An Outlook of Digital Twins in Offensive Military Cyber Operations

Clara Maathuis
Open University, The Netherlands
clara.maathuis@ou.nl

Abstract: The outlook of military cyber operations is changing due to the prospects of data generation and accessibility, continuous technological advancements and their (public) availability, technological and human (inter)connections increase, plus the dynamism, needs, diverse nature, perspectives, and skills of experts involved in their planning, execution, and assessment phases respecting (inter)national aims, demands, and trends. Such operations are daily conducted and recently empowered by AI to reach or protect their targets and deal with the unintended effects produced through their engagement on them and/or collateral entities. However, these operations are governed and surrounded by different uncertainty levels e.g., intended effects prediction, consideration of effective alternatives, and understanding new dimensions of possible (strategic) future(s). Hence, the legality and ethicality of such operations should be assured; particularly, in Offensive Military Cyber Operations (OMCO), the agents involved in their design/deployment should consider, develop, and propose proper (intelligent) measures/methods. Such mechanisms can be built embedding intelligent techniques based on hardware, software, and communication data plus expert-knowledge through novel systems like digital twins. While digital twins find themselves in their infancy in military, cyber, and AI academic research and discourses, they started to show their modelling and simulation potential and effective real-time decision support in different industry applications. Nevertheless, this research aims to (i) understand what digital twins mean in OMCO context while embedding explainable AI and responsible AI perspectives, and (ii) capture challenges and benefits of their development. Accordingly, a multidisciplinary stance is considered through extensive review in the domains involved packaged in a design framework meant to assist the agents involved in their development and deployment.

Keywords: cyber operations, digital twins, artificial intelligence, explainable AI, responsible AI

1. Introduction

"They won the war but lost the peace." (Jonathan Maberry)

The digital transformation process redrew and continues to redraw the ways how strategies, policies, and businesses are thought, built, and used in different domains by adapting, developing, combining, and deploying advanced and intelligent technologies like AI, cyber-physical systems, and digital twins (Puriwat, W., & Tripopsakul, 2021; Maathuis & Chockalingam, 2022c). Specifically, through their inherited modelling and simulation capacity, the implementation and use of digital twins is still incipient in critical domains, e.g., military and cyber security, and while they could pose unexpected implications through their deployment, they start to show benefits in tasks like target intelligence while enhancing system's characteristics, e.g., adaptivity, flexibility, and accuracy which are important for simulating critical decision-making processes and providing (real-time) decision-making support to relevant stakeholders/users (Glaessgen & Stargel, 2012)). Moreover, when building and conducting offensive operations in the military cyber domain, i.e., through OMCO, the agents involved should first understand what such technologies mean and imply, and afterwards incorporate proper socio-technical dimensions in the means/methods considered. Recent efforts reflect the advantages of implementing and integrating different modelling and simulation techniques in the military domain, however specifically focusing on defining, designing, and building advanced techniques like digital twins for OMCO is lacking, and implicitly, misconceptions or development impediments could occur. It is then the aim of this research to understand what digital twins mean and establish the basis for their design for being developed and deployed in OMCO. Specifically, the objectives of this article are further defined: (i) to understand and define what digital twins mean in the OMCO context, (ii) to assess how XAI and RAI dimensions could be embedded when building them, and (iii) to capture, structure, and analyse challenges and opportunities occurring when building and deploying them.

To achieve these objectives, multidisciplinary research is conducted in a Design Science Research approach having the following contributions:

- To the scientific community for opening a research path on investigating how digital twin solutions could be designed and deployed in the military cyber domain using XAI and RAI technologies.
- To the military domain by providing understanding and awareness regarding the meaning of digital twins when building and deploying OMCO.

- To different industry organizations stressing the need for joining efforts between academic researchers and practitioners from different fields involved when building digital twins systems since lessons learned together with effective and efficient solutions could be communicated, propagated, and embedded in different domains while contributing to responsible and explainable results and decisions.
- To society as it argues for conducting research and development not only through military or military-technical lenses, but through interdisciplinary lenses in a systemic socio-technical approach.

The remainder of this article is structured as follows. Section 2 discusses relevant research and existing standards at the moment of speaking. Section 3 presents the approach considered when conducting this research. Section 4 reflects on the meaning and important characteristics of OMCO, and important aspects involved when building them. Section 5 proposes a working definition for building and deploying digital twins in OMCO. Section 6 reflects on challenges and opportunities surrounding and occurring when building and deploying digital twins in OMCO. Section 7 concludes the findings of this research while reflecting on further research ideas.

2. Related research

The increasing interest and efforts of different communities reflect the necessity for building digital twin solutions in both military and cyber domains using advanced techniques under the Industry 4.0. umbrella with paradigms like AI, IoT, cloud computing, and blockchain. Accordingly, a series of studies are discussed as they are relevant and for identifying the knowledge gap that this research tackles.

The first step when building any kind of system/solution is proper understanding of underlying concepts and methods. In this sense, a large body of studies are focused on defining d*igital twins* generally, however, a clear definition lacks and implicitly confusion still exists. On this behalf, Fuller et al. (2020) discuss the misconceptions between terms related i.e., digital model and digital shallow providing their definitions, differences, and corresponding applications in manufacturing, healthcare, and smart cities. Furthermore, Qian et al. (2022) see them as complex digital systems containing a data-driven software and hardware emulation platform, i.e., a cyber replica of physical systems, and consider as architecture requirements: latency, reliability, scalability, safety, security, and privacy. Herein, Aheleroff et al. (2021) treat them as a service with considerable advantages for smart scheduled maintenance and real-time monitoring applications. VanDerHorn & Mahadevan (2021) and Barricelli, Casiraghi & Fogli (2019) discuss their characteristics, application, needs and opportunities. Moreover, on establishing requirements for building and deploying digital twins, Moyne et al. (2020) consider integrating re-usability, interoperability, interchangeability, maintainability, extensibility, and autonomy aspects, and propose a corresponding object-oriented architecture. Moreover, understanding challenges like model consistency and orchestration involved during their development, maintenance, and verification is critical (Van Den Brand et al., 2021).

On digital twin applications, Liu et al. (2021) conduct a review arguing for building such models to benefit of their advantages when verifying, validating, and optimizing the system, and in run-time simulations with massive data being generated and used. Specifically, Kritzinger et al. (2018) and Cimino, Negri and Furnagalli (2019) focus on analysing the application in manufacturing for simulating and optimizing production systems through element-level and whole assembly virtualization handling aspects like functionality, maintenance, safety, and performance. In the military domain, Mendi, Erol & Dogan (2021) discuss the advantages of their application, e.g., low fault tolerance, cost-effective, and efficient for military systems that match realistic real-world conditions, for instance in logistics development and aircraft deployment. Particularly, Silvera et al. (2020) discuss their implementation in military naval-platforms during their life cycle that supports tasks like maintenance intervention and downtime handling and present the F-110 IMPS frigate fully integrating a digital twin able to connect, extract and process data overboard equipment and crew members all over the ship, and further support manoeuvring and piloting ship training in a realistic environment. Moreover, Lee, Van Bossuyt & Bickford (2021) propose a digital twin military decision-support framework for developing an Unmanned Aerial System for demonstrating route selection capability during mission, i.e., route optimization module recommends the optimal route based on variables like potential UAS damage or destruction by adversary's action(s). Moreover, Song et al. (2022) explore their application for equipment battle damage test assessment considering prediction, real-time, and combat decision-making functionalities. Maathuis, Pieters & Van Den Berg (2021) propose an intelligent modelling and simulation solution for effects classification and proportionality assessment in military cyber operations that can serve as the core of a military cyber digital twin. Remaining in the cyber arena, Talkhestani et al. (2019) highlight their contribution for cyber-physical

production systems integrating important aspects like synchronization with the real asset, active data acquisition from environment, and simulation ability. Vielberth et al. (2021) build a digital twin-based cyber range for Security Operations Centre analysts where attacks on industrial systems are simulated for incident detection and prevention learning purposes.

On the existing standards applicable for DT development and deployment in different domains, Flamigni et al. (2021) recall, e.g., (i) ISO 23247 Digital Twin framework for manufacturing that establishes general requirements, proposes a reference architecture, provides basic information attributes for corresponding elements, and establishes requirements for information exchange between the elements embedded in the reference architecture (ISO, 2021), (ii) ISO/TC 184/SC 4 Industrial data for dealing with the meaning, structure, representation, and quality management of the information necessary for building a system focusing on aspects like interoperability, manufacturing, and visualization (ISO, 2001), (iii) ISO/IEC JTC 1/SC 27 Information security, cybersecurity, and privacy protection for protecting data and ICT systems used (ISO, 2017), and (iv) ISO/IEC JTC 1/SC 42 Artificial Intelligence for providing guidance when building and integrating AI solutions (ISO, 2017). Moreover, IEEE P3144 Digital Twin maturity model and assessment methodology in industry proposes a maturity model for industry applications and assessment methodologies for content, processes involved, and corresponding maturity levels.

These studies contain important elements when grasping the meaning of digital twins and building corresponding systems/solutions in different domains. Specifically, while efforts for building them in military and cyber domains exist, to the best of our knowledge, tackling the class of OMCO is lacking, thus this is the knowledge gap that this research tackles for building proper, responsible, and transparent intelligent OMCO.

3. Research methodology

To achieve the objectives of this research, the following research questions are formulated following a logical path:

- How to define digital twins in the OMCO context?
- How to embed XAI and RAI mechanisms and techniques when building digital twins in OMCO?
- What are the main challenges and opportunities occurring when building and deploying digital twins in OMCO?

Accordingly, a multidisciplinary viewpoint is adopted by proposing a design framework as a socio-technical artefact pursuing a Design Science Research methodological approach (Peffers et al., 2007; Venable, Pries-Heje & Baskerville, 2017; Peffers, Tuunanen & Niehaves, 2018). The artefact represents the first effort in this sense and merges concepts, methods, and techniques from digital twins, cyber security, military operations, and AI domains. Therefore, the following research activities are taken:

Problem definition: recent years reflect the transition from classical modelling and simulation solutions to advanced and intelligent solutions like digital twins that facilitate the integration, simulation, and functionality of cyber, physical, and data layers that characterize specific systems. This transition implies before capturing and building corresponding solutions, their proper understanding and design that matches one's aims and considers relevant socio-ethical norms and values. Since OMCO are still in their infancy regarding the existence of models and methods that assist their development, deployment, and assessment phases, this research aims to produce an intervention by defining digital twins in OMCO and reflecting on challenges and opportunities that they imply. Hence, an extensive literature review is conducted by combing keywords like *digital twin, military, AI, definition, challenge,* and *limitation* in scientific databases like IEEE, ACM, and Springer plus industry and governmental publications and standards like IEEE and ISO.

Design and development: the components of the proposed framework, i.e., the definition, and analysis of challenges and opportunities of digital twins in OMCO are developed and proposed.

Evaluation: the results on this research are analysed and captured in corresponding structures that form together the proposed artefact having direct exemplification on concrete moments of OMCO phases.

Communication: the research conducted, and the results obtained are disseminated through this article.

4. Offensive military cyber operations

At the NATO Warsaw Summit in 2016, cyberspace won its official warfare battlefield status being recognized as an operational domain (NATO, 2016a) and being perceived as 'a radical shift in the nature of the wartime battlefield' (Solce, 2008) due to characteristics like dynamism, embedded uncertainty, attribution issue, and incipient rules and regulation. The operations conducted in this battlefield are defined as 'part of a military operation in which cyber weapons/capabilities are used to achieve military objectives in front of adversaries inside and/or outside cyberspace' (Maathuis, Pieters & Van Den Berg, 2018a). While these operations are classified as intelligence, defensive, or offensive (Maathuis, Pieters & Van Den Berg, 2018b), they imply the need and intention for achieving well-defined objectives by conducting agents that use (intelligent) cyber weapons for engaging deliberate and/or dynamic military targets. For instance, in an intelligence Cyber Operation, proper adversary data is collected and analysed to gather useful insights for further use, e.g., to make sure that minimal collateral damage would be produced on civilian side; in a defensive Cyber Operation, relevant infrastructure should be defended through proper mechanisms that (actively) prevent target's engagement by adversaries, i.e., cyber threat hunting; and in an offensive Cyber Operation, all measures should be considered in the design of the intelligent cyber weapon used to engage the target for avoiding, limiting, or controlling the expected collateral damage.

Recently, a series of Cyber Operations like Stuxnet and the ones in Georgia and Ukraine surprised the global audience through their aims, target selection, and effects produced. Furthermore, long debates were carried out about their offensive nature, legitimacy, and the possibility of further developing and deploying OMCO started from been seen as a tabu to now been perceived as reality. Herein, targets could be influenced, altered, or damaged via cross-domain instruments (Borghard & Lonergan, 2019) (i) as an extra option for leaders, (ii) in conjunction with other military capabilities, (iii) to achieve a form of psychological ascendancy, or (iv) to produce fewer expected casualties (Smeets, 2018). Conducting these operations implies going through different targeting phases, i.e., design and development (phases 1 to 3), deployment (phases 4 and 5), and assessment (phase 6) (NATO, 2016b; Maathuis, Pieters & Van Den Berg, 2021). In these phases, different stakeholders are involved to make sure that the objectives defined are achievable and a series of methods and mechanisms are considered (Maathuis, 2022a) through the application of diverse modelling and simulation solutions that mirror or embed realistic field settings.

5. Defining digital twins in offensive military cyber operations

Albeit digital twins are perceived as a key technology introduced during the digital transformation process in the Industry 4.0., they have a history of two decennia with even earlier fundaments. The origin is attributed to Michael Grieves with his *mirror space model* and his further research with John Vickers at NASA projects on astronautics and aerospace area (Grieves & Vickers, 2017) defining digital twins as 'a virtual representation of a physical product' that merges the benefits of both physical and virtual worlds, and which contains three components: physical product, virtual representation of the physical product, and bi-directional data connection from the physical product to the virtual representation plus information and processes from the virtual representation to the physical product (Jones et al., 2020). Accordingly, in Figure 1 a series of definitions for Digital Twins are considered as basis for this research.

Source	Digital Twin definition
(Grieves & Vickers, 2017)	A set of virtual information constructs that fully describes a potential or actual physical manufactured product from the micro atomic level to the macro geometrical level.
(Glaessgen & Stargel, 2012) - NASA	An integrated multiphysics, multiscale, probabilistic simulation of an as-built vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its corresponding flying twin.
(Li et al., 2021)	A high-fidelity and up-to-date representation of an actual physical asset in operation that reflects the current asset condition and includes relevant historical data about the asset.
(Song et al., 2022)	A technological means to digitally create a dynamic virtual model of physical entities with multi-dimensions, multi-space time scales, multi-disciplines, and multi-physical quantities to simulate and depict the attributes, behaviours, and rules of physical entities in the real environment.
(Jones et al., 2020)	A dynamic and self-evolving digital/virtual model or simulation of a real-life subject or object (part, machine, process, human, etc.) representing the exact state of its physical twin at any given point of time via exchanging the real-time data as well as keeping the historical data.

Figure 1: Digital twins definitions selection

These definitions reflect the key three components, and further show that there are different perspectives and ways of providing understanding to the digital twins concept, and its meaning could be tailored to the application area (Vielberth et al., 2021). Considering that misconceptions and confusion with related topics like digital model or digital shadow exist, and the fact that no agreed definition for digital twins exist (Hribernik et al., 2021; Fuller et al., 2020), to assure their proper design, development, and deployment in OMCO, a systemic perspective is adopted and the following definition is proposed:

Digital twin in OMCO = a technological system that embeds the cyber abstractization, representation, and mirroring of a physical system in its realistic environment, physical system, and their corresponding data and communication flows in an OMCO.

The elements of this definition are:

- *Technological system*: whole entity containing its physical, cyber, and data and communication elements.
- *Cyber abstractization, representation, and mirroring*: cyber/virtual/digital components of the system.
- *Physical system*: system's physical elements contained and virtualized.
- *Data and communication flows*: data transmitted between the cyber and physical components together with their corresponding communication infrastructure.

In other words, a digital twin in OMCO is an advanced (intelligent)system that embeds the virtual, physical, plus data and communication elements of an OMCO system/entity. Given this, the following digital twins in OMCO architecture useful for training, exercises, and real operations is proposed in Figure 2 where continuous arrows depict information and results communication between targeting phases in an operation, and the doted arrows depict the information and results between the integrating component and the rest of the components. The architecture should be modular and configurable (Silvera et al., 2020), and contains two components:

- *Digital Twin Layers*, i.e., either three digital twin modules and an integration module or four stand-alone digital twins where the *Integration DT* communicates and takes results from the other three stand-alone Digital Twins.
- *Digital Twin Levels*, i.e., the physical, data and communication, and cyber components of a whole digital twin or four integrated digital twins.

Additionally, acknowledging that systems would have either an analytical, predictive, or simulation function for supporting different military cyber decision-making processes, it is the responsibility of military Commanders and their teams on how they interpret and use the results presented by the digital twins, hence it is necessary that such systems embed XAI and RAI methods since their design phase: a must for RAI for respecting and incorporating socio-ethical norms and values, and during the whole process and when presenting final results for XAI respecting military-technical and socio-legal-ethical requirements, norms, and values (Arrieta et al., 2020; Agarwal & Mishra, 2021; Maathuis, 2022a; Maathuis, 2022b). Such measures assure the development and deployment of responsible and accountable OMCO.

For demonstration, an OMCO is developed, deployed, and assessed in the phases illustrated in the left side of the architecture where the final results of the Integration DT could be of further use as lessons learned or input for future operations, cyber or other. For instance, in Design and Development, the target is selected, its core vulnerability is identified and further an exploit is built in an intelligent cyber weapon that can predict the levels and probabilities of (un)intended effects and conduct a responsible and explainable proportionality assessment for target engagement; furthermore, the effects are assessed in relation to the aims defined and dependencies. Herein, a prototype would be made by defining and deploying multiple instances of the system that would be aggregated while accounting the requirements and interactions with the physical and cyber environments (Grieves, M., & Vickers; Jones et al., 2020).

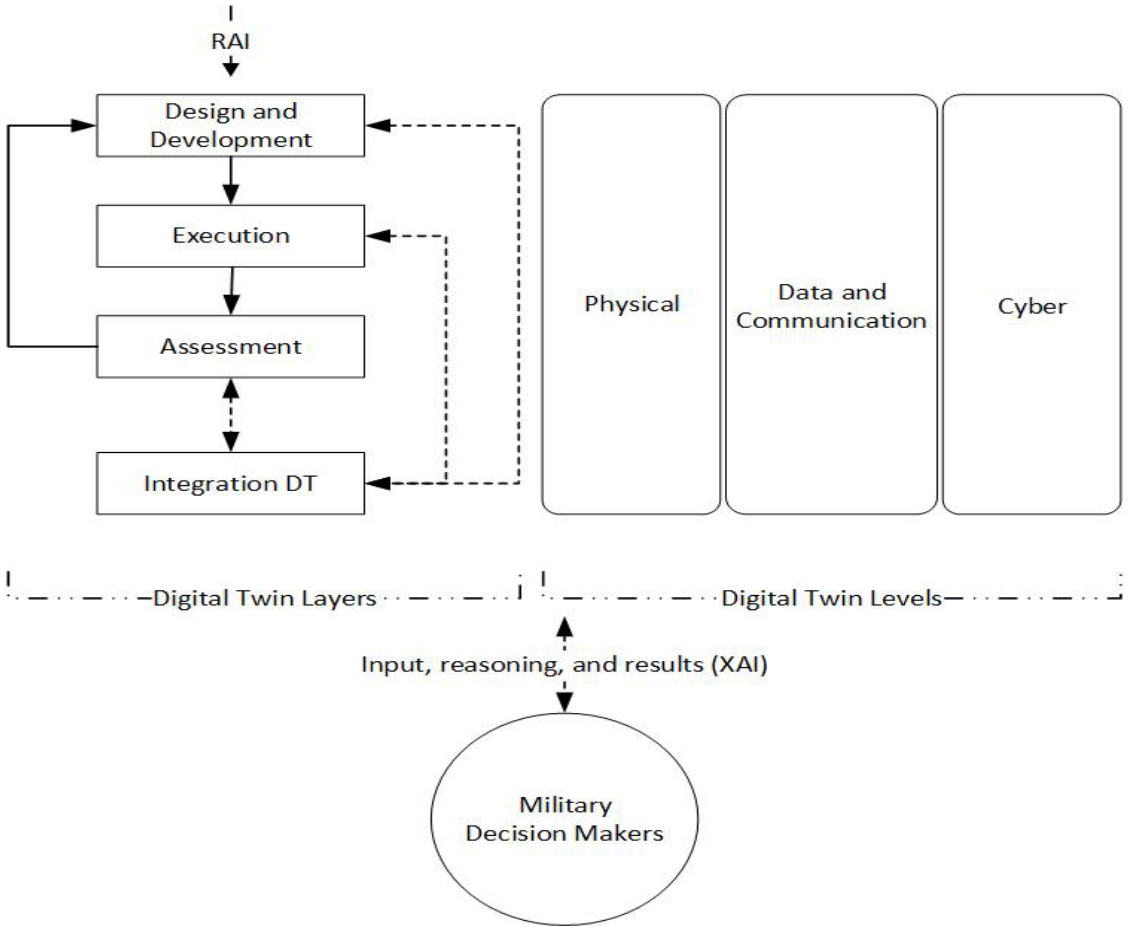

Figure 2: Digital twins architecture

6. Challenges and opportunities when building digital twins in offensive military cyber operations

As part of the ongoing digital transformation process and strongly tied to several digital and intelligent technologies, as any other type of technology, digital twins present challenges and benefits/opportunities of/through its use. For scoping purposes, for each category, three clusters are considered.

As challenges, the following main clusters are defined:

- Standardization, governance, and regulation that consider muti-stakeholder perspective (Talkhestani et al., 2019; Singh et al., 2021; Flamigni et al., 2021): since these systems are developed and deployed in settings where multi-stakeholders are involved, proper standards, governance and regulation mechanisms should be considered while matching the objectives and functionality defined.
- Data and algorithms (Jones et al., 2020; Qian et al., 2022; Song et al., 2022): such systems are data sensitive and rely on relevant and high-fidelity representations and data added to properly built and deployed AI models, e.g., relevant data should be collected, analysed, used, and shared between the levels and layers of the system.
- Safety, security, privacy, and reliability (Glaessgen & Stargel, 2012; Vielberth et al., 2021; Chockalingam & Maathuis, 2022) and reliability issues: if unproperly managed and through their non-integration from the design phase of a digital twin on all its layers and levels, these have the potential of opening doors to unintended and intended cyber safety and security incidents by altering system's behaviour having large-scale and massive impact. For instance, such an operation could not be able to make a distinction between military and civilian objects, and by this produces massive collateral damage on civilian side, thus the system is not reliable in an operation.

As benefits, the following main clusters are discussed:

- Awareness and understanding, decision support, and education (Mendi, Erol & Dogan, 2021; Talkhestani et al., 2019): such systems facilitate understanding system's behaviour, supporting concrete decision-making processes, and producing/enhancing different learning activities. For instance, these systems could not only produce intelligence to current operations, but also through their assessment for future operations.
- Modelling and simulation for, e.g., live life-cycle testing, monitoring, optimization (Steinmetz et al. 2018; Jones et al., 2020; Hribernik et al., 2021): through their nature, digital twins model and simulate different systems and processes, e.g., allow mirroring and testing the execution of an operation of a dual-use target to avoid the unintended effects expected to be produced; or allow live monitorization of the path followed and the action taken by the intelligent cyber weapon launched using different optimization techniques.
- Accessibility and cost reduction (Barricelli, Casiraghi & Fogli, 2019; Jones et al., 2020; Aheleroff et al., 2021): through its design interfaces, such systems are directly accessible to users and facilitate the general cost reduction for implementation and deployment.

7. Conclusions

Conducting OMCO in a transparent and responsible way represents a complex process where different stakeholders, disciplines, methods, and (intelligent)technologies are involved considering their aims and effects assessed. Therein, modern enhanced modelling and simulation technologies like digital twins present different advantages, e.g., able to mirror, test, and monitor adversary's environment and target's execution in its context with minimal costs for producing (as much as possible)intended effects while avoiding, minimizing, and/or controlling the unintended effects. However, no real consensus exists regarding the definition of digital twins and how such technology should be designed and deployed in the military cyber domain, and these facts could imply unexpected consequences for the {military-cyber} stakeholders involved, and the broader audience impacted by their actions. Hence, this article addresses these aspects through offensive and socio-technical lenses using a Design Science Research methodological approach by defining digital twins in OMCO, proposing a design model, and analysing main challenges and benefits of their adoption and implementation. This research aims at opening a new research direction to produce and enhance awareness of the decision-makers involved and further support their development and deployment in real operational settings.

Moreover, this research pursues by investigating other dimensions involved in the processes of building digital twins in different phases of OMCO taking into account several socio-ethical aspects of AI (i) that should be involved since their design, and (ii) that are impacted through their execution for allowing such operations to be perceived as real operational alternatives.

References

Agarwal, S. & Mishra, S. (2021). Data and Model Privacy. In *Responsible AI*, pp. 153-170.

Aheleroff, S., Xu, X., Zhong, R. Y., & Lu, Y. (2021). Digital twin as a service (DTaaS) in industry 4.0: an architecture reference model. *Advanced Engineering Informatics*, *47*, 101225.

Arrieta, A. B. et al. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*, pp. 82-115.

Barricelli, B. R., Casiraghi, E., & Fogli, D. (2019). A survey on digital twin: Definitions, characteristics, applications, and design implications. *IEEE access*, *7*, 167653-167671.

Borghard, E. D., & Lonergan, S. W. (2019). Cyber operations as imperfect tools of escalation. *Strategic Studies Quarterly*, *13*(3), 122-145.

Cimino, C., Negri, E., & Fumagalli, L. (2019). Review of digital twin applications in manufacturing. Computers in Industry, 113, 103130.) ((Kritzinger, W., Karner, M., Traar, G., Henjes, J., & Sihn, W. (2018). Digital Twin in manufacturing: A categorical literature review and classification. IFAC-PapersOnLine, 51(11), 1016-1022.

Chockalingam, S., & Maathuis, C. (2022). An Ontology for Effective Security Incident Management. In *International Conference on Cyber Warfare and Security*. 17(1), 26-35.

Flamigni, F., Pileggi, P., Barrowclough, O. & Haenisch, J. (2021). First report on standards relevant for digital twins – Change2Twin. https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5dab9d442&appId=PPGMS

Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital twin: Enabling technologies, challenges and open research. *IEEE access*, *8*, 108952-108971).

Glaessgen, E., & Stargel, D. (2012). The digital twin paradigm for future NASA and US Air Force vehicles. In *53rd AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics and materials conference 20th AIAA/ASME/AHS adaptive structures conference 14th AIAA* (p. 1818).

Hribernik, K., Cabri, G., Mandreoli, F., & Mentzas, G. (2021). Autonomous, context-aware, adaptive Digital Twins—State of the art and roadmap. *Computers in Industry*, *133*, 103508.

Grieves, M., & Vickers, J. (2017). Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. In *Transdisciplinary perspectives on complex systems* (pp. 85-113). Springer.

Hribernik, K., Cabri, G., Mandreoli, F., & Mentzas, G. (2021). Autonomous, context-aware, adaptive Digital Twins—State of the art and roadmap. *Computers in Industry*, *133*, 103508.

IEEE (2022). Standard for Digital Twin Maturity Model and Assessment Methodology in Industry. IEEE P3144. https://standards.ieee.org/ieee/3144/10837/

ISO (2001). Industrial data. ISO/TC 184/SC 4. https://committee.iso.org/home/tc184sc4

ISO (2017). Information security, cybersecurity, and privacy protection. ISO/IEC JTC 1/SC 27

ISO (2017). Artificial Intelligence. ISO/IEC JTC 1/SC 42. https://www.iso.org/committee/6794475.html

ISO (2021). Digital Twin framework for manufacturing. ISO 23247. https://www.iso.org/obp/ui/#iso:std:iso:23247:-1:ed-1:v1:en

Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020). Characterising the Digital Twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, *29*, 36-52.

Kritzinger, W., Karner, M., Traar, G., Henjes, J., & Sihn, W. (2018). Digital Twin in manufacturing: A categorical literature review and classification. *IFAC-PapersOnLine*, *51*(11), 1016-1022.

Lee, E. B. K., Van Bossuyt, D. L., & Bickford, J. F. (2021). Digital Twin-Enabled Decision Support in Mission Engineering and Route Planning. *Systems*, *9*(4), 82.

Li, L., Aslam, S., Wileman, A., & Perinpanayagam, S. (2021). Digital Twin in Aerospace Industry: A Gentle Introduction. *IEEE Access*.

Maathuis, C., Pieters, W., & Van Den Berg, J. (2018a). A computational ontology for cyber operations. In *European Conference on Cyber Warfare and Security 2018*, pp. 278-288.

Maathuis, C., Pieters, W., & Van den Berg, J. (2018b). Assessment methodology for collateral damage and military (Dis) Advantage in cyber operations. In *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)* (pp. 1-6). IEEE.

Maathuis, C., Pieters, W. & Van Den Berg, J. (2021). Decision support model for effects estimation and proportionality assessment for targeting in cyber operations. *Defence Technology*, Vol. *17*, No. 2, pp. 352-374.

Maathuis, C. (2022a). On Explainable AI Solutions for Targeting in Cyber Military Operations. In *International Conference on Cyber Warfare and Security*. 17(1), 166-175.

Maathuis, C. (2022b). On the Road to Designing Responsible AI Systems in Military Cyber Operations. In *European Conference on Cyber Warfare and Security*. 21 (1), 170-177).

Maathuis, C., & Chockalingam, S. (2022c). Responsible Digital Security Behaviour: Definition and Assessment Model. In *European Conference on Cyber Warfare and Security*. 21(1).

Mendi, A. F., Erol, T., & Dogan, D. (2021). Digital twin in the military field. *IEEE Internet Computing*.

Moyne, J., Qamsane, Y., Balta, E. C., Kovalenko, I., Faris, J., Barton, K., & Tilbury, D. M. (2020). A requirements driven digital twin framework: Specification and opportunities. *IEEE Access*, *8*, 107781-107801.

NATO (2016a). NATO Warsaw Summit 2016. https://www.nato.int/cps/en/natohq/events_132023.htm

NATO (2016b). *NATO Standard AJP-3.9 Allied Joint Doctrine for Joint Targeting*. NATO Standardization Office.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45-77.

Peffers, K., Tuunanen, T., & Niehaves, B. (2018). Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research.

Puriwat, W., & Tripopsakul, S. (2021). The impact of digital social responsibility on preference and purchase intentions: The implication for open innovation. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(1), 24.

Qian, C., Liu, X., Ripley, C., Qian, M., Liang, F., & Yu, W. (2022). Digital Twin—Cyber Replica of Physical Things: Architecture, Applications and Future Research Directions. *Future Internet*, *14*(2), 64.

Silvera, J. I., Luquero J. M., Cajade, A. & Bustelo, M. (2020). Navantia's digital twin implementation perspective in military naval platform life cycle. NATO STO-MP-MSG-171.

Singh, M., Fuenmayor, E., Hinchy, E. P., Qiao, Y., Murray, N., & Devine, D. (2021). Digital twin: origin to future. *Applied System Innovation*, *4*(2), 36.

Smeets, M. (2018). The strategic promise of offensive cyber operations. *Strategic Studies Quarterly*, *12*(3), 90-113.

Solce, N. (2008). The battlefield of cyberspace: The inevitable new military branch-the cyber force. *Alb. LJ Sci. & Tech.*, *18*, 293.

Song, M., Shi, Q., You, Z., Hu, Q., & Chen, L. (2022). On the Architecture and Key Technology for Digital Twin Oriented to Equipment Battle Damage Test Assessment. *Available at SSRN 4062470*.

Steinmetz, C., Rettberg, A., Ribeiro, F. G. C., Schroeder, G., & Pereira, C. E. (2018). Internet of things ontology for digital twin in cyber physical systems. In *2018 VIII Brazilian symposium on computing systems engineering (SBESC).* 154-159). IEEE.

Talkhestani, B. A., Jung, T., Lindemann, B., Sahlab, N., Jazdi, N., Schloegl, W., & Weyrich, M. (2019). An architecture of an intelligent digital twin in a cyber-physical production system. *at-Automatisierungstechnik*, *67*(9), 762-782.

Van Den Brand, M., Cleophas, L., Gunasekaran, R., Haverkort, B., Negrin, D. A. M., & Muctadir, H. M. (2021). Models Meet Data: Challenges to Create Virtual Entities for Digital Twins. In *2021 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)* (pp. 225-228). IEEE.

VanDerHorn, E., & Mahadevan, S. (2021). Digital Twin: Generalization, characterization and implementation. *Decision Support Systems*, *145*, 113524.

Venable, J. R., Pries-Heje, J., & Baskerville, R. L. (2017). Choosing a design science research methodology.

Vielberth, M., Glas, M., Dietz, M., Karagiannis, S., Magkos, E., & Pernul, G. (2021). A digital twin-based cyber range for SOC analysts. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 293-311). Springer.