The Current State of The Art and Future of European Cyber Range Ecosystem

Csaba Virág
Talgen Cybersecurity
Tallinn, Estonia
csaba.virag@talgen.com

Jakub Čegan
Masaryk University
Brno, Czech Republic
cegan@fi.muni.cz

Tomáš Lieskovan
Brno University of Technology
Brno, Czech Republic
tomas.lieskovan@vutbr.cz

Matteo Merialdo
RHEA Group
Brussels, Belgium
m.merialdo@rheagroup.com

***Abstract*—The Cyber Range Focus Group (CRFG) is established in the context of the four Horizon 2020 pilots contributing to the establishment of a European Cybersecurity Competence Network, with the purpose to horizontally coordinate the activities related to cyber ranges across the four pilots and contribute to the creation of a European ecosystem for cyber ranges, bringing together providers of both range infrastructure and range content. As the cyber domain is a non-deterministic complex one with a constantly evolving knowledge and threat landscape, simulation environments are emerging as the means to raise cyber resilience and dexterity. The EU cyber range ecosystem is constantly developing as the services become more affordable and accessible for more organizations and individuals through open-source technologies and federation of those resources. In contrast, a cyber range ecosystem-focused marketplace is foreseen to boost the market implementation, accessibility, and affordability.**

I. Introduction

Cyber ranges and the ecosystem around them are a hot topic when addressing cybersecurity capabilities, building cyber resilience, conducting research, or experimentation with infrastructure modifications. This paper explores the current state of the art of cyber ranges and exercises in Europe and explores ecosystem around it from a technological perspective. The paper utilizes the findings and outcomes of the *Cybersecurity Competence Center pilot* projects through its Cyber Range Focus Group, which concludes the four pilot projects and the European Cyber Security Organisation (ECSO).

Cyber ranges and connected services come in various forms, and there is still clarification required when it comes to defining them. ECSO defines cyber ranges as follows: A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organization's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. A cyber range includes a combination of core technologies for the realization and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases [1].

This definition tackles the range and the connected services from a technical perspective. At the same time, there is a need to define the ecosystem around it. Looking at the technological requirements and services offered by cyber ranges, the current ecosystem can be mapped and stakeholders can be identified, along with the potential impact this ecosystem can bring for the EU in its efforts to establish and maintain digital sovereignty and strategic autonomy. Stakeholders in the cyber domain are very diverse: governments, private entities, NGOs, individuals, machines, all focusing on a slightly or completely different agenda, yet with one common goal: to function and maintain business continuity in a safe and cyber-secure manner. To understand the benefits of cyber ranges and the its ecosystem the *Why*, *What* and *How* should be explored.

This exploration will sort cyber ranges and related services from the loosest integration to the tightest one. The paper does not try to discuss all details in-depth but shifts the focus from cyber ranges as a technical solution to cyber ranges as facilitators and the ecosystem to achieve cyber resilience.

II. WHY

In recent years the whole industry suffers from a constant lack of cybersecurity experts to protect both *normal* and industrial IT/OT systems, critical information infrastructures, and organizations themselves [2]. Cybersecurity is still an important global issue for governments worldwide and commercial institutions and is becoming increasingly more, as the mashing of human and machines continue through the exponentially growing number of digital interactions. It is well known that the cybersecurity market was worth $ 370 million in 2017 [3] and according to Gartner, it was projected to grow to $ 1,500 million in 2021 [3]. The assumption is indirectly confirmed by an analysis by ISACA with 2,366 respondents from industry, banking, and the public sector from around the world (North America 41%, Europe 33%, and Asia 12%) [2].

Cyber ranges help to close this skills gap by the education of the next generation of experts. Cyber ranges can provide a small virtual place to realize simple training for just a few students or robust virtualized infrastructure for international cybersecurity exercises for hundreds of participants [4]. Cyber ranges enable generic cybersecurity and digital upskilling and education and improve capability development efforts by adding context, relevance, and personalization.

Competence building through traditional education and training programs usually takes years to complete or rarely

 Cite this article as follows: C. Virág, J. Čegan, T. Lieskovan and M. Merialdo. *The Current State of The Art and Future of European Cyber Range Ecosystem*, 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, pp. 390-395, doi: 10.1109/CSR51186.2021.9527931.

produces professionals with applicable hands-on experience. It takes usually years to adopt to a certain working environment and understand the system for the workforce to be fully operational by getting experience with the tools, challenges and unique features of the digital and cyber ecosystem and supply chains. Humanity is shifting towards relying on smart technology, developing its *smart ecosystem*, hence the approach towards education and training is in transition too.

Beyond competence building [5], cyber ranges enable organizations to experience their level of cyber exposure and cyber resilience. A customized turnkey cyber range solution offers *real world* functions, the same way as the real internet and network, but in a fully controlled environment. The suitable cyber range enables to develop and conduct light-touch and/or custom exercises, based on the organization's own environment and situation, with realistic and automated scenarios; and to create and execute continuous, online, organization-wide cybersecurity training & awareness programs to inflict collective change of behavior for crisis avoidance and management, and thus, ultimately, cyber resilience.

Cyber ranges can support the experimentation with Digital Twins, a virtual version of physical infrastructure, simulating devices, services and functions. This way, new service and/or device integration can be simulated, analyzed, and trained before actual implementation, saving costs and discrepancies in operations. By simulating the infrastructure, actual attack vectors, tools, and tactics transformed from cyber threat intelligence aid SOC teams to prevent, mitigate, and defend IT and OT networks.

III. WHAT

There are several use cases for the cyber ranges as described above, and not every cyber range can fulfill all of them. It is pretty common that cyber range is specialized in one of them, and the others are available but not pushed. Cyber ranges come in various *outfits*: open source, custom-made, commercial, cloud, on-premise, research, military, education, etc. For each use case, it is crucial to understand that, to meet the specific requirements of the use case fully, a cyber range must possess or expose specific functionalities or capabilities. The challenge is how to differentiate among them in accordance to the achievable benefits expected by using them and how to identify the required level of services offered by them.

Cyber ranges are fundamental for security research across a wide range of security domains. By their very nature, cyber ranges are themselves being developed by researchers worldwide to research new attack detection and mitigation methods, malware emulation, and more [1]. Another classic use case of cyber ranges is testing. Security and stability of systems and applications can be tested in a controlled way to identify potential vulnerabilities before their live deployment and use [1]. Lately, the most important use cases have become those connected with cybersecurity education, competence building, and development of cyber capabilities. Its expansion is closely connected with the development of quality content.

One unit of the content is often called a scenario, and it is focused on one goal (e. g., penetration testing training, cyber defense exercise etc.). The scenario may contain only a virtual environment for users to interact with, or it may also include a storyline with specific objectives, some practical or theoretical challenges, or different types of questions [1].

Hands-on activities for purposes of this article can be divided into two groups: Capture The Flag (CTF) and Cyber Defense Exercises (CDX) [1]. CTF can be further divided into the attack only, the defense only, or attack-defense scenarios, where every type trains the trainees' capability. The Attack-defense scenario makes trainees fight against each other and practice both capabilities simultaneously. CDXs put trainees in the Blue team's role, protecting infrastructure against attackers – Red team. The goal of CDX is often not only a technical one, but essential parts of the exercise are often communication, crisis management, and law aspects of cybersecurity.

Unlike the training or CTF, CDXs need the cyber range simply because they are too big and too complicated to develop, handle, and evaluate. Most of these CDXs also need one to two years to be developed and tested for their official run. All previously mentioned qualities of the cyber range are used not only during the event (e.g., scenario management, infrastructure management, data collection, evaluation). During the development period, repeatability, scalability, and automation also save a significant amount of expert labor. [6]

As discussed before cyber ranges are more than training and exercises platform and there is a growing demand for additional services: IT/OT simulation, behavioral analyses (human + machine), cyber-physical interactions (cy-phy), etc. As the attack surface is constantly growing a safe, secure and cost-effective measure is required to safeguard the enourmous amount of various types and security standards of the interconnected devices and services. Such tasks can only be performed if there is access to hands-on experience with incident response capabilities, automation tools, analytics, means to priotize and act on potential threats and resilience improvements.

A. Ecosystem and marketplace

Marketplaces enable providers and customers to create value by enabling a fast and effective interaction with each other. The value created increases even more for participants of multi-sided marketplaces, which key feature is the network effect: a platform becomes more attractive to potential new customers as more customers engage with it. In other words, the value increases for all participants as more customers actively use the platform (snowball effect).

ECHO H2020 followed these assumptions while designing its cyber ranges marketplace within the ECHO Federated Cyber Range (E-FCR) [7] implementation, a place for cyber range and related services providers to publish their services, negotiate with customers and join forces with other providers (federation) to provide eventually more complex service packages. While designing the E-FCR Marketplace, a few principles were taken into account:

- Capability to attract participants

- Capability to create demand economies of scale
- Advantage of reduced time-to-market
- Quality standards: to be successful, the Marketplace needs to facilitate the exchange of values, which means that the services provided through the E-FCR maintain certain quality standards which the E-FCR itself can guarantee.
- Simplicity of doing business
- Ecosystem: the overall goal of setting and vision of the E-FCR Marketplace goes well beyond the single organization perspective and includes the whole European network of centres of competences around it: the Marketplace will foster an *ecosystem of E-FCR members* with different roles – cyber range providers and customers, academia, collaborators, policy makers and communities. This ecosystem ideally falls within the overall vision for the European Network of the Centre of Competences.

Via the E-FCR Marketplace, Customers can request cyber range services from multiple cyber ranges using the E-FCR. The E-FCR Marketplace acts as a middleman between the Customer and the Cyber Range Provider(s) and Content Providers. This simplifies the interactions of the Customer who only has to deal with a single entity (the E-FCR) for the request and the definition of the Services. [8] The E-FCR Markeplace is addressing ecosystem demands, buy not being bounded to training services, but also leverages simulations, testing environment, emulation environments and enabling easy federation: the objective is to cover every possible Service offered by cyber range and related service providers.

IV. HOW

A. Federation, Interconnectivity

To achieve the affordable accessibility of cyber range services sharing of range resources (physical and logical) is envisioned. Technical interconnection and federation between different cyber ranges is a central engineering research topic, subject of research from several Horizon H2020 projects (among them, ECHO H2020) and from the European Defense Agency (EDA). Benefit of federating cyber ranges is to more easily overcome capacity and capability limitations of the single ranges and offer more complex environments and scenarios, potentially spanning multiple sectors [7]. There are various options for technical interconnection of cyber ranges:

- Layer 1 physical interconnection
- Layer 2 datalink interconnection
- Software Defined WAN (SD-WAN)
- Layer 3 logical interconnection

1) Layer 1 physical interconnection: Physical interconnection of cyber ranges into a federation is likely the most performant solution, but also extremely challenging and expensive, in particular for a commercial perspective. Physical interconnection means a whole dedicated physical network (e.g., fibre optics cabling) must be deployed between CRs. A commercial federation would then be reasonably unsustainable because of economics, coordination and management (ownerships of physical mediums for interconnections and so on).

2) Layer 2 datalink interconnection: Layer 2 VPN emulates the behaviour of a LAN across an L2Switched, IP or Multiprotocol Label Switching (MPLS)-enabled IP network, allowing Ethernet devices to communicate with each other as they would, when connected to a common LAN segment. To limit high-latency and possible intermittency of connectivity issues, at least an extremely reliable WAN solution must be adopted, like MPLS. But building an MPLS-based layer 2 VPN assumes cooperation between an Internet Service Provider (ISP) and the Cyber range Providers with costly investments and contracts. Plus, such configurations are natively static, so not suitable to dynamic reallocation of network resources while instantiating/deinstantiating scenarios for cyber range purposes. [7]

3) Software Defined WAN: SD-WAN is a cutting-edge breed of solutions meant to manage and optimize interconnection of a large number of multiple remote sites/infrastructures. Such architectures typically include at least a single physical/virtual dedicated appliance for each branch site plus a main appliance and/or a controller. This approach does not seem actually feasible for commercial cyber range federation, unless, as a single commercial entity, it manages to deal with ISPs for the SD-WAN service delivery as EDA did in its Federated Cyber Range initiative.

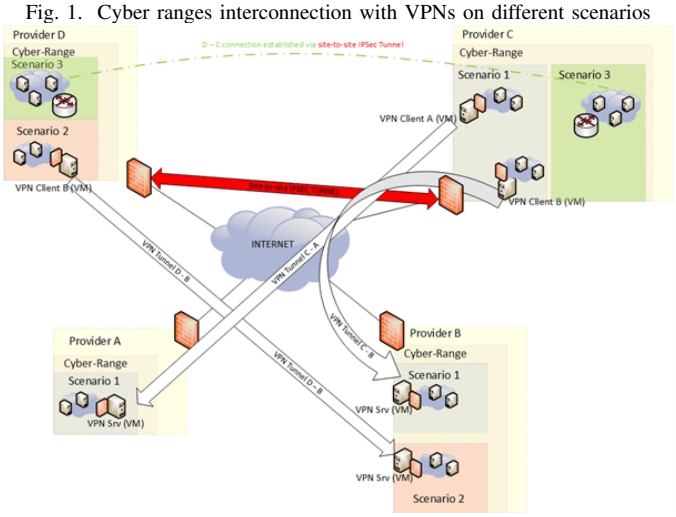
4) Layer 3 logical interconnection: Due to the configuration complexity and the needed investments for Layer 1, 2 and SD-WAN interconnections, a simple and generally technically viable approach is to focuse on Layer 3 VPN. Also in this case, several options have been analysed in the context of the ECHO H2020 project.

5) Fully-meshed network of VPN site-to-site tunnels: A fully-meshed network of VPN site-to-site tunnels among Providers could provide a deep integration of infrastructures, but would bring overwhelming efforts in terms of management of routing policies (e.g., possible overlapping networks inside different scenarios, routing configuration complexity with interaction between infrastructures) and governance of cross-provider configurations (e.g., security reasons).

6) Client-to-server Layer 3 VPN: Within the Layer 3 logical interconnection option, the ECHO team studied another possibility which may overcome the above-mentioned challenges and could avoid the stretching/merging of virtual infrastructures: the sharing of cyber range resources among several Providers, simply allowing each member of the federation to reach other member's resources via VPN Layer 3. Such solution would consist on opening a client-to-server Layer 3 VPN between different scenarios in different Cyber Ranges. As illustrated in the example below, Scenario 1 includes resources from Provider A, B and C while Scenario 2 includes resources from Provider D and B. In the first case, A and B will provide their own VPN packages for the client VPN connection to C (the package could consist of either a complete Virtual Machine (VM) with its configuration or the VM requirements with configuration). Provider C will take care of its own Domain Name System (DNS) and Network Address Translation (NAT) configurations (to apply on the provided package) in order to guarantee proper access to

remote resources from its own part of Scenario 1. In the second case, B will provide VPN-client package to D that will take care of its own DNS and NAT configurations (to apply on the provided package) in order to guarantee proper access to remote resources from its own part of Scenario 2. In all cases, the server side of the VPN will need ad hoc Port Address Translation (PAT) rules (on the edge firewall of its infrastructure) in order to properly forward incoming VPN traffic from different remote Cyber ranges (VPN clients) to the correct scenario (VPN server) [7].

Fig. 1. Cyber ranges interconnection with VPNs on different scenarios



The aforementioned solution seems particularly simple to be used within a commercial federation approach: a simple, replicable VPN VM can be developed and can be easily configured depending on the characteristics of each federated cyber range. Within the ECHO H2020 project, after an initial analysis and subsequent tests, this approach was adopted to develop ECHO Federated Cyber Range system (E-FCR).

B. Software as a Service or On-Premise software

There are two types of licensing and delivery of the entire solution: cloud and on-premise software. Each solution has its advantages and disadvantages, so it is not possible to define in advance which solution is better for the cyber ranges, it always depends on the specific situation and financial possibilities.

Software as a Service is a type of service where the application is hosted completely by the supplier, there is no need to worry about the hardware, the applications are available via a thin client or a web browser. Licenses are based on monthly subscriptions. The advantage of the cloud is a very small initial investment, but the monthly fee is usually high, so in the case of on-premise, the hardware would pay over time. Cloud security depends on the vendor, but most of the time the supplier has security technologies that ordinary institutions cannot afford. In case of access, the advantage of cloud access is virtually from anywhere, but an Internet connection is always required. [7]

The hardware and software are deployed locally on the client side, the client takes care of and associates the hardware and software. The disadvantage of on-premises is the large initial investment, but the monthly operating costs are already relatively small. The security of the entire solution depends on the organization that procures the on-premise solution. Access to the on-promise solution is also possible locally, i.e. in offline mode, so there is no need for Internet access. On-Premise is owned by the organization, which is also responsible for maintenance, updates or any failures and outages.

TABLE I
CLOUD OR ON-PREMISE

	Cloud	**On-Premise**
Initial costs	low	high
The need for a subscription	yes	no
Security	usually high	depends on the organization
Access	only over Internet	over Internet & locally
Implementation	fast and easy	usually slow and challenging
Configuration options	less customizable	fully customizable
Maintenance	provided by the supplier	provided by the organization
Dependence	full dependence on the supplier	full independence

C. Resource sharing and Open access

Whatever cyber range variant is chosen, the scenarios, trainings and *the contents* themselves are always the biggest limitation. Creating scenarios and trainings or any specific *content* usually is very time consuming, when creating a good training can take weeks or months. This fact greatly limits the possible further exploitation of the entire cyber range capacity. The solution to this situation is to share resources.

By sharing resources is meant the sharing of already created trainings, scenarios and other contents, artifacts (referred generally as *Contents* from now on) . There is currently no central database for these Contents, so now organizations need to share these Contents with each other. Unfortunately, Contents are always tied to a specific platform and are not easily transferable to another platform. Organizations that want to share scenarios and Contents must share the same platform. In the case of already functional cyber ranges, it is necessary to unify platforms, so that one or more organizations have to switch to another platform, which is very time consuming. Contents also require supporting methodology and tools, that has to be interdisciplinary and quickly adoptable.

CONCORDIA H2020 followed these assumptions while developing interchangeable content that originates in the open-source KYPO Cyber Range Platform content description [9]. For that reason, virtual machines, networks, and training scenarios are entirely described in human-readable data-serialization languages JSON and YAML or use open-source software Packer to build virtual machines and Ansible for describing machine content [4].

Another option is to share resources in the sense of sharing the cyber range between multiple organizations. Cyber range is usually not needed every day and every hour of the day. In the case of an agreement, it is possible to share the cyber

range between several organizations and thus reduce the time and cost of maintenance.

It would be most appropriate to create one central platform on the cyber range, one central database of trainings and scenarios, where everything would be open-source and with broad community support. While this approach creates the opportunity for co-creation and access to affordable services, the traditional *commercial versus open-source* evaluation in regards of customer demand has to be assessed. At the same time, a sparkling open-source community would ensure the high-quality added value services of the commercial offerings.

D. Updates

It is necessary to update practically anything today, including the cyber range. However, there are three levels of updates:

1) Operating system and packages update: From a security perspective, it is necessary to regularly update the operating system and all its packages. Even if the cyber range platform is up to date, an outdated operating system can lead to security breaches. The problem with operating system and package updates is their possible future incompatibility, so it is needed to check individual dependencies and be prepared for a situation where the system may not work properly after updating. For this situation, it is necessary to have a system backups and a version control system.

2) Cyber range updates: Every piece of software needs to be updated and this also applies to the cyber range. Updates are used to add new features to the cyber range, improve stability or patch security issues. These updates go hand in hand with operating system updates, where updates can cause incompatibilities with the cyber range platform and vice versa. These two updates must take place in a coordinated manner.

3) Update of scenarios and Contents: It is necessary to look at this issue in two ways. The first is the updating of scenarios and Contents due to the updating of the cyber range platform, which may not be up to date with old versions. This happens especially after updating with several versions of the platform, when to eliminate it is usually necessary to update the platform after individual versions up to the most current version. The second way of looking is to update scenarios and Contents (trainings especially) due to the obsolescence of the issue. Cyber security is the area that is changing the most. Majority of the attacks and vulnerabilities that were current 5 years ago are now obsolete and virtually all devices are already resistant to these attacks. Cyber security must be taught on current and near future threats, which necessarily leads to a constant update of individual scenarios, contents and trainings.

In the long run, it would seem that this problem could be solved by not updating any part and *preserving* the whole solution. This solution is definitely not recommended because it leads to incompatibility with newer versions of scenarios and Contents. From a security point of view, this is not possible, because the whole solution becomes prone to an attack from the inside, where the cyber range could be attacked by training or the scenario itself.

E. Case of using cyber range

As already touching the topic above, cyber range can be used in many ways by organizations and individuals. Thanks to its architecture, it meets high demands for performance, flexibility and reliability. The most common ways to use:

1) Teaching: Probably the most interesting use of cyber range is in teaching. Parameters such as:

- Fast environment recovery
- Ability to run one scenario multiple times
- Possibility of access from anywhere, eg from home
- Possibility of centralized monitoring of the progress of individual students
- Support for individual and - in case of exercises - team performance evaluation

Cyber range meets all these parameters, and therefore seems to be the best option for use in teaching not only cyber security.

2) Cyber security testing: The cyber range is also an ideal tool for use in cyber security testing. It can be used to test both software and connected hardware. The following parameters are important for cyber security testing:

- Separation of the environment from the Internet
- Separation of individual scenarios from each other
- Quick recovery of the scenario
- Possibility of running multiple scenarios in parallel

These parameters make the cyber range a good technical tool for cyber security testing. This testing can be performed, for example, in industrial networks, where whole or part of industrial networks can be virtualized using cyber range.

3) Use in business: Cyber range can also be used in business. Cyber range can be used to train employees or to test their skills, or to simulate attacks on the company's infrastructure and train countermeasures. Important parameters for use in business:

- Simple environment
- Fast scenario recovery
- Easy creation of scenarios
- Embedding in the company's infrastructure
- Support for risk assessments and evaluations

V. Building European Cyber Range Ecosystem

A. Stakeholders

All pilots have addressed the definition of the cyber range and related services ecosystem through conducting market researches, surveys, and analytics. While approaching the topic from a technical perspective, it is crucial to bear in mind what the ultimate goal of the EU is, as a sustainable ecosystem has to be in line with the higher-level strategies. The EU cybersecurity strategy sets the roadmap for higher cyber resilience, technological sovereignty, and leadership through increasing the capabilities of critical public and private sectors: hospitals, energy grids, railways, data centers, public administrations, etc. New AI-powered Security Operations Centers are being launched along with the Joint Cyber Unit. Simulation environments like cyber ranges serve as affordable connectors and facilitators for all of these stakeholders. Cyber ranges and

the ecosystem around them have an impact on everyone: institutions and agencies, governments, private sector, individuals, academia, and research.

B. Ecosystem

The usual approach to ecosystem identification regarding cyber ranges usually reflects on the potential end-users and beneficiaries. However, cyber ranges and related services have their ecosystem, while the same stakeholder usually provides most services, yet the rise of the various service providers is already visible in the European market. The ecosystem consists of the platform owners (range providers), content producers, service providers, users.

C. Standardisation

Currently, there is no standard for defining what is considered a cyber range or cyber range-related service. Neither are there standards defining technical requirements for a cyber range and their federation or inter-connectivity. Due to this reason, cyber ranges at the time of writing of this paper can come in the form of a handful of virtual machines running on a laptop and in the form of a multi-million euro worth of facility (e.g., Estonian MoD's Cyber Range). While building a sustainable ecosystem, it is vital to set minimum standards and definitions so the stakeholders can understand each other better, both from a technical and a business perspective. Standardization might be approached less from a technical and more from a business use-case or a meta-schematic aspect.

D. Human aspects

Stakeholder engagement goes beyond developing an ecosystem on the technical level. Based on the researches and findings of the pilots' cyber ranges and related services are still in their early implementation stages due to their costs (accessibility), the acceptance (demand), understanding the benefits (costs), and ease of setup to support the right usage (complexity). The standardization or at least defining the levels of cyber range capacity and service requirements enable the faster and more cost-effective implementation where technology providers, platform owners, content ecosystems can optimize their efforts to reach more potential customers.

E. Impact

Cyber resilience cannot be achieved without enabling and expecting all stakeholders to contribute to it, and in the end, the efforts invested in pursuing it shall benefit the human user and society as a greater good. The impact of a defined ecosystem enabled to provide affordable access to the cyber range, and connected services are higher situational awareness, faster up- and re-skilling through targeted and customized training and education, resilient society and organizations prepared for incidents are regularly exercising their skills and procedures.

VI. Conclusion

In this paper, the systematic overview from a technical perspective of the cyber range ecosystem has been described as identified and addressed through the research activities of the *Pilot projects*. The purpose was to summon the key findings on technological dependencies, reasoning and accessibility, and the various services' demands. A few ranges exist with multiple functions, while connectivity, content sharing, or federation of ranges is a viable option to optimize resources. Through defining technical standards and moving towards a more systematic development of *Contents* that can be distributed through a commonly accepted technical solution (*Marketplace*), the stakeholders can easier meet, and a sustainable ecosystem can be created. Eventually, this would enable European Union to meet a vital milestone in its pursuit of ultimate cyber resilience and digital sovereignty.

Acknowledgment

This paper is funded by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 830927, project CONCORDIA.

This paper is funded by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 830943, project ECHO.

This paper is funded by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 830892, Project SPARTA.

References

[1] The European Cyber Security Organisation (ECSO) , *Understanding Cyber Ranges: From Hype to Reality*. The European Cyber Security Organisation (ECSO), 2020.

[2] Information Systems Audit and Control Association (ISACA), *State of Cybersecurity 2020*. Information Systems Audit and Control Association (ISACA), 2019.

[3] C. Metinko, "Cybersecurity Training Sees Flood Of M&A," https://www.forbes.com/sites/mergermarket/2018/08/17/cybersecurity-training-sees-flood-of-ma/#10399fb52266 [Online; accessed 2021-05-25], 2018.

[4] J. Čegan, "Cyber Range as a Tool For Cyber Security Education," in *IS2 - Information Security Summit*. Tate International s.r.o., 2020, pp. 16–21.

[5] SPARTA, *D9.1 Cybersecurity skills framework*. Strategic programs for advanced research and technology in Europe (SPARTA), 2020.

[6] E. Suni, J. Piispanen, J. Nevala, J. Päijänen, and K. Saharinen, *D7.1 Report on existing cyber ranges, requirements*. Cyber Security for Europe (CyberSec4Europe), 2020.

[7] M. Merrialdo, *D6.1 E-FCR High-Level Design*. European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO), 2019, internal deliverable, version 1.1.

[8] I. Raisr and M. Merrialdo, *D6.5 E-FCR HIGH-LEVEL DESIGN*. European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO), 2020, internal deliverable, version 1.0.

[9] KYPO CRP Team, Masaryk University, "KYPO Cyber Range Platform Documentation," https://docs.crp.kypo.muni.cz/user-guide-advanced/sandboxes/sandboxes-overview/ [Online; accessed 2021-05-25], 2020.