Cybersecurity of Cyber Ranges: Threats and Mitigations

Sami Noponen, Juha Parssinen, Jarno Salonen
VTT Technical Research Centre of Finland Ltd, Finland

Abstract

Cyber ranges are often used to enhance the cybersecurity posture of a company by training relevant skills. These environments are traditionally used to host exercises that simulate cybersecurity scenarios, improve the cybersecurity skills of employees and enhance the security of networks and processes. By using digital twins, it is possible to organise more targeted cyber range trainings to companies operating in the critical infrastructure sector. Especially in this sector it is important to consider the cybersecurity of these environments themselves as they often may handle company-specific confidential information. This study presents several cybersecurity related threats and challenges that cyber ranges may face during different phases of use. Cyber threats may be exposed to the actual systems that the ranges are meant to protect if these issues are not taken into consideration and mitigated. Malicious attackers may use the information in the cyber ranges to learn the weaknesses in the actual system. We approach the subject by reviewing the relevant literature, which is currently very limited especially when looking at the cybersecurity issues of cyber ranges. We divide the subject into the different phases of cyber range development and use, and also discuss relevant cloud security issues. Finally, we present actions to mitigate the identified cybersecurity threats and issues in cyber ranges when using them for training and awareness activities.

Keywords: Cyber range, Cybersecurity, Cyber training, Testbed, Digital Twin, Cloud security

1. Introduction

Cybersecurity incidents worldwide have increased both in numbers and complexity in recent years. Attackers have be_come more organized and use more sophisticated tools and attacks than before. At the same time, there is an ongoing chronic shortage of cybersecurity skills and professionals. According to a study by Deloitte [1] the reason for this is the rise of new technologies and evolving threats at a rate which is faster than what current cybersecurity professionals can handle. According to Check Point, corporate networks experienced over 50% more attacks weekly in 2021 when compared to the previous year [2]. Another study revealed that more than half of the workforce works remotely 2 days a week or more, which has increased the need for remote access to corporate networks and assets [3]. This not only emphasises strict security policy implementation in companies, but also puts pressure on the threat detection, mitigation and counterattack measures that should be trained proactively in order to help the cybersecurity professionals act in the right way during an actual cyber attack.

One of the most effective ways of tackling the threat is training current IT professionals to improve their cyberse_curity skills. The use of various cybersecurity IT training environments has become a commonplace in recent years. More recently this trend has been expanding into the industrial sector as well due to the developments in Digital Twin (DT) technology and Industrial Internet. Digital twins are digital representations of physical systems or devices that can be connected to a training environment. According to Grieves [4], the term was introduced in 2003 and defined DT as the concept of a virtual, digital equivalent to a physical product and virtual products were defined as representations that are virtually indistinguishable from their physical counterparts. Tao et al. [5] have studied the state-of-the-art on DT in industry and Boschert et al. [6] the next generation DT. Use cases for digital twins can be found from e.g. healthcare, disaster management and smart cities; basically in any industry where data can be collected from digitally connected sensors. This is the case in the Industrial Internet of Things (IIoT) and Industry 4.0. Some of the digital twins and environments are specifically designed for critical infrastructure. Studies [7] and [8] note that there are cybersecurity threats related to digital twin deployments. In the context of critical infrastructure, this technology is very important, because cybersecurity training with the actual systems is basically impossible due to their restricted availability and also since it is very likely to cause physical damage to the equipment. Replaying cyber attacks in a system belonging to a critical infrastructure may render the expensive equipment unusable, cause environmental damage and even threaten human lives.

Digital twins serve many purposes, but our research focuses on training environments, cyber ranges (CR), that digital twins may be only part of. According to Becue et al. [9], DTs serve as strongest ally of CRs to support cybersecurity testing and training, also supporting cyber risk anticipating and impact prediction. The purpose of CRs is to raise awareness about cyber security, train people to

 | DOI: 10.20533/ijisr.2042.4639.2022.0117

handle various cybersecurity related situations and enhance the overall cybersecurity capa_bility of a company. These environments are most often called cyber ranges, but other common terms for similar technology such as testbeds or digital training platforms have been used too. These terms have some variation in definitions and are therefore explained as follows. Davis and Magrath conducted a survey of cyber ranges and testbeds in 2013 [10] focusing on various testbeds with labels such as attack lab, computer network operations (CNO) testbed, or testbed for network warfare of cyber war, as well as CRs and define that they are often built to support CNOs. Yamin et al. [11] have studied cyber ranges and security testbeds, the latter of which are mainly referred to as testbeds for Internet security research. Digital training platforms have been studied by e.g. Jianqi [12] with the focus on training digitization and networking and Chechina et al. [13] who use it for traffic flow simulation. The aims and purposes of these environments vary, but this study focuses on platforms and services that are focused on cybersecurity training and therefore the primary focus is on CRs since according to the existing literature testbeds and digital training platforms are used for more focused topics that may support network or information security, but not cybersecurity as a whole. Despite years of progress, CRs are still a new and emerging technology. According to ECSO [14] CRs today are ”already very mature to be able to deliver several use cases, yet immature to deliver some of the market expectations and the ultimate promises that cyber ranges aim to fulfil”.

The use of CRs for training can enhance the cybersecurity posture of a company, but the environment itself can pose serious threats. This article is extended from our article WAITING FOR PROCEEDINGS [15], in which we presented the most severe cybersecurity threats related the deployment and use of CRs. The study was done by reviewing relevant literature about the subject, which we found out to be limited in amount. This journal article extends the topic by covering the threat landscape more comprehensively and covering more threats and mitigations. This aspect of threats against CRs is not yet much discussed in the scientific literature, but by combining several sources that describe various issues in CR development, we can form a general view of the most serious threats. Deploying a CR is a huge effort, and it involves various information exchanges between people and devices. For providing the best results, the training scenarios and technology involved should match the context. Because of this, the scenarios deployed in CRs may contain confidential information such as network architecture, process data, access credentials and software. CRs are often located in a cloud, and therefore any cloud security issues are very relevant. If a digital twin or a CR is compromised by hackers, they most likely have the necessary information and potential to attack the real-world counterpart of the system. Also, in the current threat landscape cyber excercises may be disturbed by denial of service attacks as part of hybrid operations. The remainder of the article is structured as follows. In chapter two we present the methods used for literature review and provide background information about CRs and their use cases. In chapter three, results, we present the identified threats and risks related to the use of CRs. Also, mitigation methods are presented. Chapter four concludes our work, summarizing the main findings from the study.

2. Materials and Methods

The approach in this study is on identifying different cybersecurity challenges and threats that arise when setting up and operating cyber ranges and finding relevant mitigations on the threats. In our article WAITING FOR PROCEEDINGS [15] we reviewed the current scientific literature on the topic. This journal article also covers the mitigation aspect better by mapping the mitigations with threats in section III. As the cybersecurity approach of the CRs themselves is novel in the scientific sense, also white papers and other reports are included in the study. The source articles cover several issues on cyber ranges and other similar environments, but none of them has the cybersecurity aspect of the platform as their main focus.

The main search term for our study was cyber range (CR), but since the virtual training environments include also other terms, we expanded our search to include digital twins, digital training environments, testbeds and simulation environments. The keywords were selected to fulfil the purpose of the review. Currently there are a lot of recent publications about cyber ranges and digital twins. We found a total of 2734 hits with either of these terms in the title from the three recent years. More specific search terms were used in the literature review for training environments such as “cyber range”, “digital twin”+“cyber training”, “security”+”testbed”, and “virtual training environment”. These were combined with ”cyber security”, ”cyber threats” and ”risks”. VTT’s proprietary tool ”eKnowledge search” was the most important source when conducting the searches. It consists of a huge up-to-date index of e-books, magazines, scientific articles and journals. In ad_dition to eKnowledge search, also Google and Google Scholar were used. Only a few relevant studies covering the main aspect of this work were found and all of those are included in this article. We noted a challenge when searching specifically the cyber threats in training environments themselves. The searches yielded hundreds of results because of

 | DOI: 10.20533/ijisr.2042.4639.2022.0117

fairly common search terms, but the results were mostly irrelevant to our subject and focusing on other topics. For example, when using search terms like “cyber range”+“cyber threats”, the results cover issues that CRs are built to train people, not issues in the CR environments themselves. The resulting number of relevant publications was very limited, and therefore we expanded the search to cover 10 previous years, and also included articles that were not peer-reviewed, such as white papers. Finally, as a result, we found 7 sources that considered that the Cyber Range or Digital Twin can cause cybersecurity challenges. These 7 sources are arranged from [24] to [28] in References.

2.1. Different definitions of CRs

The term “cyber range” originates from defence research, and they have been defined by DARPA [16] in 2008 as inter_active simulated platforms for representing networks, systems, tools, and/or applications in a safe, legal environment that can be used for developing cyber skills or testing products and/or services. The DARPA National cyber range Project (NCP) started in the beginning of the last decade with the objective of building a “scale model” of the internet to carry out cyber war games. Cyber ranges can be used for facilitation and training activities but also for fostering certification and general education and awareness.

NIST [17] defines cyber ranges as virtual environments that use actual network equipment, as required. According to NIST they can range from single stand-alone ranges in a single schoolhouse or an organization to internet replicating ranges that are accessible from all over the world. Karjalainen et al. [18] introduce the concept of cyber arenas. They describe the need for next generation cyber ranges that are capable of providing a more complex infrastructure for cybersecurity trainings and exercises that is needed because of the accelerating digital transformation. Murray [19] elaborates the concept of cyber arenas even further by introducing the Open Cyber Arena Virtual Lab project for delivering high quality, experiential cybersecurity learning in the form of virtual labs and virtual lab classrooms.

Cyber ranges can be also seen as digital twins (DT) but the two terms have different definitions. Digital twins refer to a digital representation of a single device or a small system and they offer a smaller subset of functionalities than cyber ranges and focusing mainly on the functional elements of the original device or system. Cyber ranges on the other hand can be used to clone a large environment consisting e.g. of multiple production lines and house digital twins of specific IT/OT systems. More on the history and definition of Digital Twins can be read from [20].

Grieves and Vickers [21] define digital twins as 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. They also specify that when the digital twin is at its optimum, any information that could be obtained from inspecting a physical manufactured product can be obtained from its twin. In the recent study by Yamin et al. [22] a complementary literature review of different CRs, use cases and features is presented. They state that the interest for CR training has grown during the recent years, and most of the uses cases of CRs is centered around the needs for red and blue team training.

2.2. Basic functions of cyber range

This subchapter lists the functionalities and capabilities of a CR in brief. A broader view on the different features and different use cases of CR environments can be found from studies [14] and [23]. CRs consist of multiple technologies that are used to construct an environment that has specific functionalities for the trainees. A CR can be a general training platform for various cyber aspects, or it can be a complete digital twin of a specific network environment. The size of a range varies; often the training platform is organized for small group of participants, but big competitions can host thousands of participants. When training consists of cybersecurity aspects, it is usually built or configured around a specific scenario and targeted set of trainees. Targeted trainees are usually screened, and the level of technical knowledge has to be estimated in order to customize the training for them. Exercises in the CR involve a realistic and repeatable simulation that allows trainees to identify any weaknesses in the target system and points of improvement. One of the benefits is that the exercises can run scenarios that are too dangerous to organize in the actual environment. The basic building blocks of the CR are hardware and software components used to build up to the scenarios developed for a specific training. Often, when the CR platform itself is ready, the work required to create a new cyber exercise in a CR is focused on the specific new scenario and the related machines that need to be configured for it.

2.3. Different use cases for cyber ranges

Operators of CRs are often companies that offer these environments as a service or a product to other companies. CRs can be developed and operated in-house for supporting the company R&D and security awareness. Also, universities and other research institutes operate CRs to train students and other target groups. When an organization decides to use

 | DOI: 10.20533/ijisr.2042.4639.2022.0117

CRs for training purposes there are two options; the training platform can be built in-house or bought as a commercial product or service. When building a CR in-house, it can be implemented into a cloud environment, or deployed on a specific physical gear. A survey by Suni et al. [23] lists different use cases and target environments for CRs. As seen in the survey, the target environments are spread to multiple sectors. When conducting a widespread cybersecurity training or exercise, multiple cyber ranges can be interconnected. Federation of CRs brings multiple environments together for expanding the capabilities of the training. The users of a CR can be categorized as following:

- Cyber range provider / operator : In-house made cyber range, Internal use or external service.
- Cyber range attendee: using commercial range provided by third party.

On Premises cyber range is physical environment deployed at an organisation. This option is usually the most expensive one and better suited for exercises having strict security and privacy requirements. More flexible and cheaper option is to host the environment in a public or private cloud. Drawbacks of public cloud deployments are that they have technology constraints. According to [14] there are limitations on control of data flows and attack types, such as Denial of Service.

Private clouds are maintained by a private organisation, and therefore have total control of the infrastructure. The CR deployment can also combine both public and private cloud technologies to hybrid cloud, which offer the best of both worlds, such as stronger controls and natural scalability.

3. Results

This chapter lists the identified threats and lists actions on how to mitigate them. The threats of a cyber range training vary on exercise type, goal of exercise and also on the type of the platform. The risks arise on different phases such as, building the CR, developing and implementing the scenarios and exercise/training phase. If mistakes are made during the implementation phase of a CR, more risks are to follow in the exercise phase. The highest number of threats are faced if an organization builds and operates the CR in-house, handles confidential data in the exercises and provides internet access to the environment. If employees only participate to external CR training with no company-specific content, the number and level of potential threats is significantly lower. The following subchapters list and discuss the identified challenges and risks in different phases following by cloud related threats. Finally, mitigations for several of these issues are presented.

3.1. CR Deployment

Several challenges are faced when deploying a CR. The challenges during this phase rise from many aspects and will affect the overall cybersecurity and usefulness of the training platform. Design challenges are not the same as cybersecurity challenges, but the implications can affect the cybersecurity of the platform. In [28] a design life cycle for testbeds is presented. One of the biggest challenges mentioned in the literature [25], [8] is converting the actual system into a virtualized environment in an accurate way. This is caused by the size and complexity of the target system architecture. Documentation that describes the target system is often inadequate and spread to several divisions within the organization. Building a virtual representation of a specific system or subsystem often requires a huge effort. In this process, we often realize that every component cannot be accurately represented, and compromises have to be made in order to make the CR operational. If this phase is not done correctly, the training and setup will not match the real system. In this case the applicability of the lessons learnt from the CR training session will be reduced. Another potential drawback is creating unrealistic training scenarios that do not match situations or systems in real life. Knowing the audience and their skills is essential when planning the trainings.

One of the cyber risks related to deployment phase is the reuse of user credential (login/password) information from the real system [8]. This mistake is easily done when converting the original system into the virtualized format. If people outside the organization have access to the CR environment that has actual access control information, this becomes a major cybersecurity threat. Even in the case that the participant list doesn't include any non-organisation members, original access credentials should never be used. Interoperability is another big concern when creating a virtual environment as mentioned by [27]. Also, authors of [28] note that the maintenance of the platform may become an issue because of the system complexity and the constant discovery of new vulnerabilities from the software components used in the system.

3.2. Physical Threats

Physical security threats concern local, on-premises CR deployments that are created with actual hardware such as servers, laptops, switches, cables etc. Devices containing sensitive data can be stolen or the environment can be physically damaged. Participants may connect their personal

 | DOI: 10.20533/ijisr.2042.4639.2022.0117

devices in the CR and cause harm unintentionally or on purpose. Also, people who are not participating the training may see or hear contents of the training if the area is not isolated and guarded.

3.3. Communication Threats

Data communication threats are mostly present when the users are connected to the CR remotely. Attacker may cause various issues if he or she is able to gain access to the traffic or intercept it. Fortunately most of the protocols used for remote access use encryption for concealing the contents, especially login credentials. More on communication related threats are listed on the subsection Cloud Risks. Local CR setups may include communication related threats as well, if the participants are using their own computers and are able access to other participants traffic or personal data.

3.4. Virtual Machines and Containers

Almost every CR use virtualization and container techniques since those are easy to control and reinitialize. One of the greatest threats related to virtual machines is virtual machine escape. It is an exploiting technique in which an attacker runs code on VM to break out and interact directly with the hypervisor. This could give the attacker access to the host and all other VMs running on it. Container technology introduces another attack surface through container tools, orchestration, and added complexity. MITRE [31] has introduced a ATT&CK Matrix for container systems. Most serious threats on using containers are related to their privileges. Privileges can be misconfigured or exploited in a way that they provide access to the system running the containers.

3.5. Training

As mentioned in [8] a significant security concern within a digital twin being such a close representation of an actual system is that if the twin is obtained by a hacker, it can then serve as a blueprint to the real system, identifying components, their interfaces and behaviour. This immediately gives any hackers an internal view of the potential target system which helps them identify any vulnerable attack points. In this scenario, one can assume that prior to the physical system attack, the hackers would have an entire script mapped out using the compromised digital twin, allowing penetration of the actual system with minimum detection or disruption. Digital twins can also be used for attack testing the interfaces of a physical system, thereby allowing the attacker to fine-tune their attack mechanisms.

During cyber training, the trainees might enter various information such as access credentials into the CR. When offering a CR to train various groups of people, it is important to clean the range from user-related data between each session [25]. When organizing the exercises, it should be taken into account that the participants do not act the same way as in a real situation as noticed by [26]. This may lead to false conclusions when examining the results after the training is over.

3.6. Cloud Threats

The CR training environments running on a cloud have similar kinds of risks as any other cloud applications. The MITRE ATT&CK® Matrix [30] for Enterprise has a specific section for cloud-based adversary tactics and techniques based on real-world observations. Techniques from its sections ”Initial Access”, ”Credential Access” and ”Discovery” are introduced briefly in the following text. The Valid Account and Default Account techniques explain how adversaries may obtain and abuse the credentials of default or existing accounts as means of gaining foothold to the cloud services. Default accounts include ones that are built into the underlying operating system or default provider set accounts on any software or cloud services used to build the CR training environment. Phishing and its sub-techniques explain how adversaries can obtain existing, compromised credentials using social engineering, including targeted phishing messages. This is also known as spear phishing.

The Brute Force and its several sub-techniques explain how adversaries may use password guessing and password cracking to gain access to accounts when passwords are unknown or in cases when password hashes are obtained. One of the sub_techniques, namely Credential Stuffing, shows how adversaries may obtain credentials from breach dumps of unrelated accounts to gain access to target accounts through credential overlap. In these cases adversaries are taking advantage of the tendency for users to use the same passwords across personal and business accounts.

Adversaries may also take advantage of a weakness in Internet-facing systems and services used to build the CR training environment as explained in the Exploit Public-Facing Application technique. The weakness in the system can be a bug, a glitch, or a design vulnerability. Important sources for the security risks of cloud based applications implemented using web technologies are the OWASP top 10 [32] and CWE top 25 [33] which highlight the most common web-based vulnerabilities.

The Escape to Host technique explains how adversaries may break out of a container which is used in the CR based training environment to gain access to the underlying host. This can allow an

 | DOI: 10.20533/ijisr.2042.4639.2022.0117

adversary access to other containerized resources from the host level or to the host itself.

The Forge Web Credentials, Steal Application Access Token and Steal Web Session Cookie techniques explain how adversaries may forge or steal credential materials that can be used to gain access to web applications or Internet services used to build the CR training environment. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies, application access tokens, or other similar techniques to authenticate and authorize user access. These can be stolen through social engineering and typically require the users some kind of action to grant access, or adversaries can find them from e.g., configuration files of services, source code or binary files which they have access to as explained in the Unsecured Credentials technique and its sub-techniques.

Adversaries may use different kind of discovery techniques. These techniques help adversaries analyse the environment in concern and make detailed planning on how to attack. The Account Discovery and its sub-techniques explain how adversaries may collect accounts used by users, remote support, services, or for administration of resources within the cloud service provider.

The Software Discovery technique and its sub-technique Security Software Discovery explain how adversaries may dis_cover and enumerate software, services and resources that are available within a targeted cloud service, or use a cloud service dashboard GUI with stolen credentials to gain useful information. Important pieces of information for adversaries are also what kind of security software, configurations, defensive tools, and sensors are installed in the CR training environment. This may include things such as firewall rules and antivirus software. Adversaries may also collect detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.

3.7. Mitigating

In this subsection we discuss how to mitigate the identified risks and threats from different aspects of CR deployments. As CR solutions are unique, exact mitigation actions for specific solutions cannot be presented. We have identified and selected the mitigations that are relevant for threats. Some of the presented mitigations were selected from the results of literature review. The first step for mitigation is preventive; identify the needs of each CR environment and the organized training session. What level of information does it have to contain for a meaningful exercise? What kind of capabilities are required? For example, is Internet connection from the CR required? Only the necessary functions should remain in the environment.

Term ‘cyber exercise hygiene’ presented by [35] refers to a practise for ensuring that the contents of the exercise do not leak outside. This prevents the risk that the messaging used in exercises won’t be misinterpreted as real messages. It is possible that outsiders may hear discussions about the exercise contents or may be able to read data from screens if the environment is not protected or isolated. In Tiber-EU-framework [36] sensitive systems are not called by their real name. Instead, code names during the exercises are given to protect the real identity. This prevents the leaking of sensitive data, if the environment is somehow compromised. Automation or CR functions are often used to decrease the need or resources and shorten the time needed for setting up exercises. Authors of [29] present a review of CRs that use automation at different phases of CR use. Automation can mitigate human errors that are common when setting up environments manually, especially during network and system configuration.

The study [8] presents different applications of software protection technologies in the context of digital twins. This technology hardens the software and makes it exceedingly difficult for a hacker to use it as a blueprint, as well as making the twin software more difficult to modify without being caught. Also, there are techniques that can lock both the software and data to specific devices (computers) by using various types of data and copy protection technologies (such as Whitebox Cryptography) and hardened APIs. The ultimate goal is to render the software inoperable and/or to ensure that the data is inaccessible if the software and/or data is copied to another machine, thereby preventing propagation of the twin implementations between devices.

The MITRE ATT&CK® Matrix [30] for Enterprise also contains mitigations for adversary techniques. Most of them are well-know and strongly recommended like Update Software and Network Segmentation. For mitigating Valid Accounts and its sub-techniques, there are several proposed mitigation techniques. Application Developer Guidance mitigation ensures that applications do not store sensitive data or credentials insecurely, Password Policies demand that the default user_name and password should be changed immediately after the installation, and Privileged Account Management proposes to follow best practices for the design and administration of an enterprise network to limit privileged account use across administrative tiers.

There are several mitigations for phishing techniques including Antivirus/Anti-malware, Network Intrusion Prevention, Restrict Web-Based Content and User Training to identify social engineering techniques and phishing emails. To mitigate Brute Force and its sub-techniques there are Account Use Policies which set account lockout

 | DOI: 10.20533/ijisr.2042.4639.2022.0117

policies after a certain number of failed login attempts to prevent passwords from being guessed. Also, Multi-factor Authentication and User Account Management to reset accounts that are known to be part of breached credentials can be used. There are also techniques like Cloud Service Discovery which cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

For mitigating the risks that occur during the training phase, the trainees should be informed what they are allowed to do in the exercise and what is prohibited: e.g. connecting personal devices to the range. Trainees are also responsible for the cybersecurity of an exercise, during it and after. In some cases, a non-disclosure agreement might be required. The Table 1 below summarizes the results of most important mitigations to identified threats.

Table 1. Threats and Mitigations

Threat	Mitigations
Deployment phase errors	Automation
Physical threats	Physical protection, Excercise hygiene
Leaking of Sensitive data	Encryption, Segmentation
Communication Threats	Encryption, Authentication
Cloud Threats	See MITRE [30]
IPR Theft	Copy protection technologies
Virtual Machine Threats	Strict patch policy
Container Threats	Careful configuration, Patching
Phishing	Training, Anti-Virus, IDS

4. Conclusions

Deploying a cyber range requires a considerable effort to have it operational. In this process, cybersecurity issues might be easily forgotten, even when the purpose of the training environment is to enhance the organizational cybersecurity level. People planning the use of cyber ranges will face resource constraints when building the system and planning and deploying scenarios. This means that compromises have to be made and there is also the threat that cybersecurity issues are not the top priority. Also, if the training is bought as a service, it is not easy to compare the providers and select the best one. Currently there is a huge number of companies offering cyber ranges both as a product and as a service. It might be difficult to identify the most suitable provider that takes the issues related to cybersecurity into account. We have identified that the most threatening cybersecurity issues are related to the online virtual training environments. The potential risks and threats may arise from several phases of cyber range use. Cyber ranges located in the cloud are especially vulnerable to various attacks and various defensive mechanisms have to be used for ensuring a secure operation. We presented a selection of relevant mitigation measures for the identified threats. Also, the role of trainees themselves for maintaining the cybersecurity during the exercise is significant. Even when adequate security protections are in place, it should be considered very carefully, whether it is reasonable to handle confidential information in the CR environment. Common term cybersecurity hygiene and practices related to it should be applied to cover the exercises as well.

One conclusion of our review is that there are no scientific studies focusing specifically to this subject. So far only small consideration is made to the cybersecurity of training environments. This presented a limiting factor to our research since there is only a small number of relevant studies discussing about this topic. There are a lot of studies related to CRs, but none of them focus on what kind of cybersecurity threats the environment itself can present. By successfully attacking into a CR or gaining access to a digital twin, the attackers might find information that they need to gain access to the actual real-world target. The benefits of cybersecurity training with cyber ranges can be significant, but the threats related to this have not been discussed properly. Especially in the case of critical infrastructure applications, the threats of exposing the weaknesses of real systems to malicious third parties, might lead into serious consequences if realized. By attacking successfully into a cyber range or gaining access to a digital twin, adversaries can collect all the information necessary to compile an effective cyber attack against the actual target in the real world. Potential field of future research is to study discovered vulnerabilities and attacks aimed to cyber ranges and digital twins. We expect this kind of findings to appear and attacks to happen during the next few years.

5. References

[1] Deloitte. (2018).The changing faces of cybersecurity Closing the cyber risk gap. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aodaen.PDF. (Access Date: May 4 2021).

[2] Check Point Software Technologies, Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed. https://pages.checkpoint.com/cyber-securityreport-2022. (Access Date: Febuary 25 2022).

[3] Check Point Software Technologies, The 2022 Workforce Security Report. https://pages.checkpoint.com/remoteworkforce-report.html. (Access Date: 25 February 2022).

[4] Grieves, M. (2014). "Digital twin: manufacturing excellence through virtual factory replication." White paper 1: 1-7. https://www.3ds.com/fileadmin/PRODUCTS-SERVICES/DELMIA/PDF/Whitepaper/DELMIA-APRISO-Digital-Twin-Whitepaper.pdf. (Access Date: 25 February 2022).

 | DOI: 10.20533/ijisr.2042.4639.2022.0117

[5] Tao, F., Zhang, H., Liu, A., Nee, A. Y. (2018). Digital twin in industry: State-of-the-art. IEEE Transactions on Industrial Informatics, 15(4), 2405-2415. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8477101. (Acc-ess Date: 25 February 2022).

[6] Boschert, S., Heinrich, C., Rosen, R. (2018). Next generation digital twin. In Proc. tmce (Vol. 2018, pp. 7-11). Las Palmas de Gran Canaria, Spain. https://www.researchgate.net/profile/StefanBoschert/publication/325119950 Next Generation Digital Twin/links/5af952ca0f7e9b026bf6e553/Next-Generation-Digital-Twin.pdf (Access Date: 25 February 2022).

[7] Kummerow, A., Rusch, D., Nicolai, S., Brosinsky, C., Westermann, D., and Naumann, A. (2021). Attacking dynamic power system control centers - a cyber-physical threat analysis. 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2021, pp. 01-05, DOI: 10.1109/ISGT49243.2021.9372285.

[8] Hearn, M., Rix, S. (2019). Cybersecurity Considerations for Digital Twin Implementations. Industrial Internet Consortium. IIC Journal of Innovation. Industrial Internet Consortium.

[9] Becue et al., (2018). "CyberFactory#1 — Securing the industry 4.0 with ´cyber-ranges and digital twins," 14th IEEE International Workshop on Factory Communication Systems (WFCS), 2018, pp. 1-4. DOI: 10.1109/WFCS.2018.8402377.

[10] Davis, J., Magrath, S. (2013). A survey of cyber ranges and testbeds. Department of Defence, Australian Government. https://apps.dtic.mil/sti/pdfs/ADA594524.pdf (Access Date: 15 February 2022).

[11] Yamin, M. M., Katt, B., Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88, 101636. DOI: 10.1016/j.cose.2019.101636.

[12] Jianqi, Z. (2021). "Design and Application of Modern Cognitive Appren_ticeship Training Platform in The Context of Information Technol_ogy," 2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), pp. 22-25, DOI:10.1109/ICMTMA52658.2021.00014.

[13] Chechina, A., Churbanova, N., Garibyan, A., Trapeznikova, M. (2021). Digital Training Platform for Comprehensive Traffic Simulation. International Journal of Online & Biomedical Engineering, 17(13).

[14] European Cyber Security Organization ECSO. SG5 PAPER Understanding cyber ranges: From Hype to Reality. SWG 5.1 I cyber range Environments and Technical Exercises. https://www.ecs-org.eu/documents/uploads/understanding-cyber-rangesfrom-hype-to-reality.pdf (Access Date: 25 May 2021).

[15] Noponen, S., Parssinen, J., Salonen, J. (2021). Review on Cybersecurity Threats ¨Related to Cyber Ranges. International Conference for Internet Technology and Secured Transactions (ICITST-2021).

[16] DARPA Broad Agency Announcement. (2008). National cyber range. DARPA BAA-08-43. https://www.wired.com/imagesblogs/threatlevel/files/darpaarfpcyberrange.pdf (Access Date: 20 May 2021).

[17] NIST. (2020). The cyber range (Draft): A Guide. Guidance Document for the Use Cases, Features, and Types of cyber ranges in Cybersecurity Education, Certification and Training Prepared by the National Initiative for Cybersecurity Education (NICE) cyber range Project Team. https://www.nist.gov/document/cyber-range-guide (Access Date: 27 May 2021).

[18] Karjalainen, M. and Kokkonen, T. (2020). "Comprehensive Cyber Arena; The Next Generation cyber range", IEEE European Sym_posium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, pp. 11–16. DOI: 10.1109/EuroSPW51379.2020.00011. (Access Date: May 28 2021).

[19] Murray, D. (2019). Open Cyber Arena Virtual Lab. https://online.suny.edu/iitg/view/project-view/entry/729/ (Access Date: 28 May 2021).

[20] Eckhart, M., Ekelhart, A. (2019). Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook. DOI: 10.1007/978-3-030-25312-714.

[21] Grieves, M., Vickers, J. (2016). Origins of the Digital Twin Concept. DOI: 10.13140/RG.2.2.26367.61609.

[22] Yamin, M.;Katt, B; Gkioulos, V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security. Volume 88. 2020. ISSN 0167-4048. DOI: 10.1016/j.cose.2019.101636. (Access Date: 5 August 2021).

[23] Suni, E., Piispanen,J., Nevala, J., Paij ¨ anen, Jani., Saharinen, K. (2020). Cyber Security for Europe D7.1 Report on existing cyber ranges. https://cybersec4europe.eu/wpcontent/uploads/2020/09/D7.1-Report-on-existing-cyber-rangesand-requirement-specification-for-federated-cyber-ranges v1.0 submitted.pdf (Access Date: 15 May 2021).

[24] Nagarajana.S., Ananda, S., Sakthivelb. U. (2020). Impact of Cloud Security in Digital Twin. Advances in Computers, Volume 117 # 2020 Elsevier Inc.ISSN 0065-2458 All rights reserved. DOI: 10.1016/bs.adcom.2019.09.005.

[25] Winter, H.; System Security Assessment Using a cyber range. 7th IET International Conference on System Safety, incorporating the Cyber Security Conference. 2012.

[26] Deckard, G. Cybertropolis: Breaking the Paradigm of cyber-ranges and Testbeds. 2018 IEEE International Symposium on Technologies for Homeland Security (HST). Woburn, MA, USA. https://ieeexplore.ieee.org/document/8574134 (Access Date: 14 May 2021).

[27] Singh, S., Shehab, E., Higgins, N., Fowler, K., Tomiyama, T., Fowler, C. (2018). Challenges of Digital Twin in High Value Manufacturing. SAE International - Aerospace Systems and Technology Conference, London.

 | DOI: 10.20533/ijisr.2042.4639.2022.0117

https://www.researchgate.net/publication/328912587 (Acc-ess Date: 17 May 2021).

[28] Frank, M., Leitner, M., Pahi, T. (2017). Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education. Co-located Conference: IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congres(DASC/PiCom/DataCom/Cyber SciTech). pp. 38–46.

[29] Gustafsson, T., Almroth, J. (2021). Cyber Range Automation Overview with a Case Study of CRATE. DOI 10.1007/978-3-030-70852-8 12.

[30] Mitre Corporation. Matrix on Cloud. https://attack.mitre.org/matrices/enterprise/cloud/ (Access Date: 19 May 2021).

[31] Mitre Corporation. Matrix on Containers. https://attack.mitre.org/matrices/enterprise/containers/ (Ac-cess Date: 10 April 2022).

[32] The Open Web Application Security Project® (OWASP) foundation. Top 10 Web Application Security Risks. https://owasp.org/www-project-top-ten/ (Access Dat-e: 28.05.2021).

[33] Mitre Corporation. CWE Top 25 Most Dangerous Software Weaknesses. https://cwe.mitre.org/top25/archive/2020/2020 cwe top25.html (Access Date: 28 May 2021).

[34] Secure Collaborative Intelligent Industrial Assets SECOIIA. (2020). A European H2020 Poject. https://secoiia.eu (Access Date: 28 May 2021).

[35] Kyberturvallisuuskeskus. Instructions for organising cyber exercises. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions%20for%20organising%20cyber%20exercises.pdf (Access Date: 4 April 2022).

[36] European Central Bank TIBER-EU Framework. (2018). How to implement the European framework for Threat Intelligence based Ethical Red Teaming. https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereuframework.en.pdf (Access Date: 14 May 2022).

Acknowledgment

This article is based on research conducted in the Secure Collaborative Intelligent Industrial Assets (SeCoIIA) project that aims at securing the digital transition of manufacturing industry towards more connected, collaborative, flexible and automated production techniques. The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871967.