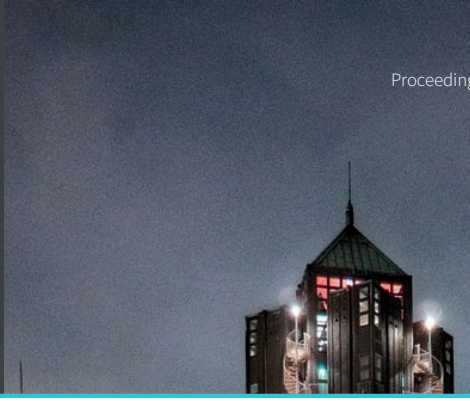
Proceedings of the Hamburg International Conference of Logistics (HICL) – 28



Sandra König, Stefan Rass and Stefan Schauer

Cyber-Attack Impact Estimation for a Port

HICL

Published in: Digital Transformation in Maritime and City Logistics
Carlos Jahn, Wolfgang Kersten and Christian M. Ringle (Eds.)
September 2019, epubli

Cyber-Attack Impact Estimation for a Port

Sandra König[1], Stefan Rass[2] and Stefan Schauer[1]

1 – Austrian Institute of Technology

2 – University of Klagenfurt

Purpose: We investigate consequences of a cyber-attack on a port through a simulation model. Motivated by the impact of NotPetya on the container company A.P. Møller-Maersk and the entire supply chain we propose a method to estimate the consequences. Such estimation is a first step towards the identification of protection measures.

Methodology: We represent a port as a network of interdependent cyber and physical assets. The operational state of each component is measured on a 3-tier scale and may change due to external problems. The components reaction on security incidents is modeled using Mealy automata.

Findings: An implementation of the model as a network of coupled Mealy automata allows simulation of the dynamics after a security incident. This gives an overview on the expected condition of each component over time. The results can be visualized to identify parts that are particularly at danger.

Originality: The approach takes into account different kind of information on the cyber and physical system but also learns from past incidents. The automata simulation model provides estimate on the future behavior. Existing data may be used for validation.

Keywords: Cyber-attack, Cascading Effects, Port Security, Supply Chain

First received: 17.May.2019 **Revised:** 11.June.2019 **Accepted:** 14.June.2019

1 Introduction

During the last years, critical infrastructures (CIs) have developed into complex and sensitive systems. Manifold dependencies exist between different CIs, leaving them vulnerable to failure in other systems and resulting reduced support in, e.g., electricity (Fletcher, 2001). At the same time, single CIs grow and become more heterogeneous. The probably most significant change during the last decade is the increasing digitalization that yields an interconnection between formerly separated physical and cyber systems. Physical processes are controlled through Industrial Control Systems (ICS), data is stored and analyzed and physical processes may be adapted due to this collected information (e.g., if a water supplier detects reduced quality of ground water, pumps may be switched off remotely). Not to the least, digitalization aims at increasing efficiency and simultaneously reducing costs.

Despite the many advantages of linking physical and cyber systems, this also paves the way for new threats. Recent incidents such as Stuxnet (Karnouskos, 2011), the hacking of the Ukrainian power provider in 2015 (E-ISAC, 2016) and 2016 (Condliffe, 2016) demonstrated impressively the potentially huge impact on CIs but also on society. Until 2017, the number of reported cyber incidents in the maritime sector has been relatively low (Verizon, 2017), despite some incidents as the hacking of the computer controlling containers enables drug traffic in Antwerp (Bateman, 2013). In the aftermath of the impact of NotPety on A.P. Møller-Maersk (Greenerg, 2018), awareness has risen. When the COSCO Shipping Line was hit by a cyber-attack in July 2018, it affected the organization network but business operation was still possible (World Maritime News, 2018). Later the same year, the

ports of Barcelona and San Diego reported on cyber-attacks (Cimpanu, 2018b). Malware attacks such as WannaCry and NotPetya (both in 2017) also affected the maritime sector.

In this article, we take a hybrid view on nowadays complex CIs through the concept of hybrid situational awareness. Based on this model we investigate consequences of a cyber-attack on the overall system. Motivated by the consequences of NotPetya, we illustrate the approach by investigating the impact of such an attack on a port.

2 Hybrid View on Critical Infrastructures

The way most CIs have developed over the past years results in a big system consisting of two interconnected subsystems, namely the physical and the cyber system. Information on the individual systems is available but typically not combined to understand the behavior of the overall system. The knowledge about the subsystems is often called Physical Situational Awareness (PSA) and Cyber Situational Awareness (CSA), respectively. People may have domain expertise in either the physical or the cyber domain, but hardly both. However, it is exactly the cross impact that bears high risks, and limited view on only cyber or physical domains may lead to a failure of the overall security policy. The issue that a good risk model needs to tackle is bridging isolated expertise and views. This requires a unifying model describing both cyber and physical assets in the same terms, so that the two are compatible for a joint simulation model. The knowledge about the overall system is termed Hybrid Situational Awareness (HSA) and extends PSA and CSA by explicitly taking into account interdependencies. As in (Schauer et al., 2018), we divide the HSA in two components: a module

focusing on detection of suspicious correlation of events (called the correlation engine) and another module focusing on the consequences of an incident in this hybrid setting (called the propagation engine).
In Section 2.2, we propose a simulation model of error propagation in such a hybrid system. In essence, the model is a network of interconnected Mealy automata, where the "automata" describes the individual evolution of an asset, and it is "Mealy" to account for asset interdependencies, using domain-specific common vocabulary between distinct domain experts. In Section 2.3, we sketch an implementation of the model that we use in the remainder of the paper.

2.1 Existing Approaches

Various approaches exist to model cascading failures in a network. Classical network models working with topological properties (Wang and Chen, 2008; Holme, 2002; Motter et al., 2002) are generally applicable but at the same time are not able to take into account domain characteristics which makes them error-prone when it comes to predictions. Recent approaches work with networks of networks or interconnected networks (Buldyrev et al., 2010) and show that these behave different than single networks. The high complexity of cyber-physical networks makes it impossible to perfectly predict future behavior, yielding an increasing number of stochastic models. These include advanced Markov chain models (Wu and Chu, 2017; Wang, Scaglione and Thomas, 2012; Rahnamay-Naeini and Hayat, 2016), branching process models (Dobson, Kim and Wierzbicki, 2010; Qi, Sun and Mei, 2015; Qi, Ju and Sun, 2016) and other high-level stochastic models (Dong and Cui, 2016). While the probabilistic nature of cascading failures is

essential (and thus incorporated in our model), we prefer an event-driven model through automata.

In the context of port security, different approaches on security exist (Andritsos and Mosconi, 2010; Andritsos, 2013) but focus mostly on physical security. An approach towards harmonization of cyber and physical components is presented in (Papastergiou and Polemi, 2014) but models of how to combine information from both sources are currently missing.

2.2 Simulation-Based Approach

The simulation-based approach proposed in (König et al., 2019) models a critical infrastructure as a directed graph $G = (V, E)$, where each vertex $v \in V$ corresponds to an asset of the CI and edges represent dependencies of one asset on other one. Each asset individually maintains a "state of health" that changes over time, either directly upon an incident or indirectly by notifications of state changes received from other assets. Figure 1 shows the overall model (left) with internal models specific for each CI (right). We assume that the state of health is measured on a three-tier scale, ranging from "functional" (normal working condition) to "affected" (impaired functionality but the asset still works to some extent) up to "outage" (temporary or permanent breakdown). Any such change of state of an asset is communicated (as notifications) to other assets, which in turn may, but not need to, change their states accordingly. Hence, an asset will react on incoming signals from other assets and itself emit notifications to dependent assets. The natural model to capture such behavior is a probabilistic Mealy automaton, in which a state transition is triggered by an incoming symbol α (signal) and may cause an output symbol (outgoing notification β), but only so with a

probability p (or $p = 1$ if the transition is deterministic). The simulation itself then starts with an initial signal that is the incident, which goes to all assets, respectively representing
Mealy-automata, directly affected by the incident. Their state transitions and according outgoing signals to other dependent assets then trigger further cascading effects in other assets and so on.

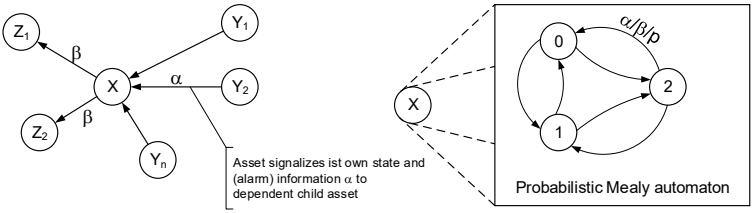


Figure 1: Dependency structure (left) and inner model (right)

A bit more formal, the infrastructure model is a directed graph where each node representing an asset is a probabilistic Mealy automaton

$$M = (S, \Sigma, \Sigma, \delta, \lambda, s) \tag{1}$$

where S denotes the set of all states an asset can be in, Σ is the input and output alphabet (assumed to be equal here, but this can be generalized), δ a transition relation, λ an output function and $s \in S$ the initial state. Since transitions happen only with a certain probability, δ assigns a probability distribution to each pair of state and input symbol.
Before we show how the model helps estimating the impact of a cyber-attack on a port, we give an overview on the implementation in the next section, including some remarks on how to specify the model parameters.

2.3 Remarks on Implementation

Overall, the considered spreading process is an event-based discrete time simulation, implementable in tools like OmNet++, ns-3 or others. Our research prototype (Schauer et al., submitted) is a designated implementation of the mechanisms described above. It allows the user to draw and connect the important physical and cyber assets on a web application while the actual simulation is done in an application programming interface (API). The prototype provides two main outputs: first, a distribution of the final state for each asset and second an overview on which assets are affected after a fixed time interval.

While the implementation of a system of coupled probabilistic Mealy automata is not technically difficult, the model comes with a large number of parameters that need to be specified. Each transition within each Mealy automaton (asset) has an incoming alarm, an outgoing notification and a probability of occurrence. We treat this problem with a machine-aided parameterization method, which we sketch below.

It is useful to assume that all assets share the same state space and to fix a common set of incident notifications Σ exchanged between assets (at least for reasons of understandability between the assets, since a dependent asset should "understand" what its parent node notifies it about). The elements of Σ can be arbitrary structures, and we assume those to be string-encodings of alert messages, containing (among others) at least a timestamp, criticality level and impact information for the notifying asset. This information can then be processed by the receiving asset to update its own state based on the current one (the function $\delta: \Delta(S \times \Sigma) \to S$), and update other assets accordingly (function $\lambda: S \times \Sigma \to \Sigma$). The symbol Δ here denotes the simplex taken over all triples in $S \times \Sigma \times S$, corresponding to the

probabilities that a transition happens. In the specification, this amounts to ascribing a value p to the state transition from $s_1 \rightarrow s_2 = \delta(s_1, \alpha)$ upon input symbol α and output symbol $\beta = \lambda(s_1, \alpha)$, thus describing the transition as a triple $\alpha/\beta/p$ (cf. right hand side of Figure 1). The terms α and β are alert or status notification strings that assets can exchange, and whose specification depends on the application context. As such, specification may be in a common syntax to capture all sorts of relevant information; a laborious and complex, yet not technically difficult, task. Estimating the probabilities p is a different story: we propose computing these values from example instances of transitions $s_1 \rightarrow s_2$ with labels α/β and transition flags 0/1 labeled by experts to indicate when a transition would occur (under the conditions α and from the state s_1) or when it would not occur. Given many such examples, we can step forward by fitting a logistic regression model to this training data and compute (predict) the values p for any transition using that model.

3 Consequences of a Cyber-Attack on a Port

For the upcoming analysis, we consider a fictitious European port as an example CI since ports are crucial for supply and trade and limited functionality significantly affects society. In course of the ongoing digitalization, the integration of information and communication technology (ICT) systems became more and more important for ports for automation as well as control purposes. As for any other infrastructure, this paves the way for sophisticated attacks, ranging from ransomware attacks (Georgia Institute of Technology, 2017) to advanced persistent threats (Tankard, 2011).

In response to these threats, new regulations and standards have been developed, such as the Interim Guidelines on Maritime Cyber Risk Management by the International Maritime Organization (IMO) in 2016 (IMO, 2016). The ISO 28001 standard (International Organization for Standardization, 2007) focuses on the overall security of supply chains and explicitly takes into account the interaction between all involved partners. Although some approaches have been defined to assess cyber threats in maritime supply chains (Kotzanikolaou, Theoharidou and Gritzalis, 2013; Polemi and Kotzanikolaou, 2015; Schauer, Polemi and Mouratidis, 2018), a holistic view taking into account both cyber and physical information seems to be missing so far. Such a holistic view is necessary to understand consequences of a cyber-attack, which in turn is a core duty in risk management. In the remainder of this section, we consider a fictitious cyber-attack and investigate its effect on a port.

3.1 Scenario Description

While the considered cyber-attack is purely artificial, it is inspired by reports on NotPetya (Countercept, 2017) and aims at illustrating potential consequences of such an incident. Thus, it inherits some major characteristics of NotPetya while it does not intent to reconstruct the event. NotPetya started with a compromised update of the MEDoc accounting software and spread like a worm to other machines and organizations. Different from WannaCry, NotPetya did not spread over the internet, but through interconnected networks using stolen credentials form infected machines (Countercept, 2017). This way, it also affected Windows computers that were fully patched and not using the MEDoc software. NotPetya used two encryption mechanisms: one that only encrypts files of a certain type and

one that encrypts the Master File Table (MFT) that allows reading files from the hard drive (Countercept, 2017). Encryption of the MFT is possible by modification of the Master Boot Record (MBR) that controls the system start. If both the MFT and the MBR are encrypted, all data is lost. If only the MFT is encrypted but not (yet) the MBR, it is possible to recover some data (Countercept, 2017).

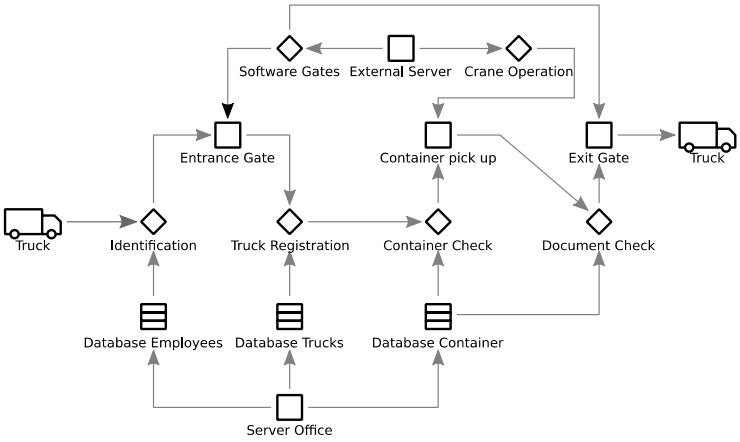


Figure 2: Important components for container pick up

In order to keep the procedures and the results comprehensible, we do not model the entire port but only consider a truck picking up a container at the port for further distribution. The steps of this business process are as shown in Figure 2 where besides special icons for trucks and databases squares are used to represent physical assets and diamonds represent software supported processes. When the truck arrives at the port, the driver is required to identify as an employee who is authorized to enter the area. After passing the entrance gate (and potentially a security scanner ensuring it

does not carry dangerous goods), a formal check of the truck follows, i.e., if it is on the list of registered and approved trucks. Next, all information about the requested container is checked: does the driver have permission to pick it up and is the container available (off the ship and cleared customs)? All these checks rely on databases about personal, trucks and container, respectively. After successful registration, the driver receives a printed barcode containing the information on where to pick up the container, i.e., where to park so that the crane can load the container on the truck. Once the container is on the truck, its barcode is checked (if necessary, also other characteristics such as temperature). Finally, all documents are checked at the exit gates and the driver is authorized to leave the port. Operation of both the gates and the cranes is governed by software provided by an external partner, such as Maersk.

3.2 Impact Simulation

Simulation of an attack according to the proposed method is done with the tool described in Section 2.3 (we use the online version (AIT, 2019) for visualization). The state of an asset is measured on a 3-tier scale to represent the impact due to the attack in terms of data loss (depending on the encryption mechanism, as described in Section 3.1) or to represent functionality. In both cases, higher numerical values indicate more severe problems.

If a cyber-attack hits the office network, it causes failure of all connected PCs and laptops, compromising databases and customer data. Other components such as gates or cranes depend on servers and software provided by partners and are thus more affected if a partner is victim of a cyber-attack.

We consider two different scenarios:

1. The case where a cyber-attack hits the ports own network (starting at the node server office)
2. The case where the external provider is hit (starting at the node external server)

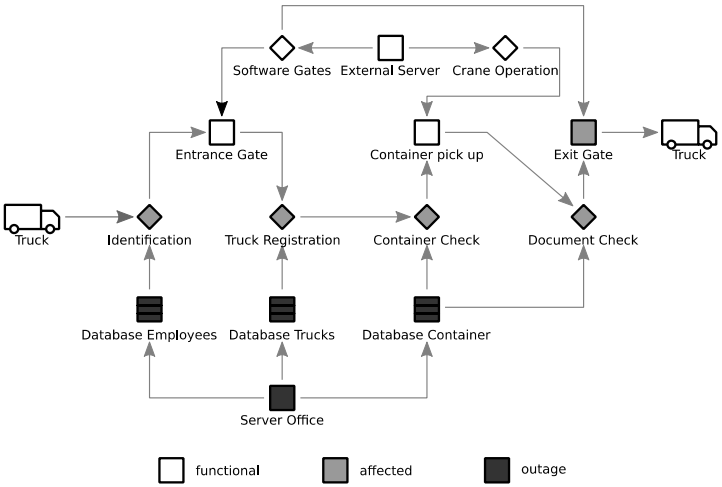


Figure 3: Consequences of a cyber-attack on the office network

In the first case, this will cause loss of information stored in the different databases, which in turn affects the corresponding checks. Most of this work can be done manually, so that the entire process slows down significantly but operation should still be possible. Potential consequences are illustrated in Figure 3. The exit gate is not facing operational problems but due to the delays along the line it is not able to provide the optimal service (e.g., further checks may be necessary before a truck may leave the ports premises).

In the second case, the cyber-attack directly affects functionality of the gates as well as the cranes that allow picking up a container. This virtually interrupts transportation to and from the port, as shown in Figure 4. The color codes in the picture (black, grey, white) directly correspond to the states (failure, affected, working), thus providing an immediate visual guidance of which parts are affected to which degree. Theoretically, this relates our work to percolation, which asks for the evolution of large clusters within a graph; in our case, the question would be about the potential rise of a giant red area within our network, expressing a large-scale impact from an attack. We do not explore this theoretical route any further here, and leave it as subject of future considerations.

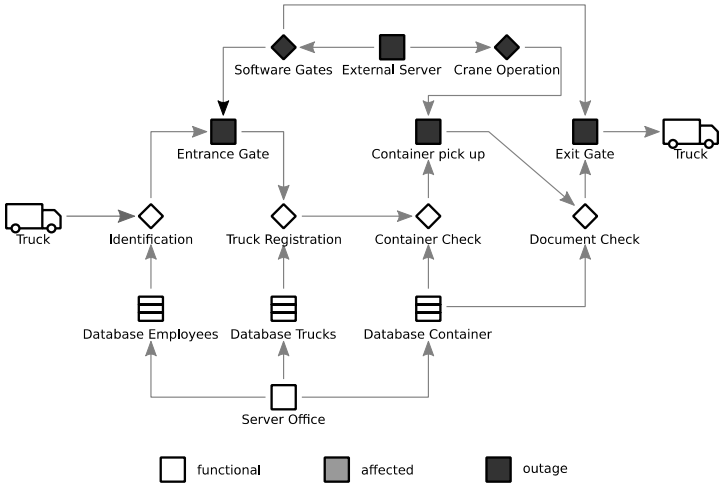


Figure 4: Consequences of a cyber-attack on the external network

A comparison of the two examples illustrates that a port may be even more sensitive to disruptions of services provided by external partners than to direct (targeted) attacks to the port itself. This illustration works with single simulations of each scenario but the tool used allows for iterated simulation to allow statistical inference on the results.

3.3 Comparison with Reported Impact

Many companies were affected by NotPetya, e.g., the pharmaceutical company Merck, FedEx's subsidiary TNT Express, the food producer Mondelez or the manufacturer Reckitt Benckiser (Greenerg, 2018). The effect it had on A.P. Møller-Maersk (that used MEDoc in an office in Odessa) is of particular interest since it affected the entire (cargo) supply chain and in particular numerous ports all over the world, e.g. India's largest container port (PTI, 2017), demonstrating the sensitivity of (maritime) supply chains.

The impact of NotPetya can only be estimated from public reports. A.P. Møller-Maersk stated at the Davos World Economic Forum in 2018 that it had to reinstall 45,000 PCs and 4,000 servers but recovered in less than two weeks (Cimpanu, 2018a). Despite a huge amount of manual work and immense effort to find an intact backup, the damage is estimated between $250 and $300 million. Not only were basically all computers of Maersk's 176aramet. 80,000 employees frozen and the booking website down, also terminals' software was affected. Designed for data exchange, the interconnection between the two networks caused many troubles. In 17 out of the 76 Maersk's terminals, gates were out of order and containers could neither be picked up nor dropped off (Greenerg, 2018).

4 Conclusion

Reported cyber incents like NotPetya and others demonstrate the strong mutual dependence of infrastructures on one another. The particular nature of advanced persistent threats to exploit a diverse spectrum of platforms and media for an attack calls for descriptive models capable of equal flexibility and diversity. We propose probabilistic Mealy automata for a generic description of the dynamics of the interplay of systems inside a CI. For a comprehensive picture about the risk of cascading effects, a simulation model necessarily needs to unite different domains, and this is a project of joint maintenance between CI providers. Given the interconnectedness of infrastructures, it is no longer sufficient to secure one's own domain, since an attack occurring at the "neighbor's site" may indirectly affect us as much (or even more) as a direct hit by an attacker. Understanding cascading effects thus appears as crucial for contemporary and future system security.

The scenarios depicted in this work have been inspired by reports about NotPetya and its relatives (precursors and successors), and compiled into a software prototype for probabilistic simulation of possible scenarios. A large entirety of these then converges into a picture about what could happen, what is likely and which parts are unlikely to be affected by certain scenarios. While a probabilistic simulation cannot deliver guarantees for the prediction, it helps prioritizing security mitigation actions and points out spots that are more vulnerable than others (and hence need quicker attention).

Future work along these lines will go deeper into the parameterization of the model in the sense of "training" it based on domain expertise (expert risk assessments or data from reported incidents).

Acknowledgements

The authors wish to thank their colleagues Thomas Grafenauer and Manuel Warum for implementing the tool that was used for the analysis.

Financial Disclosure

This work is supported by the European Commission's Project No. 740477 SAURON (Scalable multidimensionAl awaReness sOlution for protecting european ports) under the Horizon 2020 Framework Programme (H2020-CIP-01-2016-2017).

References

AIT, 2019. SAURON Propagation Engine Editor. [online] Sauron. Available at: <https://atlas.ait.ac.at/sauron/#/> [Accessed 6 May 2019].

Andritsos, F., 2013. Port security & access control: A systemic approach. In: IISA 2013. [online] 2013 Fourth International Conference on Information, Intelligence, Systems and Applications (IISA). Piraeus, Greece: IEEE, pp.1–8. Available at: <http://ieeexplore.ieee.org/document/6623728/> [Accessed 17 May 2019].

Andritsos, F. and Mosconi, M., 2010. Port security in EU: A systemic approach. In: 2010 International WaterSide Security Conference. [online] 2010 International Waterside Security Conference (WSS). Carrara, Italy: IEEE, pp.1–8. Available at: <http://ieeexplore.ieee.org/document/5730222/> [Accessed 17 May 2019].

Bateman, T., 2013. Police warning after drug traffickers' cyber-attack. [online] BBC News. Available at: <www.bbc.com/news/world-europe-24539417> [Accessed 5 Jul. 2017].

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H.E. and Havlin, S., 2010. Catastrophic cascade of failures in interdependent networks. Nature, 464, p1025.

Cimpanu, C., 2018a. Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack. Bleeping Computer. Available at: <https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/>.

Cimpanu, C., 2018b. Port of San Diego suffers cyber-attack, second port in a week after Barcelona. ZDNet. Available at: https://www.zdnet.com/article/port-of-san-diego-suffers-cyber-attack-second-port-in-a-week-after-barcelona/>.

Condliffe, J., 2016. Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks. [online] Available at: <https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/> [Accessed 26 Jul. 2017].

Countercept, 2017. NotPetya – Everything you need to know. Available at: <https://www.countercept.com/blog/notpetya-ransomware-frequently-asked-questions/>.

Dobson, I., Kim, J. and Wierzbicki, K.R., 2010. Testing Branching Process Estimators of Cascading Failure with Data from a Simulation of Transmission Line Outages. Risk Analysis, 30(4), pp.650–662.

Dong, H. and Cui, L., 2016. System Reliability Under Cascading Failure Models. IEEE Transactions on Reliability, 65(2), pp.929–940.

E-ISAC, 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid. [online] Washington, USA. Available at: <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf> [Accessed 2 Nov. 2018].

Fletcher, S., 2001. Electric power interruptions curtail California oil and gas production. Oil Gas Journal.

Georgia Institute of Technology, 2017. Simulated Ransomware Attack Shows Vulnerability of Industrial Controls | Research Horizons | Georgia Tech's Research News. [online] Available at: <http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls> [Accessed 4 May 2017].

Greenerg, A., 2018. The untold story of NotPetya, the most devastating 180arameteriz in history. WIRED. Available at: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> [Accessed 28 Mar. 2019].

Holme, P., 2002. Edge overload breakdown in evolving networks. Physical Review E, [online] 66(3). Available at: <https://link.aps.org/doi/10.1103/PhysRevE.66.036119> [Accessed 30 Oct. 2018].

IMO, 2016. Interim guidelines on maritime cyber risk management. Available at: <http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC.1-CIRC.1526%20(E).pdf> [Accessed 5 Jul. 2017].

International Organization for Standardization, 2007. ISO 28001: Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance. Geneva, Switzerland.

Karnouskos, S., 2011. Stuxnet worm impact on industrial cyber-physical system security. [online] IEEE, pp.4490–4494. Available at: <http://ieeexplore.ieee.org/document/6120048/> [Accessed 8 Aug. 2017].

König, S., Rass, S., Rainer, B. and Schauer, S., 2019. Hybrid Dependencies between Cyber and Physical Systems. In: accepted for publication. Computing Conference. London.

Kotzanikolaou, P., Theoharidou, M. and Gritzalis, D., 2013. Assessing n-order dependencies between critical infrastructures. International Journal of Critical Infrastructures, 9(1/2), pp.93–110.

Motter, A.E., de Moura, A.P.S., Lai, Y.-C. and Dasgupta, P., 2002. Topology of the conceptual network of language. Physical Review E, [online] 65(6). Available at: <https://link.aps.org/doi/10.1103/PhysRevE.65.065102> [Accessed 29 Oct. 2018].

Papastergiou, S. and Polemi, N., 2014. Harmonizing commercial port security practices & procedures In Mediterranean Basin. In: IISA 2014, The 5th International Conference on Information, Intelligence, Systems and Applications. [online] 2014 5th International Conference on Information, Intelligence, Systems and Applications (IISA). Chania, Crete, Greece: IEEE, pp.292–297. Available at: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6878835> [Accessed 17 May 2019]

Polemi, N. and Kotzanikolaou, P., 2015. Medusa: A Supply Chain Risk Assessment Methodology. In: F. Cleary and M. Felici, eds., Cyber Security and Privacy. [online] Cham: Springer International Publishing, pp.79–90. Available at: <http://link.springer.com/10.1007/978-3-319-25360-2_7> [Accessed 14 May 2019].

PTI, 2017. New malware hits JNPT operations as APM Terminals hacked globally | The Indian Express. [online] The Indian Express. Available at: <http://indianexpress.com/article/india/cyber-attack-new-malware-hits-jnpt-ops-as-apm-terminals-hacked-globally-4725102/> [Accessed 6 Jul. 2017].

Qi, J., Ju, W. and Sun, K., 2016. Estimating the Propagation of Interdependent Cascading Outages with Multi-Type Branching Processes. IEEE Transactions on Power Systems, pp.1212–1223.

Qi, J., Sun, K. and Mei, S., 2015. An Interaction Model for Simulation and Mitigation of Cascading Failures. IEEE Transactions on Power Systems, 30(2), pp.804–819.

Rahnamay-Naeini, M. and Hayat, M.M., 2016. Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach. IEEE Transactions on Smart Grid, 7(4), pp.1997–2006.

Schauer, S., Grafenauer, T., König, S., Warum, M. and Rass, S., submitted. Estimating Cascading Effects in Cyber-Physical Critical Infrastructures. CRITIS.

Schauer, S., Polemi, N. and Mouratidis, H., 2018. MITIGATE: a dynamic supply chain cyber risk assessment methodology. Journal of Transportation Security. [online] Available at: <http://link.springer.com/10.1007/s12198-018-0195-z> [Accessed 14 May 2019].

Schauer, S., Rainer, B., Museux, N., Faure, D., Hingant, J., Rodrigo, F.J.C., Beyer, S., Peris, R.C. and Lopez, S.Z., 2018. Conceptual Framework for Hybrid Situational Awareness in Critical Port Infrastructures. In: E. Luiijf, I. Žutautaitė and B.M. Hämmerli, eds., Critical Information Infrastructures Security. [online] Cham: Springer International Publishing, pp.191–203. Available at: <http://link.springer.com/10.1007/978-3-030-05849-4_15> [Accessed 23 Jan. 2019].

Tankard, C., 2011. Advanced Persistent threats and how to monitor and deter them. Network Security, 2011(8), pp.16–19.

Verizon, 2017. 2017 Data Breach Investigations Report. Available at: <http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf> [Accessed 7 May 2017].

Wang, W.-X. and Chen, G., 2008. Universal robustness characteristic of weighted networks against cascading failure. Physical Review E, [online] 77(2). Available at: <https://link.aps.org/doi/10.1103/PhysRevE.77.026101> [Accessed 30 Oct. 2018].

Wang, Z., Scaglione, A. and Thomas, R.J., 2012. A Markov-Transition Model for Cascading Failures in Power Grids. In: 2012 45th Hawaii International Conference on System Sciences. [online] 2012 45th Hawaii International Conference on System Sciences (HICSS). Maui, HI, USA: IEEE, pp.2115–2124. Available at: <http://ieeexplore.ieee.org/document/6149269/> [Accessed 27 Sep. 2018].

World Maritime News, 2018. COSCO Shipping Lines Falls Victim to Cyber Attack. World Maritime News. Available at: <https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/> [Accessed 7 May 2019].

Wu, S.-J. and Chu, M.T., 2017. Markov chains with memory, tensor formulation, and the dynamics of power iteration. Applied Mathematics and Computation, 303, pp.226–239