https://doi.org/10.53656/str2025-5-6-inn

Education in the Information Society
Образованието в информационното общество

INNOVATIVE CONCEPTION, POLICY AND STRATEGY FOR EDUCATION AND TRAINING FOR PROACTIVE CYBER COUNTERINTELLIGENCE AND DEFENCE

Petar E. Manev
University of Library Studies and Information Technologies

Abstract. The article presents an innovative conception, policy and strategy for education and training for proactive cyber counterintelligence and defense. The research concentrates around complexity and problematics of modern day cyber operations, exercise and preparedness for counterintelligence and defense. The article also exposes current challenges in the cybersecurity domain with regards to planning, preparing, training, execution and training feedback level of successful cyber exercises. The article reviews the gaps found in current cyber concepts for education and training strategies. Based on the long term participation in the largest live fire international cyber exercises and having rich experience and knowledge on the matter the author provides perspective for a new approach for addressing some of the existing gaps in cyber preparedness via way of proposing innovative conception, policy and strategies education and training for proactive counterintelligence and defense, addressing existing nowadays weaknesses during training, planning and execution of cyber operations preparedness scenarios.

Keywords: innovation, policy; education; training; cyber security; cyber-attack; cyber defense; early detection strategies

Introduction

Activities in the cyber domain of communication are an integral part of modern-day society and currently influence directly or indirectly many areas of our daily activities and existence. In addition to that, as the domain gains strategic value and importance in terms of influence and control, it is natural that the cyber domain becomes an area of intense offensive and defensive, preventive actions. As constantly evolving information and communication systems and technologies bring new possibilities and features to be used in society, often, the systems are not designed with security as a priority. However, those information systems are vital for normal daily activities and operations, thus providing a security gap that

has both offensive exploitation possibilities and defensive potential of security gap protection coverage. Many traditional approaches of strategies and policies of education and training have limitations, and in the majority were developed to address a different problem with a background of using older and more static information systems. This in turn constitutes a gap that needs to be covered with innovative conception, policy and strategy for education and training for proactive cyber counterintelligence and defense. The article presents and reviews suggestions for improvement in the area of proactive measures that can be taken into account in evaluating and improving the strategy based on research and actual hands on experience including from some of the world's largest live fire cyber exercises – NATO's Locked Shields and Crossed Swords. In the article also it is emphasized the importance of correct set up and training feedback loop as an integral part of any innovative strategy for education and training for the cyber counterintelligence and defense strategy. Analyzing and studying carefully different critical information and communication systems as part of the cyber communication deployments, including their specifics in terms of details of the components would need to be considered in the successful planning, preparing, training and feedback loops of the conception, policy and strategy for more proactive measures that in turn can provide better cyber counterintelligence and defense.

It is logical and methodological approach to disclose the essence and semantic of the key terms and present or generate suitable definitions for the research.

Cyber Exercise aims at "improving organizations' preparedness and response for severe security incidents, and at shortening and reducing the impact of cyber-attacks. An exercise involves presenting an organization with a simulated crisis scenario to resolve, which enables the organization to learn valuable lessons for developing its operations." (Finnish Transport and Communications Agency, 2023)

Cyber ranges are "interactive, simulated representations of an organisation's local network, system, tools, and applications that are connected to a simulated internet-level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing." (NIST, 2018)

Cyber Operations is the "employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." (NIST, 2025)

Blue Team is "the group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team)." (NIST, 2025)

Red Team – a "group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture." (NIST, 2025)

White Team – the "group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of their enterprise's use of information systems." (NIST, 2025)

Hotwash – the main purpose of a hotwash is to "identify strengths and weaknesses recognized during the exercise/event, which may then lead to identifying lessons to avoid repeating errors made in the past. A hotwash-up normally includes all the parties that participated in the exercise or event." (NATO, 2013)

An Advanced Persistent threat (APT) is defined by National Institute of Standards and Technology as follows: "An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives." (NIST, 2025)

Cyber operations, regarded as regular and routine activities in everyday life on the cyber communication medium, are constant, geographically dispersed, and do not adhere to regular workday routines or set timelines of operations. Those activities are always ongoing and continuous. Any type of cyber operations built around those activities can be offensive and defensive in nature. They comprise the full spectrum of undertaking in trying to defend or attack specific information systems or systems.

Cyber operations can be executed by pretty much any person or any group of persons or organizations united by a common goal. Thus those operations are usually planned and executed by or on behalf of states, governments, as well as private organizations or individuals with criminal or legal intentions and boundaries.

In bigger organizations usually the cyber operations are operationalized and executed by different sub organizations, departments and or institutions that are governed by a clear objective, vision and a developed strategy. As an example, US Space Force has developed "Comprehensive Strategy for the Space Force" (Department of the Air Force, US, 2023) which contains "strategic objectives for organizing, training and equipping the Space Force" (Department of the Air Force, US, 2023) to be able to address and execute its mission "based on the threats and challenges outlined in the National Defense Strategy and National Military Strategy." (Department of the Air Force, US, 2023)

As a subsequent set of actions and planning activities United States Space Force Command (USSPASECOM) has developed a strategic vision with clear priority objectives, that is regularly kept updated:

"Prepare and posture: We will maximize our combat readiness by 2027

– Counter threats: We will achieve and maintain space superiority

– Strengthen relationships: We will continue to build a coalition of superior military spacepower

– Expand a warfighting advantage: We will shape military space power for the future fight" (USSPASECOM, 2024)

This vision, objectives and strategy propagates down through different organizational operational and tactical bodies of the organization to the individual specialist where it is operationalized:

"It's our Cyber Operations specialist's job to protect our cyber operations across four key specialties: defense, radio frequency and satellite communications, systems, and networks. They assess and report vulnerabilities, repair and install client systems, and protect our network infrastructure to ensure missions and communications run efficiently." (USSPASECOM, 2025)

The other crucial and important issue for the organization is its **Effectiveness of Cyber Operations**. Any operation or preparation in the cyber domain can be planned and executed regardless if there is an actual ongoing conflict. Furthermore, cyber operations can be conducted supportive to a conflict or executed as standalone missions that are driven by tactical and operational needs governed by a bigger strategy domain.

For any cyber operation to be effective, it needs to go through a process of clear objective definition, planning, training and execution.

Specifically, during the last two decades with the rapid expansion and adoption globally of computerized communication information systems, naturally there is also a raise of adoption of the cyberspace as a medium of achieving goals and objectives on organizational and individual level alike. Measuring the effectiveness of such operations in the information and communications systems domains is very difficult due to the multitude of factors, mainly due to the dispersed nature of the modern-day communication systems.

Some of the main factors affecting the effective evaluation of real-world cyber operations are analysed below.

Attribution is an essential element of any cyber operation or response. Being able to definitively attribute the goals and objectives of a past or ongoing operation of an adversary has an impact on the decision making process of planning an adequate response.

Since the spread of the COVID-19 pandemic (WHO, 2020), there has been even wider adoption of remote workforces and working processes and routines. The broad adoption of dispersed Virtual Private Networks and cloud services makes pinpointing and attribution of any cyber operation much more difficult. Thus, in effect also contributes for the resilience of these information systems.

Different security vendors, organizations and governments use various metrics and definitions to attribution confidence levels. As an example the Center for

Internet Security has defined and articulates the following 3 levels of confidence - *High, Moderate and Low.* (Center for Internet Security, 2025) The definition and explanation of different level of confidence depicts the lack of an easy and fast way of attribution of offensive or disruptive cyber action to a specific entity, organization, individual or geographical location.

Not being able to conclude with certainty attribution impacts directly any planning activity for successful and proactive defensive measures and operations of the different sub units involved and tasked with proactive cyber operations activities.

So based on that, achieving the goals of the cyber operation appears to be a challenging task. A crucial importance in evaluating the success of a cyber operation and subsequently planning and defining success criteria for future cyber operations is determining the successful completion of achieving the goals of the cyber operation itself. In that respect the planning personnel also have to be able to conclude the aspect of whether the planned operation can achieve its goals in time.

As an example, shutting down or destroying a targeted adversary (information) system can be challenging. First recorded usage of a kinetic military action in that respect was on May 5 2019 (Newman 2019), when Israel Defense Forces targeted and destroyed a building believed to be part of an ongoing cyber attack. Such operations may or may not achieve its objectives. That's why kinetic methods of destroying the facilities where eventually the communication and information systems are potentially located is not reliable in terms of achieving the cyber operation goals. Such operations may or may not achieve its objectives.

In a similar kinetic action, cyber operations also in combination with conventional weapons targeting data centers in Ukraine at the start and during the Ukraine-Russia conflict were not able to produce results due to the dispersed capability of information systems deployment. To put it simply, information systems and communications systems were dispersed from premises to the cloud, being hosted by multiple different balanced datacenters across Europe. (Center for Strategic and International Studies, 2023)

As such **result evaluation** is a critical step as an important part of any learning process, exercise and or planned activity is the capability of drawing out lessons learned in order to evaluate all cycle of planning, preparing, education, training and executing processes of a cyber operation.

The results have to be objectively proved regardless and they can be positive, negative or somewhat between. Confirming the success or not of a cyber operation can take time to deduct and conclude. In general the cyber operations often have supportive and/or no direct supplement effects to another ongoing operation. Confirming the successful goal achievement of any cyber operation can take time and it is not as visible and conclusive as a kinetic operation. This can also be due to the fact that there can be wrong assumptions about the adversary both in terms

of operations and information systems used and/or the criticality level of those systems.

In that respect, the **Cyber Exercises** are suitable scientific and practical research instruments for checking different innovative approaches and technical improvements for education and training. Such an instrument can help to define the most effective and innovative cyber active and proactive counter intelligence and defense. In that respect, the proper planning, training and execution for cyber exercises is an essential element for any Cyber Operations activities, policies and strategy. Due to the difficult nature of attribution - goals achievement, result confirmation and evaluation in real-world cyber operations, it poses an even bigger challenge for the planning and success of a cyber exercise, thus making it more difficult to research possible and more effective innovations. That's why it needs specialists with a high level of theoretical and practical experience and knowledge of software and hardware as well.

An innovative approach and combination of approaches are needed in terms to better and more successfully achieve the education and training goals of a cyber exercise - mainly in a proactive manner using innovative conceptions, policies and strategies.

To achieve those goals, various types of cyber exercises can be employed. In order to more completely and proactively prepare, train, educate and execute cyber operations, different types of cyber exercises need to be planned, prepared, developed and executed with precisely defined goals based on realistic scenarios. Cybersecurity exercises are designed to test and improve an organization's ability to withstand and respond to cyberattacks. There are different types of cyber exercises designed to address different problematic or training aspect goals and objectives. Those types of cyber exercises can include the following examples.

The **tabletop-discussion-based** exercises are typically classroom-driven, with a facilitator guiding participants through discussions of one or more scenarios. Teams talk through simulated attacks, focusing on planning, communication, and decision-making. The table top exercises reveal weaknesses in response plans and improve team coordination.

Attacking versus defending training is an essential type or exercise where testing and confirming **Offensive vs. Defensive** routines are practiced. Red Team vs Blue Team where Red Teams mimic attackers to find weaknesses, while Blue Teams defend. This tests real-world security effectiveness. Purple Teams are when Red and Blue teams work together to improve the overall security posture with debriefs and feedback, incorporating lessons learned into future operations and activities. Those exercise training routines can be adapted to better test a mimic more realistic conditions that aim to bridge current gaps in cyber counterintelligence and defense.

Individual or group **Skill-Based exercises**, also known as Capture the Flag (CTF), **have** participants solve technical puzzles to „capture“ virtual flags. This develops practical skills in areas such as hacking and forensics. The concept can be used to apply innovative objectives and goals training for specific individuals or teams.

Some of the most difficult and time-consuming exercises in terms of planning and execution are the Real-World Simulation – Live-Fire exercises, where security teams respond to simulated, active cyberattacks in a controlled setting. This provides the most realistic test of response capabilities. Full live fire exercises are the most complex to plan, execute and operate and include actual live and emulated information systems, cyber ranges, multiple organizations and can span during different time zones and geo locations all that to bring increased realism and training to the participants. Different sub teams are in charge of different operational aspects of the exercise. For example, White /Blue/ Red Teams can separately work in conjunction with other teams in order to provide real feedback loops. The learning, experience and feedback benefit of those complex exercises can be even further extended with incorporating innovative conception, policy and strategy for better education of collaborative team work during cyber operations.

Individual training can also include human vulnerability testing for example **Phishing Simulations** where fake phishing emails test organization's employee awareness and susceptibility to manipulation and cyber attacks. This identifies training needs and helps reduce human error during the process of improving and bridging the knowledge gaps in education for cyber exercises and operations on individual level.

An essential part of any defense and cyber counterintelligence preparation is **Response Practice - Incident Response Drills** where cyber security teams practice their response to specific cyber incidents, like data breaches. This ensures readiness, preparedness of personnel and smooth execution of incident response plans. Adjusting, incorporating and improving those drills to include the innovative approaches in strategy for education is an essential part of the full spectrum cyber defence preparation process.

It all culminates into real life **Complex Scenarios - Hybrid Exercises** that combine multiple exercise types, often involving multiple organizations and spanning different geographical regions. These test responses to very complex attacks. Hybrid exercises include different real live events for example in conjunction with a Red Team against predefined targets for more realistic experience.

To successfully prepare and execute Cyber Operations different types and techniques in terms of training strategies can be utilized for planning, preparing and executing cyber exercises. Examples of large scale cyber exercises include and involve multinational teams, spanning across different countries, states and continents. Two such examples of complex scenarios of hybrid live fire exercises

are executed annually by The Cooperative Cyber Defense Centre of Excellence (CCCOE) - Locked Shields and Crossed Swords.

The **NATO** – **Locked Shields Cyber Exercise** is one of the biggest hybrid and live fire such in the world with unmatched complexity so far. As informed by the NATO‘s Strategic Warfare Development Command: *The Locked Shields exercise, which occurred in April 2023, included 38 countries, 5500 participating systems, and over 30 international organizations, industries and academic partners. This exercise sought to test defensive cyber operations and digital forensics while also fostering multi-national coordination.* The exercise is one of the largest “live fire” cyber exercises that incorporates live scenarios with many different organizations and teams collaborating towards a fictional scenario. *“*According to the scenario, a fictional island country located in the northern Atlantic Ocean, Berylia, is experiencing a deteriorating security situation as there have been a number of coordinated cyberattacks against Berylian military and civilian IT systems. These attacks have caused severe disruptions to the operation of government and military networks, communications, water purification systems and the electric power grid and eventually lead to public unrest and protests. For the first time the exercise includes the simulation of a reserve management and financial messaging systems of a central bank. Additionally, a 5G Standalone mobile communication platform is deployed as part of a critical infrastructure to give the first experience to cyber defenders about upcoming technology change.”(CCDCOE, 2025)

The exercise is big, complex and requires a lot of planning to be executed and to be able to achieve its goals. Due to its following the dynamics of a realistic scenario that involves many international participants, organizations and entities the exercise planning activities usually take one year and start right after the previous exercises finishes.

Similar exercises are held annually with other objectives. Another such large-scale exercise aimed at achieving the goal of training the offensive team operations is **NATO** – **Crossed Swords** Cyber Exercise

*“*The Crossed Swords (XS) exercise, conducted by the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), is designed to train cyber specialists to successfully execute a full kill chain offensive cyber operations in a simulated crisis environment and also train military command elements in command and control of offensive cyberspace capabilities.

2024 iteration of the CCDCOE exercise brought together approximately 200 participants from 40 countries, including NATO and non-NATO member states, to practice and experiment in a field that is highly relevant in today’s world.

The exercise training audience includes a Cyber Headquarters with a full planning staff, military cyber operators, digital forensic experts, and specialists from other units who are a part of, or work with their national cyber forces.*”* (CCDCOE, 2025)

Crossed Swords is another big and complex cyber exercise with emphasis on real life scenarios and live continuous feedback loop to all teams. The feedback

loop is intended to give participants an informational feedback of the progress of the exercises and mainly how each different entity and sub component of the exercise behaves, scores and progresses as part of the overall execution process. This is needed to provide calibrating and corrective action wherever needed to the participants and bring realistic ever changing and evolvement of the cyber operations of a real life environment under cyber attack.

A critical component of any preparation of any operation, including for defense response exercises is the availability of a **Test, Training and Exercise** program that has the objective to establish, present and constantly update post each exercise activity and workshop that allows to prepare participants and organizations better for real life scenarios of cyber breaches. Such a program should include a cyclic form of operation and feedback in order to constantly update its exercise and/or exercises multitude of goals to be able to achieve its designated mission - full preparedness and constant updated training of the participants. In Figure 1, an example of a National Institute of Standards and Technology (NIST) TT&E Event Methodology is depicted.

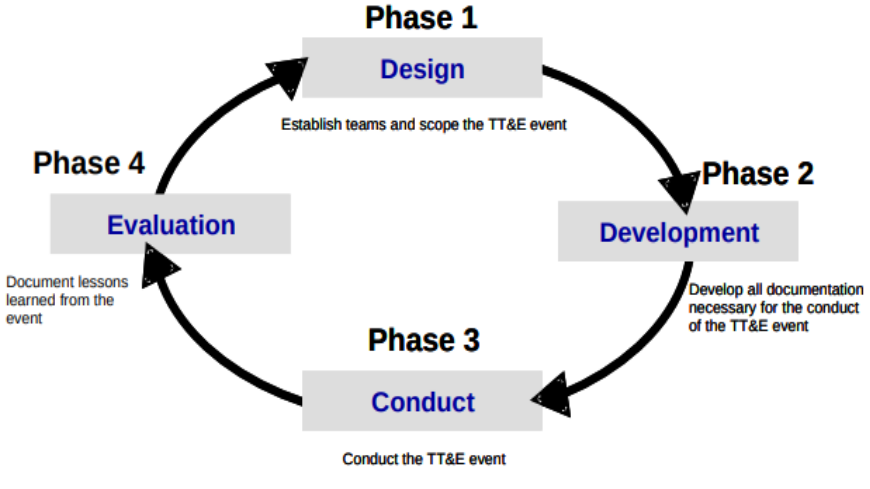

Figure 1. Test, Training and Exercise program
Source: Public data (from National Institute of Standards and Technology, TT&E Event Methodology, 2006, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf)

The diagram above emphasizes constant feedback, improvement, planning and execution methodology as part of a successful planning implementation strategy of cyber exercises.

For any streamlined operation, including cyber operations, whether defensive or offensive, to be successful, it needs clearly established guidelines, information communication procedures, **Structure, and Command**. One of the most critical and essential parts of a successful cyber operations execution is the timely and accurate exchange of information, both before, during, and after the cyber operation. Thus, it is even more important during multinational cyber exercises to have a clear cyber exercise structure, chain of command and information communication channels defined. NATO's Crossed Swords exercise from 2019 had the following structure as depicted by the diagram below:

\

Figure 2. Crossed Swords 2019 chain-of-command
Source: Public data (from Crossed Swords: A Cyber Red Team Oriented Technical Exercise, 2019, https://ristov.github.io/publications/eccws19-xs.pdf)

In the diagram above, it is essential to note the presence of different operation levels - Strategic, Operational and tactical levels of the command chain as it implements a real-life execution scenario where any cyber operation, response or action has to take a path of an approval chain. The chain of command incorporates information feedback and action evaluation consequences, including from "Legal Advisor" entities, in order to implement a more realistic cyber operations scenario, which is in line with the strategic objectives of the exercise.

In order for an organization, team or entity to achieve the highest level of cyber operation preparedness for proactive cyber counterintelligence and defense, more proactive and realistic scenarios incorporating **Innovative approaches** can be

beneficial for the cyber operations. Often enough exercises are confined to one team vs another. In real life environments it is not so obvious, there is a lack of demarcation line in cyber operations and the following considerations below must be evaluated and adopted.

Innovative Conception, Policy and Strategy for proactive preparedness are needed and need to include proactive cyber and counterintelligence and defense methods to address modern day complexities arising from ever changing needs, new feature additions and expansions of current and future cyber communications.

Non-standard hours of operation often mean reduced staffing, which can lead to slower detection and response times and as a consequence provide for **Increased Vulnerability Scenarios** of a training for cyber operation. Attackers may specifically target these periods, knowing that security teams might be less vigilant. Assume breach cyber operations during nonstandard time - simply put this is "assume breach" (aka the organization knows there is a breach but not exactly the type and extend) response operations are cyber operations done with the clear conscious and knowledge there is an unknown cyber breach ongoing - during official time off, unusual time of operation or holidays for a specific organization, culture or geo location.

Clear response and communication information involving staff who are reduced and overloaded with tasks during a cyber incident is essential for preparedness.

A time when no new system updates or changes can be made to ensure business or functional operations run smoothly is referred to as **Change freeze.** Planning and preparing a defensive cyber exercise that accounts for the change of freeze time of some critical system or communication component is vital and an integral part of a successful training and education strategy. This approach provides preparedness scenarios for offensive or defensive cyber operations, mimicking responses during critical periods of time when IT systems are undergoing changes or freezes. In terms of IT and cyber operations the term "Change freeze" refers to a specific set of critical information systems that are not allowed to have any configurational changes executed on those so that to minimize the risk of bigger negative impact of operation or total loss. For example - banking system during the Christmas holiday season. Developing specific scenarios for planning, preparing and executing cyber operations training with such constraints in mind can contribute to the overall preparedness and response not only of the required teams but also in terms of feedback information loop in order to better prepare, educate, train and respond during a cyber incident.

Planning and executing cyber operations mimicking heightened periods of public attention on major international or state internal events is an essential part of having proactive and innovative conception and strategy for education and training preparedness for cyber defense as it provides an important element often used by Advanced Persistent Threat actors, mainly **Decoy or distraction focus**. In some

cases, post breach the opponent or threat actor will stay dormant and not act until the appropriate time of operation has come. For example, there is an APT threat actor that has managed to accomplish an unnoticed breach that is awaiting a certain time period to activate - election, coronation, change of government, pandemic. During such times, even though there are heightened security measures, the main focus is on the event itself, which can result in lesser attention to other areas and aspects of the security spectrum of an entity, organisation, state and specifically, the defensive cyber operations.

In most cases, major cyber operations and exercises are executed with either the participation or assumption of the existence of major commercial vendors operating in either the defensive or targeted environments of cyber operation. This, in turn, can lead to certain training and practice conclusions from the exercise on a **Vendor assumption.** For example, it is often assumed that there are several well-known and common systems, including Windows, Linux, BSD, and others. The cyber operations as part of the cyber exercises are then planned and executed with that assumption in mind. The cyber training can involve both defense and offensive actions, which plans for executions training and feedback based on the existing systems. Thus leaving a blind spot for training, planning and execution in scenarios where the information systems involved and used are unknown or little known. This in turn leaves potential opportunities for live training scenarios uncovered. As one such example, response preparedness can be a case where the information systems involved are of an known origin, thus leaving potential defensive vulnerability preparedness scenarios unprepared for. As an example, the Russian Federation has adopted and implemented a series of „measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation“(Presidents Administration Russia, 2022). That means that such systems existence is unknown from operational existence point of view to Europe or US and other countries for example, including specifics of communication and digital footprint both in terms of offensive, defensive and operating capabilities. This proves that inclusion of such relevant or similar information systems in planning cyber exercises increases the preparedness and training capacity in terms of realistic scenarios, conception, policy and strategy for education and training for proactive cyber counterintelligence and defense.

It is common to plan, train and conduct a cyber operation with certain assumptions. One of those assumptions includes common **Operating system assumption** language. For example, there can be an assumption made during the planning and execution of a specific cyber training operation that there is the existence of Microsoft Windows operating systems in English. In cases where the cyber operation is defensive and the cyber exercises aim at training defensive teams on operating and planning protection of such an existing environment, this is very relevant. However, there can be cyber operations cases where there are

Microsoft Windows Operating Systems in other non-English languages, which, if present, for example, can greatly increase the response time, hinder it, or prevent it from providing a successful response. The problem comes from working in an environment with a non-common Operating system language assumption.

It is normal for a complex and critical communication information system to span operation during big amounts of time – decades. Maintaining, supporting and operating such systems, including its components, requires careful planning, training and resource allocation. It is common practice that as part of normal support operations, certain maintenance activities are executed in steps, over a period of time and per system component. It is expected that, as part of any such long-cycle term routine operations, maintenance, and support activities of such systems, the personnel will also change over time. Thus, in relation to these activities in such complex information system environments, it is quite common, including due to geopolitical changes, to have transfer of knowledge loss, which results in a state of presence of **Unknown systems** in the overall information communication system. The knowledge loss can be in many forms, in parts, also of bigger or smaller components, maintenance steps, or simply, certain components get replaced, and older sub-components are not properly retired. This, in turn, with time, leaves a problem to solve known as "unknown operating systems" as residing subcomponents of a bigger critical information communication system. Those unknown systems, in turn, can have unrestricted access to the same critical or other critical information systems. This problem is crucial and needs to be taken into account for any innovative conception, policy and strategy for education and training for proactive cyber counterintelligence and defense as it provides an enabling tool for both offensive and defensive cyber operations and is hidden to both attacking or defending times alike.

Conclusion

Information and communication systems are mainly designed to improve modern day activities and bring new features from ease of operationality and usability perspective. As the technology constantly evolves so do the adversaries and their respective goals and capabilities in exploiting and leveraging those information and communication systems in the cyber security domain as part of achieving a bigger and innovative offensive strategic objective. It is critical when preparing for defense against such activities to adopt a successful approach based on innovative conception, policy and strategy for education and training for proactive cyber counterintelligence and defense. It is not uncommon that modern day defensive measures do not account or struggle to account in time for the evolving nature of the cyber domain. It is critical to plan, prepare, and execute complex training exercises that mimic realistic scenarios. Thus, as an integral part of the success of the next exercise, a clear communication chain needs to

be followed, which in turn provides valuable feedback for the design of the next cyber exercise. However, not basing the design of a cybersecurity training on a realistic scenario after studying carefully big modern-day security breaches and conflicts can provide incorrect feedback in the design phase. Careful analysis needs to be in place in order to design and plan a realistic exercise based on facts from current and past real and training (research scenarios) conflicts. Existence of possibilities for kinetic actions and operations specifically targeting information and communication systems, the availability for offensive actions all year round and 24/7 which in turn require similar defensive planning, the possibility of extended threat actor or malware dwell times, the existence of diverse, including unknown multi language Operating Systems contribute to cyber security complexity that is beyond the reach of traditional methods for conducting cyber exercise. This constitutes a need for innovative concepts, policies, and strategies for education and training in proactive cyber counterintelligence and defence. It is crucial that a cyber training exercise strategy is not confined to incorrect assumptions in terms of technological, geopolitical and operational perspectives. Careful evaluation of missing components or aspects and their respective addition to the planning, preparing and executing in the cyber training exercise scenario is of extreme importance as one of the success criteria of achieving the objective of having better defensive capabilities, preparedness and counterintelligence capabilities in the current day evolving threat landscape.

Acknowledgements and funding

The article was prepared with the financial support of the National Science Program "Security and Defense", financed by the Ministry of Education and Science of the Republic of Bulgaria, in implementation of the Decision of the Council of Ministers of the Republic of Bulgaria No. 731 of 21.10.2021.

REFERENCES

CENTER FOR INTERNET SECURITY, 2025. *Words of Estimative Probability, Analytic Confidences, and Structured Analytic Techniques.* Available at: https://www.cisecurity.org/ms-isac/services/words-of-estimative-probability-analytic-confidences-and-structured-analytic-techniques.

DEPARTMENT OF THE AIRFORCE, 2023. *Congressional Report on a Comprehensive Strategy for the Space Force*. Available at: https://www.spaceforce.mil/Portals/2/Documents/Space%20Policy/CRR-FY23-Comprehensive-Strategy-Space%20Force-15-Aug-23.pdf .

MUELLER, G. B.; JENSEN, B.; VALERIANO, B.; MANESS, R. C. & MACIAS, J. M.2023. Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures. *Center for Strategic and International Studies*. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-07/230713_Mueller_CyberOps_RussiaUkraine.pdf?VersionId=tIzsIXBig6NG2QKBsqTlOIf0wENNeo87 .

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018. *Cyber Ranges*. Available at: https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2025. *Managing Information Security Risk*. p. B-1. SP 800-39. Available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf .

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2025. *Glossary Blue Team*. Available at: https://csrc.nist.gov/glossary/term/blue_team .

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2025. *Glossary Cyber Operations*. Available at: https://csrc.nist.gov/glossary/term/cyberspace_operations .

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2025. *Glossary Red Team*. Available at: https://csrc.nist.gov/glossary/term/red_team

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2025. *Glossary White Team*. Available at: https://csrc.nist.gov/glossary/term/white_team .

NEWMAN, L. H., 2019. *What Israel's Strike on Hamas Hackers Means for Cyberwar*. Wired. ISSN: 1059 – 1028.

NORTH ATLANTIC TREATY ORGANISATION, 2013. *BI-SC Training and Exercise Directive (CT&ED) 075-003*, p. A-19, Supreme Allied Commander, Europe B-7010 SHAPE Belgium, Unclassified, (Published on 02 October 2013), Available at: https://www.coemed.org/files/Branches/DH/Files_01/bi-sc-75-3_final.pdf .

NORTH ATLANTIC TREATY ORGANISATION, 2025. Crossed Swords Cyber Exercise, *Cooperative Cyber Defence Centre of Excellence*. Available at: https://ccdcoe.org/exercises/crossed-swords/ .

NORTH ATLANTIC TREATY ORGANISATION, 2025. Locked Shields Cyber Exercise, *Cooperative Cyber Defence Centre of Excellence.* Available at: https://www.ccdcoe.org/exercises/locked-shields/ .

PRESIDENT'S ADMINISTRATION, Kremlin 2022. Указ *о* мерах по обеспечению технологической независимости *и* безопасности критической информационной инфраструктуры, Available at: http://kremlin.ru/catalog/keywords/128/events/68090 .

TRAFICOM, 2023. *Situation awareness and network management-Exercises*, National Cyber Security Center, Finnish Transport and Communications Agency. Available at: https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/exercises .

UNITED STATES SPACE FORCE COMMAND, 2024. *Updated Strategic Vision.* Available at: https://www.spacecom.mil/Newsroom/News/Article-Display/Article/3683192/usspacecom-releases-updated-strategic-vision/ .

UNITED STATES SPACE FORCE COMMAND, 2025. *Enlisted Careers – Cyber Operations.* Available at: https://www.spaceforce.com/enlisted-careers/cyber-operations .

WORLD HEALTH ORGANIZATION, 2019. *COVID-19*. Available at: https://www.who.int/europe/emergencies/situations/covid-19 .

✉ **Petar E. Manev**
University of Library Studies and Information Technologies
Sofia, Bulgaria
E-mail: e.manev@unibit.bg