Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Cyber Range Federations: State of Play, Connectivity Considerations and User Awareness

Πέτρος Μαυρίκιος

Επιβλέπουσα Καθηγήτρια
Δρ. Αδαμαντίνη Περατικού

Νοέμβριος 2021

Open University of Cyprus

School of Pure and Applied Sciences

Cyber Range Federations: State of Play, Connectivity Considerations and User Awareness

Petros Mavrikios

Supervisor:
Dr Adamantini Peratikou

The present postgraduate dissertation is submitted to the

Faculty of Pure and Applied Sciences of the Open University of Cyprus,

in partial fulfillment of the requirements of a postgraduate degree in

Computer and Network Security

November 2021

Περίληψη

Καθώς ο κόσμος διασυνδέεται όλο και περισσότερο, οι συνδέσεις μεταξύ συστημάτων υπολογιστών αυξάνονται με γεωμετρική πρόοδο. Εξίσου γρήγορα αυξάνονται και οι διάφορες προκλήσεις που απειλούν αυτό το διαρκώς συνδεδεμένο περιβάλλον. Ο καλύτερος τρόπος προστασίας από τις καταστροφικές συνέπειες μιας κυβερνο-επίθεσης, αλλά και από τις πιθανές δευτερογενείς επιπτώσεις που αυτή μπορεί να προκαλέσει σε άλλους τομείς, είναι το να αναπτύξουν οι τελικοί χρήστες την ικανότητα ανίχνευσης, αναγνώρισης και αντιμετώπισης κυβερνο-επιθέσεων. Αυτές οι δεξιότητες μπορούν να αναπτυχθούν και να βελτιωθούν σε ένα εικονικό περιβάλλον όπου οι απειλές και τα φορτία τους μπορούν να εξομοιωθούν με ακρίβεια, αλλά χωρίς τις καταστροφικές τους συνέπειες: αυτά τα περιβάλλοντα είναι γνωστά ως cyber ranges.

Η παρούσα μεταπτυχιακή διατριβή θα εξετάσει την τρέχουσα βιβλιογραφία για τα cyber ranges αλλά και τις ομοσπονδίες τους, δηλαδή τις συνενώσεις δύο ή και περισσότερων cyber ranges. Οι ομοσπονδίες cyber ranges επιτρέπουν στους χρήστες να εκπαιδεύονται σε σενάρια και απειλές που κανονικά δεν θα ενέπιπταν στην ομάδα κινδύνων που απειλούν τον κλάδο ενασχόλησης του κάθε χρήστη – και κατ' επέκταση δεν θα «προσφέρονταν» από το «οικείο» cyber range – διευρύνοντας με τον τρόπο αυτό την εξοικείωση τους με ένα εκτενέστερο φάσμα απειλών. Επιτρέπουν επίσης τον συνδυασμό πόρων και την βέλτιστη αξιοποίηση τους, μέσω της προσομοίωσης πιο περίπλοκων σεναρίων σε πιο ρεαλιστικά περιβάλλοντα. Στο πλαίσιο της έρευνας μας θα εξετάσουμε διαφορετικές επιλογές διασύνδεσης και θα πραγματοποιήσουμε δοκιμές σχετικά με την απόδοση τους.

Θα παρουσιάσουμε επίσης τα αποτελέσματα έρευνας που πραγματοποιήθηκε μέσω ερωτηματολογίου για την αξιολόγηση της εξοικείωσης των χρηστών με την ασφάλεια στον κυβερνοχώρο, την υιοθέτηση από μέρους τους βέλτιστων πρακτικών και τον βαθμό έκθεσης τους στα cyber ranges και τις ομοσπονδίες τους.

Summary

As the world becomes increasingly interconnected and linkages between computer systems rise at an exponential rate, so rise at an equally exponential rate the threats associated with a perpetually connected world. The best way to protect oneself from the devastating consequences of a cyberattack and its possible spillover effects, is for end users to develop a capacity for detecting, identifying and countering cyber-attacks. This skill set is best honed in a sandbox environment where threats and their payloads can be emulated with accuracy, but without their destructive consequences: these environments are known as Cyber ranges.

This postgraduate dissertation will look into the current literature regarding cyber ranges and their federations, or the interconnection of two or more cyber ranges. Federated cyber ranges allow users to train on scenarios and threats that would not normally fall within the scope of their particular sector's exposure and thus would not normally be offered by their "home" cyber range. They also allow the pooling of resources, thereby enabling more elaborate tests to be simulated in more realistic environments. We will examine different interconnection options and undertake tests regarding connectivity performance.

We will also present the results of survey research undertaken to assess end user awareness into cyber security in general, familiarity with best practices and exposure to cyber ranges and their federations.

Acknowledgements

First and foremost, I would like to express my thanks and appreciation to my supervisor, Dr. Adamantini Peratikou, for her constant guidance and support and for always being at the other end of the line, not just for this postgraduate dissertation but throughout this degree, ever since the first e-class lecture on Networks. Thanks also to Prof. Stavros Stavrou for his support, as well as for that inspiring presentation on Cyber Security, during a CFSP seminar organized by the Ministry of Foreign Affairs of the Republic of Cyprus in late 2016 - that one presentation is what set all this in motion.

My greatest "thank you" must go to my wife Maria Georgiou, and to our children Eleni Anna and Andreas Orestis for their patience, for their understanding and for their cooperation every time that daddy had to do his homework. They are the centre of my sometimes erratic universe and my definition of the meaning of life.

Contents

Chapter 1
Introduction

1.1 Preface

In an increasingly connected world, where a successful cyber attack could have disastrous effects which are not restricted to the targeted system, but spill over to other sectors of the economy, it is of crucial importance that cyber security practitioners are trained in realistic simulations. This would allow them to hone their skills and enable them to have cyber attack response experience without being exposed to an actual incident. Given that it is inadvisable to use a live system for training purposes, or to take it offline so that users can train on it, the need arises for cyber ranges. These however tend to be focused on a particular system or subset of cyberspace, and are often limited by the experience, knowledge, and interest of their designers. This is the gap that Federated Cyber Ranges try to address, by enabling researchers and cyber security practitioners to train beyond their usual métier.

1.2 Research Aims:

To conduct a study into stand-alone and federated cyber ranges, comprising a literature review of the current level of the discipline, a presentation of federated ranges together with an explanation into their functioning, their components and their connectivity requirements, as well as users' exposure and familiarity with them, by means of an online survey.

1.3 Key Questions

- What are cyber ranges and how do they function?
- Explanation of the nature and need for federated cyber ranges.
- Testing of different interconnection options.
- Assess User awareness regarding cybersecurity, best practices as well as Cyber Ranges and their federations.

1.4 Importance of the Research:

As the world becomes more and more interlinked, the threats to data and applications increase exponentially. It is therefore crucial for cyber professionals to be able to test the possible repercussions and fallout from a specific attack within the safety of a virtual deployment. Cyber ranges exist to serve this purpose, i.e. to enable the replication of real networks within a sandboxed environment and then launch attacks on these networks in order to assess their resistance and tolerance limits, as well as the consequences of when attacks succeed.

Cyber ranges of this kind tend to be focused on that area of expertise specific to the entities running them, and while they can be quite comprehensive in the study of their own subsection of cyberspace, they are often limited to that subsection. For example, while a cyber range testing the vulnerability of an e-banking system can be very helpful in allowing researchers to draw conclusions on securing e-banking systems, it is often perceived as being unable to offer insights as to the possible consequences of a particular threat to another system, for example Electrical Grid oversight, or Air Traffic Control. This is to a large extent because the threats to one type of system are erroneously perceived as unrelated or irrelevant to another, as well as to the fact that testing for the effects of these threats on a system requires very specific information on the functioning of that system. Different systems have different services, resources, and requirements, and to draw accurate conclusions, we need to be able to study a threat across a wider range of systems, including some that we would not normally have access to, or expertise on.

Federated ranges try to fill in this gap, by pooling together different cyber ranges and testing for the effects of a particular threat across a more widespread selection of targeted systems, emulating therefore the true nature of the interconnected world. This dissertation will examine both the theoretical soundness of pooling resources in this manner, as well the technical methodology required to do so.

In preparing this postgraduate dissertation on federations of Cyber Ranges, a clear shortage of relevant academic journals was identified, while a sufficient, but certainly not exhaustive body of work was found on the issue of Cyber Ranges in general. It was therefore deemed necessary to also assess the extent to which computer users were themselves familiar with the concept.

1.5 Layout

This postgraduate dissertation attempts to address two distinct, yet inevitably interconnected issues: on the one hand it constitutes an examination of the current research work being carried out on the issue of cyber ranges and their federations. A theoretical approach is adopted in this effort, during which the functioning of cyber ranges and their federations is explained, with experimentation work being carried out in the lab in order to present and test cyber range interconnectivity options.

Interesting as the issue may be on a theoretical level, its real-world value is the actual benefit that accrues to end users from applying the theory in their everyday work environment. This is the second aspect of this postgraduate dissertation: to assess through survey research, whether mainstream users of differing prowess, given their nature as the ultimate beneficiaries of the outcome of the research, are aware of this technology and of the existence of cyber ranges as a tool in the cyber security toolbox. Given that usage of a cyber security toolbox, foremost requires awareness of the dangers in play, it was considered necessary to include in this assessment, users' general exposure and approach to cyber security issues.

Chapter 2 constitutes a review of the literature, both on the issue of Cyber ranges, as well as on the more specialized issue of cyber range federations.

Chapter 3 examines the concept of Cyber Range interconnection into federations. The various layout possibilities are presented, and possible interconnection options to be used for establishing Cyber Range Federations are outlined and explained.

Chapter 4 begins with a presentation of network connectivity performance indicators, followed by a presentation of the testing software iperf, with "demo" tests being carried out for presentation purposes. Later on in the chapter, the results of actual live tests undertaken on virtual machines and in the lab are presented for comparing results between two different interconnection protocols.

Chapter 5 introduces the reasoning behind the survey that was undertaken for the purpose of this postgraduate dissertation, briefly explains the basis for the selection of participants and makes the case for the selection of the interface used for the execution of the survey.

Chapter 6 lays out the responses of the participants in the survey and presents respondent's views on the concept of cyber security, their perceptions regarding certain practices, their familiarity with the concept of cyber ranges in general, as well as with the more specific issue of federations of cyber ranges.

Finally, Chapter 7 attempts to draw conclusions regarding the current state of the literary research on cyber ranges and their federations, as well as further steps that might follow the work presented in this postgraduate dissertation. It also attempts to draw conclusions regarding the results of the survey and more specifically lessons that might be learned regarding cyber security awareness among civil servants in Cyprus and options for their training and familiarization with cyber threats.

Chapter 2
Literature Review

2.1 Introduction

In most of the papers studied for the purposes of preparing this postgraduate dissertation, authors point to the fact that in a wired world, where systems are connected to each other, the possible outcome from a successful cyber attack is a disastrous one. Specific linkages are made to the vulnerability of various systems to attacks, and the overwhelming effects they would have on the economy, on citizens way of life, and on the provision of crucial services like electricity, water and gas. References are also made to the protection of personal data as well as national security.

Given the devastating effects that can be caused by an attack like Stuxnet or Wannacry, or the attacks on servers across the Estonian economic and government sectors in 2007, or the more recent attack on the Ukrainian electrical grid – effects that touch upon the target sectors or entities but can also have spillover effects on the economy at large and often spread beyond national borders – common sense points to the need for better training of computer professionals in order to be able to:

a) protect systems from these attacks by improving software and hardware to minimize successful attacks, and

b) develop skills to contain, mitigate and restrict the effects of successful attacks.

Clearly, it would not be a sound option to acquire this training and experience by launching attacks on live systems, as it would be very easy to find oneself faced with the very situation they are working to avoid, namely an attack on their systems which in this case would be self-inflicted. Similarly, it is often impossible to take systems offline in order to check their resilience, nor is it always feasible to replace faulty or vulnerable components with better ones. It is argued by Urias et al (2017)that it is no longer sufficient for cyber security practitioners to prove their capabilities

on the basis of professional qualifications, but rather to be able to demonstrate their ability on the basis of training in an environment that closely matches the one that they are trying to defend.

Therefore, a need becomes apparent, for a solution which would enable cyber practitioners to train and hone their skills in countering cyber attacks. Much like a physical firing range serves as a place where real ammunition is fired on virtual targets, a cyber range acts as virtual training ground where computer systems can be replicated in a sandboxed environment and then placed under attack by a series of threats in order to study their effects. Tian et al (2018) describe a cyber range as "a virtual environment that is used for cyberwarfare training and cyber technology development. It provides tools to help strengthen the stability, security and performance of cyberinfrastructures and IT systems to be used by government and military agencies. Cyber ranges function like shooting or kinetic ranges, facilitating training in weapons, operations or tactics. Thus, cyber warriors and IT professionals employed by various agencies train, develop and test cyber range technologies to ensure consistent operations and readiness for real world deployment" (Tian et al, 2018, p. 35355). Winter (2012) defines it more succinctly as "a facility allowing a model of an IT system to run in a simulated environment to perform tests and measurements that are applicable to the real world" (Winter, 2012, p. 2). He goes on to explain that their form is varied depending on the extent of a simulated environment and also on how complex it is. Another determinant is the type of threats that we want to test, as well as the skill of the professionals tasked with putting the cyber range together.

2.1 Cyber Ranges

Winter (2012) presents an excellent introduction to the concept of Cyber Ranges and sets the stage for understanding how they work for training against cyber attacks. He underlines how simple it is for a lone attacker to wreak havoc on interconnected systems, as well as systems seemingly diverse and distant from the system being targeted, while at the same time pointing out that there can be long-term losses associated with cyber attacks. For example, pollutants can be released into the environment, or other long-term damage could also ensue, sometimes even when not intended by the original attacker. The author goes on to explain that there are primarily three ways to make systems safer:

- by not connecting them - although as the world becomes increasingly interconnected this is becoming more difficult, and as the Stuxnet case pointed out, non-networked computers can also fall prey to a cyber attack

- by installing network defensive devices and systems in place, which while serving the purpose of defending against attacks, may do so at an increased cost, and also run the risk of making the system complicated at the detriment of user friendliness.

- by actively seeking and repairing any vulnerabilities

Winter (2012) also explains that a system can be considered to be sufficiently secured if the cost of countering the remaining risk is greater than the loss that may arise from exposure to that risk.

He goes on to argue that a cyber range can be used to assess the risks for cyber attacks, citing as an advantage the fact that they can be purpose-built and be focused on the specific requirements of the particular case or enterprise to be tested. At the same time, he makes the case for cyber ranges which would be able to test the security of a wide range of systems and infrastructures, i.e. a system that can be used for a variety of different attacks and network architectures. The author argues that foremost among the advantages offered by a cyber range is its ability to "wipe the grid clean" and reset or change the configuration being tested at no cost.

Davis and Magrath (2013), define three distinct Cyber Range types:

a) Simulation

b) Overlay

c) Emulation

Simulation is the process of replicating actual network components on a test server. This is defined as probably the easiest and most cost-effective cyber range creation method. The downside to this option is that although simple to set up, the models tend to be too generic and offer little parallels with the real world to allow the extraction of reliable observations. According to Davis and Magrath (2013), cyber ranges of this type were the most commonly used in the past but have become less popular due their lack of insight into real attacks, especially as technology has allowed for the use of more sophisticated models.

Photo 1: NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

(Source https://ccdcoe.org/exercises/)

Overlay is the method by which a network to be used for testing purposes is "mounted" on top of the actual network. This enables the test to be undertaken using the exact same equipment, topology and other network parameters as the live system, but does not offer the flexibility of scripting specific events and responses. A very real disadvantage is that in using the actual network for testing purposes, this method also runs the risk of exposing and hurting the network itself.

Emulation is the method by which a replica of the network to be tested is recreated using the same components as the production network. This has the best possible proximity to the production network and as a result, credible real-world conclusions can be drawn from an exercise that will be run in a cyber range of this kind. This type of cyber range lacks flexibility and can be costly in cases of extended networks with elaborate topologies. Emulation is often used in conjunction with virtualization of some components of the network. As more components are virtualized, the less the cyber range emulates the real network.

The European Cyber Security Organisation (ECSO, 2020), defines a cyber range as "a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation'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 realisation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases." (ECSO, 2020 p. 10)

They explain that the target users of cyber ranges can include decision makers, security professionals, military personnel, educators, students, and researchers, and add that a cyber range can be used for security testing and research, competence building and education as well as for the development of cyber capabilities and resilience.

Similar reference to "use cases" is made by Vykopal et al (2017a) in their paper on Masaryk University's KYPO Cyber Range. The authors distinguish between three different such options:

i. Cyber research, development and testing

ii. Digital forensic analysis

iii. Cyber security education and training

Vykopal et al (2017b) explain that the most basic cyber range participation layout is that in which an attacking "red team" is countered by a defending "blue team". This would probably unfold via a process of sniffing the target network for vulnerabilities and then exploiting them in order for the attacker to acquire privileges on the network which would enable them to carry out their aims and deliver their payloads. The authors point out that a cyber range also includes monitoring services to record traffic statistics and logging capabilities in order to draw upon the information to generate a scoring system for participants. They also present a more elaborate team "colouring" scheme which incudes, beyond red and blue, a green team (the operators of the simulation) and a white team (the exercise organisers/managers and referees).

Photo 2: KYPO Cyber Range, Masaryk University, Czechia (Source: https://crp.kypo.muni.cz/)

A typical cyber exercise life cycle, explain Vykopal et al (2017b), would go through a preparation phase, a dry run phase, an execution phase and an evaluation phase. The longest of these would be the preparation phase, spanning a number of months during which the exercise scenario is researched, planned and put in place. Also long is the evaluation phase, during which participants are debriefed in an effort to codify lessons learned and determine take-aways. The authors underline that the planning phase is the most crucial in order to strike the very fine balance between the exercise approaching reality and the model being feasible. They explain that the dry run phase can also have added value in ironing out mishaps or omissions from the planning phase. Finally, they point out that there exists a fifth phase- that of repetition, whereby an exercise scenario would be reset and run again and again with a new group of participants, each run feeding into the original exercise, thereby further improving it, and enabling its repetition with less manpower requirements.

Making reference to the federated cyber range developed by his employer, *Northrop Grumman*, Winter (2012) explains that its administrators are able to transform it into a reliable representation of a system being tested, together with the tools needed to record and analyse network traffic. Tests can be as diverse as assessing component failures or changes to network architecture, examining

for example the changes caused to network traffic by the introduction of new hardware or workstations. Winter (2012) goes on to suggest other tests, like testing the effects of policies and procedures, both with respect to efficient network-wide dissemination as well as for the presence of failure points like conflicting operating systems, or network hardware from different vendors. Cyber ranges can also be used to test for traffic and other effects of malware as well as other unplanned activities coming from penetration activity.

Cyber range testing, Winter (2012) continues, is advantageous in that it enables the users and administrators of the network being tested to take part in the tests themselves, so that they can witness in real-time the performance of the model of the system they are working on and assess system behaviour and incident handling. Winter (2012) also cites a challenge that arises from working with a cyber range, namely that for the model to be accurate, it requires considerable detail regarding the makeup of the actual system. This, the author explains, can be particularly difficult sometimes with missing documentation and institutional memory gaps regarding the system's layout and evolution. Another challenge stems from the use of virtual machines to emulate the components in the system, as well as the need to sometimes use the actual component and connect it to the model when it can not be virtualized.

This capability to reset the network quickly and with little or no cost is also touched upon by Chapman et al. (2017), who present a number of commercially available cyber range options (like those offered inter alia by the SANS Institute and Offensive Security), and then present their own suggestion for a similar testbed, with the main benefit in their proposal being that a new layout can be designed and deployed in a matter of minutes. Beyond the specifics of their own proposal, which, like others, makes use of the blue team / red team dichotomy, and uses generated and captured network traffic in order to emulate normal network usage (and thereby allowing for red team "attacker" data to be sufficiently obfuscated, as they would be in a real life attack), the authors also stipulate the various threat actors launching these attacks:

a) Cyber criminals, working for financial gain, reputation or out of malice

b) States or state sponsored actors, working for espionage purposes, or for destructive action

c) Hacktivists / Terrorists working for political, social or destructive purposes

d) Privileged insiders or partners working for financial gain.

Chapman et al. (2017) then explain that first and foremost in setting up a testbed, is network replication accuracy, and they proceed with briefly outlining different options, underlining their own preference for using Netkit. This is then matched with tcpdump and tcpreplay in order to capture and broadcast traffic in the testbed in a way that enables red team obfuscation. Data was generated by running a series of standardized network services like email, file transfer, remote access and webpage serving. A star topology network was deemed as the most appropriate layout used within a corporate environment and therefore applied in their model.

Tanasache et al (2019) underline that cyber attacks will tend to become more sophisticated, due to the increasing complexity of networks which in turn leads to increased capabilities of cyber attackers – in order to safeguard the best possible defence, the best possible training must be extended to security practitioners. This training should be undertaken in an environment that realistically represents the system being tested, and which is able to generate benign and malicious events, and varied attack scenarios, in a timely and cost-effective manner. They go on to present their own proposal which is designed to realistically represent a target system. They opt for a cloud based interface using OpenNebula, and then replicate the network topology (via the acquisition of relevant information from the network administrator). OS detection via Nmap was used then, followed by OpenVas and Nessus to identify running services. In their paper the authors test their model by trying to replicate the University of Roma's DIAG computer system. They then broadcast traffic containing both benign and malicious traffic, and use sniffer VM's to document activity.

Tam et al (2021), after a brief introduction to the concept of cyber ranges in general, present the case for making use of cyber ranges in order to enhance the skills of security practitioners in the maritime industry and to train exercise participants to have better defensive understanding of attacks as well as to cultivate their ability to minimize the effects of a cyber attack. The authors also explain the need for scalability of cyber ranges, underlining that in order to be effective training tools, the models to be run must reflect the real world to the greatest possible extent. This, however, must be carried out without replicating each and every minute detail to the detriment of speed and ease of emulation. It is, however, acknowledged that as networks become more elaborate, scalability becomes increasingly difficult, and relies on enhanced virtualization techniques – this carries additional cost with respect to financial and processing resources needed to both run the simulations, as well as to acquire and analyse the data relating to the performance of participants in the test.

Tam et al (2021) also underline the fact that it might be beneficial for different operators, rather than having to continuously upgrade their own cyber range, to connect to another cyber range in order to combine computing power, and share testing and analysis capabilities. This is one of the few papers examined in this postgraduate dissertation which makes reference to the concept of Federation, which mainly refers to the connection of cyber ranges via VPN connections. Reference is made by Tam et al (2021) to a project currently being worked by CyberMAR – the EU's "Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain" project - which aims to connect three cyber ranges.

The concept of Federated cyber ranges is also included in the exhaustive work of Yamin et al (2020) on the prevailing literature on Cyber Ranges. The authors point out that federation is one of the directions that the next steps in the evolution of Cyber Ranges might take. Federation is presented as relating to portability, multiple location support, standardization of scenarios and accessibility to a wider user base.

Photo 3: NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

(Source https://ccdcoe.org/exercises/)

The European Cyber Security Organisation – ECSO, defines federation as "a group of computing or network providers agreeing upon standards of operation in a collective fashion" (ECSO, 2020, p. 25). It is explained further that federation operates on the assumption that it would be very costly to establish a single cyber range that could cater to all needs, all scenarios and all parameters, and that the pooling of resources of different cyber ranges can be mutually beneficial. This also means that a user could make use of all the different assets in the federation according to their needs. ECSO (2020) also refers to integrated cyber ranges, whereby the cyber ranges in a federation are also able to "talk to each other" in order to disseminate scenarios making use of assets from more than one cyber range. This connectivity can be achieved via a number of methods, but once again VPN is cited as the most appropriate direction to take. It is also argued that an integrated federation requires more planning and technical prowess to pull off, compared to a simple federation.

Chouliaras et al (2021) begin their paper by touching upon the increasing sophistication witnessed in cyber attacks and underline the clear need for competent cyber security practitioners, capable of staging plausible responses and mounting defenses to these attacks, and therefore the inherent added value of cyber ranges as training areas for the development of the necessary skills. They continue by citing previous articles into the various cyber ranges in operation and argue that cyber ranges can be classified according to their use case, i.e. as existing for the purposes of Research, of Training, and for staging Competitions/Exercises. Chouliaras et al also argue that cyber ranges can be classified according to their operator, and they refer to universities, government organisations, military research facilities as well as international organisations, distinguishing also between cyber ranges whose functioning is accessible for study, and others whose details of operation are classified.

Chouliaras et al (2021) also underline that the widening scope of cyber attacks has led to discussions around the concept of cyber ranges. They state that the need for federations stems from the "consideration that a single cyber range would have enormous costs and would be extremely complicated if it was to have all the necessary features and functionalities, the whole package. Therefore, it would be better organized, and also modular and in effect realistic, if multiple cyber ranges, each within a specific area of expertise, could collaborate in order to offer to their users a wide variety of use cases and different scenarios" (Chouliaras et al., 2021, p. 7).

They continue by explaining that the fusing together of the specific knowledge and specialist capabilities of different cyber ranges into one common platform, accessible to all their users provides a broader simulation environment, while limiting costs.

Chouliaras et al (2021) refer to a number of initiatives in forging federations of cyber ranges. Explicit reference is made the EU's Cyber Range Federations project, in which eleven member states of the Union participate, including Cyprus. The authors also mention the CyberSec4Europe project, which will be referred to in the next chapter in this postgraduate dissertation.

Chapter 3
Interconnecting Federations

3.1 Federations of Cyber Ranges

While there is considerable research being carried out regarding Cyber Ranges in general, the literature is quite frugal on documenting federated cyber ranges. As documented in the literature review above, those papers which refer to federations of cyber ranges only do so in passing, mentioning their existence and that work is currently being carried out at an international level to establish federations of cyber ranges. One such project that gets repeatedly mentioned, but not in detail, is the effort currently under way at the European Defence Agency, launched in May 2017 in which eleven EU member states are participating ("EDA Cyber Ranges Federation project showcased at demo exercise in Finland," 2019.)

Extensive reference to federated cyber ranges is made by Suni et al. (2020), who in their paper reporting on the implementation of deliverables of the CyberSec4Europe project, also make the distinction between federations where the "federal" aspect ensues from cooperation and exchange of knowledge and lessons learned, and "connected" federations, in which the explicit assumption is that interconnection between two or more cyber ranges occurs.

They argue that pooling and combining cyber ranges can improve their ability to generate more realistic environments and testbeds and allow their users access to more features and capabilities than they would not normally have access to. By connecting to another cyber range, a cyber range operator can enhance what they are offering to their users without needing to incur additional cost for further investment. It is also argued by Suni et al (2020), that considerable planning needs to be undertaken in order to address smooth functioning and quality of service issues, underlining that limiting network latency is crucial for the smooth running of an interconnected federation.

3.2 Federation types

This interconnection, according to Suni et al (2020) can take different forms, which they describe as "use cases", as follows:

A: Networked Cyber Ranges, where cyber ranges can be connected to each other in a point-to-point network (starting with two cyber ranges), or in a mesh like structure (connecting three or more ranges). These connections would occur as needed in order to provide access to the resources of another cyber range, or extend the capacity of an existing range by allowing users to access tools offered in an associated cyber range, or enable smaller ranges to operate jointly to run larger exercises. Implicit in this arrangement is that the interconnectivity occurs in a way that is seamless and non-discernible to the user.

In the graphs below, we first see the peer to peer layout of an interconnection between two cyber ranges, and immediately after, we can see a depiction of a mesh interconnection of four cyber ranges.

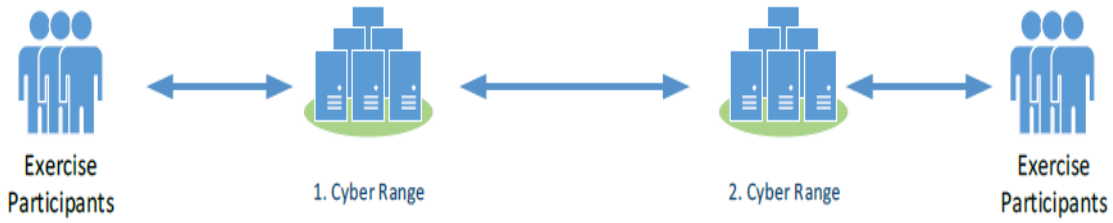

Figure 1: Peer to Peer Connection (Suni et al., 2020, p.51)

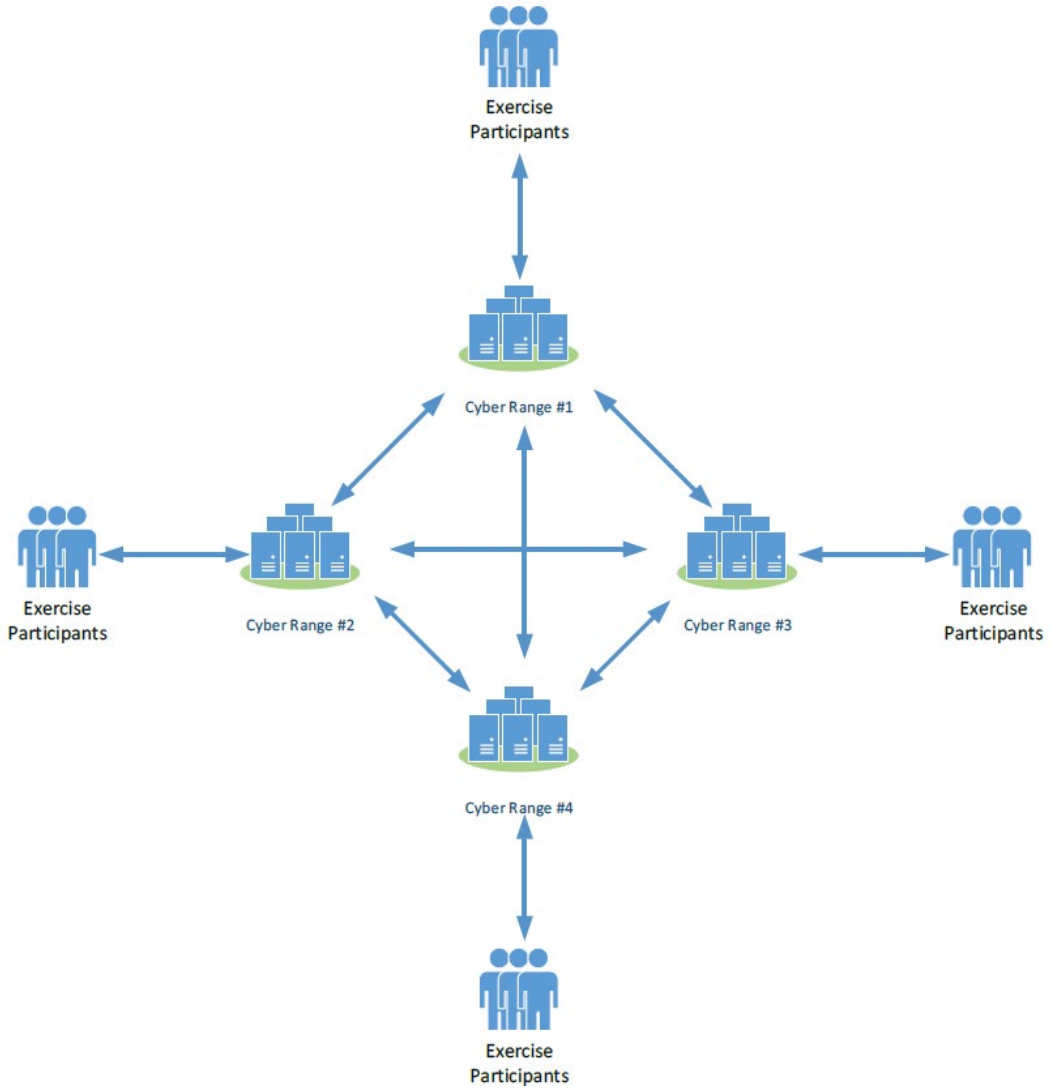

Figure 2: Mesh connection (Suni et al., 2020, p.52)

B. A Cyber Range operating as a hub, whereby the lead on any training exercises on the federated range will be maintained by this hub, which operates as the host, matching clients and resources on the connected cyber ranges as per the needs of each user and each scenario. Clients (or users) would then connect to the hub cyber range and use it to access services or training scenarios or specialized features, including those offered by the "daughter" cyber ranges. From a topological point of view, the participants accessing the cyber ranges would be "clients" connected to the hub cyber range, who would then interact with the other ranges via the hub.

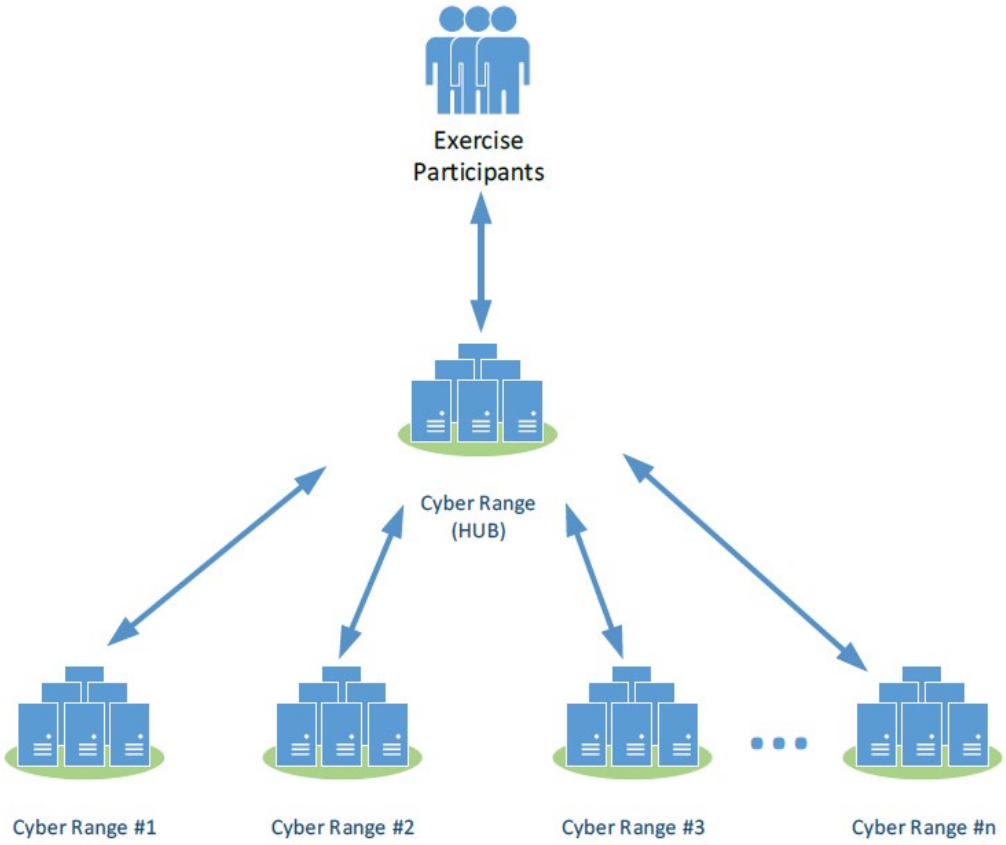

Figure 3: Cyber Range as a Hub (Suni et al., 2020, p.52)

C. A Cyber range connection with testbeds. This is the third use case mentioned in Suni et al. Here we have very specific testing and experimental environments that are not catered for in cyber exercises, nor are they designed to be used in that context. Such testbeds could be related to IoT, smart grids, AI, cyber physical devices etc. Their connection to the cyber range would be achieved by means of a point-to-point connection, so that they can be accessed by exercise participants.

Suni et al also refer to the need for individual users to also be able to join the federation. The actual federation network, referred to in the cases explained above, serves for the interconnection of the cyber ranges making up the federation, and not for the individual user who wishes to participate in an exercise. Individual users should be able to connect with the cyber range federation upon registration or receipt of an invitation that would be accompanied with connection instructions as well as appropriate login credentials. These instructions, argue Suni et al., should also provide links for the download of a VPN client which should be sufficiently hardened to preserve the federation's nature as an isolated environment and use full tunnel connections to ensure that no packets escape to the internet.

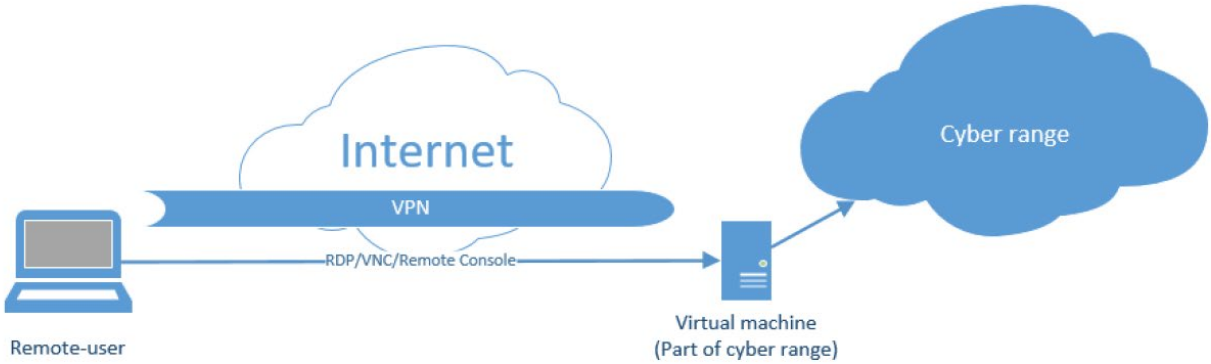

Figure 4: Remote User Connection to the Cyber range (Suni et al, 2020, p. 64)

3.3 Connectivity Options

3.3.1 Direct Connection

For a group of cyber ranges to work together as a connected federation, the crucial requirement is connectivity itself. This can take the form of a direct layer 1 connection, which although functional, would be expensive and difficult to implement and maintain. The actual task of physically connecting two separate networks would make this no small feat even across the same city, let alone across different countries. It would also render ad hoc connections nearly impossible and restrict the federation to a static form whereby only those ranges already connected to it would be able to participate in an exercise or other kind of exchange. Signing on new ranges would be a daunting task which would require a considerable investment of funds as well as time for its implementation.

3.3.2 Layer 2 Connection: MPLS

A speedier approach would be a Layer 2 interconnection via MPLS-VPN. This is often offered as an additional service by ISP's, in the same way as other more "corporate" options are offered, like ATM or Frame relay. Under MPLS, packets are directed through the ISP's network on the basis of a labelling system which determines the path to be followed, as opposed to traditional IP, under which each packet determines its own path through the network ("Understanding Layer 2 VPNs - TechLibrary - Juniper Networks", nd). MPLS paths function like a "virtual" point to point connection

inside a wider network. The system works by means of communication between dedicated routers, one on each side of the connection. On the ISP side, the router forwards the data over MPLS according to the labelling information, while on the client side, once it arrives at the exit router, the packet is no longer identified by its label, but reverts to identification by its IP header, and is then treated as layer 2 traffic. In order for the information to be carried to and from the cyber ranges' users, it must be switched to layer 3 – this is a task that must be undertaken by the cyber range operators themselves, and establishing the federation requires careful planning with in order to avoid IP addressing issues and coordinate VLANs to be used. Communication and pre-agreement among the cyber ranges is also needed for operational and monitoring purposes. An obvious disadvantage to this method is the reliance on the ISP for the provision of "premium" services. ("MPLS Routing - How Does MPLS Routing Work?," rcrwireless.com, 2014)

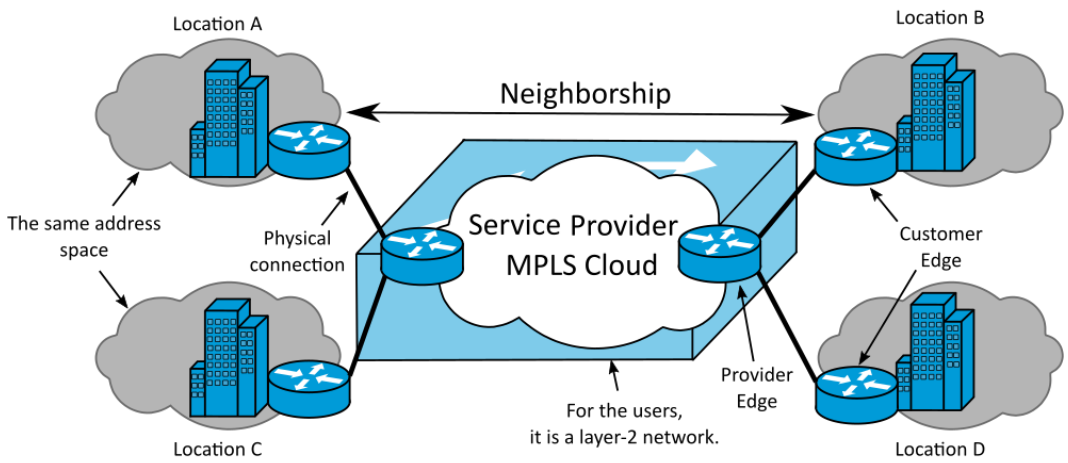

Fig 5: MPLS Layer 2 VPN

(Source: https://en.wikipedia.org/wiki/Layer_2_MPLS_VPN#/media/File:L2_MPLS_VPN_en.svg)

3.3.3 Layer 3 Connection 1: IPSEC

Perhaps the simplest solution that can be implemented for securely interconnecting cyber ranges is connecting them via layer 3 VPN. One popular iteration is IPSEC operating in tunnel mode. In tunnel mode, the original IP packet is encrypted in its entirety, and once a new header is added to it (either an AH header or an ESP header), it is sent to the other end of the tunnel. Both header methods ensure data integrity, origin authentication and protection against replay attacks, with ESP also adding limited traffic flow confidentiality to the mix. IPSEC tunnel mode is used for

network-to-network communications, host to network communications and host to host communications (firewall.cx, n.d.)

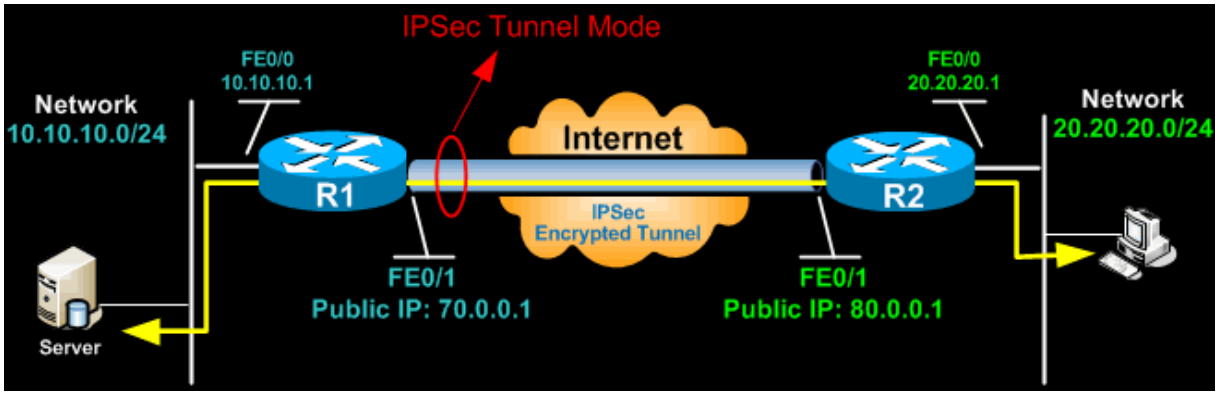

Fig 6: IPSEC Tunnel Mode

Source:

http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html#:~:text=With%20tunnel%20mode%2C%20the%20entire,VPN%20tunnel%20(IPSec%20peer).&text=Traffic%20from%20the%20client%20is,sent%20to%20the%20other%20end

The other iteration of IPSEC, transport mode, differs in that it is only the payload of the IP packet that gets encrypted. For the purposes of this postgraduate dissertation, we will focus on IPSEC tunnel mode.

IPSEC is considered to be secure although in the leaks attributed to Edward Snowden, it was suggested that work was under way by the NSA to insert vulnerabilities. (Wikipedia, 2021)

3.3.4 Layer 3 Connection 2: OpenVPN

OpenVPN is a very popular VPN protocol, owing its popularity to the fact that it is cross platform, running on Windows, macOS and Linux, as well as Android and iOS, the fact that it is open source and finally the fact that it is considered to be secure, given that it can operate on 256-encryption via a custom security protocol which is heavily reliant on OpenSSL (Techradar, 2020).

OpenVPN operates by using TUN/TAP to set up virtual network adapters to relay traffic once it has been encrypted. TUN/TAP enable user-space applications, like VPN clients, to interact with the virtual devices thereby allowing the injection and flow of packets (already processed and

encrypted). TUN is the layer 3 iteration of OpenVPN whereas TAP is layer 2. Depending on the type of connection we are interested in, we can implement TUN or TAP. If we wanted to route traffic from one point to another we would use TUN, but if we were looking to bridge two networks, then TAP would be the appropriate method - since TUN is L3, it can only route, not bridge (Saminiir 2016).

Chapter 4
Interconnectivity & Performance

4.1 Performance Tools

Before discussing performance tools, it might be useful to distinguish between the various values that they measure. The values we are interested in when it comes to network performance is throughput, latency and jitter.

Throughput is the number of data packets travelling from a point of origin to a destination within a specific timeframe and it is measured in bits per second. Throughput is often confused with bandwidth, which is the "theoretical" maximum number of packets that could arrive at the destination in the same time frame. A good analogy is that if data transfer could be seen as water flowing through a pipe, bandwidth is how wide the pipe is i.e. how much water it could carry, whereas throughput is how much water it actually carries.

Latency is the time it takes for a packet to travel from the point of origin to the destination. It is measured in milliseconds (ms).

Jitter is the variation in latency. In a situation where latency is 30ms and jitter is 20ms, this means that a packet could take from 30 to 50ms to make the journey. Jitter is an indication of congestion in the network, and it can lead to packet loss when packets arrive simultaneously and cannot all be processed.

Latency, jitter, and the ensuing packet loss are all interlinked with throughput and adversely affect network performance and user experience. Within a cyber range context, it is understandable that latency can result in poor network response times, and can affect the exercise scenario deployment, distort measurements regarding participant reaction times and render the experience ineffective by the removing the "real-time" aspect from the mix. This becomes increasingly more relevant in the framework of a federation of cyber ranges, where physical distance and pooling of resources requires sufficient network speeds and near-immediate response times.

In order to attain the best possible performance, we therefore need to be able to increase throughput and decrease latency in any given network. Before we do this however, we must perform a survey, an assessment as it were, of its current state, so that we can apply changes and modify settings in an effort to compare and contrast the "before" and "after" situation.

Various tools can be used to this end, foremost among them IPERF3.

Iperf3 is a free, open source, cross-platform command line program used in measuring throughput in real time. Using iperf3 we are able to run a series of tests regarding time intervals, data transferred, bandwidth, loss etc. Tests can assess the server, the client or both (bidirectional). It works by sending a load between the two systems being tested and reports on the bandwidth, jitter and data loss.

When it is run over TCP, in its basic structure the iperf command measures the bandwidth between a client and a server. Jitter and datagram loss can be measured by means of running iperf3 over UDP. Additional switches on the command enable the user to specify the data format, test for bidirectional bandwidth, alter TCP window size, specify different ports, and specify segment size. ("Using iPerf to Baseline Network Performance," Controlup.com, n.d.)

As a basic example of running iperf3, the windows 10 version of the software was downloaded on two systems on my home network. ("IPERF - The Easy Tutorial," openmaniak.com, n.d.)

One machine was set up to act as a server, by means of running the command "iperf3 -s" while the other machine acted as the client on which the tests were run.

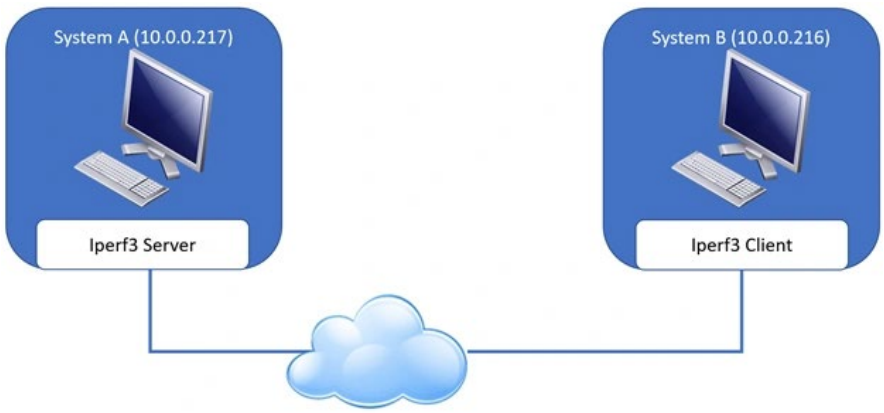

Figure 7: iperf server – client setup

(Source: https://www.controlup.com/resources/blog/entry/using-iperf-to-baseline-network-performance/)

Firstly a TCP test was run via the command "iperf3 – c 10.171.203.200 -t 30" which sent packets to the server for 30 seconds. The following results were returned, indicating a maximum bandwidth of 15.8Mbits/sec

```
C:\Users\Petros\Downloads\IPERF>iperf3 -c 10.171.203.200 -t 30
Connecting to host 10.171.203.200, port 5201
[  4] local 10.171.203.50 port 62007 connected to 10.171.203.200 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.00   sec  2.12 MBytes  17.7 Mbits/sec
[  4]   1.00-2.01   sec  2.12 MBytes  17.7 Mbits/sec
[  4]   2.01-3.01   sec  1.62 MBytes  13.7 Mbits/sec
[  4]   3.01-4.01   sec  2.00 MBytes  16.8 Mbits/sec
[  4]   4.01-5.01   sec  1.75 MBytes  14.7 Mbits/sec
[  4]   5.01-6.00   sec  1.88 MBytes  15.8 Mbits/sec
[  4]   6.00-7.01   sec  2.00 MBytes  16.7 Mbits/sec
[  4]   7.01-8.01   sec  1.75 MBytes  14.6 Mbits/sec
[  4]   8.01-9.01   sec  1.88 MBytes  15.8 Mbits/sec
[  4]   9.01-10.01  sec  2.00 MBytes  16.7 Mbits/sec
[  4]  10.01-11.00  sec  2.25 MBytes  19.1 Mbits/sec
[  4]  11.00-12.01  sec  2.12 MBytes  17.7 Mbits/sec
[  4]  12.01-13.00  sec  2.12 MBytes  18.0 Mbits/sec
[  4]  13.00-14.01  sec  2.38 MBytes  19.8 Mbits/sec
[  4]  14.01-15.01  sec  2.25 MBytes  18.8 Mbits/sec
[  4]  15.01-16.01  sec  1.25 MBytes  10.5 Mbits/sec
[  4]  16.01-17.01  sec  1.50 MBytes  12.6 Mbits/sec
[  4]  17.01-18.00  sec  1.62 MBytes  13.7 Mbits/sec
[  4]  18.00-19.00  sec  2.00 MBytes  16.8 Mbits/sec
[  4]  19.00-20.00  sec  1.88 MBytes  15.7 Mbits/sec
[  4]  20.00-21.01  sec  1.75 MBytes  14.7 Mbits/sec
[  4]  21.01-22.01  sec  2.00 MBytes  16.7 Mbits/sec
[  4]  22.01-23.01  sec  1.75 MBytes  14.6 Mbits/sec
[  4]  23.01-24.01  sec  1.62 MBytes  13.7 Mbits/sec
[  4]  24.01-25.00  sec  1.75 MBytes  14.7 Mbits/sec
[  4]  25.00-26.01  sec  1.75 MBytes  14.5 Mbits/sec
[  4]  26.01-27.01  sec  2.25 MBytes  18.9 Mbits/sec
[  4]  27.01-28.01  sec  2.00 MBytes  16.9 Mbits/sec
[  4]  28.01-29.01  sec  1.25 MBytes  10.5 Mbits/sec
[  4]  29.01-30.01  sec  1.75 MBytes  14.7 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-30.01  sec  56.4 MBytes  15.8 Mbits/sec                  sender
[  4]   0.00-30.01  sec  56.3 MBytes  15.7 Mbits/sec                  receiver
```

Figure 8: iperf TCP test demo

The test was also ran for a UDP connection, using the command "iperf3 -c 10.171.203.200 -u -t 30" which returned the following results, measuring an average bandwidth of 1.05Mbits/sec and a jitter value of 2.724ms with no packets lost.

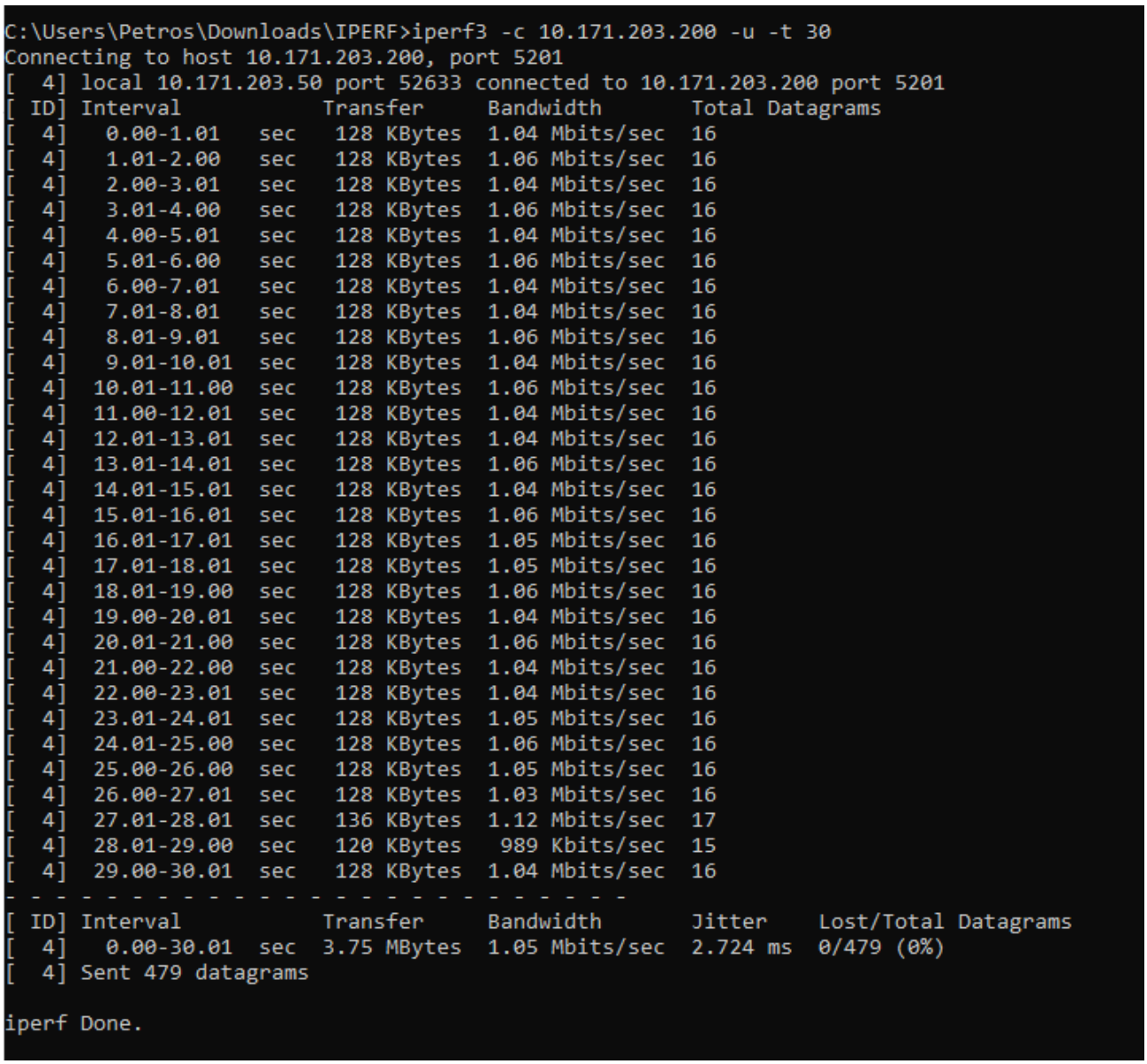

Figure 9: iperf UDP test demo

4.2 Performance Testing

4.2.1 Tests in VMware player

The tests were undertaken in my home network, with the centerpiece being an Ubuntu 18.04 Server installed inside a virtual machine using VMWare Workstation 15 Player. An OpenVPN server was established on this machine, with considerable help from Drake (2018). A regular Ubuntu 18.04 virtual machine was also setup which acted as the OpenVPN client machine. Iperf was installed on both machines and TCP testing was undertaken once the OpenVPN tunnel was in place. Tests were run with the TCP window size being changed, from 32K to 1024k. The results can be seen in the table below:

Requested Window Size	Actual Window Size	Data Transferred in 10s	Average Bandwidth
32K	62.5K	39.6MB	33.0 Mbits /s
64K	125K	47.2MB	39.6 Mbits / s
128K	**250K**	**51.2MB**	**42.8 Mbits / s**
256K	416K	48.9MB	40.7 Mbits / s
512K	416K	47.8MB	39.7 Mbits / s
1024K	416K	50.9MB	42.4 Mbits / s

Table 1: Iperf TCP Results OpenVPN

From the above results, it would appear that despite what our requested TCP window size was, iperf will assign values on the basis of certain criteria. In this instance, it seems that the largest window size that can be handled by the virtual machine under study is 416K. When the requested window size was 128K, the system yielded the best results, with 51.2MB being transferred over 10 seconds, with an average bandwidth of 42.8Mbits/s.

In the screen captures below, we can see the client screens for each of the TCP tests:

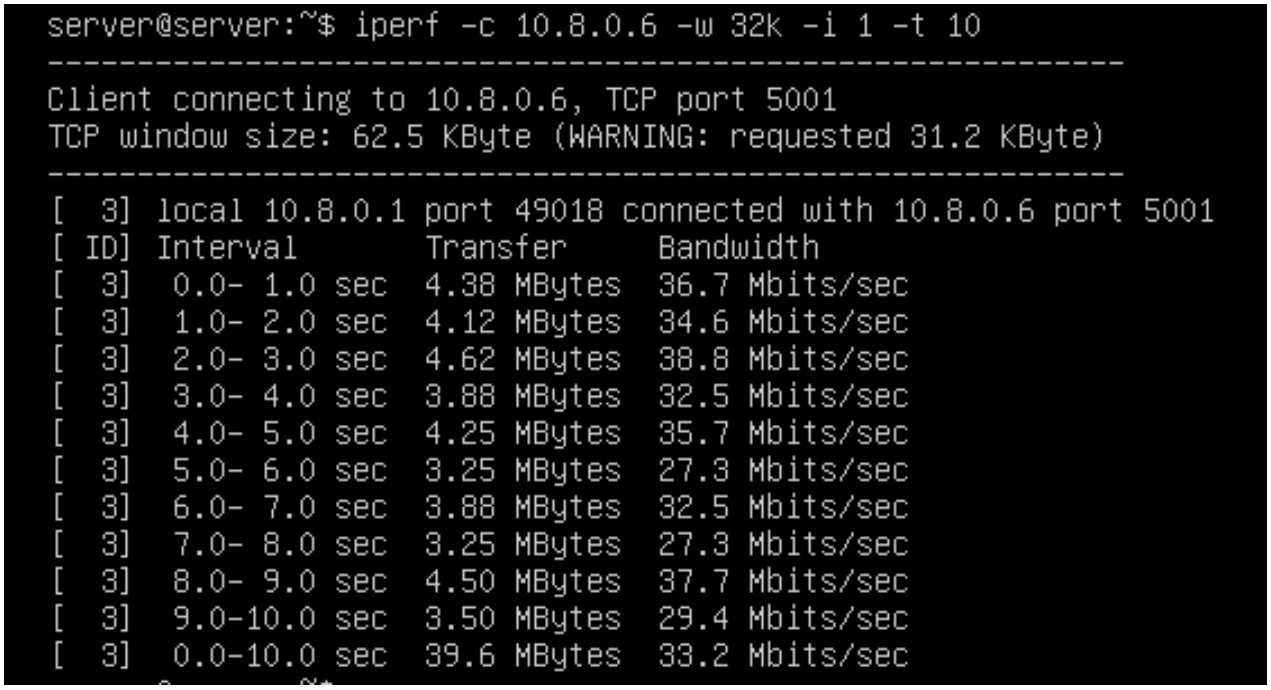

Figure 10: Iperf TCP test 32K window size (client side) OpenVPN

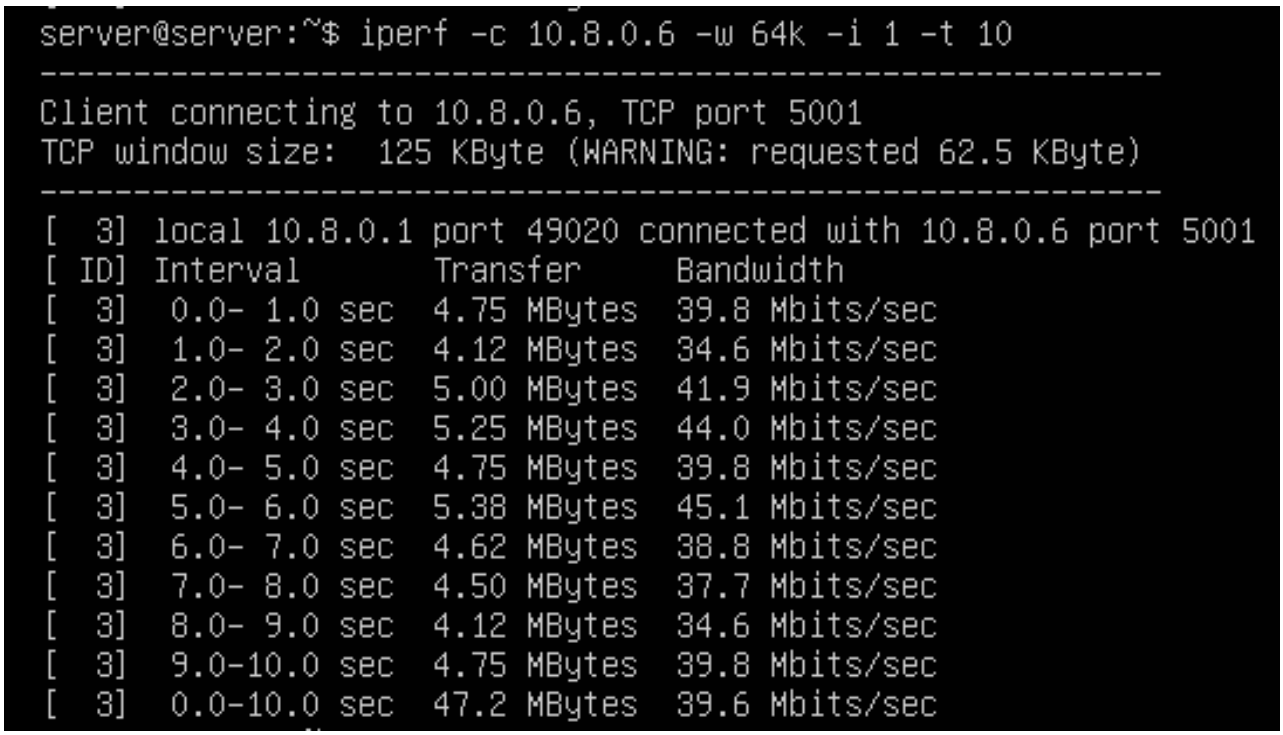

Figure 11: Iperf TCP test 64K window size (client side) OpenVPN

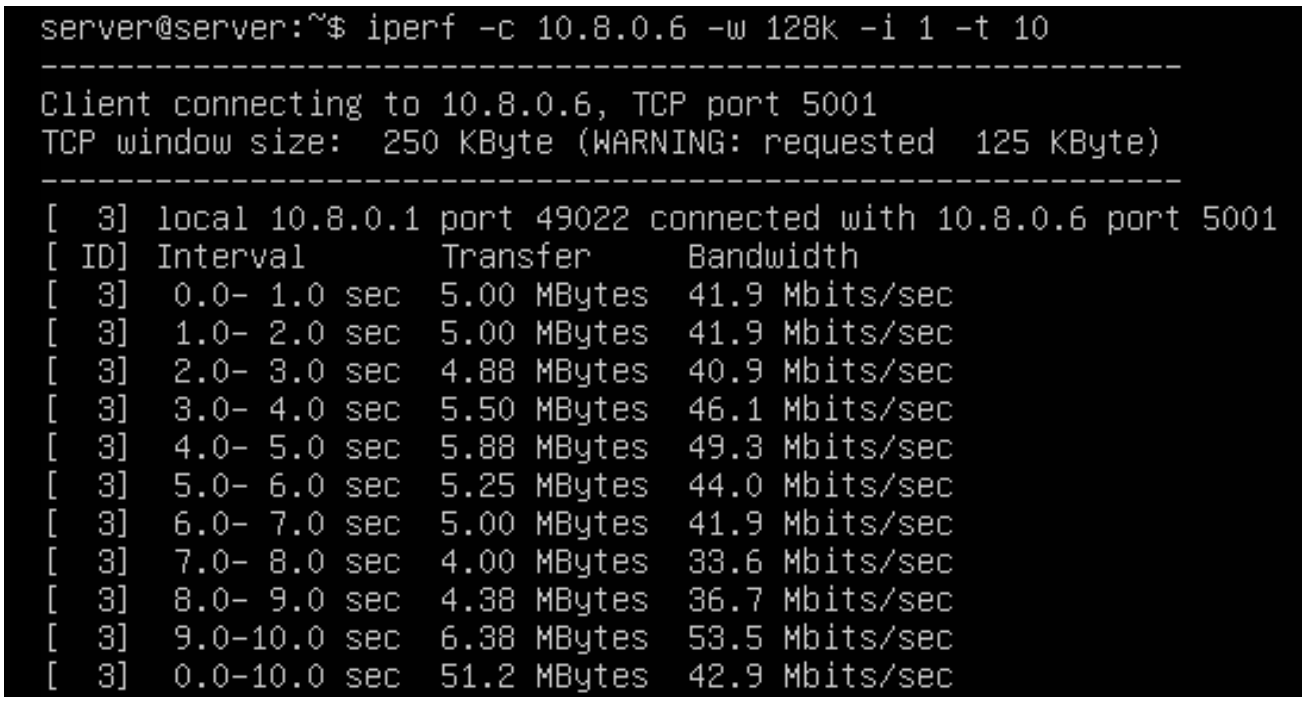

Figure 12: Iperf TCP test 128K window size (client side) OpenVPN

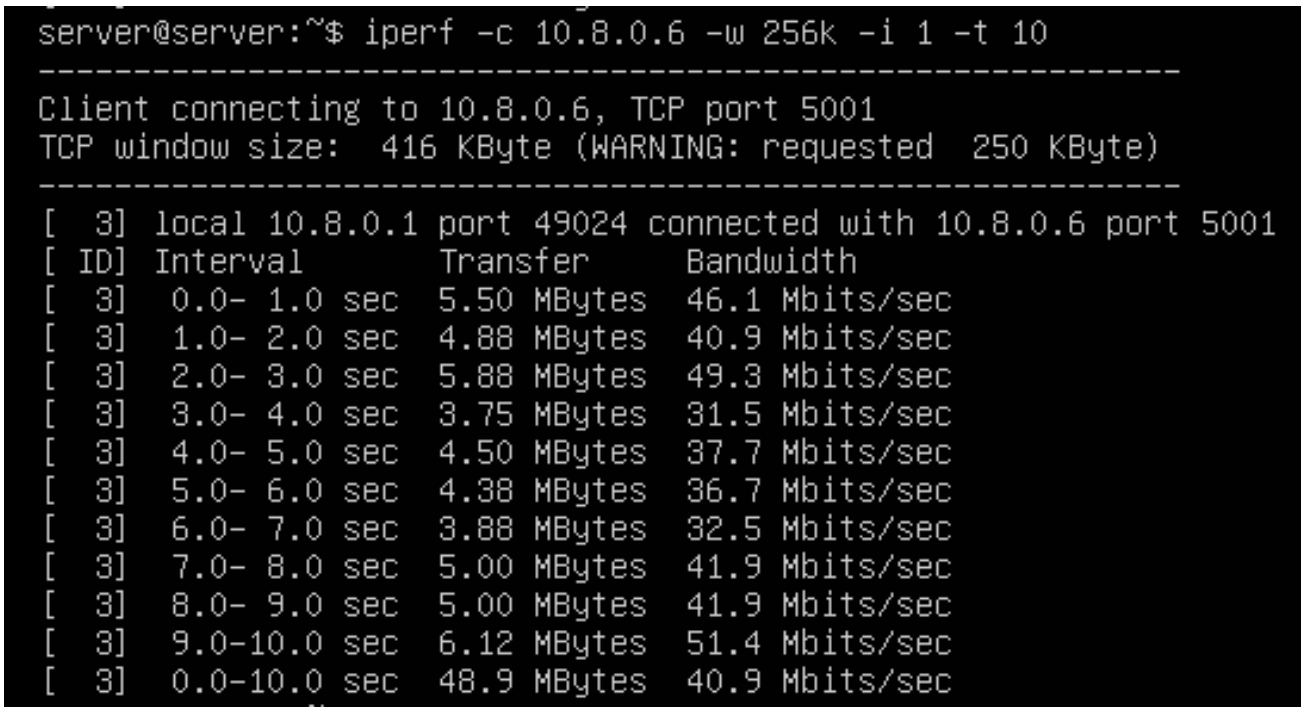

Figure 13: Iperf TCP test 256K window size (client side) OpenVPN

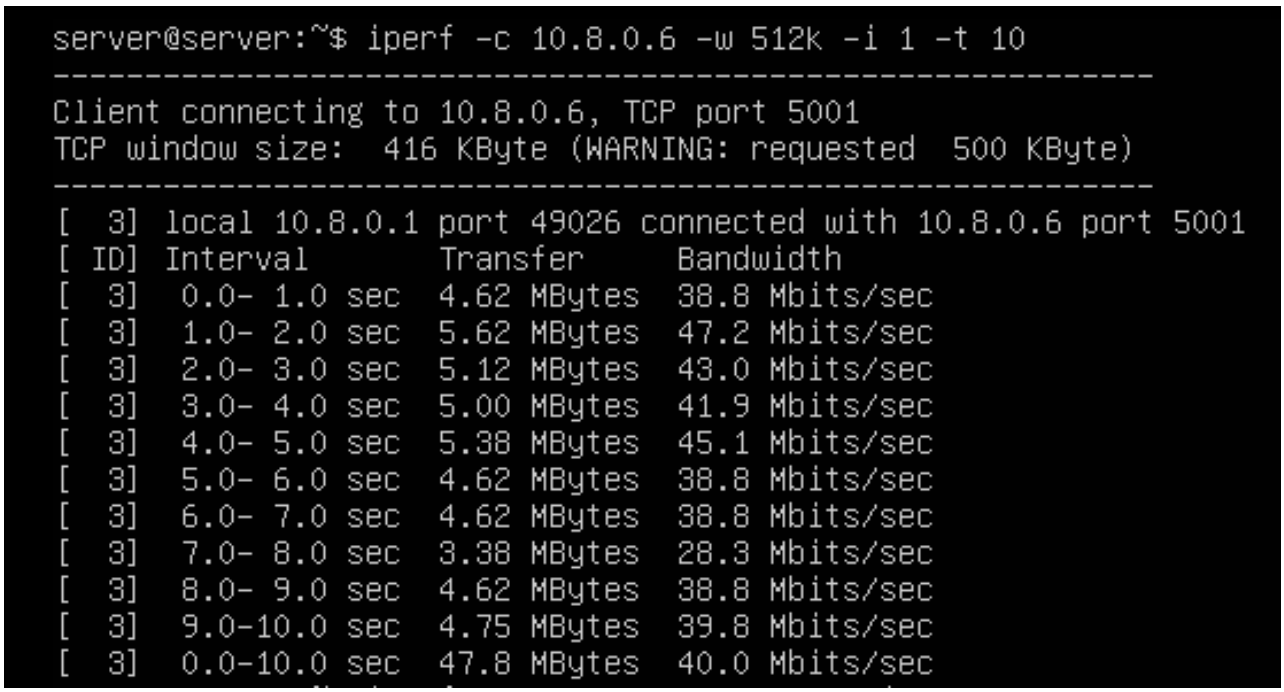

Figure 14: Iperf TCP test 512K window size (client side) OpenVPN

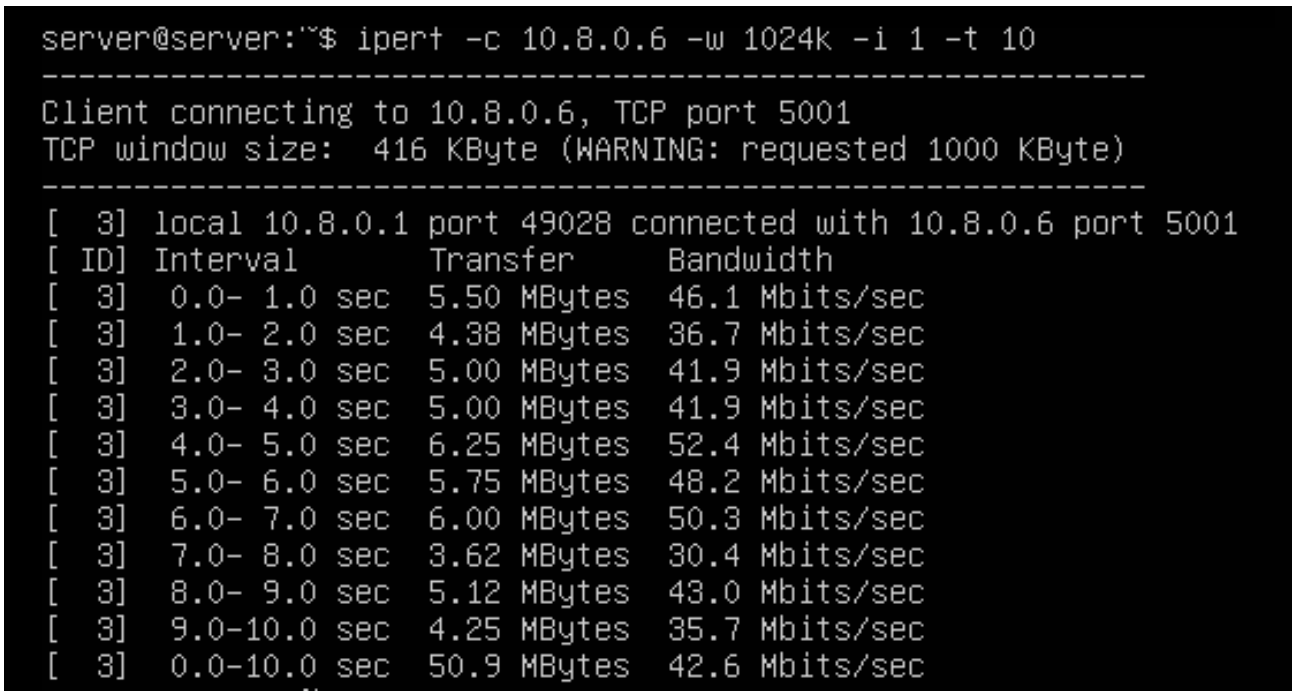

Figure 15: Iperf TCP test 1024K window size (client side) OpenVPN

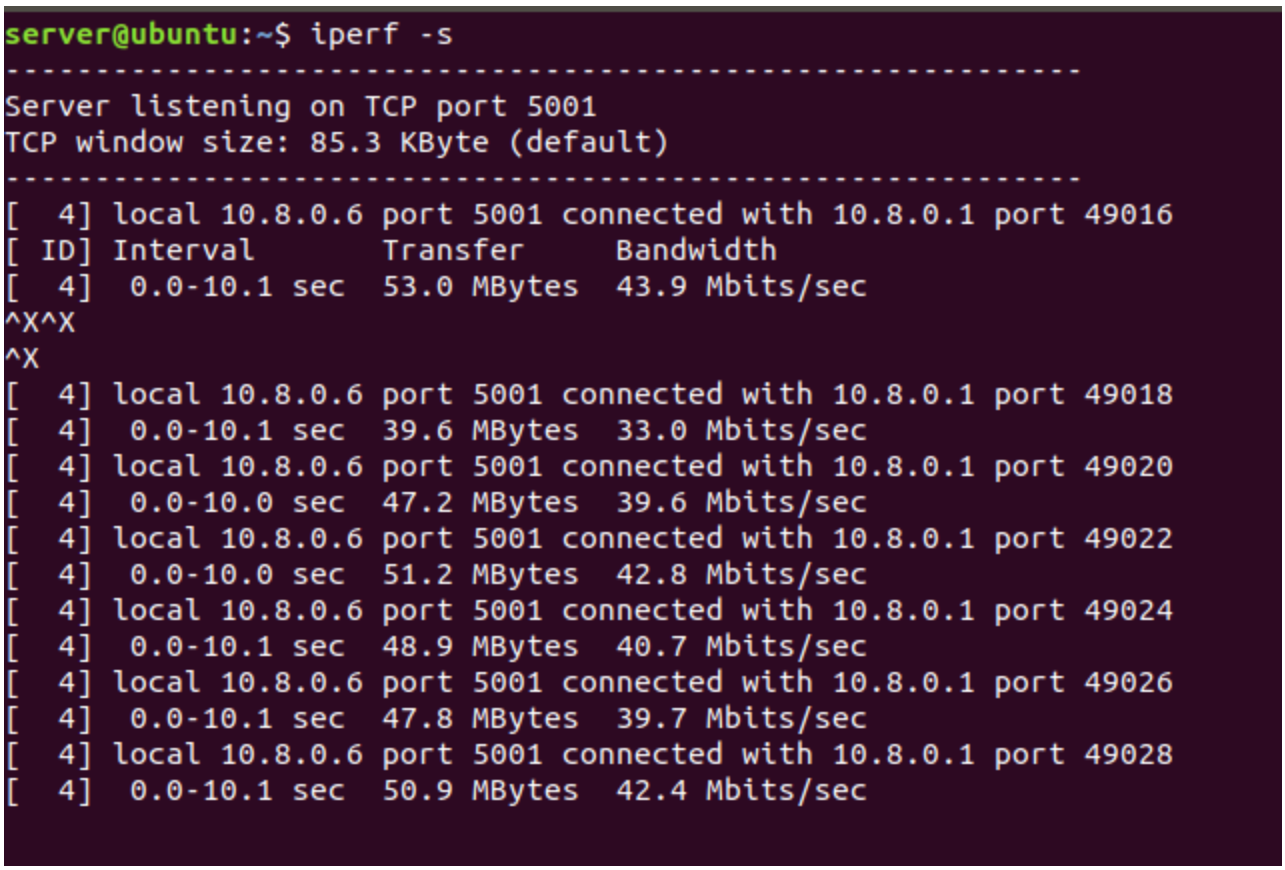

Figure 16: Iperf TCP test results server side OpenVPN

Next, a series of UDP tests were run in order to assess jitter in our connection. Our results can be viewed in the table below:

Requested Window Size	Data Transferred in 10s	Average Bandwidth	Jitter
32K	1.25MB	1.05 Mbits /s	1.003ms
64K	1.25MB	1.05 Mbits / s	1.143ms
128K	**1.25MB**	**1.05 Mbits / s**	**0.580ms**
256K	1.25MB	1.05 Mbits / s	0.654ms
512K	1.25MB	1.05 Mbits / s	0.940ms

1024K	1.25MB	1.05 Mbits / s	1.109ms

Table 2: Iperf UDP results OpenVPN

The results point to the fact that, once again, the packet size of 128K is the most efficient performer, with jitter limited to 0.580, considerably smaller than the other packet sizes except 256K which performs marginally worse than 128K.

In the screen captures below, we can see the client screens for each of the UDP tests, with the server report preceding all of them:

```
server@ubuntu:~$ iperf -s -u
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 10.8.0.6 port 5001 connected with 10.8.0.1 port 41541
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagram
s
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   1.003 ms    0/  893 (0%)
[  4] local 10.8.0.6 port 5001 connected with 10.8.0.1 port 43474
[  4]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   1.143 ms    0/  893 (0%)
[  3] local 10.8.0.6 port 5001 connected with 10.8.0.1 port 47238
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   0.580 ms    0/  893 (0%)
[  4] local 10.8.0.6 port 5001 connected with 10.8.0.1 port 37668
[  4]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   0.654 ms    0/  893 (0%)
[  3] local 10.8.0.6 port 5001 connected with 10.8.0.1 port 58475
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   0.940 ms    0/  893 (0%)
[  4] local 10.8.0.6 port 5001 connected with 10.8.0.1 port 45172
[  4]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   1.109 ms    0/  893 (0%)
```

Figure 17: Iperf UDP test (server side) OpenVPN

```
[  3]  0.0- 1.0 sec   131 KBytes  1.07 Mbits/sec
[  3]  1.0- 2.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  2.0- 3.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  3.0- 4.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  4.0- 5.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  5.0- 6.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  6.0- 7.0 sec   129 KBytes  1.06 Mbits/sec
[  3]  7.0- 8.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  8.0- 9.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  9.0-10.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  3] Sent 893 datagrams
[  3] Server Report:
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   0.000 ms    0/  893 (0%)
```

Figure 18: Jperf UDP test 32K window size (client side) OpenVPN

```
server@server:~$ iperf -c 10.8.0.6 -u -w 64k -i 1 -t 10
------------------------------------------------------------
Client connecting to 10.8.0.6, UDP port 5001
Sending 1470 byte datagrams, IPG target: 11215.21 us (kalman adjust)
UDP buffer size:  125 KByte (WARNING: requested 62.5 KByte)
------------------------------------------------------------
[  3] local 10.8.0.1 port 43474 connected with 10.8.0.6 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 1.0 sec   131 KBytes  1.07 Mbits/sec
[  3]  1.0- 2.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  2.0- 3.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  3.0- 4.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  4.0- 5.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  5.0- 6.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  6.0- 7.0 sec   129 KBytes  1.06 Mbits/sec
[  3]  7.0- 8.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  8.0- 9.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  9.0-10.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  3] Sent 893 datagrams
[  3] Server Report:
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   0.000 ms    0/  893 (0%)
```

Figure 19: Iperf UDP test 64K window size (client side) OpenVPN

```
server@server:~$ iperf -c 10.8.0.6 -u -w 128k -i 1 -t 10
------------------------------------------------------------
Client connecting to 10.8.0.6, UDP port 5001
Sending 1470 byte datagrams, IPG target: 11215.21 us (kalman adjust)
UDP buffer size:  250 KByte (WARNING: requested  125 KByte)
------------------------------------------------------------
[  3] local 10.8.0.1 port 47238 connected with 10.8.0.6 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 1.0 sec   131 KBytes  1.07 Mbits/sec
[  3]  1.0- 2.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  2.0- 3.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  3.0- 4.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  4.0- 5.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  5.0- 6.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  6.0- 7.0 sec   129 KBytes  1.06 Mbits/sec
[  3]  7.0- 8.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  8.0- 9.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  9.0-10.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  3] Sent 893 datagrams
[  3] Server Report:
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   0.000 ms    0/  893 (0%)
server@server:~$
```

Figure 20: Iperf UDP test 128K window size (client side) OpenVPN

```
server@server:~$ iperf -c 10.8.0.6 -u -w 256k -i 1 -t 10
------------------------------------------------------------
Client connecting to 10.8.0.6, UDP port 5001
Sending 1470 byte datagrams, IPG target: 11215.21 us (kalman adjust)
UDP buffer size:  416 KByte (WARNING: requested  250 KByte)
------------------------------------------------------------
[  3] local 10.8.0.1 port 37668 connected with 10.8.0.6 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 1.0 sec   131 KBytes  1.07 Mbits/sec
[  3]  1.0- 2.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  2.0- 3.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  3.0- 4.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  4.0- 5.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  5.0- 6.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  6.0- 7.0 sec   129 KBytes  1.06 Mbits/sec
[  3]  7.0- 8.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  8.0- 9.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  9.0-10.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  3] Sent 893 datagrams
[  3] Server Report:
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   0.000 ms    0/  893 (0%)
server@server:~$ _
```

Figure 21: Iperf UDP test 256K window size (client side) OpenVPN

```
server@server:~$ iperf -c 10.8.0.6 -u -w 512k -i 1 -t 10
------------------------------------------------------------
Client connecting to 10.8.0.6, UDP port 5001
Sending 1470 byte datagrams, IPG target: 11215.21 us (kalman adjust)
UDP buffer size:  416 KByte (WARNING: requested  500 KByte)
------------------------------------------------------------
[  3] local 10.8.0.1 port 58475 connected with 10.8.0.6 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 1.0 sec   131 KBytes  1.07 Mbits/sec
[  3]  1.0- 2.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  2.0- 3.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  3.0- 4.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  4.0- 5.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  5.0- 6.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  6.0- 7.0 sec   129 KBytes  1.06 Mbits/sec
[  3]  7.0- 8.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  8.0- 9.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  9.0-10.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  3] Sent 893 datagrams
[  3] Server Report:
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec   0.000 ms    0/  893 (0%)
server@server:~$
```

Figure 22: Iperf UDP test 512K window size (client side) OpenVPN

i

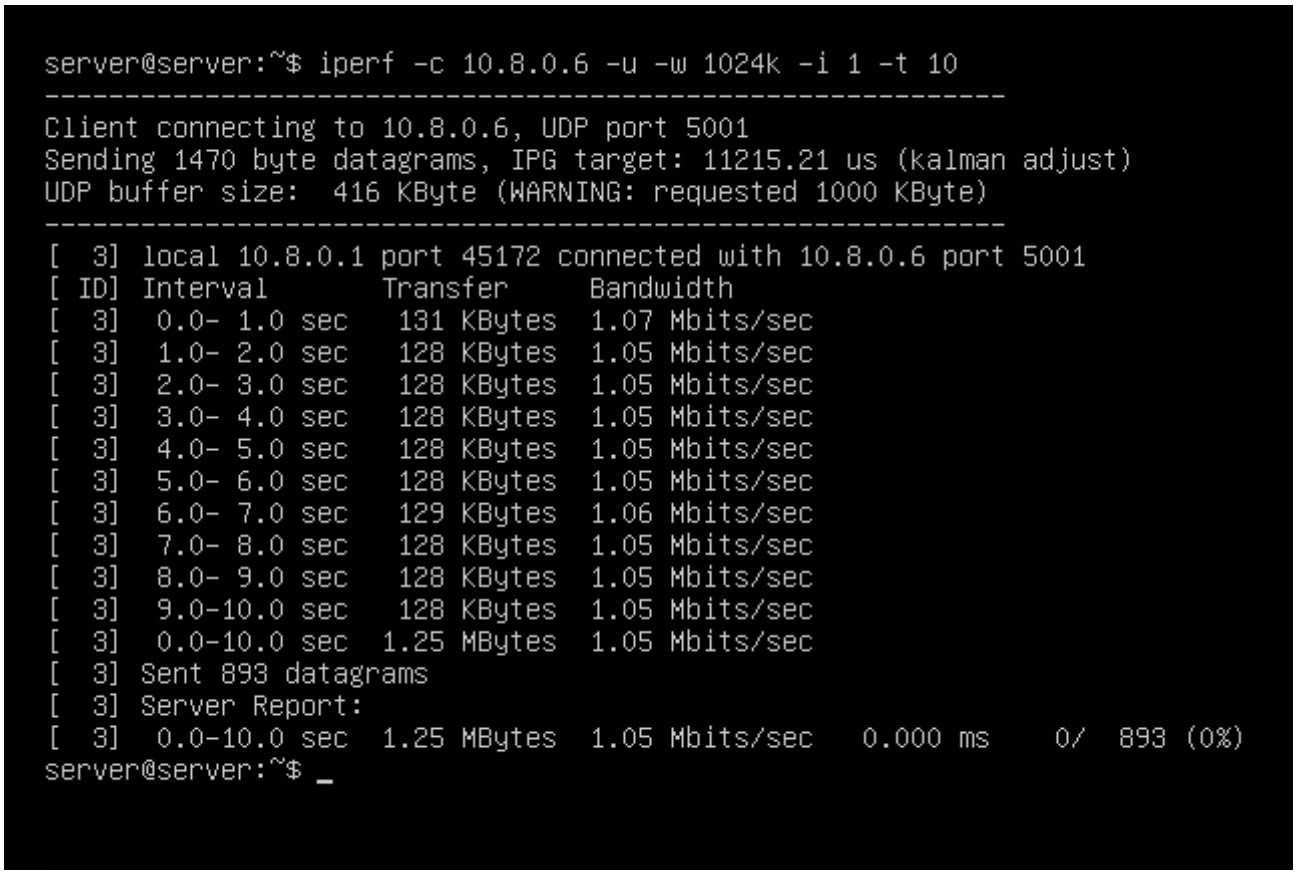

Figure 23: Iperf UDP test 1024K window size (client side) OpenVPN

For reasons of comparability, similar tests were ran using the standard IP addresses assigned to the virtual machines, in order to assess connection speeds without using a VPN tunnel. The results for TCP tests are summarized in the table below:

Requested Window Size	Window Size	Data Transferred in 10s	Avg Bandwidth
32K	62.5K	57.2 MB	47.8 Mbits /s
64K	125K	81.6MB	68.1 Mbits / s
128K	250K	105MB	87.5Mbits / s
256K	416K	106MB	89.0Mbits / s

512K	**416K**	**109MB**	**90.8Mbits / s**
1024K	416K	102MB	85.8Mbits / s

Table 3: Iperf TCP results – standard connection

```
server@ubuntu:~$ iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
[  4] local 192.168.1.246 port 5001 connected with 192.168.1.241 port 39430
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.1 sec  57.2 MBytes  47.8 Mbits/sec
[  4] local 192.168.1.246 port 5001 connected with 192.168.1.241 port 39434
[  4]  0.0-10.1 sec  81.6 MBytes  68.1 Mbits/sec
[  4] local 192.168.1.246 port 5001 connected with 192.168.1.241 port 39436
[  4]  0.0-10.0 sec   105 MBytes  87.5 Mbits/sec
[  4] local 192.168.1.246 port 5001 connected with 192.168.1.241 port 39438
[  4]  0.0-10.0 sec   106 MBytes  89.0 Mbits/sec
[  4] local 192.168.1.246 port 5001 connected with 192.168.1.241 port 39440
[  4]  0.0-10.0 sec   109 MBytes  90.8 Mbits/sec
[  4] local 192.168.1.246 port 5001 connected with 192.168.1.241 port 39442
[  4]  0.0-10.0 sec   102 MBytes  85.8 Mbits/sec
```

Figure 24: Iperf TCP results (server side) Standard Connection

It is evident from these figures that as expected, the standard, non-tunneled connection outperforms OpenVPN with considerably larger speeds and data transferred for the same window size. In our test the 512K window size proved out to be the most efficient one, transferring 109MB at a rate of 90.8Mbits/s.

WINDOW SIZE	DATA STANDARD	DATA OPEN VPN	OPENVPN to STANDARD	SPEED STANDARD	SPEED OPENVPN	OPENVPN to STANDARD
32K	57.2	39.6	69.2%	47.8	33	69.0%
64K	81.6	47.2	57.8%	68.1	39.6	58.1%
128K	105	51.2	48.8%	87.5	42.8	48.9%
256K	106	48.9	46.1%	89	40.7	45.7%
512K	109	47.8	43.9%	90.8	39.7	43.7%
1024K	102	50.9	49.9%	85.8	42.4	49.4%

Table 4: Standard Connection Vs. OpenVPN TCP performance

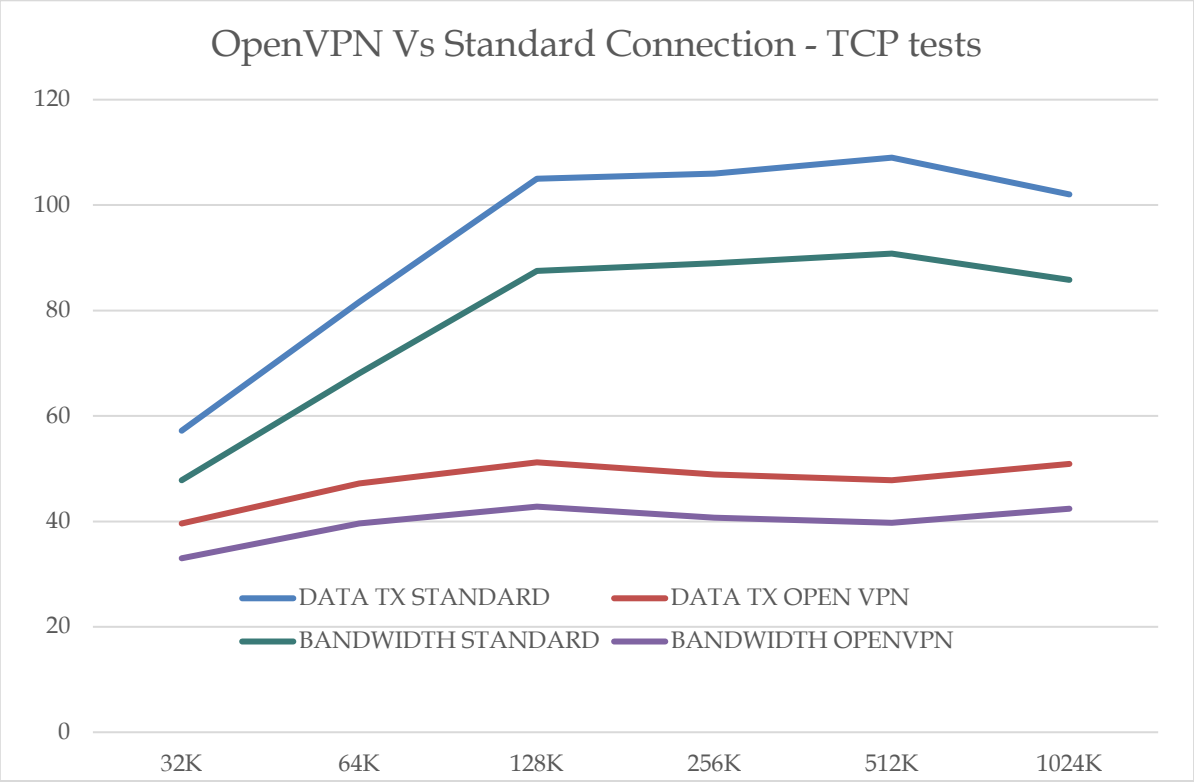

Figure 25: OpenVPN vs Standard Connection TCP tests

As stated above, figure 24 clearly indicates that the standard connection is hands down the better performer among the two protocols and its performance peaks at 512K. OpenVPN peaks at 128K slumps at 256K and 512K and seems to be recovering at 1024K.

Turning to the UDP side of things, the table below presents the performance of the standard connection with respect to jitter:

Requested Window Size	Data Transferred in 10s	Average Bandwidith	Jitter
32K	1.25MB	1.05 Mbits /s	0.137ms
64K	1.25MB	1.05 Mbits / s	0.103ms

128K	1.25MB	1.05 Mbits / s	0.191ms
256K	1.25MB	1.05 Mbits / s	0.132ms
512K	1.25MB	1.05 Mbits / s	0.099ms
1024K	1.25MB	1.05 Mbits / s	0.131ms

Table 5: Iperf UDP results - standard connection

The results show that OpenVPN is more vulnerable to jitter than the non-tunneled connection which performs marginally better at the 512K window size vis-à-vis other window sizes. As might be expected, the standard connection outperforms OpenVPN on all window sizes.

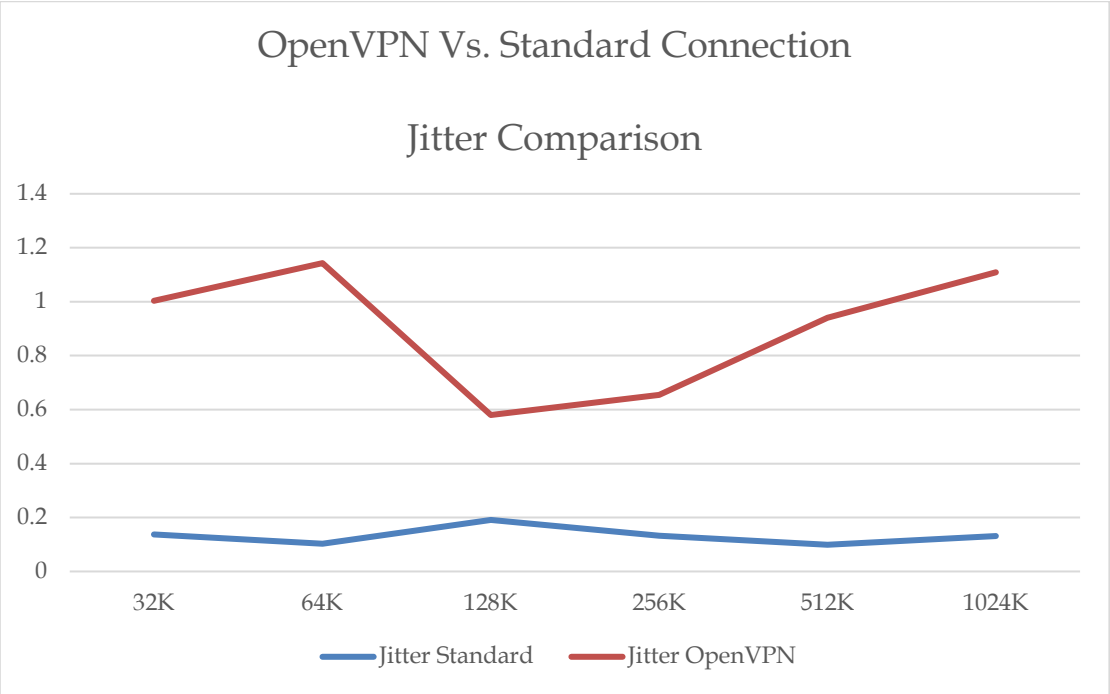

Figure 26: OpenVPN vs Standard Connection UDP tests

4.2.2 OUC Cyber Range labs tests

Separate tests were run in the cyber range established at OUC labs, for the purposes of comparing the performance of different connectivity options, in order to feed into the research presented in Peratikou et al (2021).

As it was rather difficult for me to replicate locally the elaborate environments set up in the OUC labs the results of those tests were made available to me for the purposes of this postgraduate dissertation and are presented below:

Window Size	Throughput (Standard)	Throughput (OpenVPN)	Throughput (IPSEC)
128K	1.985	1.715	1.78
256K	5.55	4.22	4.57
512K	12	10.4	10.9
1024K	25.1	19.45	20.85

Table 6: OUC Lab Raw TCP tests – Standard, OpenVPN and IPSEC connections

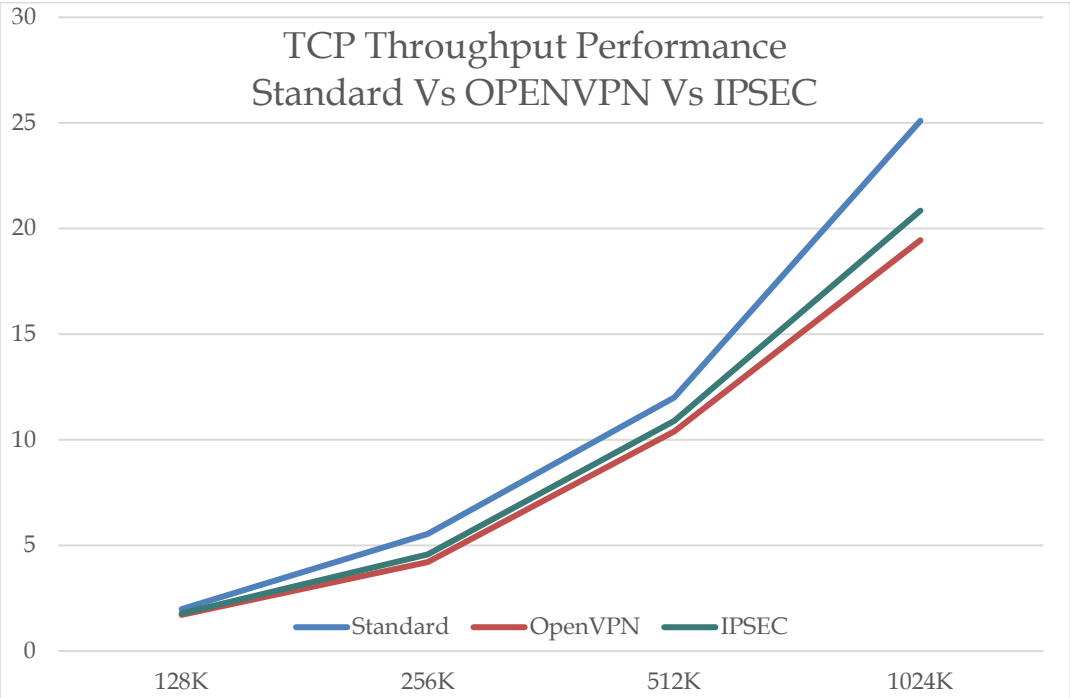

Figure 27: OUC Lab Raw TCP Test results (throughput)

As expected, the standard connection is the best performer, whereas OpenVPN and IPSEC present the speed loss that one normally associates with VPN connections. Between the two VPN connections IPSEC would appear to be performing better especially when the window size increases to 1024K.

UDP tests results for jitter with a fixed bandwidth of 1500 and their outcome is presented below:

Window Size	Jitter (Standard)	Jitter (OpenVPN)	Jitter (IPSEC)
128K	0.017	0.478	0.306
256K	0.01	0.634	**0.242**
512K	0.005	0.418	0.382
1024K	0.013	0.635	0.668

Table 7: OUC Lab UDP Jitter results

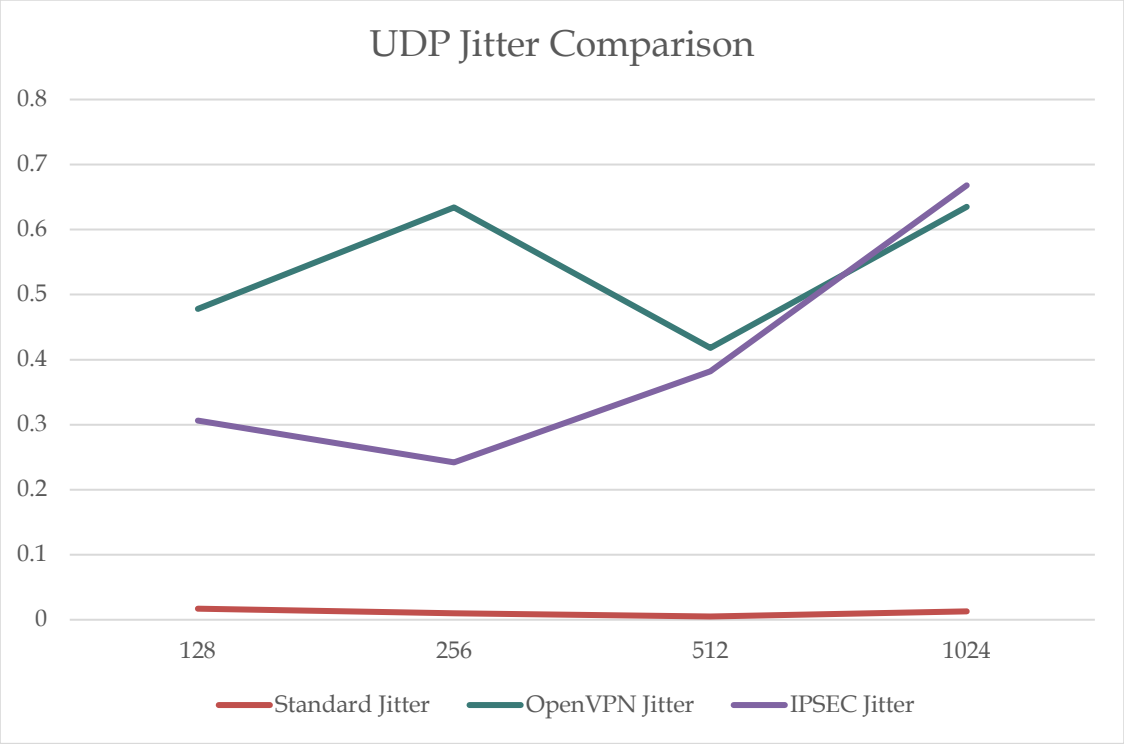

Figure 28: OUC Lab Jitter Comparison

As in the TCP tests, also in UDP it would appear that the standard non-tunneled connection is immune to the perils associated with jitter, only barely recording negligible values. The two tunneled connections do however display considerably higher jitter values, with the IPSEC tunnel appearing as the most efficient one, at least for all window sizes smaller than 1024K, where the OpenVPN tunnel registers a negligibly smaller jitter value.

Peratikou et al. carried this work forward in their paper by explaining that "iperf3 is configured by default to take advantage of large packets and TCP window scaling" (Peratikou et al., 2021, p124). This introduces a certain bias into the results generated by iperf3. This bias is especially visible in packets of smaller size given the fact each packet takes a certain time to be processed, which basically requires more packets in order to deliver the same amount of data, and also required a higher rate of packets per second to achieve the same throughput. According to Soucy (n.d.), also cited in Peratikou et al, in order to compensate for this bias, a set of multipliers is applied to each window size of the iperf3 results. Peratikou et al. apply the multipliers to the raw data as presented in tables 6 and 7 above and arrive at the following "adjusted" rates:

Window Size	Multiplier	Adjusted Throughput (Standard)	Adjusted Throughput (OpenVPN)	Adjusted Throughput (IPSEC)
128K	1.6842	3.343	2.888	2.998
256K	1.2549	6.965	5.296	5.735
512K	1.1130	13.356	11.575	12.132
1024K	1.0535	26.443	20.148	21.966

Table 8: OUC Lab Multiplier Adjusted iperf TCP test results

The adjusted results, while somewhat equalizing out the picture, provide no major change to the initial assessment, namely that the standard, non-tunneled connection continues to outperform the two tunneled options, with once again IPSEC performing better than OpenVPN.

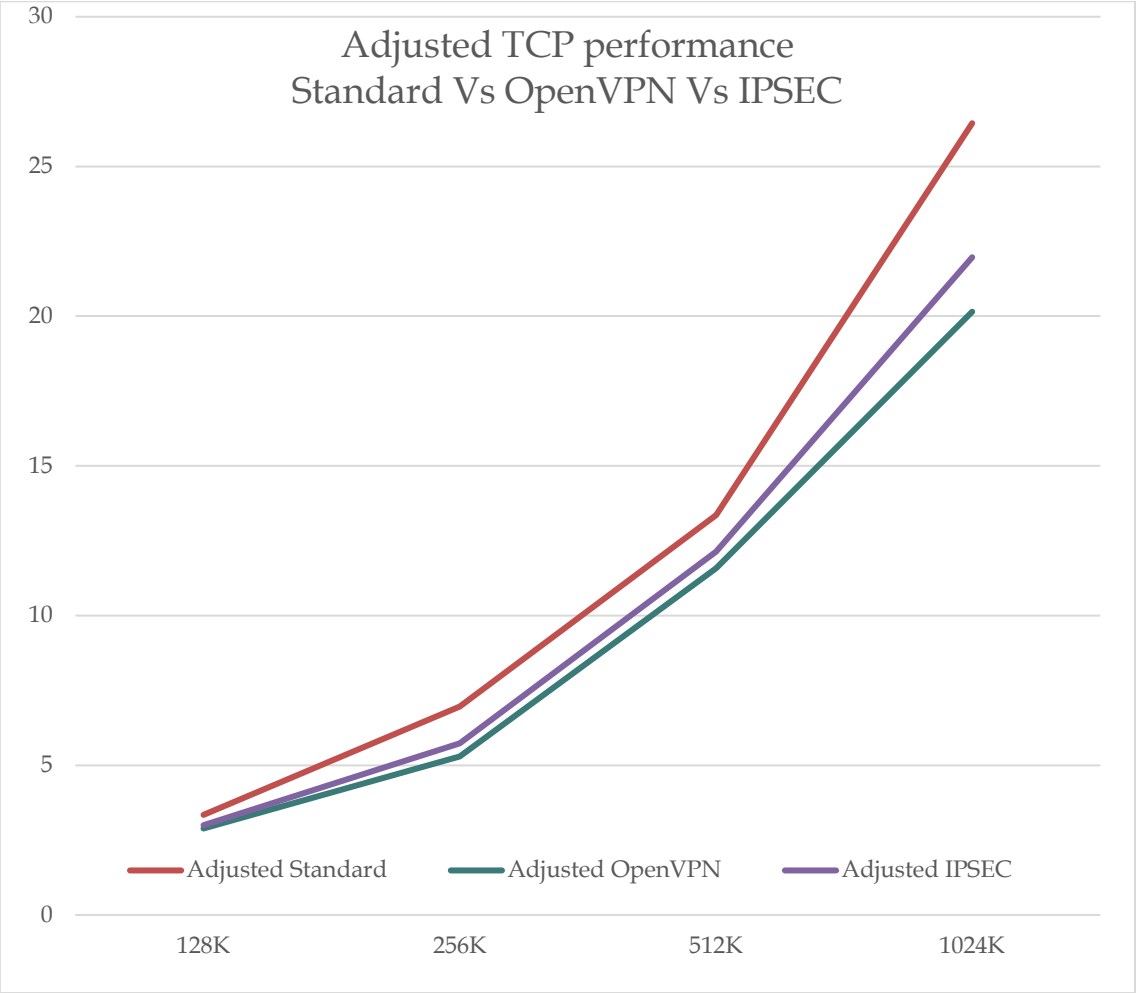

Figure 29: OUC Lab Multiplier Adjusted iperf TCP test results

These results are presented as percentages of each adjusted tunneled value compared to its adjusted counterpart of the standard connection as follows:

Window Size	Throughput (Adjusted Standard)	Throughput (Adjusted OpenVPN)	Adjusted Standard to adj. OpenVPN	Throughput (IPSEC)	Adjusted Standard to adj. ISPEC
128K	3.343	2.888	86.39%	2.998	89.68%
256K	6.965	5.296	76.04%	5.735	82.34%
512K	13.356	11.575	86.67%	12.132	**90.84%**

1024K	26.443	20.148	76.19%	21.966	83.07%

Table 8: Multiplier Adjusted iperf TCP results as percentages of Standard connection

Once again, the supremacy of IPSEC over OpenVPN is underlined, with IPSEC outperforming the efficiency of its rival in all window sizes, and with the 512K window size appearing to be the most efficient performer, registering a throughput equivalent to 91% of the one yielded by the standard connection. Peratikou et al conclude their study underlining that there is no discernible performance difference between the two protocols.

Chapter 5
Survey Research

5.1 Rationale

In preparing this paper on Federated Cyber Ranges, a clear shortage of relevant academic journals was identified, while a sufficient, but certainly not exhaustive body of work was found on the issue of Cyber Ranges in general. It was therefore deemed necessary to also assess the extent to which computer users were themselves aware of the concept.

5.2 Questionnaire

A questionnaire was determined to be the most appropriate method in assessing respondent's exposure to federations of cyber ranges. It was comprised of twenty-one multiple choice questions and was prepared using Google Forms, in the format of an online survey, in which setup there was no kind of logging whatsoever, so we are unable to assign responses to particular respondents, nor identify any of the participants. The survey starts with questions of a demographic nature (questions 1-3), followed by general computer/cyber security questions (questions 4 – 13) and concludes with questions relating to cyber ranges and federations (questions 14-21).

Using Google Forms ensured that users could easily be invited via an email, containing a link granting them access, in order to respond to the questionnaire. From a design point of view Google Forms comes with ready-made layouts, is very easy to use and guides the researcher in selecting the appropriate layout. Google Forms also prepares a graphical grouping of responses and allows the user to export all responses in a spreadsheet format, thereby facilitating further processing. It was made clear to users, both at the email invitation and in the disclaimer of the survey itself that this was a completely anonymous questionnaire – this stipulation can be considered as conducive to a more honest, and less reserved response.

5.3 Methodology

Given the nature of my employment in the Foreign Service of the Republic Cyprus, I thought that an appropriate sample of respondents could be found among my colleagues at the Ministry of Foreign Affairs of the Republic of Cyprus – I therefore reached out to Ministry staff of various tiers. I also tried to ensure that the sample included IT practitioners working in the Ministry of Foreign Affairs, as well as in other government departments whose work is related to Foreign Affairs. I also reached out to academics involved in various joint government – academia IT projects. A conscious effort was made to ensure the best possible gender balance.

Invitations to participate in the questionnaire were emailed to 80 participants, of which 59 chose to respond to the questionnaire, which was open for responses during the month of April 2021.

A copy of the questionnaire, including the disclaimer present at its beginning section - which participants were required to agree with before providing answers - can be found in Appendix A.

Chapter 6

Survey Analysis and Interpretation

6.1 Answers to the Questionnaire

Question 1 referred to Gender – Out of the 59 respondents, 25 were female and 34 were male, translating to 42.4% and 57.6% respectively.

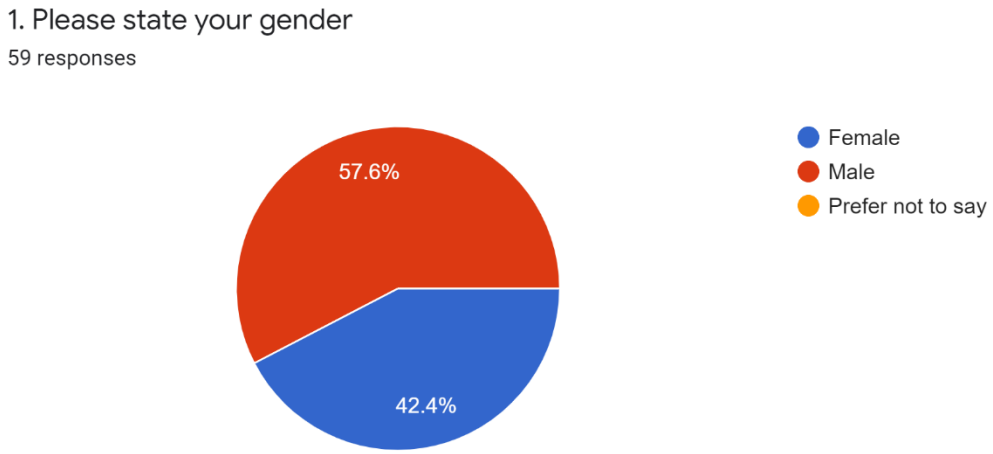

Figure 30 – Respondent's Gender

Question 2 referred to respondents' age group. Just one person was in the 18-30 cohort (1.7%), 31 persons in the 31-45 cohort (52.5%), 25 in the 46-60 age group (43.4%), while 2 respondents were over sixty years old (3.4%).

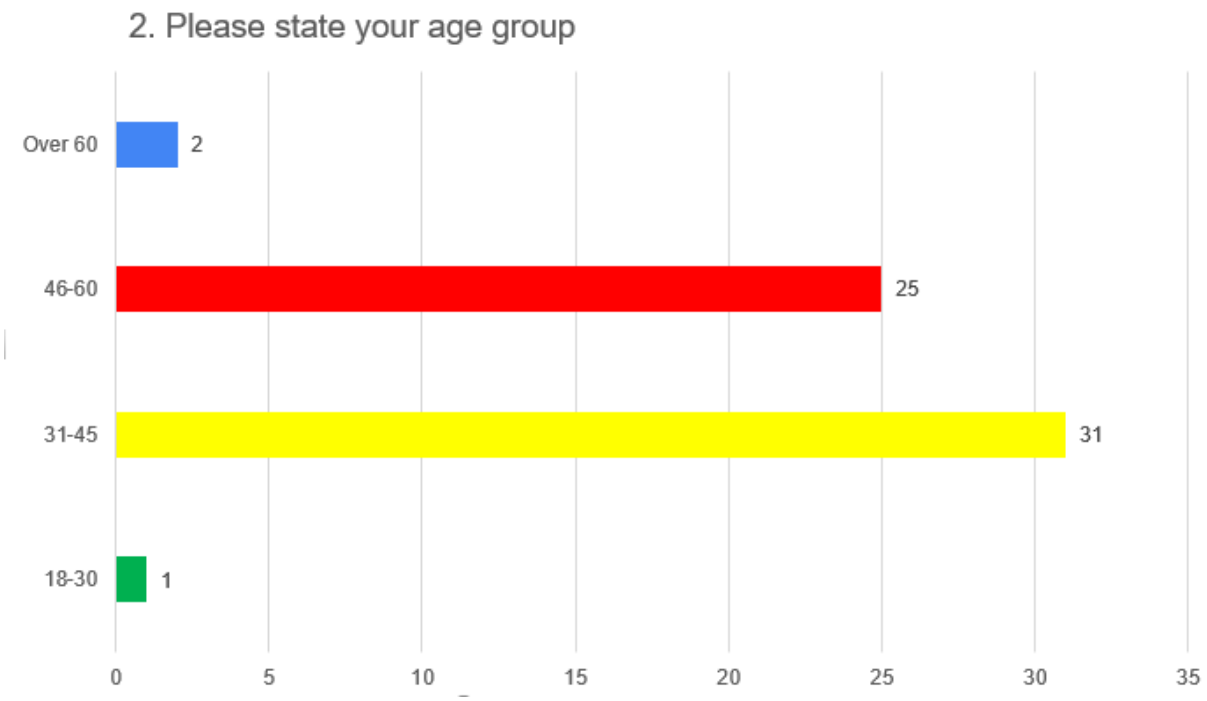

Figure 31 – Respondents' age groups

Question 3 sought to classify respondents on the basis of their work duties. 32 persons classified themselves as Professional, Scientific, or Academic (54.2%), 11 persons as Management (13.6%), 8 were Secretarial, Administrative or Security staff (13.6%), 6 respondents were working in IT (10.2%), and two either had other duties or were not employed (3.4%).

Figure 32 – Respondents' work duties

Question 4 asked respondents to classify their computer literacy level. 4 people identified themselves as basic users (6.8%), 32 as average users (54.2%), 13 as power users (22%), while 10 individuals classified their computer prowess to be at the level of an IT professional.

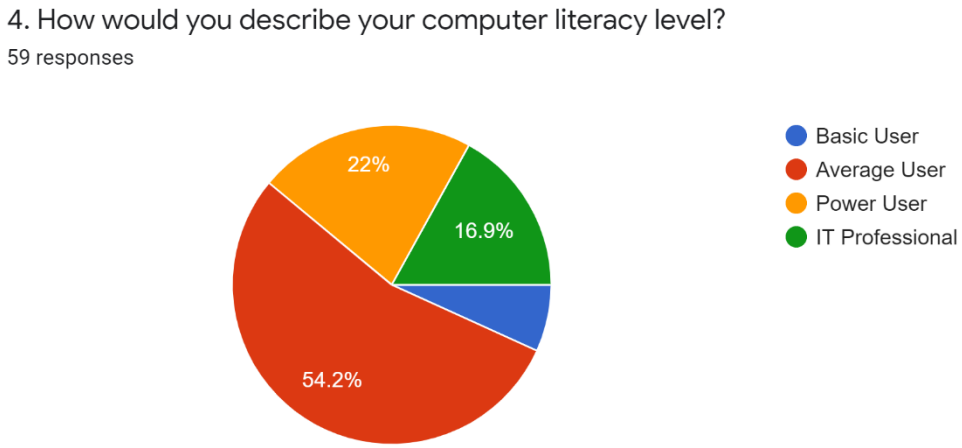

Figure 33 – Respondents' computer literacy level

In Question 5, relating to purpose of computer use, one person stated that they generally use computers for non-work related activities (1.7%), 10 persons use them for work related activities (16.9%) and everyone else, 48 people or 81.4% use them for both.

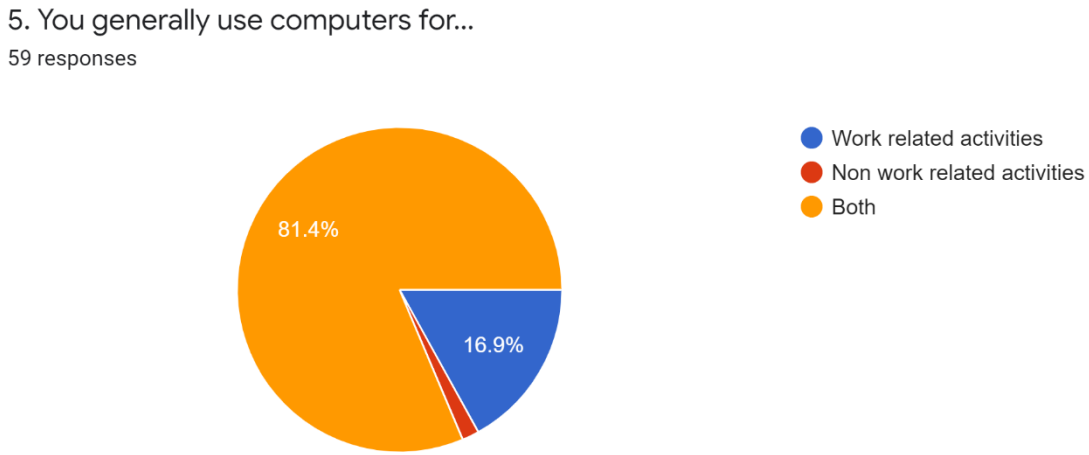

Figure 34 – Respondents' computer use purpose

Question 6 asked respondents if they were familiar with the term cyber security. All respondents bar one, were familiar with the term, translating to 98.3%.

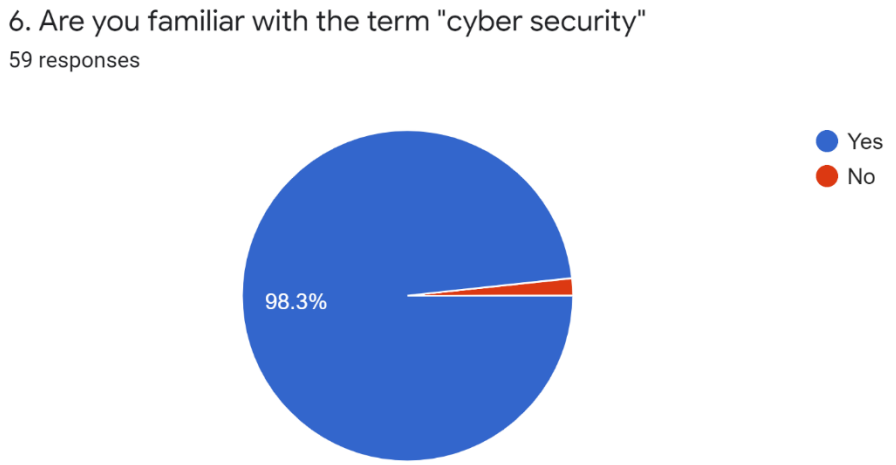

Figure 35 – Respondents' familiarity with the term "cyber security"

Question 7 required users to describe their actions for protecting against malicious activity. Two persons responded that it was not their job to worry about cyber security (3.4%), 26 persons answered that they rely on software already installed (44.1%) and 31 respondents (52.5%) felt that they proactively take steps to protect the privacy and sensitivity of their information.

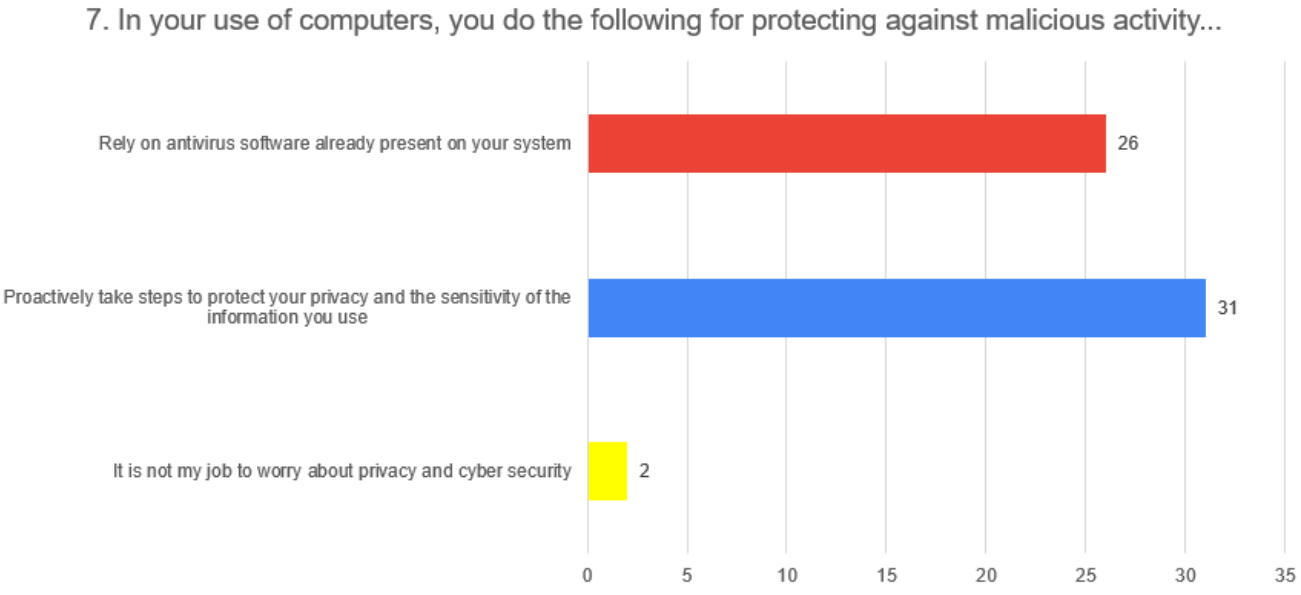

Figure 36 – Respondents' action against malicious activity

Question 8 referred to respondent's use of passwords across accounts. Four people (6.8%) responded that they have the same password which they use everywhere, 17 people said that they have a few easy to remember passwords (28.8%), 11 try to have a different password for each account (18.6%), 8 try to have a different password for each account and change it regularly (13.6%), 10 try to have a different complicated password for each account (16.9%) and another 9 said that they try to have a different complicated password for each account and change it regularly.

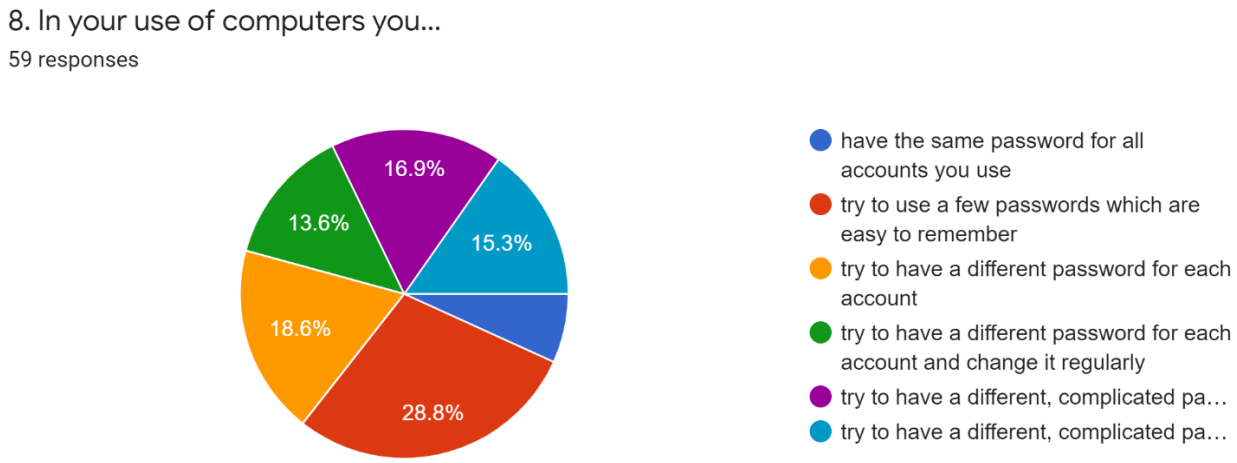

Figure 37 – Respondents' password usage

Question 9 tried to assess how respondents remember their passwords. 7 people replied that they only have one password and they have memorized it (11.9%). 6 persons stated that they have their passwords written down on a piece of paper (10.2%), 7 use their browser's memory to save passwords (11.9%), 8 use an online password manager (13.6), 4 use an offline password manager (6.8), while 27 persons stated that they use another method for remembering passwords (45.8%). With the benefit of hindsight, it could be commented that this particular option would have been better if it was an open-ended response of the form "Other – please specify" as it would have offered insights into what other methods respondents use.

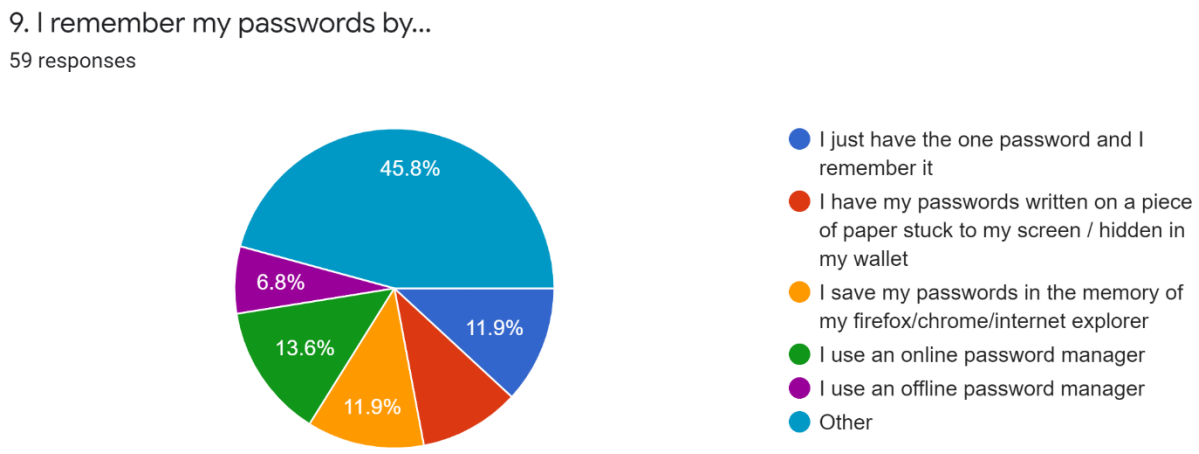

Figure 38 – Respondents' method for remembering passwords

Question 10 asked if respondents used encryption, with 24 of them responding that they did, 24 responding that they did not (40.7% each way) and 11 people said that they did not know (18.6%).

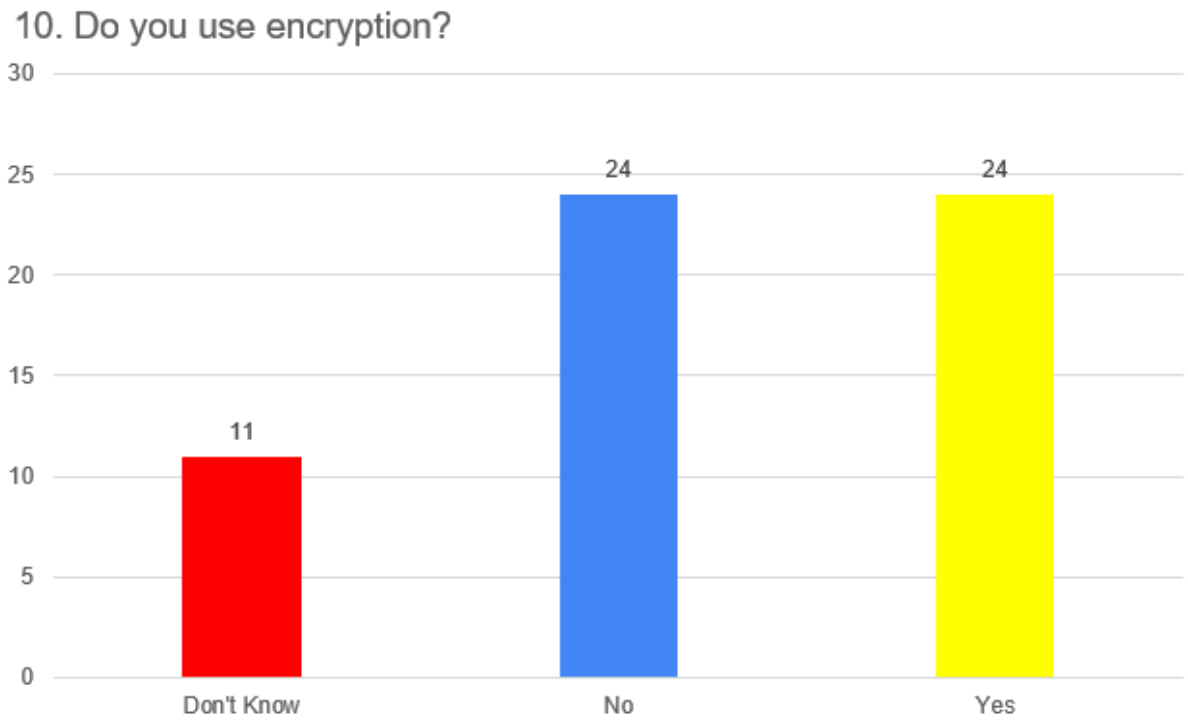

Figure 39 – Respondents' use of encryption

Question 11 sought to record user's views on the gravity of cyber attacks. An overwhelming majority of 52 people (88.1%) responded that cyber attacks could have devastating effects on a

global scale, 6 of them (10.2%) felt that this is something that should worry their government or their employer, while one person (1.7%) stated that cyber attacks do not worry them at all.

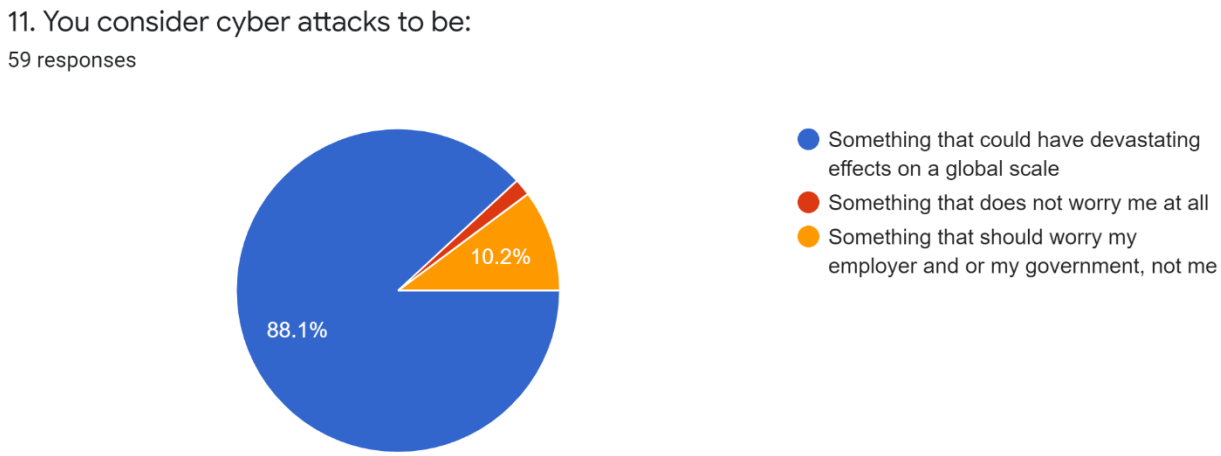

Figure 40 – Respondents' use of encryption

Question 12 asked whether respondents felt secure when using computers and the internet in their workplace. 39 persons responded that they do not feel secure (66.1%), while 20 responded that they do (33.9%).

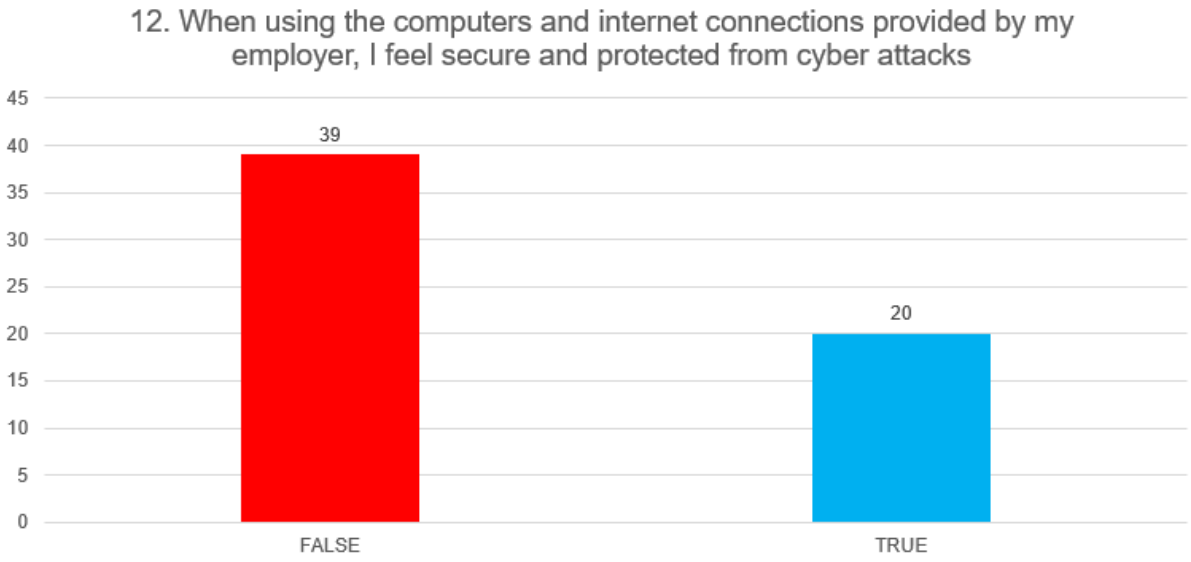

Figure 41 – Respondents' perception of cyber security in the workplace

In question 13, 57 persons considered cyber warfare to be a possible tool or parameter in international relations (94.9%), while only two did not (5.1%)

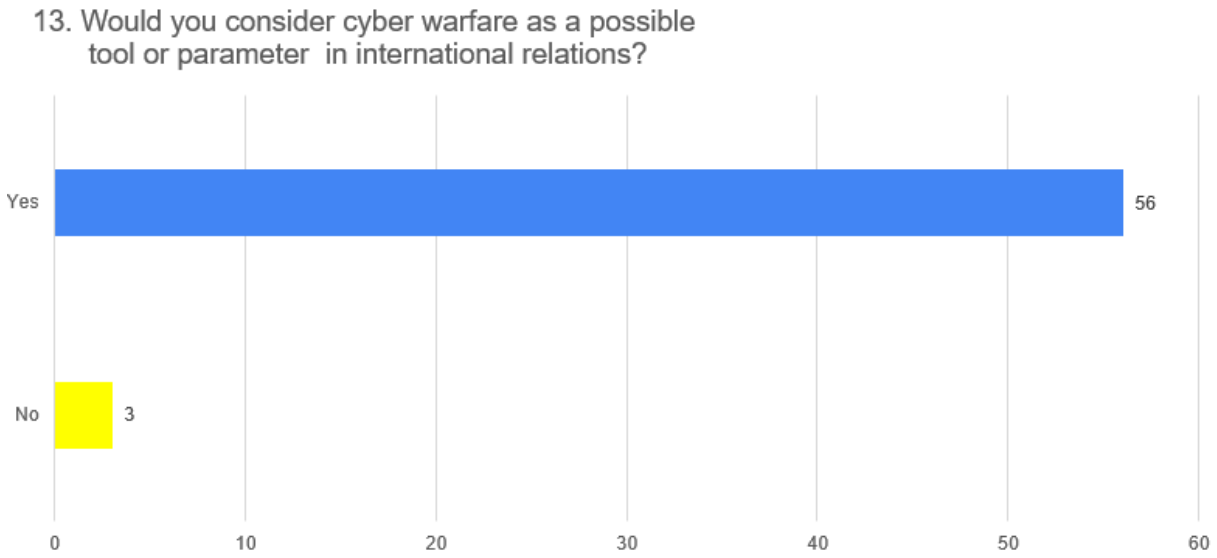

Figure 42 – Cyber warfare in International Relations

In responding to question 14, all survey participants felt that cooperation among EU member states on Cyber Security was necessary (100%)

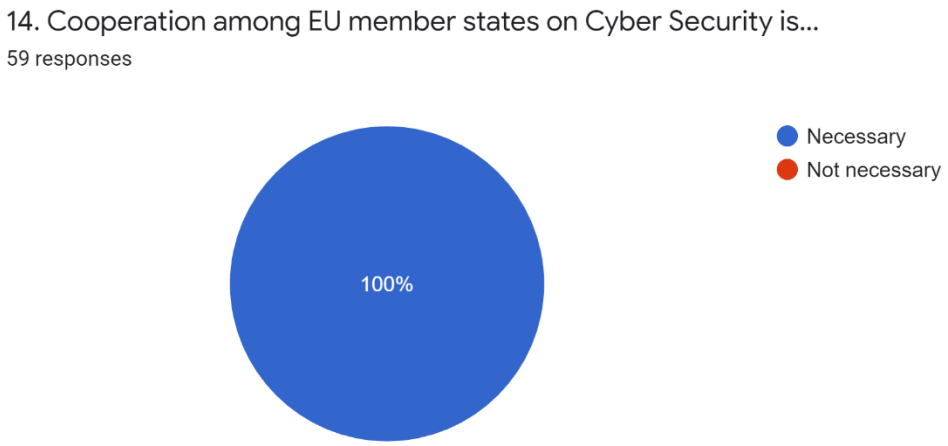

Figure 43 – Necessity of EU Cooperation on Cyber Security

Question 15 tested whether users were familiar with the term VPN, to which 42 respondents replied in the affirmative (71.2%) whereas 17 replied in the negative (28.8%)

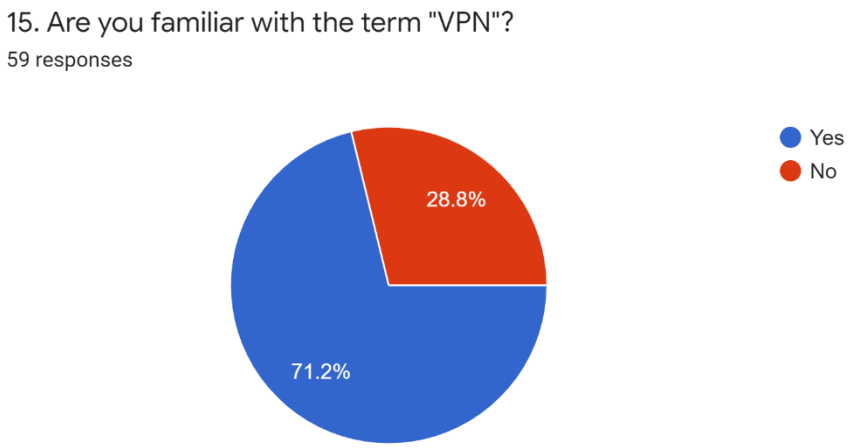

Figure 44 – Familiarity with the term VPN

When asked in question 16 whether they used VPN, 18 respondents said they did not know (30,5%), 6 said they never did (10.2%), 29 responded that they use VPN sometimes (49.2%) , while 6 stated that they always use VPN (10.2%).

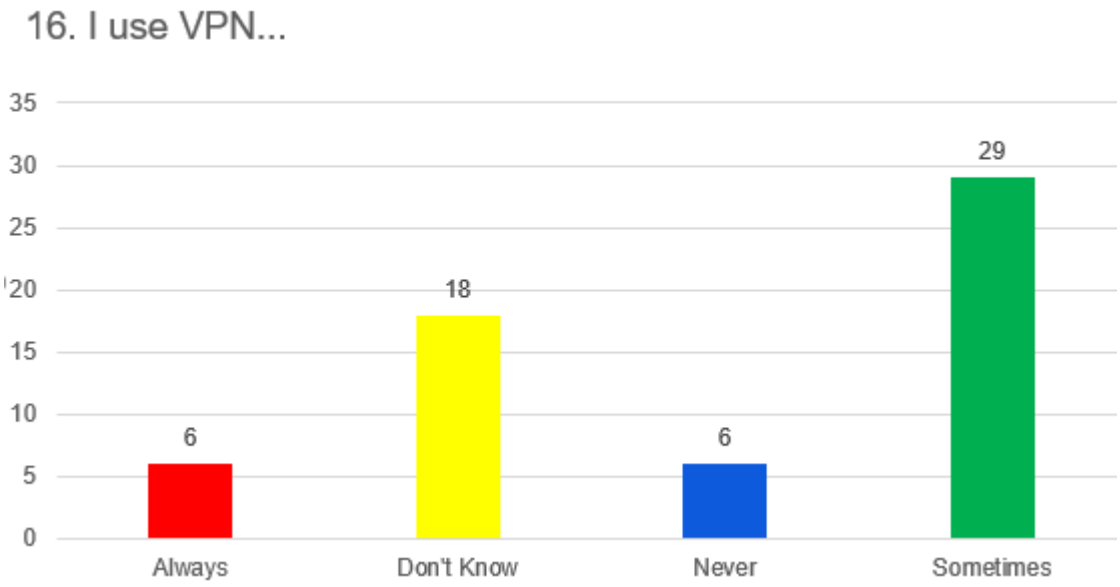

Figure 45 – VPN Usage

In question 17, 33 participants responded that they were familiar with the term VLAN (55.9%) whereas 26 were not (44.1%).

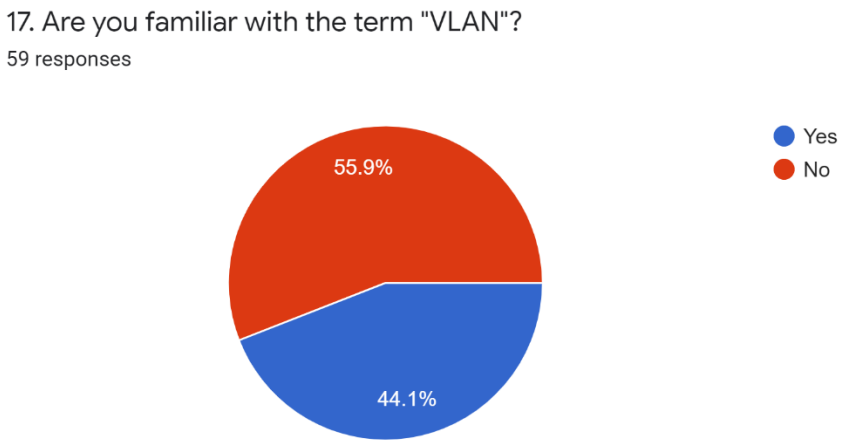

Figure 46 – Familiarity with the term VLAN

Question 18 introduced Cyber Ranges to questionnaire, testing for respondents' familiarity with the term. 20 respondents (33.9%) replied that they were familiar with the term, whereas 39 were not (66.1%)

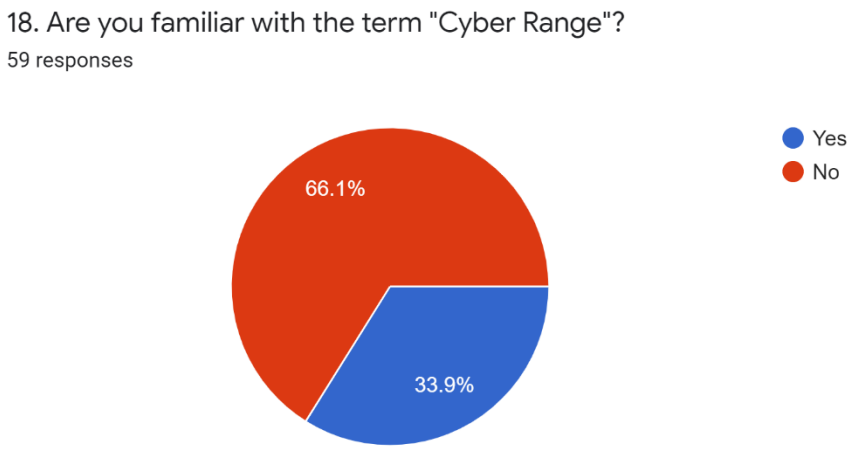

Figure 47 – Familiarity with the term "Cyber Range"

Immediately afterwards, question 19 tested for familiarity with the term "Federated Cyber Ranges", to which only 11respondents replied in the affirmative (18.6%). 48 respondents were not familiar with the term (81.4%)

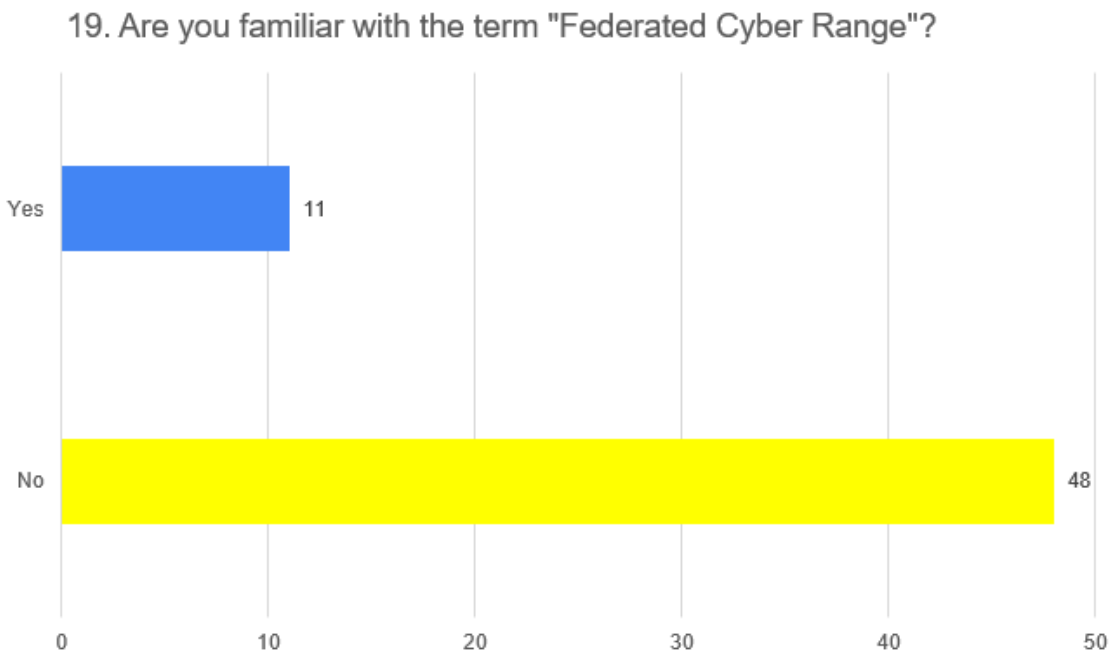

Figure 48 – Familiarity with the term "Federated Cyber Range"

Question 20 sought respondents preferred method for interconnecting federated cyber ranges. 49 of them replied that they did not know (83.1%), 1 person recommended a layer 2 VPN connection (1.7%), and 9 respondents recommended a layer 3 VPN connection. The option for a physical connection was not selected by any respondents.

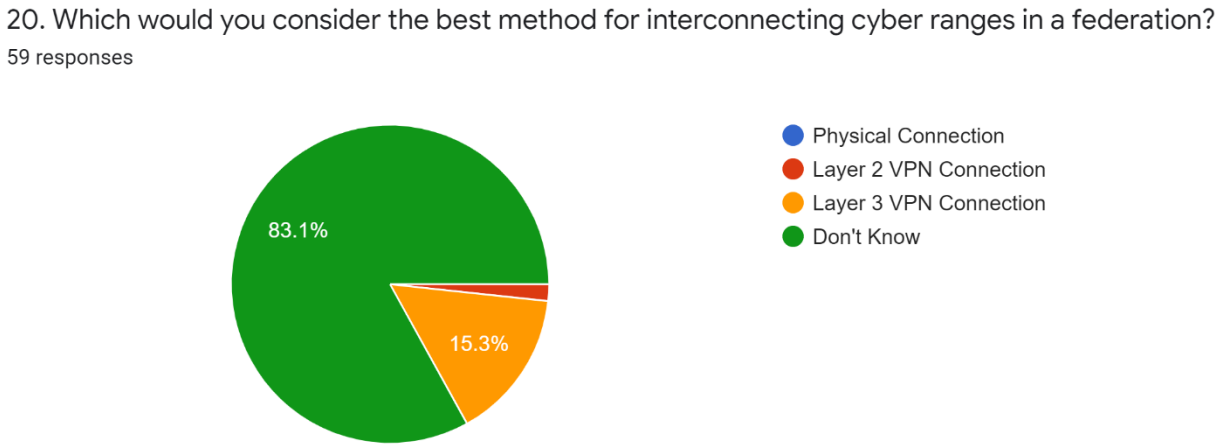

Figure 49 – FCR interconnection recommendation

Finally, question 21 sought recommendations for a layer 3 VPN connection for a federation of cyber ranges. 50 persons responded that they did not know (84.7%) leaving 9 people expressing an

opinion. Of these, 1 person replied that it depended on the deployment complexity (response option was "other, please specify" (1.7%), and two people suggested OpenVPN (3.4%). Three people recommended IPSEC (5.1%) and another 3 expressed a preference for VXLAN (5.1%).

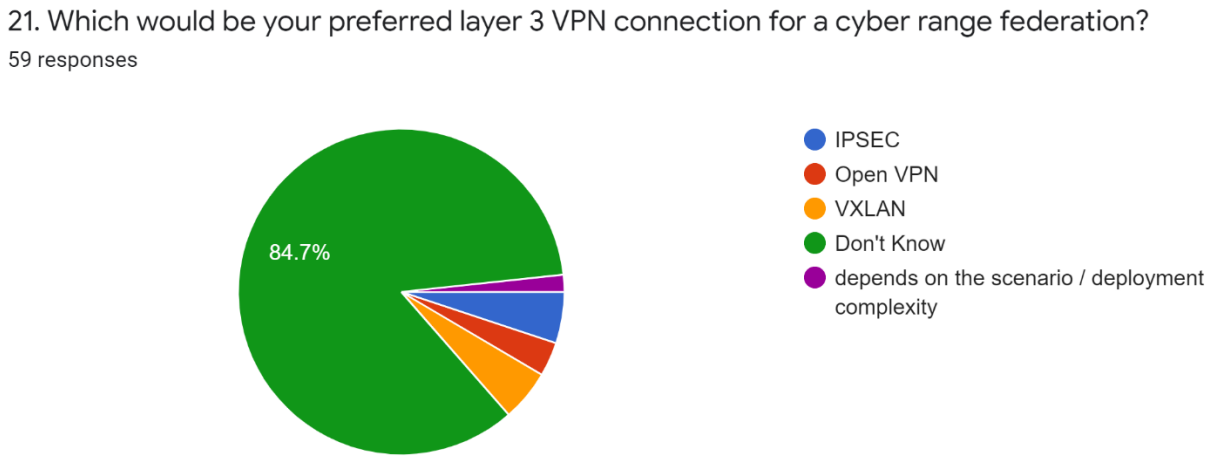

Figure 50 – FCR Layer 3 VPN connection preference

Chapter 7
Conclusions

7.1 How does it all come together?

The first message one gets after looking into this issue, is the fact that the bibliography on federated cyber ranges remains quite restricted, indicating that limited research has been undertaken in the subject matter of this postgraduate dissertation. It would appear, therefore, that there is considerable scope for further study, both into cyber ranges themselves, as well as their federations.

A continuation to the work in this postgraduate dissertation, might be to actually witness and document federations of cyber ranges in operation. This further study should begin with their interconnection over VPN in a real environment (as opposed to a virtual machine), in order to assess and evaluate their functioning, but also to document user experience stemming from the participation in a cyber exercise. For example, a study like the one carried out by Vallaots (2017) regarding the interconnection of cyber ranges in Czechia and Estonia would be useful in drawing conclusions regarding real life deployment. While working on virtual machines has the advantages of minimal cost and ease of system alterations, a clear record of reality can only be achieved with the use of a live environment.

Turning to the results of the questionnaire, the first aspect that must be noted is the fact that a lot of respondents were completely unaware of the concept of cyber ranges, even more so with regard to federated cyber ranges. This would point to the fact that the technology is still not quite at the point where everyday users are exposed to it - certainly not among the survey participants, who were almost in their entirety members of the civil service of the Republic of Cyprus. Their responses to the wider - and more basic - cyber security questions point to the fact that there is room for Cypriot civil servants to be made more aware of the dangers to which they are exposed when using computers.

It might be worthwhile to extend participation in this questionnaire to a wider base of Cypriot civil servants, perhaps with the questionnaire itself supplemented with additional questions, in order to better assess user exposure to cyber security as well as their general awareness of the dangers to themselves and their organisations. A study of this kind might point out conceptual mistakes, erroneous practices, and areas where further training is needed. Furthermore, it could also point to employer side limitations as well as the need for organizational methodologies to be altered.

Another questionnaire, more specific to cyber ranges and their federations, addressed primarily to IT practitioners, would be useful in charting their awareness of the concept, their exposure to it and their willingness to engage in cyber exercises. Given respondents full support for EU-wide cooperation in this subject, it might be interesting to see responses from Ministry of Foreign Affairs, Ministry of Defence and government IT practitioners from all EU member states, and particularly from those states where substantial work is already being carried out in the form of cyber ranges already in operation.

Given my professional exposure as a foreign policy practitioner, coupled with my personal keen interest in cyber security, the subject matter of this postgraduate dissertation falls within the scope of my professional and academic interest: the need for sections of government, and especially those dealing with sensitive or classified information, to protect themselves and their employees from danger while at the same time investing in the most secure systems and the best training for their staff. Participation in a federated cyber range would be conducive to this scenario.

Notwithstanding whatever usefulness the subject matter of this postgraduate dissertation may have for understanding cyber ranges and their federations, it must be underlined that it refers to a single section of the current research into cyber security, and still comes short of answering what continue to be gnawing questions that demand further research:

- are there any lessons to be learned by studying the increasing incidence of, and consequences from, cyber attack weaponization, primarily when undertaken by state agents?

- what would be the benefits that would accrue to the European Union, its member states and their partners and allies, as they come together in a variety of ways, including through cooperating on federated cyber ranges, to mitigate the scope for, and the possible aftermath of, cyber and hybrid warfare?

Bibliography

Chapman, S., Smith, R., Maglaras, L., Janicke, H., 2017. Can a Network Attack Be Simulated in an Emulated Environment for Network Security Training? Journal of Sensor and Actuator Networks 6, 16. https://doi.org/10.3390/jsan6030016

Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., Ferrag, M.A., 2021. Cyber Ranges and TestBeds for Education, Training, and Research. Applied Sciences 11, 1809. https://doi.org/10.3390/app11041809

Davis, J., Magrath, S., 2013. A Survey of Cyber Ranges and Testbeds.

ECSO, 2020. Understanding Cyber Ranges: From Hype to Reality. Available at https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf

EDA Cyber Ranges Federation project showcased at demo exercise in Finland [WWW Document] 2019. URL https://eda.europa.eu/news-and-events/news/2019/11/07/eda-cyber-ranges-federation-project-showcased-at-demo-exercise-in-finland (accessed 11.30.21).

Drake, M, 2018. How To Set Up an OpenVPN Server on Ubuntu 18.04 [WWW Document], n.d. . DigitalOcean. URL https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-18-04 (accessed 11.30.21).

IPERF - The Easy Tutorial [WWW Document], n.d. URL https://openmaniak.com/iperf.php (accessed 3.17.21).

IPsec, *Wikipedia*. Oct. 30, 2021. Accessed: Nov. 23, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=IPsec&oldid=1052631074

MPLS Routing - How Does MPLS Routing Work?, 2014. RCR Wireless News. URL https://www.rcrwireless.com/20140513/fundamentals/mpls-routing (accessed 3.10.21)

OpenVPN puts packets inside your packets [WWW Document], 2016. . saminiir's hacker blog. URL https://www.saminiir.com/openvpn-puts-packets-inside-your-packets/ (accessed 4.6.21).

Peratikou, A., Louca, C., Shiaeles, S., Stavrou, S., 2021. On Federated Cyber Range Network Interconnection, in: Ghita, B., Shiaeles, S. (Eds.), Selected Papers from the 12th International Networking Conference, Lecture Notes in Networks and Systems. Springer International Publishing, Cham, pp. 117–128. https://doi.org/10.1007/978-3-030-64758-2_9

Soucy, R.: Network Router Performance Testing How-To. URL

http://soucy.org/vyos/NetworkPerformanceTesting.pdf. (accessed 11.27.2021)

Suni et al., 2020. Report on existing cyber range, D7.1 CyberSec4Europe Project

Tam, K., Moara-Nkwe, K., Jones, K.D., 2021. The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training. Maritime Technology and Research 3, 16–30. https://doi.org/10.33175/mtr.2021.241410

Tanasache, F.D., Sorella, M., Bonomi, S., Rapone, R., Meacci, D., 2019. Building an emulation environment for cyber security analyses of complex networked systems, in: Proceedings of the 20th International Conference on Distributed Computing and Networking, ICDCN '19. Association for Computing Machinery, Bangalore, India, pp. 203–212. https://doi.org/10.1145/3288599.3288618

Tian, Z., Cui, Y., An, L., Su, S., Yin, X., Yin, L., Cui, X., 2018. A Real-Time Correlation of Host-Level Events in Cyber Range Service for Smart Campus. IEEE Access 6, 35355–35364. https://doi.org/10.1109/ACCESS.2018.2846590

Understanding Layer 2 VPNs - TechLibrary - Juniper Networks [WWW Document], n.d. URL https://www.juniper.net/documentation/en_US/junos/topics/concept/vpn-layer-2-overview.html (accessed 3.10.21).

Urias, V.E., Leeuwen, B.V., Stout, W.M.S., Lin, H.W., 2017. Dynamic cybersecurity training environments for an evolving cyber workforce, in: 2017 IEEE International Symposium on Technologies for Homeland Security (HST). Presented at the 2017 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1–6. https://doi.org/10.1109/THS.2017.7943509

Using iPerf to Baseline Network Performance [WWW Document], n.d. . ControlUp. URL http://www.controlup.com/resources/blog/entry/using-iperf-to-baseline-network-performance/ (accessed 3.30.21).

Vallaots A.,2017, Federation of Cyber Ranges, Master's Thesis , University of Tartu

Vykopal, J., Ošlejšek, R., Celeda, P., Vizváry, M., Tovarňák, D., 2017a. KYPO Cyber Range: Design and Use Cases. pp. 310–321. https://doi.org/10.5220/0006428203100321

Vykopal, J., Vizváry, M., Ošlejšek, R., Celeda, P., Tovarňák, D., 2017b. Lessons learned from complex hands-on defence exercises in a cyber range. pp. 1–8. https://doi.org/10.1109/FIE.2017.8190713

Williams, Mike, 2020, What is OpenVPN? A closer look at this popular VPN encryption protocol [WWW Document]. TechRadar. URL https://www.techradar.com/news/what-is-openvpn-a-closer-look-at-this-popular-vpn-encryption-protocol (accessed 4.6.21).

Winter, H., 2012. System security assessment using a cyber range, in: 7th IET International Conference on System Safety, Incorporating the Cyber Security Conference 2012. Presented at the 7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012, pp. 1–5. https://doi.org/10.1049/cp.2012.1521

www.firewall.cx, n.d. Understanding VPN IPSec Tunnel Mode and IPSec Transport Mode - What's the Difference? [WWW Document]. URL http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html
(accessed 3.10.21).

Yamin, M.M., Katt, B., Gkioulos, V., 2020. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security 88, 101636. https://doi.org/10.1016/j.cose.2019.101636

Appendix A
Survey Questions

DISCLAIMER

This survey is made up of twenty one multiple choice questions relating to Cyber Security. Providing answers to the questions requires no more than a few minutes.

PURPOSE OF RESEARCH: This questionnaire has been prepared in order to document participants' general knowledge on cyber security, aims to assess the use of federations of cyber ranges and participants' awareness of their existence.

POTENTIAL RISKS & BENEFITS: There are no risks expected for you due to your participation in this research, nor are there any direct benefits. The questions in this study will pertain to your experiences in the environment and any perceptions that you have of it.

PRIVACY AND CONFIDENTIALITY: Your confidentiality will be protected to the maximum extent allowable by law. No identifiable information will be collected from you and all anonymous data will be stored on encrypted sites and password protected computers. Your name will not be linked with your data in any way. Only the appointed researchers will have access to the research data.

RIGHTS TO PARTICIPATE, SAY NO, OR WITHDRAW: You have the right to say no to participate in the research. You can stop at any time after it has already started. There will be no consequences if you stop, and you will not be criticized.

By clicking the arrow button below, I indicate that I am 18 years of age or older and I voluntarily agree to participate in this study.

1. Please state your gender

- Male
- Female

2. Please state your age group

- 18 - 30
- 31 – 45
- 46 – 60
- Over 60
- Prefer not to say

3. What is the nature of your work duties?

- Secretarial / Administrative / Security
- Professional / Scientific / Academic
- Management
- IT
- Other / Not Employed

4. How would you describe your computer literacy level?

- Basic User
- Average User
- Power User

- IT Professional

5. You generally use computers for...

- Work related activities
- Non work related activities
- Both

6. Are you familiar with the term "cyber security"

- Yes
- No

7. In your use of computers, you do the following for protecting against malicious activity...

- Proactively take steps to protect your privacy and the sensitivity of the information you use
- Rely on antivirus software already present on your system
- It is not my job to worry about privacy and cyber security

8. In your use of computers you...

- have the same password for all accounts you use
- try to use a few passwords which are easy to remember
- try to have a different password for each account
- try to have a different password for each account and change it regularly
- try to have a different, complicated password for each account
- try to have a different, complicated password for each account and change it regularly

9. I remember my passwords by...

- I just have the one password and I remember it
- I have my passwords written on a piece of paper stuck to my screen / hidden in my wallet
- I save my passwords in the memory of my firefox/chrome/internet explorer
- I use an online password manager
- I use an offline password manager

10. Do you use encryption?

- Yes
- No
- Don't Know

11. You consider cyber attacks to be:

- Something that could have devastating effects on a global scale
- Something that does not worry me at all
- Something that should worry my employer and or my government, not me

12. When using the computers and internet connections provided by my employer, I feel secure and protected from cyber attacks

- True
- False

13. Would you consider cyber warfare as a possible tool or parameter in international relations?

- Yes
- No

14. Cooperation among EU member states on Cyber Security is...

- Necessary
- Not necessary

15. Are you familiar with the term "VPN"?

- Yes
- No

16. I use VPN…

- Never
- Sometimes
- Always
- Don’t know

17. Are you familiar with the term "VLAN"?

- Yes
- No

18. Are you familiar with the term "Cyber Range"?

- Yes
- No

19. Are you familiar with the term "Federated Cyber Range"?

- Yes
- No

20. Which would you consider the best method for interconnecting cyber ranges in a federation?

- Physical Connection
- Layer 2 VPN Connection
- Layer 3 VPN Connection
- Don't Know
- Other

21. Which would be your preferred layer 3 VPN connection for a cyber range federation?

- IPSEC
- OpenVPN
- VXLAN
- Don’t Know
- Other