14th International Defense and Homeland Security Simulation Workshop, 004
21st International Multidisciplinary Modeling & Simulation Multiconference

2724-0363 © 2024 The Authors.
doi: 10.46354/i3m.2024.dhss.004

Pharmaceutical Logistics under Cyberattack Conditions

Larissa Schachenhofer[1,*], and Patrick Hirsch[1]

[1]Institute of Production and Logistics, Department of Economics and Social Sciences, University of Natural Resources and Life Sciences Vienna, Feistmantelstraße 4, 1180 Vienna, Austria

*Corresponding author. Email address: larissa.schachenhofer@boku.ac.at

Abstract

Cyber incidents are among the most common risks for organizations nowadays. Organizations that are part of the critical infrastructure are at risk of falling victim to a cyberattack. As drug shortage can severely affect patient's health and well-being, our examination focuses on the pharmaceutical industry under cyberattack conditions. We analyze aspects of logistics processes and warehousing typical for pharmaceutical wholesalers. Through conducting a thorough desk research as well as expert interviews, and developing a hybrid simulation model, we aim to identify significant limitations regarding resource capacities and other bottlenecks that may moderately to severely restrict or adversely affect mitigation measures taken during the response phase. Key findings will suggest an optimal layout setting of a warehouse to allow employees to overtake tasks during a cyberattack when automatized processes cannot be conducted temporarily. Furthermore, the developed simulation model can be used to derive relevant mitigation measures, which can effectively and significantly limit the damage to the organization under cyberattack conditions. The novel contribution of this work consists of identifying vital leverage points related to pharmaceutical processes to increase resilience toward cyber incidents in the future.

Keywords: Cyberattack; cyber incident; supply chain risk management; pharmaceutical industry; hybrid simulation model

1. Introduction

Cyberattacks are increasing in number, and their sophistication is affecting the state, society, and organizations across multiple industries. Consequently, the European Commission identified several lacks regarding the Network and Information Systems (NIS) Directive as the first EU cybersecurity law, such as an insufficient understanding of the leading cyber threats and cyber resilience across the Member States and organizations operating in the EU. To react to the growing threat level and eliminate the deficits of the NIS Directive, in December 2020, the Commission proposed a revised set of future-oriented rules to foster cyber resilience across the EU. A political agreement was achieved in 2022, and the new Directive, the NIS 2, was formally adopted later in the same year (European Commission, 2023). It will replace the old Directive on 18 October 2024. NIS 2 counteracts the existing regulatory deficits resulting from the differing implementation of the NIS Directive in the EU Member States by harmonizing them. The initial objective of the NIS 2 Directive to create a high level of cybersecurity in the EU remains the same, yet within a modernized legal framework (Austrian Federal Chancellery, s.a.).

The NIS 2 Directive contributes to improving cybersecurity within the EU member states. However, the sophistication of cyberattacks advances fast, so we see the need for potentially rapid implementable measures beyond the legislative requirements stated in the NIS 2 Directive. This recommendation holds especially true for organizations being part of the critical infrastructure. These organizations are the

backbone of a working state, and their high relevance to society increases the risk of becoming the target of a cyberattack. Medical care is especially critical for society as medication is essential for preventing, treating, and diagnosing diseases. Consequently, the availability and assurance of product quality is a high-priority goal for the healthcare system.

Thus, our research, as part of the research project CONTAIN "Efficient Reaction to IT Security Incidents in Transnational Supply Chains" (Austrian Research Promotion Agency, 2023), focuses on the specific conditions of pharmaceutical logistics under cyberattack conditions. The aim of our research is to analyze factors that need consideration in order to increase the level of cybersecurity in the pharmaceutical industry.

The remainder of this paper is structured as follows. Section 2 depicts the state of the art of research concerning pharmaceutical conditions under cyberattack conditions. Section 3 elaborates on the materials and methods used for the analysis. Section 4 presents the results that can be reported so far, which are also briefly discussed. In section 5, critical conclusions are drawn, and suggestions for further research are provided.

2. State of the art

Despite efforts by the public and private sectors, medication shortages are a prevalent and persisting issue (US Food & Drug Administration, 2019). Drug shortage, according to the US Federal Food, Drug, and Cosmetic Act, is defined as "a period when the demand or projected demand for the drug within the United States exceeds the supply of the drug" (US Food & Drug Administration, 2023), and can be applied to other nations accordingly. In many cases, drug shortage occurs among drugs that are lower in price compared to other marketed drugs. For patients, the implications can be severe as drug shortages can cause serious harm to the patient's health. They might initiate treatment delays, thereby increasing the period of patient suffering and spurring disease progression.

Moreover, alternative treatments might be less well-tolerated or effective. This can result in reduced patient well-being and heightened societal morbidity (US Food & Drug Administration, 2019). Furthermore, healthcare providers can be severely burdened as drug shortages aggravate or even prevent them from providing vital healthcare services. For example, emergency response teams might have to adapt procedures and retrain first responders without further ado to effectively change from routinely used drugs, unavailable for a specific period, to substitutes. Hospitals and clinics might have to change their IT systems to incorporate adaptions towards available drugs and simultaneously ensure accurate dosing and dispensing of substitutes. Moreover, the limited availability of certain drugs can lead to a need for rationing these drugs in favor of high-priority cases (US Food & Drug Administration, 2019).

From a supply chain perspective, healthcare delivery systems and their actors are critical. Typically, shortages emerge at one or several of these upstream stages. Thus, scientific studies on implementing and optimizing logistics systems to manage medication inventory effectively are growing. For example, Demessie et al. (2020) examined implementing a logistics management information system in public health facilities in northeastern Ethiopia. The authors found that stockouts occurred, among other reasons, due to poor availability and use of recording forms and, thus, suggest the implementation of a logistics management information system. Also, Zwaida et al. (2021) recommend the usage of efficient inventory management in order to avoid shortage issues in hospitals, using an online solution that automatically takes drug refilling decisions by utilizing a deep reinforcement learning model. Automated and digital solutions are broadly used nowadays. The pharmaceutical industry is heavily automatized, yet high automatization becomes an issue under cyberattack conditions. This holds especially true for organizations with no alternative manual processes, which can be temporarily utilized as a fall-back strategy in such a scenario. Schachenhofer et al. (2022) have analyzed the consequences of an internet blackout on different organizations including the health sector. The authors found that the lack of information, which goes hand in hand with such an event, places a special burden on affected organizations, which can lead to a downwards goal alignment. In the case of healthcare organizations, which bear an absolutely crucial responsibility for the health of society, this must be avoided at all costs. Bruzzone et al. (2022) analyzed hybrid and cyber threats in critical infrastructures as a form of hybrid warfare by proposing a simulation model which allows simulating various cyber threats. The authors state that ideal targets are easily damaged and challenging to repair, while actual physical damage is difficult to cause through cyberattacks. Yet, when it comes to the pharmaceutical industry, impacts on pharmaceutical production plants, automatic order picking machines, intelligent conveyor belt systems, and other digital-based machines, physical damage can be caused either by compromising production or impacting logistics processes in pharmaceutical warehouses and thus pharmaceutics' availability to society.

Rojas et al., 2023 model the distribution system of a dental clinic distribution network as retail, which is a unique perspective. The authors apply Monte Carlo simulation to address demand uncertainty as well as improving inventory management and patient care. They found that the implementation of an inventory control system, which allows for an enhanced identification of supply and demand, is critical as well as technology-based solutions to increase inventory visibility and tracking accuracy. Yet, the findings are

limited to inventory management of dental clinics. Further research is needed to adapt the suggested approach to other healthcare settings.

Improta et al. (2021) analyzed the drug flow of three Italian hospitals. By implementing a simulation model, which integrates inventory sharing and vendor-managed inventory with lateral transshipment to identify the lot size and service level values of each warehouse, the total costs of the supply chain could be minimized. The authors found that the "make-to-order" strategy, which involves pulling demand through production orders, encompasses enormous advantages for organizations. However, demand can only sometimes be balanced through lateral transshipments of the same echelon, as there might not be enough of the demanded medical product in stock. Furthermore, make-to-order production requires high flexibility and a relatively short production time per item-unit. Otherwise, customers might withdraw an order request, especially if comparable products have a shorter manufacturing time or are even immediately available.

However, Improta et al. (2021) completely ignore extreme circumstances during crises such as cyberattacks. While efficiency considerations make sense regarding storage costs for large quantities of products under normal conditions, they can have severe consequences for the availability of medicines during cyber incidents.

Okereafor and Adebola (2021) analyzed cybersecurity lessons related to the healthcare industry during COVID-19 and found that, despite hospitals and other organizations directly involved in providing healthcare services to society, also pharmaceutical companies, as well as medical supply and logistics actors, were particularly hard hit by cyber threats such as ransomware and malware during COVID-19. Mattingly (2021) examined the role of outsourcing facilities in overcoming drug shortages. The author found that, while these facilities operate within a regulatory framework that does not stand against their ability to provide access to drugs currently in shortage, they do not necessarily take on that role. She further stated that the reasons for this are not yet completely clear and, hence, need to be explored further.

Drug shortages are more likely to occur under exceptional circumstances, such as cyberattacks, which is why cybersecurity is gaining importance in the pharmaceutical industry and most other industries. Del Giorgio Solfa (2022) states that in the pharmaceutical industry cybersecurity encompasses several sub-domains, namely, identity management and data security, network security, application security, cloud security, mobile security, and user education. As digital technologies are increasingly used in diverse functions for providing medical products and improving customer experience, the number of cyberattacks, data breaches, and other cyber incidents in this area is increasing. The findings of the study suggest that (1) digital operations can be improved by focusing on cybersecurity, (2) supply chain risks are positively associated with digital operations, and (3) organizations can respond to supply chain risks by enhancing the visibility of their respective supply chain networks as well as their ability to assess possible risks which go along with using digital operations. Despite these important findings, the study also states significant limitations, such as its generalizability, thus revealing the need for further research in this area.

Hence, considering the research gaps in the relevant scientific literature, our research project, CONTAIN, aims to identify pharma-specific aspects that need attention during a cyber incident. According to Kannan and Swamidurai (2023), modeling and simulation are highly relevant to cybersecurity research, as cybersecurity simulation enables the imitation of cyberattacks as well as the assessment of a system's risk exposure. Therefore, we intend to contribute to an improved understanding of pharmaceutical processes under cyberattack conditions by utilizing a modeling approach. For this purpose and in contrast to Kannan and Swamidurai (2023), who used system dynamics modeling to investigate indirect cyberattacks and their consequences on a hypothetical small business IT system, we are developing a hybrid simulation model. This model will depict the processes of a pharmaceutical wholesaler and will be designed in the way of a digital twin (DT) of the real-world system. According to VanDerHorn & Mahadevan (2021), DTs are characterized by (1) representing a single instance of a physical system and (2) data or information of the physical system being used in order to update the states of the DT over time. While there are several concepts of applying DTs in different services, the application in the health care sector is, according to Maizi et al. (2023), still in the cradle stage. The authors developed a DT prototype for healthcare operations management for means of decision support in an addiction treatments clinic. We follow an innovative approach by combining the concept of DTs with healthcare and cybersecurity. With the development of a DT and a quantitative analysis, we intend to derive relevant measures for Business Continuity Management (BCM). According to Tammineedi (2010), BCM aims to enable the uninterrupted availability of core business resources to support vital business activities during a business disruption and expedite returning to business as usual.

3. Materials and Methods

The findings of this research are based on a comprehensive literature review in which the scientific databases Web of Science and Google Scholar were utilized. Keywords used for searching relevant literature were cybersecurity/ cyberattack/ cyber incident AND pharma/ pharmaceutics/ pharmaceutical industry, as well as multi/ hybrid simulation modeling. The snowballing method was applied, and articles were selected according to their relevance to our research

and topicality. Nevertheless, the number of studies linking cybersecurity to the pharmaceutical industry was manageable. Approximately 60 studies were considered relevant, out of which 12 were of high relevance for this paper.

Based on an expert interview and iterative bilateral talks with the pharmaceutical experts of the research project, critical business processes will be depicted via the Business Process Model and Notation (BPMN). BPMN is the standard for graphically illustrating business processes using a distinct semantic scheme (Chinosi & Trombetta, 2012). Based on these process depictions, a simulation model will be developed. Our methodological procedure is also illustrated in Figure 1.

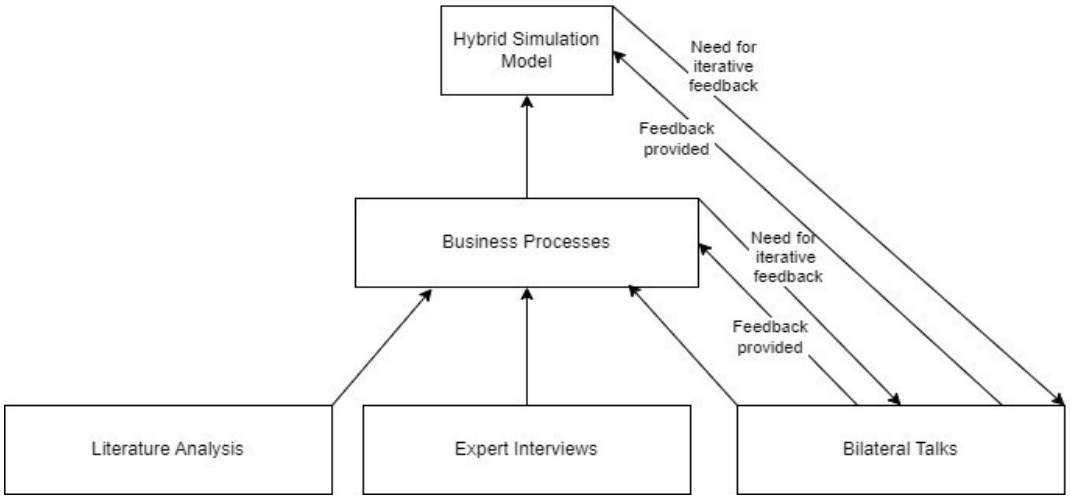

Figure 1. Methodological procedure of the presented research

Modeling approaches can be categorized according to System Dynamics (SD), Discrete Event Simulation (DES), and Agent-Based Modeling (ABM) (Howard et al., 2023). SD, developed by Forrester, can be applied to analyzing complex systems and their behavior over time, including inherent feedback loops (Forrester, 1997). For example, Schachenhofer et al. (2023) used SD to depict and analyze the impact of an internet blackout on information flows within organizations. Such feedback behavior, which often follows distinct and commonly encountered patterns, also called archetypes, is easily disregarded and unrecognized. These patterns can have adverse effects on the prevalent conditions of a specific situation (Mandl, 2019), which also applies to IT security incidents such as cyberattacks.

DES emphasizes sequences of discrete events that can change a system's state and is typically utilized to illustrate and examine production systems and logistics processes (Hubl et al., 2011; Pernkopf & Gronalt, 2020). While DES focuses on the process perspective, ABM emphasizes defined agents, their individual behavior, and the interaction between multiple agents in a system (Vrabič et al., 2021; Værbak et al., 2021). Combining two or more simulation approaches, often called Hybrid Simulation (HS) approach (Barbosa & Azevedo, 2017) or multi-method simulation, is possible. Different modeling paradigms combined allow us to depict and analyze the underlying behavior of highly complex systems as accurately as possible (Howard et al., 2023). Kummer et al. (2023) used hybrid simulation modeling, for example, to analyze and optimize a water-based municipal solid waste management system by combining ABM and DES.

Similarly, HS is beneficial for capturing both the process-oriented perspective and the behavioral level of agents and their interactions under cyberattack conditions.

Thus, we will combine the simulation approaches of DES and ABM. With the hybrid simulation model currently under development using the simulation software AnyLogic, we specifically aim to test different scenarios with varying resource capacities. This will serve the purpose of identifying critical bottlenecks that a pharmaceutical wholesaler might encounter under cyberattack conditions. These bottlenecks are vital in increasing cybersecurity, as they might constitute relevant leverage points for mitigation measures to increase the cyber resilience of actors in the pharmaceutical industry.

4. Preliminary Results and Discussion

The literature analysis revealed that cybersecurity related to the pharmaceutical industry requires further research to generate a deeper understanding of aspects that need to be considered when increasing cyber resilience in the pharmaceutical industry. Vrabič et al. (2021) state that DTs, representing physical processes accurately and consistently, improve process-related understanding. At the same time, the authors refer to issues regarding the development of DTs, which can impact the robustness and resilience of DTs themselves, suggesting an intelligent agent-based

architecture for resilient DTs in manufacturing processes. For the currently developed hybrid simulation model regarding pharmaceutical processes under cyberattack conditions, this resilient architecture suggested by Vrabič et al. (2021) can also be of interest. However, this has to be evaluated during the further development process.

Moreover, several aspects must be considered while pursuing our analysis in this research field.

(1) The pharmaceutical industry differs from other industries insofar as the consequences of one actor being highly impacted in conducting its business processes for a limited period of time can affect the availability of certain drugs for pharmacies, hospitals, and end-users (Del Giorgio Solfa, 2022). The conditions under which these severe effects can come into play are currently being analyzed. However, the period of restricted access to the digital operations of an actor in the pharmaceutical industry plays an important role.

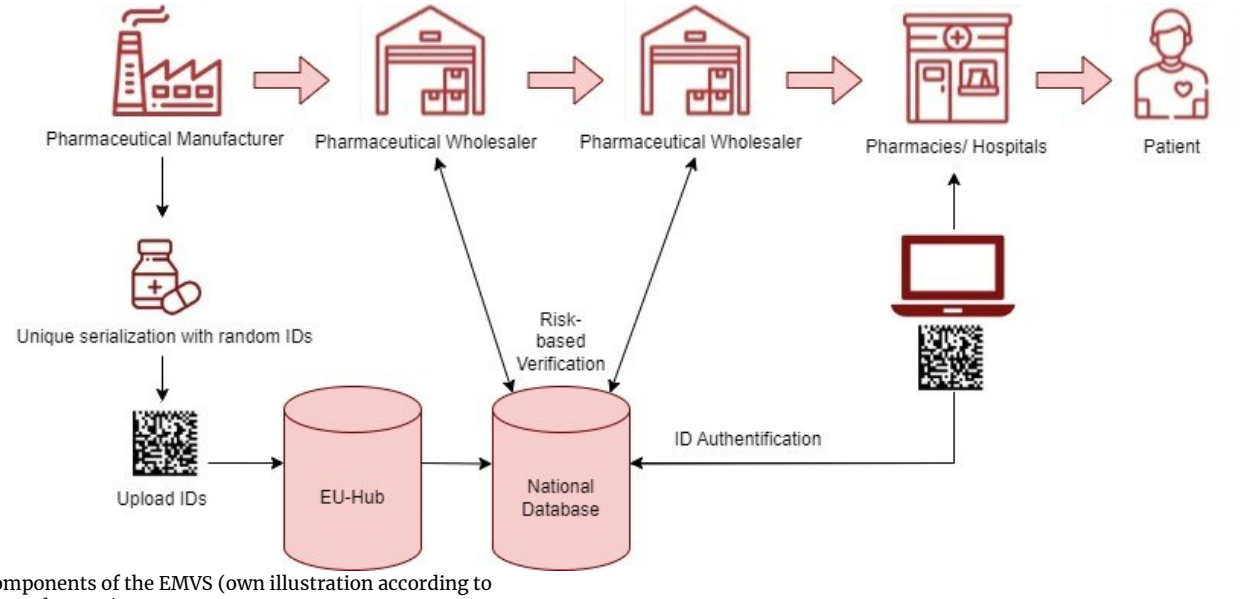

Figure 2. Components of the EMVS (own illustration according to COSYS Ident GmbH, s.a.)

(2) Market conditions of the pharmaceutical drug market differ from classical market conditions since drug shortages cannot be immediately dealt with through increased production, as several regulatory approvals are necessary for modifying existing production plants and building new ones. Also, finding new sources for active pharmaceutical ingredients (APIs) takes time and the application process of new manufacturers that wish to address a prevalent drug shortage through selling their newly developed product (US Food & Drug Administration, 2019).

(3) Medicines are subject to strict regulations to ensure they cannot be falsified or counterfeited. Falsified medicines mimic real medicines, while counterfeit medicines do either not comply with intellectual property rights or infringe trademark law (European Medicines Agency). The problem especially occurs in developing countries and has its origin in a highly fragmented pharmaceutical supply chain system, in which information is not shared between the different parties (Hasan & Khondker, 2022). In contrast, in Europe different online systems are used at all levels of the medicines supply chain to counteract this issue. Accordingly, there is a high dependency on these systems, as the verification of medicines requires both the functionality of these systems and the ability to access them digitally. Temporarily unverifiable products can, therefore, not be handed over during a period of restriction.

The European Medicines Verification System (EMVS) components are the European HUB, repositories, and the infrastructure for connecting the EU hub with the national systems (COSYS Ident GmbH, s.a.), which is also depicted in **Errore. L'origine riferimento non è stata trovata.**.

(4) Pharmaceutical products vary significantly in terms of their logistics and storage requirements. Some are temperature-sensitive and must be cooled or stored under other special conditions, e.g., sunlight protection (Feyisa et al., 2021). Furthermore, the handling of medicines for the professional treatment of drug addiction, such as medicines

derived from opium, is subject to strict international controls (CORDIS EU, 2019).

(5) While initially hesitant, the degree of automatization in the pharmaceutical industry has grown in recent years (Hole et al., 2021). However, the dependence on digital systems and processes is also rising with an increasing automation level. This condition will likely constitute an issue under cyberattack conditions.

Del Giorgio Solfa (2022), however, sees the broad adoption of digital processes in the pharmaceutical industry not necessarily as disadvantageous. Despite being a crucial tool for effective knowledge management and information sharing, he highlights the chance to utilize digital transformation for predicting future risks. The advancement of organization's risk management through addressing cybersecurity-related issues can also contribute to managing supply chain risks more effectively in the future. Hasan and Khondker (2022) further explain how blockchain technology can improve traceability, visibility, and security to the drug supply system, bringing more options to the table to prevent counterfeited drugs from entering the legal supply chain and, thus, enabling another form for drug verification across the pharmaceutical supply chain.

However, implementing these new approaches to increase the cybersecurity of pharmaceutical supply chains is still in its infancy. The cyberattack scenario likely involves the compromise of one or more digital systems, affecting information management along the supply chain or processes conducted automatically, such as automatic order-picking systems. The developed model will reflect a real-world use case of a pharmaceutical wholesaler. The objective is to model the flow of goods in this pharmaceutical wholesaler's facility under cyberattack conditions. Possible workarounds and alternative processes are reviewed and evaluated considering their relative efficiency, as well as resource-related and timely restrictions.

5. Conclusions

Cybersecurity is an increasingly important topic across several industries. This short paper and our currently developed hybrid simulation model emphasize the pharmaceutical industry and its circumstances.

The literature analysis clarified that (1) there are few studies regarding cybersecurity in the pharmaceutical industry, and (2) digital systems such as the drug verification system are critical for a working medicines supply chain. As the impairment of digital access to such a system or compromising the data correctness is a potential scenario from a cyberattack perspective, we will focus our research efforts further on this case. Pharmaceutical wholesalers are essential nodes in the logistics network of the drug supply chain, as they often account for a high percentage of the handling volume. As we are provided with real-world data from a pharmaceutical wholesaler, we are deepening our analysis particularly from this perspective. Detailed business processes were created based on the literature analysis, expert interviews, and bilateral talks. The business processes constitute the fundament for developing the hybrid simulation model. For this purpose, the logic of the business processes will be implemented into the simulation environment using real world data. A comprehensive, quantitative analysis in the course of the simulation study will enable us to test potential workarounds, e.g., conducting core processes manually for a defined time frame. Furthermore, we will analyze resource capacities, e.g., regarding employees, and, thus, identify potentially critical bottlenecks such as location-based restrictions. On the one hand, we will focus on deriving relevant mitigation strategies in terms of vital BCM measures, and on the other hand, we will also look at the recovery phase after a cyberattack.

This will enable us to derive effective mitigation strategies from our analyses and, based on them, provide our industry partners with critical recommendations for action. With our expected research results, we aim to generate vital knowledge for the pharmaceutical industry to reduce the potential for damage in the event of a cyberattack and quickly regain the ability to act. The analysis in the current simulation study will allow us to provide further statements concerning critical leverage points that might enable actors in the pharmaceutical industry to increase their level of cybersecurity. Consequently, taking these measures into action also potentially strengthens cyber resilience in the pharmaceutics industry in the long run. As we analyze a pharmaceutical wholesaler under the conditions of a cyberattack, future research could investigate the impact of a cyber incident on pharmaceutical manufacturers. Further research could also build on our results by using similar modeling approaches for actors in other industry branches, as there might be reoccurring patterns pointing out core aspects of successful mitigation strategies.

Funding

The research leading to these results has received funding from the KIRAS programme. KIRAS is a research, technology and innovation funding programme of the Republic of Austria, Federal Ministry of Finance. The Austrian Research Promotion Agency (FFG) has been authorised for the programme management (FFG grant number: 902707).

Acknowledgments

We thank the CONTAIN project team for their cooperation and practical input.

References

Austrian Federal Chancellery. Die neue NIS-2-Richtlinie. https://www.nis.gv.at/nis-2-richtlinie.html

Austrian Research Promotion Agency (FFG). (2023). CONTAIN. https://projekte.ffg.at/projekt/4791800

Barbosa, C., & Azevedo, A. (2017). Hybrid Simulation for Complex Manufacturing Value-chain Environments. Procedia Manufacturing, 11, 1404–1412. https://doi.org/10.1016/j.promfg.2017.07.270

Bruzzone, A., G., Massei, M., & Giovannetti, A. (2022). Hybrid and cyber threat in towns, critical infrastructures and Industrial Plants. In A. G. Bruzzone, B. Goldberg, & F. Longo (Eds.), Proceedings of the 12th International Defense and Homeland Security Simulation Workshop (DHSS), 19th International Multidisciplinary Modeling & Simulation Multiconference. https://doi.org/10.46354/i3m.2022.dhss.006

Chinosi, M., & Trombetta, A. (2012). BPMN: An introduction to the standard. Computer Standards & Interfaces, 34(1), 124–134. https://doi.org/10.1016/j.csi.2011.06.002

CORDIS EU. (2019). Access to Opioid Medication in Europe: Fact Sheet. https://cordis.europa.eu/project/id/222994

COSYS Ident GmbH. EMVS - European Medicines Verification System. https://www.cosys.eu/european-medicines-verification-system

Del Giorgio Solfa, F. (2022). Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry. International Journal of Technology, Innovation and Management (IJTIM), 2(2). https://doi.org/10.54489/ijtim.v2i2.98

Demessie, M. B., Workneh, B. D., Mohammed, S. A., & Hailu, A. D. (2020). Availability of Tracer Drugs and Implementation of Their Logistic Management Information System in Public Health Facilities of Dessie, North-East Ethiopia. Integrated Pharmacy Research & Practice, 9, 83–92. https://doi.org/10.2147/IPRP.S262266

European Commission. (2023). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - FAQs. https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

European Medicines Agency. Falsified medicines: overview: Falsified vs. counterfeit medicines. https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview

Feyisa, D., Jemal, A., Aferu, T., Ejeta, F., & Endeshaw, A. (2021). Evaluation of Cold Chain Management Performance for Temperature-Sensitive Pharmaceuticals at Public Health Facilities Supplied by the Jimma Pharmaceuticals Supply Agency Hub, Southwest Ethiopia: Pharmaceuticals Logistic Management Perspective Using a Multicentered, Mixed-Method Approach. Advances in Pharmacological and Pharmaceutical Sciences, 2021, 5167858. https://doi.org/10.1155/2021/5167858

Forrester, J. W. (1997). Industrial dynamics. Journal of the Operational Research Society(48), Article 10 (1997), 1037–1041.

Hasan, K. S., & Khondker, S. R. (2022). Utilizing Blockchain Technology in Cyber Security to Secure Pharmaceutical Industry Supply Chain. Conference Paper.

Hole, G., Hole, A. S., & McFalone-Shaw, I. (2021). Digitalization in pharmaceutical industry: What to focus on under the digital implementation process? International Journal of Pharmaceutics: X, 3, 100095. https://doi.org/10.1016/j.ijpx.2021.100095

Howard, D. A., Jørgensen, B. N., & Ma, Z. (2023). Multi-Method Simulation and Multi-Objective Optimization for Energy-Flexibility-Potential Assessment of Food-Production Process Cooling. Energies, 16(3), 1514. https://doi.org/10.3390/en16031514

Hubl, A., Altendorfer, K., Jodlbauer, H., Gansterer, M., & Hartl, R. F. (2011). Flexible model for analyzing production systems with discrete event simulation. In Proceedings of the 2011 Winter Simulation Conference (WSC) (pp. 1554–1565). IEEE. https://doi.org/10.1109/WSC.2011.6147873

Improta, G., Scala, A., Trunfio, T. A., & Guizzi, G. (2021). Application of Supply Chain Management at Drugs Flow in an Italian Hospital District. Journal of Physics: Conference Series, 1828(1), 12081. https://doi.org/10.1088/1742-6596/1828/1/012081

Kannan, U., & Swamidurai, R. (2023). INDIRECT CYBER ATTACK ON PHARMACEUTICAL COMPANIES. Journal of Pharmaceutical Negative Results(14), Article 2, 1766–1782. https://doi.org/10.47750/pnr.2023.14.02.222

Kummer, Y., Youhanan, L., & Hirsch, P. (2023). Operational analysis and optimization of a water-based municipal solid waste management system with hybrid simulation modeling. Sustainable Cities and Society, 99, 104890. https://doi.org/10.1016/j.scs.2023.104890

Maizi, Y., Antoine, A., & Bendavid, Y. (2023). Designing a Digital Twin Prototype for an Addiction Treatments Clinic. In Proceedings of THE 22ND INTERNATIONAL CONFERENCE ON MODELING AND APPLIED SIMULATION. CAL-TEK srl.

https://doi.org/10.46354/i3m.2023.mas.014

Mandl, C. E. (2019). Managing complexity in social systems: Leverage Points for Policy and Strategy. Springer.

Mattingly, A. N. (2021). The role of outsourcing facilities in overcoming drug shortages. Journal of the American Pharmacists Association : JAPhA, 61(1), e110-e114. https://doi.org/10.1016/j.japh.2020.08.027

Okereafor, K., & Adebola, O. (2021). HEALTHCARE CYBERSECURITY LESSONS FROM COVID. International Journal in IT & Engineering (IJITE), Article 4. Advance online publication. https://doi.org/1776

Pernkopf, M., & Gronalt, M. (2020). A simulation-based sizing approach for automated log yards. Simulation Modelling Practice and Theory, 104, 102123. https://doi.org/10.1016/j.simpat.2020.102123

Rojas, G. N., Ortiz, O. C., Velasco, Peredo, J., Gutierrez, Ramos, A., & Torres, Mendoza, R (2023). Dental Clinic Inventory Management with Monte Carlo Simulation. In Proceedings of THE 22ND INTERNATIONAL CONFERENCE ON MODELING AND APPLIED SIMULATION. CAL-TEK srl. https://doi.org/10.46354/i3m.2023.mas.008

Schachenhofer, L., Hirsch, P., & Gronalt, M. (2023). How internet blackouts affect information flows in organizations - Analyzing cascade effects and feedback loops. International Journal of Disaster Risk Reduction, 98, 104101. https://doi.org/10.1016/j.ijdrr.2023.104101

Schachenhofer, L., Gronalt, M., & Hirsch, P. (2022). ISIDOR: Analysing the Consequences of an Extensive and Prolonged Internet Outage with System Dynamics. In A. G. Bruzzone, B. Goldberg, & F. Longo (Eds.), Proceedings of the 12th International Defense and Homeland Security Simulation Workshop (DHSS), 19th International Multidisciplinary Modeling & Simulation Multiconference. https://doi.org/10.46354/i3m.2022.dhss.003

Tammineedi, R. L. (2010). Business Continuity Management: A Standards-Based Approach. Information Security Journal: A Global Perspective, 19(1), 36–50. https://doi.org/10.1080/19393550903551843

US Food & Drug Administration (2019). Drug Shortages: Root Causes and Potential Solutions: A Report by the Drug Shortages Task Force.

US Food & Drug Administration (2023). Frequently Asked Questions about Drug Shortages. https://www.fda.gov/drugs/drug-shortages/frequently-asked-questions-about-drug-shortages#:~:text=The%20Federal%20Food%2C%20Drug%2C%20and,ability%20to%20supply%20the%20market.

Værbak, M., Ma, Z., Demazeau, Y., & Jørgensen, B. N [Bo N.] (2021). A generic agent-based framework for modeling business ecosystems: a case study of electric vehicle home charging. Energy Informatics, 4(S2). https://doi.org/10.1186/s42162-021-00158-4

VanDerHorn, E., & Mahadevan, S. (2021). Digital Twin: Generalization, characterization and implementation. Decision Support Systems, 145, 113524. https://doi.org/10.1016/j.dss.2021.113524

Vrabič, R., Erkoyuncu, J. A., Farsi, M., & Ariansyah, D. (2021). An intelligent agent-based architecture for resilient digital twins in manufacturing. CIRP Annals, 70(1), 349–352. https://doi.org/10.1016/j.cirp.2021.04.049

Zwaida, T. A., Pham, C., & Beauregard, Y. (2021). Optimization of Inventory Management to Prevent Drug Shortages in the Hospital Supply Chain. Applied Sciences, 11(6), 2726. https://doi.org/10.3390/app11062726