVs) where security measures can come into effect have been defined for attack processes. These POIVs pose a connection between the attack process on the one and security measures on the other hand. The goal of this paper is to present an outlook of how both, the process models as well as the POIVs as connective elements could be useful for developing a DSS that seeks to give recommendations regarding the implementation of the most effective security measures for certain POIVs.

Furthermore, the research will show the necessity of a combined approach for countering physical and cyber terrorist threats.

FORMULATION OF HYPOTHESIS: TERRORIST

There is no internationally or legally binding definition of terrorism. However, various sources agree that the term terrorism describes violent, illegal action of one or more individuals against society or other targets. The aim of these actions is to influence the political and social behaviour according to the terrorist's objective by creating fear and terror (18 U.S.C. § 2331; Department of Defense 2010; Department of Homeland Security 2006). Typical terrorist objectives can originate from ideological, political or religious motives but divergent or mixed motives are not excluded.

A multitude of different weapons and an equally high number of attacked assets can be observed for terrorist attacks that have been committed to date. Based on the analysis of previous attacks, which was conducted in the context of the research project RE(H)STRAIN, it was documented that railway traffic is an attractive target for attackers. This attractiveness is unaffected by the used weaponry, because the subjective impact of attacks on society (passengers) is high, due to the daily use of the attacked target. Examples for this effect are the attempted gun attack in a Thalys train in 2015, the attacks on the Metro in Brussels in 2016 or London in 2015, the knife attack in a German regional train close to Wuerzburg in 2016 or the axe attack in Germany at Duesseldorf train station (BBC News 2015, 2016; Gray 2015; Oltermann and Rawlinson 2016; BBC News 2017).

All these examples as well as additional attacks have two fundamental observations in common. Firstly, the attackers' intention, to create fear and terror, is rather similar despite the wide range of differing motives. Secondly, weapons were used to cause physical damage to people or tangible objects. Accordingly, the subsequent axioms on behaviour and intention of terrorists can be defined. They will serve as working hypotheses for this research.

Table 1. Working hypotheses "terrorist"

1.	All terrorists aim to create a maximum of fear and terror in the targeted society. To achieve this goal, major damage to persons and/or property is done, independent of the chosen weapon.
2.	According to the first axiom and because terrorists seek suitable conditions to execute their attack, similar intentions of terrorists lead to a comparable process of planning and operating, regardless of the chosen weapon or the selected target/asset.

PROCESS MODELLING AS AN OPPORTUNITY TO ASSESS PHYSICAL TERRORIST ATTACKS

Based upon the hypotheses in table 1, it can be proven that neither the exact place of an attack nor the precise weapon are decisive for the evolving process steps – especially during the phase of preparation. The level of

abstraction in the generic process model neglects the choice of weapon, the choice of asset as well as the terrorists' capability – and merely focusses on the modus operandi. This leads to a facilitation of the real processes but is useful in developing a generic process model.

Of course, parameters such as chosen weapons and assets as well as the terrorist's capability to carry out an attack influence the probability of detection and the extent of damage, e.g., different numbers of victims or different time of recovery; however, their impact on the processes of planning or preparation is limited. Consequently, this process model may serve as a theoretical basis for further research. Assuming the rightness of the hypotheses, attacks can be described in this abstract process model, which can be further applied to all kinds of terrorist attacks. To develop a reliable process model, various iteration steps had to be taken.

The process model in figure 1 incorporates all possible steps of the attacker, including the planning and execution of an attack. The developed process for physical attacks is based upon research results of previous projects (RiKoV[2]) as well as interviews with experts with a scientific background. In its current state, the process model does not account for the adaptability of the attackers. For example, the terrorists could try to avoid the security measures that they are aware of or integrate them in their planning process, so that they are not effective anymore.

All measures that might interrupt the attack process are referred to as measures of successful prevention. They deter, detect, or neutralise attacker or weapon. The points where these measures come into effect and interrupt or influence the attack process are referred to as "points of intervention" (POIVs) in the course of the project RE(H)STRAIN. The effect of different security measures at these POIVs was discussed within the project as well as with experts. By using such POIVs, it is possible to determine whether security measures are applicable or not for each step in the planning and execution phase.

Currently, these POIVs are linked to an existing security measure database that was developed for public transportation systems by the joint research project RiKoV (Brauner 2017). It contains additional information about current and future security measures for the prevention and mitigation of physical attacks. Referring to Brauner et al. (2015), the combination of a structural interview guideline for experts and a scenario process model in a semi-quantitative assessment methodology allows estimating the effectiveness of single and combined security measures in each POIV. The developed process model in RiKoV is able to assess physical attacks on public transportation systems and to estimate the change of vulnerability in the context of different security designs. The new process model presented in this paper will become a framework to assess security designs for cyber-attacks that can have hidden or obvious effects (damages). Therefore, it can be used in risk and crisis management systems to improve decision-making by end-users. In the following section, the development of a process model for terrorist cyber-attacks is examined.

[2] Risks and costs of terrorist threats to railbound public transport (funded by the German Federal Ministry of Education and Research, Grant-No.: 13N12305)

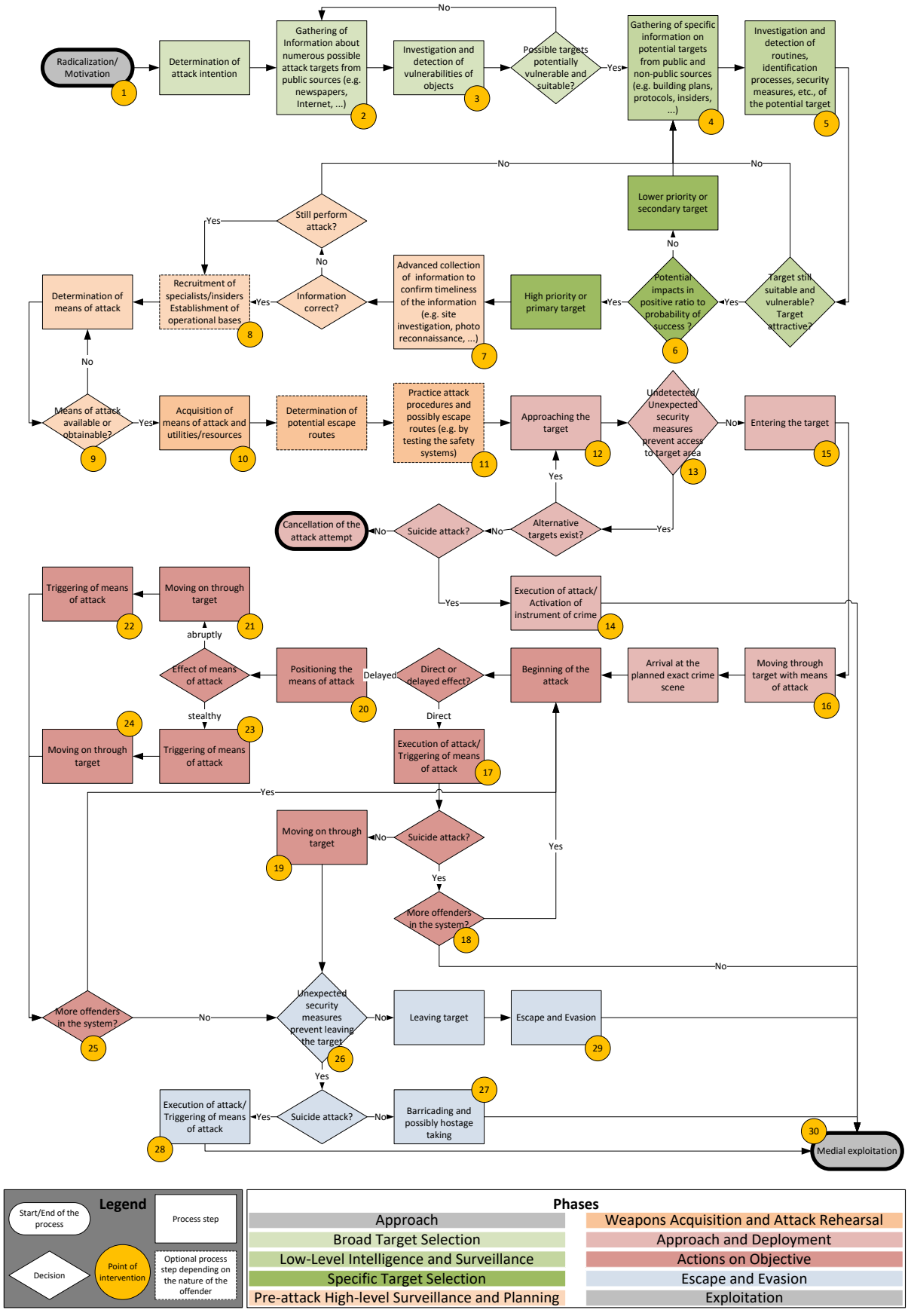

Figure 1. Attack process model (physical attack)

TRANSFER TO CYBER-ATTACK PROCESSES – FORMULATION OF HYPOTHESES: CYBER TERRORIST

Both frequency and dimension of cyber-attacks have increased in recent years. For this reason, we assume that this form of attack will be used by terrorists or has already been used, even if it has not been specifically proven. This includes classic cyber-attacks to disturb or destroy IT systems as well as attacks using IT systems to cause physical consequences (e.g. train crashes). The intention of a terrorist attack follows the similar heuristic behaviour explained in table 1.

Generally, cyber-attacks can roughly be divided into five different steps. The first step comprises the gathering of intelligence using techniques such as social engineering. The initial intrusion of the asset, step two, is followed by a phase of horizontal spreading to gain command and control in the targeted system, which can take up to several months. The intrusion becomes visible during the final steps, the escalation of privileges that eventually leads to the execution of the intended attack. Examples for this strategy are the already mentioned Stuxnet cyber-attacks from 2007 to 2010 (Subhash Lakshminarayana et al. 2016; Bambauer 2014) or the ongoing BlackEnergy-attacks against the Ukrainian power grid (Industrial Control Systems Cyber Emergency Response Team and Department of Homeland Security 2017).

There is no common international definition for cyber terrorism, similar to the lack of exact definitions for terrorism. The sources that mention the term at all often use definitions for terrorism, enhanced by including that cyber terrorism is a form of terrorism using the Internet as a weapon, i.e., using Internet technologies to attack computer systems (German Federal Ministry of the Interior 2017; Combs and Slann 2007; Federal Bureau of Investigation 2007; Tafoya 2011; United States Army Training and Doctrine Command 2007; Department of Defense 2016; Department of Homeland Security 2013). The sources emphasise that cyber-attacks can take place combined with conventional, i.e., physical attacks. This has to be considered by setting up security designs. The hypotheses of table 1 can be adapted to cyber-attacks as follows:

Table 2. Working hypotheses "cyber terrorist"

1.	All terrorists aim to create a maximum of fear and terror in the targeted society. To achieve this goal, major damage to persons and property is done, independent of the chosen weapon.
2.	According to the first axiom and because terrorists seek suitable conditions to execute their attack, similar intentions of terrorists lead to a comparable process of planning and operating, regardless of the chosen weapon or the selected target/asset.
3.	The goal of each cyber terrorist is to make the cyber-attack real, i.e., according to hypothesis one, creating physical damage by using IT systems as a weapon.
4.	The combination of a physical attack and a conventional cyber-attack is possible.

TRANSFER OF THE PHYSICAL PROCESS MODEL TO CYBER TERRORIST ATTACKS

Due to the similarity of the hypotheses of physical and cyber terrorist attacks, we assume that the approach to create a process model can be transferred to cyber-attacks. In addition, three scientific and industrial experts confirmed this transfer as being possible. While two of the experts stated that the use of process modelling is an uncommon method in the sector of IT systems security, all agreed on the general transferability (Lo Iacono 12/5/2016; Kuklok 12/28/2016).

Based on the hypotheses, a generic process model was developed for cyber terrorist attacks, independent of weapons and targets. This enables the development of POIVs. As in the model for physical attacks, the adaptive capabilities of the attacker are not taken into consideration.

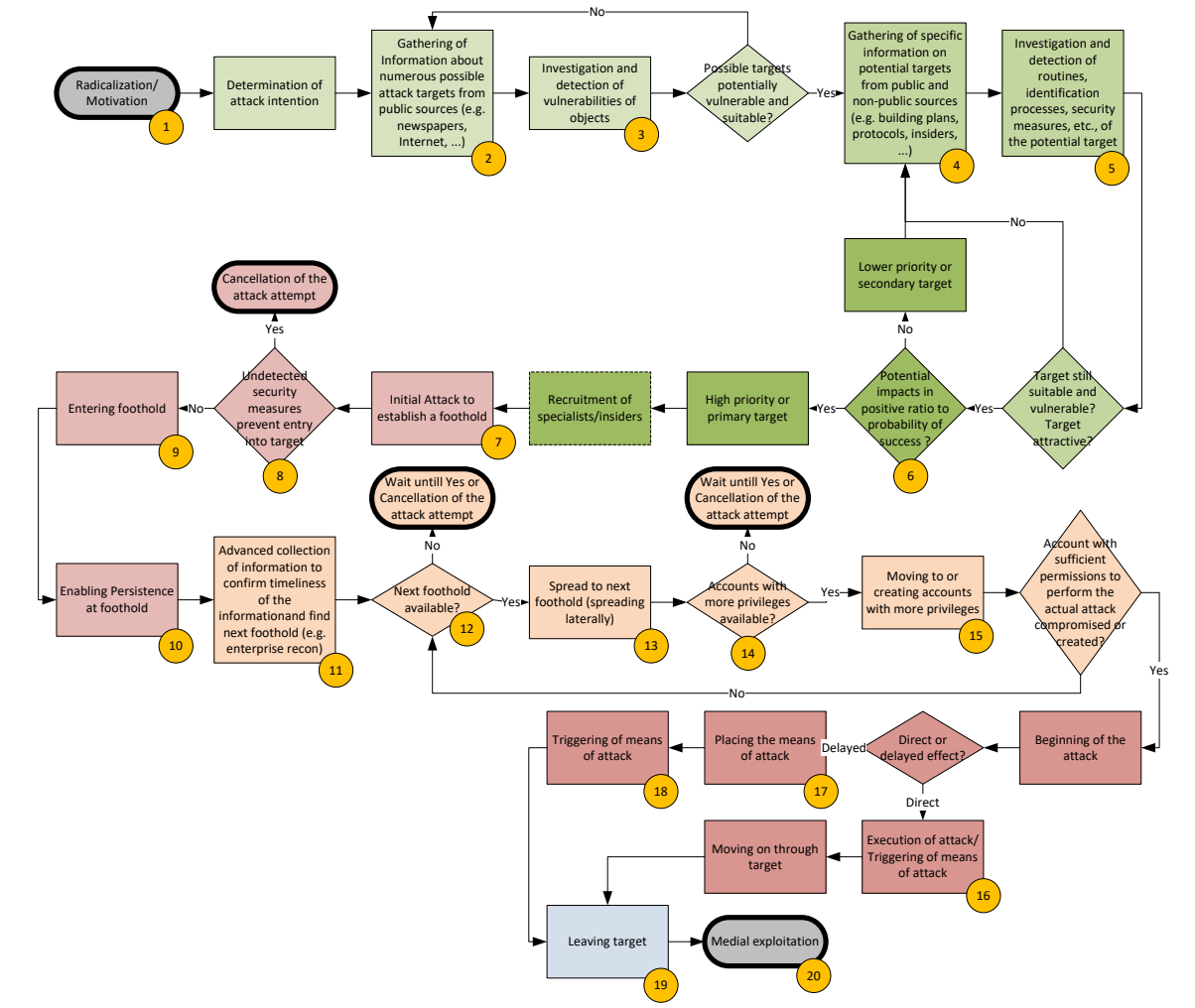

Figure 2. Attack process model (cyber-attack)

These POIVs depict potential places within the process model where security measures can come into effect. As mentioned above, intervention in this context means that the attack is either interrupted or influenced in a favourable way from a counter-terrorist-point of view. That raises the question, which of the multitude of various security measures is most likely to influence or interrupt the attack process most effectively? In order to answer this question, an immense quantity of information has to be considered and processed. The subsequent section explains how the process model could contribute to providing recommendations to potential end-users (e.g. station service providers). Furthermore, it is discussed, which data could additionally be required for the future development of a DSS that deals with the implementation of security measures.

ASSESSMENT OF REASERCH IN CONTEXT OF DECISON SUPPORT PERSPECTIVES

In a world of growing complexity and interdependency of business and industrial operations, decision support systems have gained popularity within various industrial branches over the last few years (Ishizaka and Nemery 2013). In general, such systems aim to help decision-makers assess complex – even sparsely known – situations (Sprague 1980; Valverde 2011). In order to do so, DSS condense and organise information that was usually extracted from one or more databases. The outcome is valuable – meaning relevant – knowledge, which is useful to estimate and evaluate the multifaceted consequences of different complex action alternatives (Valverde 2011). Thus, the ranking of different alternatives can be considered a form of decision support. Weighting different alternatives with help of different factors and taking into account a large amount of information seeks to,

among others, enhance business performance – meaning in this context to enhance a system's reaction to disruptions. Of course, evolving expenses for the various forms of enhancement need consideration as well. Comparing the costs for different organisational or technical security measures while also considering their potential effectiveness within an existent system and giving a recommendation about the most efficient solution could serve as an example.

In the field of risk and crisis management, decision-makers usually consider various criteria when making their choices. For example, when assessing multifaceted vulnerabilities or predicting probabilities of the occurrence of certain events. In this context, there are different phases or situations where decision support tools can be helpful. Different projects in the past were concerned with decision support issues in the context of emergency response (e.g. SOCIONICAL[3], STEP[4] and many more). During planning phases, DSS can support the ranking of different assets regarding their vulnerability or their importance for an organisation or a society. A compilation edited by Gheorghe (2005) describes the use of DSS for risk and vulnerability management – though mainly in the context of industrial risks (Spadoni and Bonvicini 2005).

The focus of this paper is to provide support during planning phases (risk assessment). Although a process model that includes POIVs and a list of security measures forms a solid informational basis, it does not deliver sufficient data for a DSS. Providing a mere summary of available security measures is not enough. Therefore, the effectiveness of each security measure, its respective costs as well as the possibility of implementation, need consideration, too.

As the effectiveness of security measures is an important factor in the context of decision support in the examined field (Adler and Fuller 2009; Brauner 2017), a qualitative rating (*high*, *low, none*) for each security measure will be added to the database. This rating refers to the security measures' effectiveness in relation to a certain attack process step. Especially from an economic point of view, costs and required effort for the implementation of security measures are decisive factors in the decision process. Adding these aspects to the process model will improve the groundwork for a DSS.

In addition to the qualitative approach outlined above, agent-based simulations as well as real large-scale exercises can assess the effectiveness of security measures more precisely. These methods have the advantage that they produce large amounts of data for evaluating and comparing security measures under different conditions. On the downside, simulations require large amounts of information to be processed and large-scale exercises are time-consuming and costly. Making use of the qualitative rating leads to a less precise, but quick assessment that produces transparent and comprehensible results.

The approach presented above is not exhaustive. The paper is supposed to outline an idea that – if further developed – could become a DSS. As presented in the previous section, the process model for terrorist cyber-attacks derives from the model for physical attacks. Three experts with scientific research and industrial background have verified its general transferability but as some expressed their doubts regarding the universal applicability of the individual steps, the process model is currently still in the process of validation. Nevertheless, the holistic and universal model of attack process steps and the collection of available security measures are the basis for offering decision support in the context of identifying additional protection for IT-systems regarding terrorist attacks. With the process model as a basis and if all factors mentioned above are considered in a database, decision-makers will be able to make choices regarding most suitable and most effective security measures for their individual needs.

CONCLUSION, OUTLOOK AND FURTHER RESEARCH

The initially formulated research questions in this paper can be answered as follows: According to different experts, the basic characteristics of physical terrorist attacks can be transferred to cyber terrorist attacks. The development of attack processes is sparsely spread within the IT-community and possibly error-prone. A statement can be made about how effective security measures are for each process step. The quality of such statements is dependent on the quality of the available databases of security measures. It is difficult to depict the uncertainty regarding the different possible terrorist reaction to security measures or unforeseen obstacles. The recurring re-evaluation and continuation is essential for the successful use of the presented approach.

The developed decision support framework will be validated by end-users. In addition, future developments will be used to continuously improve and adjust the process models. Through this, the inclusion of new events (of currently unknown dimensions) of physical and cyber threats will be ensured and will contribute to the process

[3] http://www.socionical.eu/

[4] https://www.fit.fraunhofer.de/de/fb/risk/projects/step.html

of decision-making regarding suitable security measures. It is important to keep in mind the discrepancy between reality and model that results from the abstraction of real processes. Additionally, the database of security measures will be extended and maintained to keep it up to date and expandable.

The previously introduced hypotheses have to be discussed concerning the validation of changing terrorist behaviour in the future. Recent attacks support the assumptions, but new, yet unknown forms of terrorism could question these. Future research will be executed on new modi operandi including the combination of physical and cyber-attacks. To depict such attacks, parts of both process models will be fused. The processes of planning and preparing both – physical and cyber-attacks – might be comparable and only divide up into separate processes during the execution of the planned attack. This approach could possibly contribute to the basis for a holistic risk management strategy.

An adjustment of the process models based on the hypotheses may be necessary. Furthermore, the models should be validated and constantly improved with additional expertise. Even the development of a DSS based on the first results of this research in progress paper has to be critically evaluated with regard to its feasibility.

For further research, it is planned to enrich the decision support framework with railway station relevant and specific data. This could allow the inclusion of further and more precise factors of vulnerability and therefore enable a more suitable and profound decision-making. Additionally, a concrete statement concerning the practicability and feasibility of security measures could be possible. Another point is the implementation of the terrorists' reaction to security measures, which could also be depicted by enriching the presented process model with simulation data.

REFERENCES

Adler, Richard; Fuller, Jeff (2009): Decision Support for Countering Terrorist Threats against Transportation Networks. In JSS 2 (3). DOI: 10.5038/1944-0472.2.3.5.

Bambauer, Derek E. (2014): Ghost in the Network. In University of Pennsylvania Law Review 162 (5), pp. 1011–1091. Available online at http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9439&context=penn_law_review, checked on 11/25/2016.

BBC News (2015): France train shooting: Attack 'was well prepared'. In BBC News, 8/26/2015. Available online at http://www.bbc.com/news/world-europe-34055713, checked on 1/6/2017.

BBC News (2016): Brussels Explosions: What we know about airport and metro attacks. In BBC News, 4/9/2016. Available online at http://www.bbc.com/news/world-europe-35869985, checked on 1/6/2017.

BBC News (2017): Germany axe attack: Seven injured at Duesseldorf train station. In BBC News, 3/10/2017. Available online at http://www.bbc.com/news/world-europe-39225847, checked on 3/17/2017.

Boyle, Emma (2016): UK rail network attacked by hackers four times in a year. In The Independent, 7/13/2016. Available online at http://www.independent.co.uk/life-style/gadgets-and-tech/uk-rail-network-railways-hacked-four-times-hackers-trains-a7135026.html, checked on 11/25/2016.

Brauner, Florian (2017): Securing Public Transportation Systems. An Integrated Decision Analysis Framework for the Prevention of Terrorist Attacks as Example. Wiesbaden, s.l.: Springer Fachmedien Wiesbaden. Available online at http://dx.doi.org/10.1007/978-3-658-15306-9.

Brauner, Florian; Maertens, Julia; Bracker, Holger; Mudimu, Ompe A.; Lechleuthner, Alexander M.: Determination of the effectiveness of security measures for low probability but high consequence events: A comparison of multi-agent-simulation & process modelling by experts. In Leysia Palen, Monika Büscher, Tina Comes, Amanda Hughes (Eds.): ISCRAM 2015. The 12th International Conference on Information Systems for Crisis Response and Management 24-27 May in Kristiansand, Norway.

Chen, Binbin; Schmittner, Christoph; Ma, Zhendong; Temple, William G.; Dong, Xinshu; Jones, Douglas L.; Sanders, William H. (2015): Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective. In Floor Koornneef, Coen van Gulijk (Eds.): Computer Safety, Reliability, and Security, vol. 9338. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 277–290, checked on 12/16/2016.

Combs, Cindy C.; Slann, Martin W. (2007): Encyclopedia of Terrorism. Rev. ed. New York: Facts On File.

Department of Defense (Ed.) (2010): Dictionary of Military and Associated Terms. Available online at http://www.dtic.mil/doctrine/dod_dictionary, checked on 1/5/2017.

Department of Defense (Ed.) (2016): DOD Dictionary of Military and Associated Terms. Arlington County, Virginia. Available online at http://dtic.mil/doctrine/new_pubs/dictionary.pdf, checked on 1/13/2017.

Department of Homeland Security (2006): National Infrastructure Protection Plan. DHS, NIPP 2006.

Department of Homeland Security (Ed.) (2013): National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. Washington, D.C. Available online at https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf, checked on 1/13/2017.

Federal Bureau of Investigation (Ed.) (2007): Terrorism 2002 - 2005. Washington, D.C. Available online at https://www.fbi.gov/stats-services/publications/terrorism-2002-2005, checked on 1/15/2017.

Gabriel, Alexander (12/5/2016): Vulnerablitäten des ETCS - insbesondere der Mobilfunkverbindungen - gegenüber Cyberangriffen. Interview with Luigi Lo Iacono. Köln.

Gabriel, Alexander (12/28/2016): Vulnerablitäten des Schienenverkehrs - insbesondere des ETCS - gegenüber Cyberangriffen. Interview with Oliver Kuklok. Köln, Assenheim.

German Federal Ministry of the Interior (Ed.) (2017): BMI - Cyberterrorismus. Available online at http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyberterrorismus/cybersterrorismus_node.html, updated on 1/15/2017, checked on 1/15/2017.

Gheorghe, Adrian V. (Ed.) (2005): Integrated Risk and Vulnerability Management Assisted by Decision Support Systems. Relevance and Impact on Governance. Dordrecht: Springer (Topics in Safety, Risk, Reliability and Quality, 8). Available online at http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10228693.

Gray, Melissa (2015): 3 stabbed at London Tube station in terror attack, police say. In CNN, 12/7/2015. Available online at http://edition.cnn.com/2015/12/05/europe/london-tube-stabbings/, checked on 1/6/2017.

Industrial Control Systems Cyber Emergency Response Team; Department of Homeland Security (2017): Cyber-Attack Against Ukrainian Critical Infrastructure | ICS-CERT. Available online at https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01, updated on 3/17/2017, checked on 3/17/2017.

Ishizaka, Alessio; Nemery, Philippe (2013): Multi-criteria Decision Analysis. Methods and Software. 1. Aufl. s.l.: Wiley. Available online at http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=593377.

Kawalec, Piotr; Rżysko, Marcin (2016): Modern methods in railway interlocking algorithms design. In Modern Techniques of Design and Implementation of Highly Flexible Controllers (44), pp. 38–46. DOI: 10.1016/j.micpro.2015.11.018.

McGoogan, Cara; Willgress, Lydia (2016): UK rail network hit by multiple cyber attacks last year. In The Telegraph, 7/12/2016. Available online at http://www.telegraph.co.uk/technology/2016/07/12/uk-rail-network-hit-by-multiple-cyber-attacks-last-year/, checked on 11/25/2016.

Oltermann, Philip; Rawlinson, Kevin (2016): Teenager shot dead after attacking passengers on train in Germany. In The Guardian, 7/19/2016. Available online at https://www.theguardian.com/world/2016/jul/18/about-20-people-injured-in-axe-attack-on-train-in-germany, checked on 1/6/2017.

Spadoni, Gigliola; Bonvicini, Sarah (2005): ARIPAR-GIS, TRAT, OPTIPATH, EHHRA-GIS. Features and application of some tools for assisting decision-makers in risk management. In Adrian V. Gheorghe (Ed.): Integrated Risk and Vulnerability Management Assisted by Decision Support Systems. Relevance and Impact on Governance. Dordrecht: Springer (Topics in Safety, Risk, Reliability and Quality, 8), pp. 349–360.

Sprague, Ralph H. (1980): A Framework for the Development of Decision Support Systems. In MIS Quarterly 4 (4), pp. 1–26. DOI: 10.2307/248957.

Stamm, Bernhard (2011): Die Eisenbahn ohne Lichtsignale. Das European Rail Traffic Management System als Zukunft des europäischen Bahnnetzes. In Bulletin - Fachzeitschrift von Electrosuisse und Verband Schweizerischer Elektrizitätsunternehmen 102 (10), pp. 22–25. Available online at http://www.bulletin-online.ch/uploads/media/1110_Seite_022-025.pdf, checked on 11/24/2016.

Strandberg, Veronica (2013): Rail bound traffic—a prime target for contemporary terrorist attacks? In J Transp Secur 6 (3), pp. 271–286. DOI: 10.1007/s12198-013-0116-0.

Subhash Lakshminarayana; Zhan-Teng Teo; Rui Tan; David K Y Yau; Pablo Arboleya (2016): On False Data Injection Attacks Against Railway Traction Power Systems, checked on 12/16/2016.

Tafoya, William L. (2011): Cyber Terror. In FBI Law Enforcement Bulletin Volume 80 (11), pp. 1–7. Available online at https://leb.fbi.gov/2011/november/leb-november-2011, checked on 1/15/2017.

Tschirner, Simon; Sandblad, Bengt; Andersson, Arne W. (2014): Solutions to the problem of inconsistent plans in railway traffic operation. In Journal of Rail Transport Planning & Management (4), pp. 87–97. DOI: 10.1016/j.jrtpm.2014.10.002.

United States Army Training and Doctrine Command (Ed.) (2007): A Military Guide to Terrorism in the Twenty-First Century. TRADOC G2 Handbook No. 1. Fort Leavenworth, Kansas. Available online at https://rdl.train.army.mil/catalog-ws/view/100.ATSC/898B610C-E6C9-4CF9-B6D4-7278BB558772-1302982125245/dcsint_hdbk1/dcsint_hdbk_1.pdf, checked on 1/15/2017.

18 U.S.C. § 2331: US Code Title 18 §2331. Available online at http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2331&num=0&edition=prelim#sourcecredit, checked on 1/6/2017.

Valverde, Raul (2011): A Risk Management Decision Support System for the Real Estate Industry. In International Journal of Information and Communication Technology 1 (3), pp. 139–147.

World Economic Forum (2012): Global Risks 2012. Seventh Edition. With assistance of Marsh & McLennan Companies, Swiss Reinsurance Company, Wharton Center for Risk Management, University of Pennsylvania, Zurich Financial Services. 7th ed. Cologny/Genf: World Economic Forum (Insight report). Available online at http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf, checked on 11/25/2016.

World Economic Forum (2016): The Global Risks Report 2016. 11th Edition. With assistance of Marsh & McLennan Companies, Zurich Insurance Group, National University of Singapore, Oxford Martin School, University of Oxford, Wharton Risk Management and Decision Processes Center, University of Pennsylvania. 11th ed. Cologny/Genf: World Economic Forum. Available online at http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf, checked on 11/25/2016.