Unveiling the user requirements of a cyber range for 5G security testing and training

Anna Angelogianni[1], Ilias Politis[1], Pier Luigi Polvanesi[2], Antonio Pastor[3] and Christos Xenakis[1]

[1]Systems Security Lab (SSL), University of Piraeus, Greece
{*angelogianni, ipolitis, xenakis*}*@unipi.gr*
[2]OSS Product Development Unit, BA Digital Services - Ericsson, Genova - Italy
pierluigi.polvanesi@ericsson.com
[3]CTIO unit, Telefonica I+D, Madrid, Spain
antonio.pastorperales@telefonica.com

***Abstract*—Cyber ranges are proven to be effective towards the direction of cyber security training. Nevertheless, the existing literature in the area of cyber ranges does not cover, to our best knowledge, the field of 5G security training. 5G networks, though, reprise a significant field for modern cyber security, introducing a novel threat landscape. In parallel, the demand for skilled cyber security specialists is high and still rising. Therefore, it is of utmost importance to provide all means to experts aiming to increase their preparedness level in the case of an unwanted event. The EU funded SPIDER project proposes an innovative Cyber Range as a Service (CRaaS) platform for 5G cyber security testing and training. This paper aims to present the evaluation framework, followed by SPIDER, for the extraction of the user requirements. To validate the defined user requirements, SPIDER leveraged of questionnaires which included both closed and open format questions and were circulated among the personnel of telecommunication providers, vendors, security service providers, managers, engineers, cyber security personnel and researchers. Here, we demonstrate a selected set of the most critical questions and responses received. From the conducted analysis we reach to some important conclusions regarding 5G testing and training capabilities that should be offered by a cyber range, in addition to the analysis of the different perceptions between cyber security and 5G experts.**

***Index Terms*—5G, Security, Cyber Range, Testing Training**

I. Introduction

Cyber security is more than a recent trend. The penetration of technology as well as the extend of the advancements have radically changed our everyday lives. From basic functions to smart living, technology has proved that it is here to stay and thrive, as are cyber threats. The need for realistic yet controlled cyber security training is imperative, especially in modern years where both criminals and cyber attacks are becoming sophisticated. Cyber ranges are proven to be effective towards this direction, offering convincing scenarios and network setups. DARPA is developing the National Cyber Range for military cyber-war training, fact that indicates the importance of cyber ranges for security preparedness even in the case of critical infrastructures [1]. While literature offers multiple examples of successfully-integrated cyber range environments and lessons learned, to our best knowledge there are no works on cyber ranges focusing on 5G cybersecurity testing and training. Yet following latest developments, 5G networks reprise a significant field for modern cyber security in terms of criticality, introducing a novel threat landscape. Reaching from simple mobile users to Internet of Things (IoT) and smart farming, the applicability of such advanced network goes far. Practical as well as theoretical vulnerabilities have been already identified even in the lately introduced 5G network generation. Although there are numerous research works analysing fractures of this wide landscape; focusing either on the edge, the cloud, the virtualisation mechanisms, the protocol or signaling flows or even hardware attacks, there is no work focusing on the needs of 5G security auditors or red and blue team members that desire to gain a 5G-specific training and have an active role in the evolution of next generation networks. The demand for skilled cyber security specialists though, is high and still rising.

Therefore, it is of utmost importance to provide all means to experts that aim to increase their preparedness level in the case of an unwanted event. Although there are many platforms dedicated to a variety of cyber security categories (i.e., web, crypto etc.), there is no platform offering a realistic and complete 5G testbed. The need for novel cyber ranges that offer 5G capabilities, where entry-level to experienced cyber security professionals may access, is apparent. In this work we have managed to gather a set of questions to understand user's needs thus attain the requirements of such a testing and training platform both from both the attacker's and the defender's perspective.

The EU funded SPIDER project[1] proposes an innovative Cyber Range as a Service (CRaaS) platform that leverages and extends the capabilities of existing telecommunication testbeds and cyber ranges with the most recent advances in telecommunications management and emulation to offer a highly sophisticated environment for cyber security testing and training. SPIDER is addressed to 5G experts, platform administrators, cyber security professionals or regular employees of telecommunication operators that aim either to test their

[1]https://spider-h2020.eu/

network against attacks, advance their cyber security skills or even gain cybersecurity awareness to protect their organisation from social engineering attacks. Since, at the time of the research, there were no 5G cyber ranges, in order to gain a perspective on the stakeholder's needs, questionnaires have been created and distributed to the related stakeholders. The results from the questionnaires were used as the basis for the establishment of the user requirements from the SPIDER 5G cyber range platform [2].

This paper aims to present the evaluation framework, followed by SPIDER, for the extraction of the user requirements. To validate the defined user requirements, SPIDER developed and implemented a novel methodology, based on both closed and open format questions, which were circulated among the personnel of telecommunication service and infrastructure providers, security service providers, managers, engineers, cyber security personnel and researchers. The analysis of the collected responses indicates that the security experienced personnel putted emphasis on the attacks against the network users and 5G Telecom Service Providers (TSP's) as opposed to the cyber security experts that opted for network users and 5G Telecommunication Infrastructure Providers (TIP's). Furthermore, 5G security experts slightly leaned towards Defender's rather than Attacker's side.

The rest of the paper is organised as follows. Section II analyses the related work on the field. Section III analyses the methodology used for the questionnaires while section IV is dedicated to the retrieved results. Section V draws the conclusions.

II. Related Work

A. Cyber Ranges used for Cybersecurity training

Extended studies on testbeds and cyber ranges are presented in [3] and [4]. The latter analyses how cyber ranges have been proposed to offer training environments for Smart Grids, Internet of Things (IoT), SCADA and Cyber-Physical systems network installations. Cyber ranges are even employed in maritime systems [5] for training, testing and risk estimation. Specific telecom testbeds though have not been discussed in recent literature. A framework for the development and assessment of cybersecurity exercises is described in [6]. The analysis concludes that competitive exercises often fail to satisfy learner's needs. In [7] the lessons learned from cyber range defence training are thoroughly analysed.

B. 5G Cybersecurity Requirements

ENISA's report in [8] discusses the 5G security requirements based on the 3GPP standards. The authors in [9] and [10] surveyed the 5G related challenges, offering a categorisation of 5G technologies and attacks. More specifically, the key 5G technologies include i) Software Defined Networking (SDN), ii) Network Function Virtualization (NFV), iii) Multi-access Edge Computing (MEC) and Cloud and iv) Network Slicing. Both [9] and [10] were used as a basis for the questionnaire's 5G related section. Our work in [11] identifies and categorises the threats of the Radio Access Network (RAN) for all network generations, including 5G.

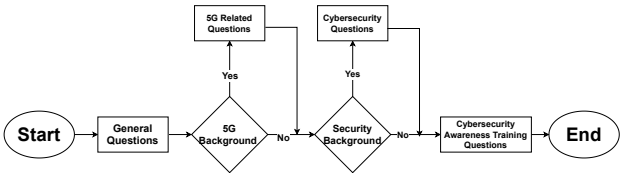


Fig. 1: Questionnaire Flow

C. The SPIDER case

The EU funded SPIDER project proposes an innovative Cyber Range as a Service (CRaaS) platform which delivers a realistic yet emulated environment for modelling and testing of network services, applications and security mechanisms that require a safe environment to omit the risk of proprietary data loss or adverse impact upon existing networks. SPIDER leverages of this testbed to further offer cyber security training capabilities for both experts and non-experts.

III. Methodology

A. Study design and procedure

The questionnaire was divided into 4 categories: i) General Questions, ii) Questions related to the 5G Infrastructure which are dedicated to medium to expert 5G personnel, iii) Questions dedicated to cyber security exercises for participants with relative background, iv) Questions related to cyber security awareness for participants which indicated not relative background. The flow of the questionnaire is illustrated in Fig. 1.

The questionnaire was distributed within the partner organisations of the project to people with the following positions and job titles:

- Cyber Security professionals, highly trained Ethical Hackers and Penetration Testers
- Security researchers, Ph.D. students and R&D engineers from the fields of Systems, Cybersecurity, Networks and IoT
- Master students and young professionals with a very good technical background
- Experienced project managers dealing with various types of cybersecurity projects
- Telecom Infrastructure Provider employees with senior experience in Product development and testing as well as Customer product introduction and support with a mix of solid technical background on 5G and Security
- Telecom Operator employees with demonstrated experience in cybersecurity and network deployment and operation

B. Ethics

The researcher's ethical framework was reviewed by the ethical and security board of the project. Participants were asked to fill Participant Informed Consent Forms (PICF) to ensure that they knew their rights and more importantly that

they participate voluntarily and can thus withdraw at any time without penalties. Furthermore, the participants were explicitly informed about the data collected for the purposes of this study as well as the contact person per organisation. The questionnaire did not collect any personal data hence the researchers could not deduce individual's answers.

IV. Results

Our data were collected between June to October 2020. Overall, the total amount of the related to stakeholders, that participated in the questionnaire for the validation of the user requirements, was 124 individuals. The questionnaires have been distributed internally using virtual tools such as Google or Microsoft Forms, depending on the internal organisation's policy. The results of the questionnaire were statistically processed using Microsoft's Excel tool.

A. Sample and participant demographics

Our final simple included $N = 124$ participants in total, a percentage of 50% (or $n_{5G} = 60$) of whom expressed a 5G-related background, and 77% (or $n_{Sec} = 96$) expressed expertise in cybersecurity. In absolute numbers, $n_{5G\&Sec} = 54$ of the participants indicated both a 5G and cybersecurity background while $n_{neither} = 21$ expressed no relevant background in either 5G or cybersecurity. In our original questionnaire and results, there is a third category of participants with a background in economics and risk which accounted $n_{Risk} = 32$ nevertheless, we don't discuss this category and the related questions and results in this work due to space limitation.

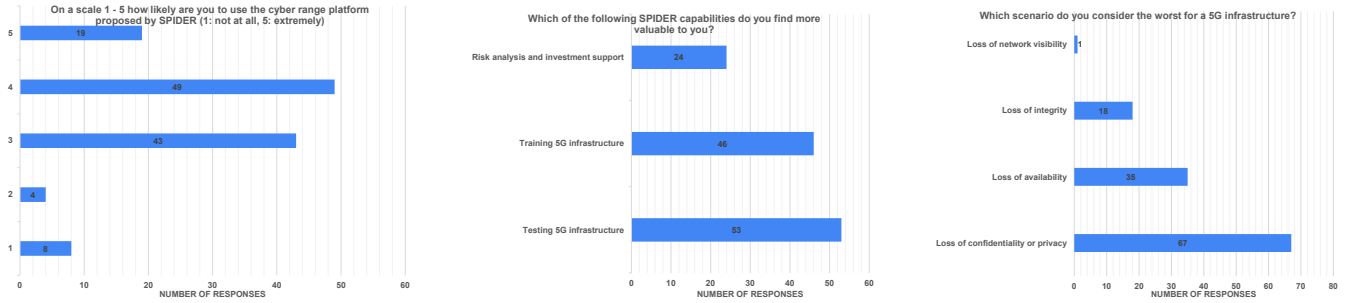
B. Qualitative and Quantitative evaluation of responses

1) ***General***
From the statistical process of the answers, for the General questions part of the questionnaire we may deduce that the majority of stakeholders are keen on using a cyber range platform such as the one proposed by SPIDER (Fig. 2a). In absolute numbers, $n = 111$ of the participants expressed a medium to extreme likelihood on using such technology. The testing part of the infrastructure is of more interest than the training (Fig. 2b), which indicates that the current 5G landscape certainly lacks tools that may render both the job of the administrator and the job of the security analyst easier. The worst threat against a 5G network according to the received answers was the lose of confidentiality/privacy (Fig. 2c). This finding is particularly interesting after the era of GDPR and other privacy related regulations indicating that in the modern world, privacy is gradually starting to be perceived as more important even than the availability.

2) ***5G Related***
Regarding the 5G-related responses, it is evident that the stricking majority would use a cyber range to test the security of a 5G infrastructure Fig. 3a. In total $n = 46$ out of $N_{5G} = 60$ of the participants with a relevant 5G background agreed that a cyber range would be useful tool to test the security of their 5G infrastructure. The 5G experts further recognised the core network as one of the most critical domain to protect, followed by Transport, IoT and Cloud. The results for the importance of RAN security from the expert's side, were inconclusive (Fig. 3b). When it comes to RAN security, attacks against authentication were found to be the most important (Fig. 3c) followed by attacks against privacy, which is in line with the latest research works published on the field of Radio Access security [12], [13]. Likewise, for the IoT domain, attacks against the authentication were concluded to be of high priority (Fig. 3d). For the MEC domain, attacks against operation, administration, maintenance and provisioning (OAMP) were ranked the highest (Fig. 3e), while for Transport domain, the priority was given to the DDoS attacks (Fig. 3f). For the core domain, which is the focus of 5G experts, the most important threat is the signaling of legacy networks due to the interaction between two networks, followed by signaling storms (Fig. 3g). Lastly, the worst attack type for the Network Slicing was the one against the resources of the slice (Fig. 3h) and for the Virtual Environments domain was determined to be the unauthorised access (Fig. 3i).

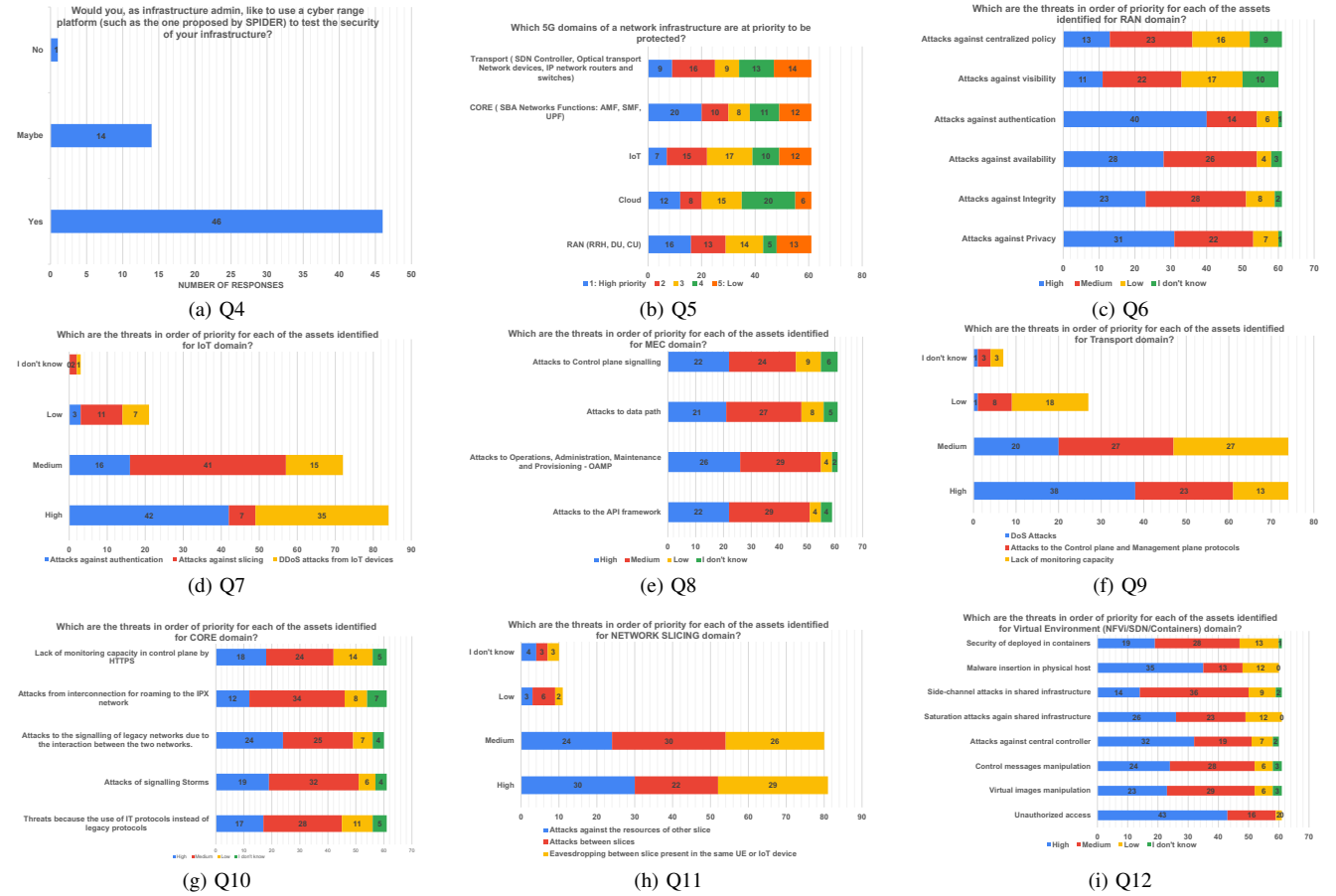
3) ***Cyber Security***
On the cyber security training aspect of the questionnaire, all participants $N_{sec} = 96$ admitted an interest to use a cyber range platform for 5G training (Fig. 4a) with 78% agreeing that they would use a cyber range for 5G training. Cyber security experts recognised as main target the network users (Fig. 4b) followed by 5G Telecom Service Providers (TSP's). The analysis of the collected responses indicates the importance of both network users and 5G Telecom Service Providers (TSP's) for the 5G experts, as opposed to the security experienced personnel that putted emphasis on network users 5G Telecommunication Infrastructure Providers (TIP's).The main reason for them to use such a platform would be get the latest knowledge (Fig. 4c) followed by maintaining readiness. The majority of the cyber security experts showed a slight preference towards the attacker's side (Fig. 4d). Although the results for the participants with a 5G background were inconclusive (i.e., "lack of preference") they leaned towards the Defender. This result perhaps indicates that cyber security professionals without prior experience with 5G technologies prefer their testing and defend processes more automated while they choose to dedicate their training on attacking techniques. Furthermore, most of the cyber security experts favored self-paced, individual exercises over team based (Fig. 4e) with a 48% result against 33%.

4) ***Cyber Security Awareness Training***
For Cyber Security Awareness training users indicated an interest in acquiring safer internet habits to prevent attackers from penetrating the corporate network. The other subjects in order of preference included training for malwares (i.e., adware, spyware, viruses, trojans etc.) either coming from the web or from removable media (Fig. 5a).



(a) Q1 (b) Q2 (c) Q3

Fig. 2: General Questions



(a) Q4 (b) Q5 (c) Q6

(d) Q7 (e) Q8 (f) Q9

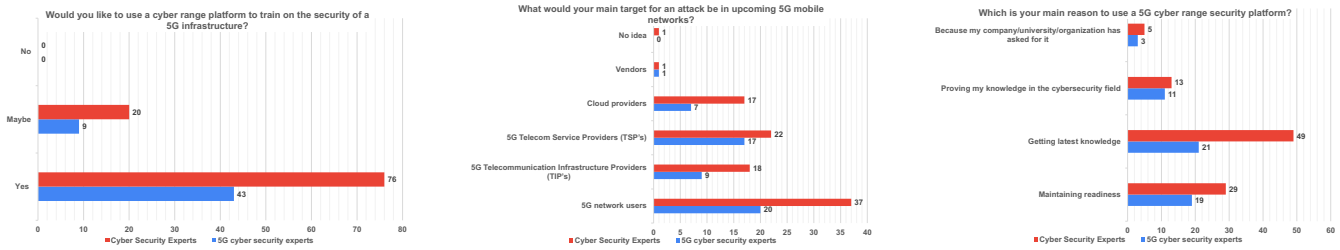
(g) Q10 (h) Q11 (i) Q12

Fig. 3: 5G Testing

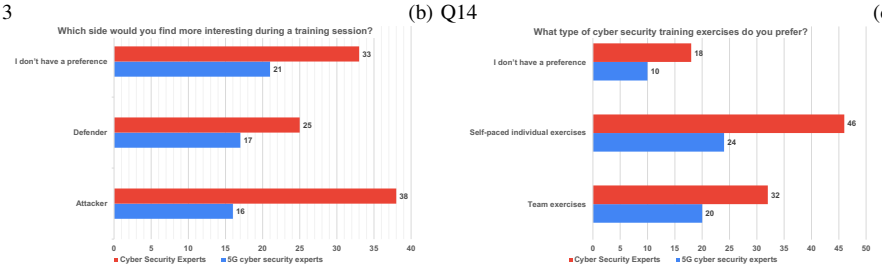
Physical security and clean desk policy were marked as less important compared to cyber threats. Regarding the measures and controls which can be demonstrated in to prevent mobile malware, participants agreed that understanding the risk of downloading application from utrusted sources is of major importance (Fig. 5b). Using anti-malware software was the second most popular answer, indicating that even for the applied controls, user's apprehension of security is vital. Lastly for remote users that connect to the corporate network, Virtual Private Network (VPN) training is the most needed form of training to establish secure connection, followed by firewalls for filtering the received connections (Fig. 5c). Cloud-based solutions were marked as of the least importance. This finding is particularly interesting and could indicate that users find cloud solutions rather confusing.

V. Conclusion

The area of 5G security is novel, hence growing along with the evolution of the 5G integration in our society. Security is estimated to have a pivotal role, especially in this new threat landscape. Security and awareness training should be

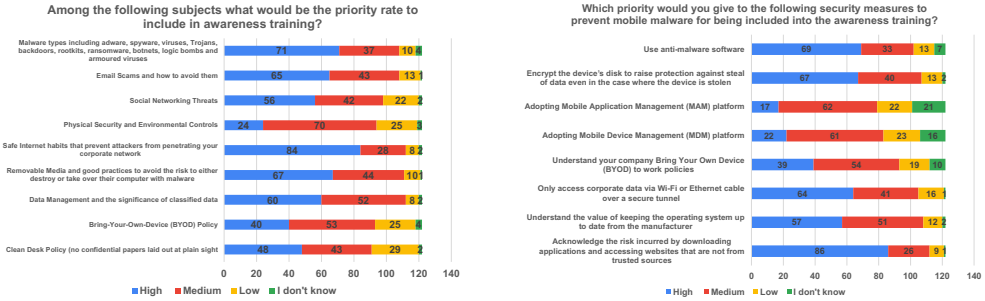


(a) Q13 (b) Q14 (c) Q15

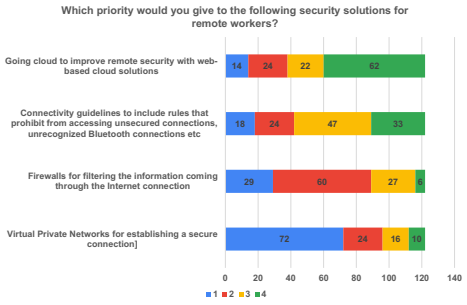


(d) Q16 (e) Q17

Fig. 4: Cyber Security Training



(a) Q18 (b) Q19



(c) Q20

Fig. 5: Cyber Security Awareness

a major pillar towards the direction to facilitate the secure development of such technologies. Towards this direction the proposal of SPIDER is to use cyber range technology to enable a realistic yet safe testbed that professionals may use to test and advance their skills both in both red and blue team training. By distributing the questionnaire, we managed to gain an inner perspective of how professionals evaluate the current state of the 5G cybersecurity field thus, establish the set of user requirements which were used as the basis for the design of both the platform and the scenarios to-be-used for the testing and training processes.

ACKNOWLEDGMENT

This research has received funding from the European Union's Horizon 2020 EU Research & Innovation program under Grant Agreement no 833685 (H2020-EU.3.7.4-SPIDER).

REFERENCES

[1] B. Ferguson, A. Tall, and D. Olsen, "National cyber range overview," in *2014 IEEE Military Communications Conference*, 2014, pp. 123–128.

[2] P. Gouvas, A. Angelogianni, I. Politis, C. Xenakis, N. Gerosavva, A. Alvarez, M. Athanatos, J. Pajo, A. Pastor, J. N. Mendoza, A. Mozo, S. Vakaruk, M. Giribaldi, I. Karapistoli, M. Ghering, G. Alexopoulos, G. Spanoudakis, A. Mozo, P. Polvanesi, and A. Brignone, "White paper: Pilot use case scenarios and architecture of the spider project,"

Tech. Rep., January 2021. [Online]. Available: https://spider-h2020.eu/wp-content/uploads/2021/01/SPIDER--WHITEPAPER-1.pdf

[3] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, and M. A. Ferrag, "Cyber ranges and testbeds for education, training, and research," *Applied Sciences*, vol. 11, no. 4, 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/4/1809

[4] M. M. Yamin, B. Katt, and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," *Computers & Security*, vol. 88, p. 101636, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404819301804

[5] K. Tam, K. Moara-Nkwe, and K. Jones, "The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training," *Maritime Technology and Research*, vol. 3, no. 1, pp. Manuscript–Manuscript, 2021.

[6] A. Brilingaitė, L. Bukauskas, and A. Juozapavičius, "A framework for competence development and assessment in hybrid cybersecurity exercises," *Computers & Security*, vol. 88, p. 101607, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404819301580

[7] J. Vykopal, M. Vizvary, R. Oslejsek, P. Celeda, and D. Tovarnak, "Lessons learned from complex hands-on defence exercises in a cyber range," in *2017 IEEE Frontiers in Education Conference (FIE)*, 2017, pp. 1–8.

[8] G. Milenkovic and M. Dekker, "Security in 5G specifications: Controls in 3GPP Security Specifications (5G SA)," European Union Agency for Cybersecurity (ENISA), Tech. Rep., 02 2021.

[9] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[10] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 196–248, 2020.

[11] A. Angelogianni, I. Politis, F. Mohammadi, and C. Xenakis, "On identifying threats and quantifying cybersecurity risks of mnos deploying heterogeneous rats," *IEEE Access*, vol. 8, pp. 224 677–224 701, 2020.

[12] T. Akhtar, C. Tselios, and I. Politis, "Radio resource management: approaches and implementations from 4g to 5g and beyond," *Wireless Networks*, vol. 27, no. 1, pp. 693–734, 2021.

[13] J. Rodriguez, G. P. Koudouridis, X. Gelabert, M. Tayyab, R. Bassoli, F. H. Fitzek, R. Torre, R. Abd-Alhameed, M. Sahedin, I. Elfergani *et al.*, "Secure virtual mobile small cells: A stepping stone towards 6g," *IEEE Communications Standards Magazine*, 2021.