Information and data protection in XR training scenarios: straightforward solutions to comply with modern requirements[1].

Mr. Andrea D'Angelo, Ms. Federica Genna, Mr. Stefano Mazzaro
Fondazione SAFE
Via Mere snc, 37038 Soave (VR)
ITALY

andrea@safe-europe.eu; federica@safe-europe.eu; stefano.mazzaro@safe-europe.eu

ABSTRACT

The use of Extended Reality (XR) in military training has been emerging for several years. Just like any innovative technology, this implies the use of lesser-known solutions, which bring additional security and privacy implications. The paper presents challenges and solutions identified during the development of XR simulations to support CBRN training, with a particular focus on information and data protection. Fondazione SAFE experience in chairing a NATO MSG-HFM-RTG on XR for CBRN and the internal development of XR CBRN training scenarios will be analysed.

The paper presents key research questions addressed by SAFE in previous projects, to fully comply with NATO/ EU MS regulations on cyber security and data protection. An important takeaway is that, in training scenarios delivered via XR systems, the technical content (i.e., the characterisation and coding parameters of the CBRN event) could be considered classified and stand-alone headsets shall be prioritized when possible, adapting accordingly the coding of the XR experience. Classification shall also be foreseen for After-Action Report produced automatically by the XR training system to assess the trainees' procedures. Finally, the paper presents some of the challenges and solution to tackle in a simple yet effective way those issues and formulate valuable recommendations.

1. INTRODUCTION

1.1 The use of XR and VR technology in the military context

The technological evolution driving the integration of synthetic environments into the military world is evident for both NATO countries and some of their most established competitors on the international scene, like the PRC [1]. In this context, armed forces around the globe are increasingly exploring the introduction of XR and VR devices to perform different task [2]. Among those, training tasks represent the most widely accepted use of the technology considering the intrinsic advantages it brings, namely the cost-savings compared to real-life exercises and the possibility to simulate potentially dangerous scenarios -such as pilots' training on advanced platforms, CBRN scenarios, and medical ones- aimed at a wider audience of trainees and with almost absent health and safety-related risks. Nowadays, even tasks such as mechanical maintenance and handling of munitions are exploring the potential benefits of an Extended Reality approach to increase readiness and preparation of operators [3].

[1] This publication reflects only the authors' view and NATO STO is not responsible for any use that may be made of the information it contains.

XR and VR technology however is also expected to provide a much-needed edge during combat operations of the future. The evolution in the field saw the application of a similar technology -that is, the transmission of a large flow of information directly in front of the operator's eyes- on Head-up Displays (HUD) first and Head-mounted Displays (HMD) later, with their application in military aircraft. While the use of HUDs and HMDs constitute an essential requirement of modern military aviation, a more conservative approach towards the technology for applications on the ground can be found. Among recent applications we find head-mounted systems that allow armoured vehicles crews to have unobstructed, 360° view for improved situational awareness and easier targeting; the extension of the very same concept to the troops to be transported in the vehicle has also been studied, in order to provide the same tactical advantage once they dismount [4].

However, immense technological and economic efforts have also been made to develop such warfighting solutions for the benefit of every dismounted soldier and platform. A prime example of this evolution is represented by the U.S. Army Integrated Visual Augmentation System (IVAS) Program, a $22 bn initiative that aims to combine and enhance “sensing, decision making, target acquisition, and target engagement” for soldiers on the ground through a “ruggedized […] MR headset based on Microsoft’s commercially available HoloLens” [5]. The system -effectively dedicated to warfighting and expected to be procured in up to 120.000 units- aims at uniting advanced optics -i.e., pass-through cameras for external vision, complemented by night-vision goggles and thermal-vision equipment-, an advanced C2 suite to improve battlefield situational awareness, a target acquisition system, and a larger, wearable battery, among other enhancements.

As military systems -even the ones not related to XR/VR training- become more and more connected, cyberattacks can exploit vulnerabilities in those complex networks. This is even more worrying considering that, as the ongoing armed conflict in Ukraine has shown, the cyber domain offers innovative and relatively cheap methods to degrade adversary assets, and the intent of major Actors to leverage those capabilities during conventional conflicts. After all, in the context of future peer or near-peer conflicts involving the Alliance, cyber security management is expected to play an essential role [6]. Thus, to fully exploit the potential of the new technologies without opening new and dangerous vulnerabilities, the resilience and security of such systems shall always represent the state-of-the-art in the field.

1.2 XR/VR shortcomings identified so far in military applications.

With the introduction of every novel technology, especially in the military field, a whole new array of shortcomings is bound to be identified at end-users’ level. In that sense, the U.S. Department of Defense identified four main issues related to the use of XR/VR systems at present times, both from a training and operational perspective [5]:

(1) Affordability, as the R&D and procurement process for such advanced and widely distributed (in the specific case, on an individual basis) technology can be particularly expensive. With defence budgets weakened by inflation and the ever-increasing cost of weapon systems, the advantages of cheaper solutions (on the long run) are sometimes overlooked.

(2) Technological Maturity: while some technologies related to XR and their use in actual operative scenarios can be considered well established, others are still showing teething problems. Furthermore, the state-of-the-art is constantly evolving at a very high pace. Considering the lengthy nature of military procurement in general, the technological gap between the adopted solution and its competitors on the market -at the time of the actual adoption- can be greatly exacerbated.

(3) Personnel, for the newly adopted technology may translate in a greater strain on existing specialized profile (i.e., IT specialists, cybersecurity personnel) with the need of integrating the force structure to meet the demand. This goes in contrast to the current trend of reducing the manpower allocated to training and shifting it to active roles.

(4) Cybersecurity. The eventual cybersecurity vulnerabilities of XR systems are to be assessed and covered continuously, particularly in cases where the system is used for weapons maintenance and image classification that could be used by adversaries to acquire information on weapons systems. Furthermore, with an envisioned warfighting role for XR/VR devices, the same concern applies to the potential breaking of the adversary into C2 or targeting systems, thus revealing the position of friendly forces and assets.

While those issues can be ascribed to the fields of procurement, sustainability of the capacity, and integration into the existing force, another factor has been highlighted during operational testing of the IVAS, this time pertaining to human factors. In fact, it was not uncommon for users to experience physiological issues when using the device [7]. This crucial finding can be linked to a strand of studies regarding the interaction of human factors and XR technology, especially pertaining to the risks of cognitive overload [8], assessment of correct depth perception, Information Filtering, and Object Selection among others [9].

2. CURRENT STANDARDS FOR NATO CYBERSECURITY.

According to NATO Doctrine about Cyber Operation [10], "Cyberspace is far more than merely the Internet. All devices reachable via cyberspace could be potential targets and potential threats.". NATO recognised cyberspace as a domain of operations in 2016 and is now recognised as such alongside the traditional domains of air, land, and sea [11]. At the 2021 NATO Summit in Brussels, the Alliance also recognised that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as an armed attack [12]. Moreover, in the last iteration of its Strategic Concept adopted in June 2022 the Alliance recognised the ever-contested state of cyber space, where "Malign actors seek to degrade [our] critical infrastructure, interfere with [our] government services, extract intelligence, steal intellectual property and impede [our] military activities." [13]. In the same document, the enhancement of cyber defences is mentioned as a crucial point, especially in the context of the integration of new and disruptive technological solutions developed together with the private sector. It is also stated how the conventional OPSEC approach based on prevention, detection, countering, and response, equally applies to the cyber domain. The latest development in terms of NATO cyber policy comes from the 2023 NATO Summit in Vilnius, where the Allies endorsed a new concept to reinforce the contribution of cyber defence to NATO's overall deterrence and defence posture. At the Vilnius Summit, Allies also restated and enhanced the Cyber Defence Pledge of 2016 [14] and committed to more ambitious goals to strengthen national cyber defences as a matter of priority, including for critical infrastructures. Leaders also announced the first comprehensive NATO Cyber Defence Conference in Berlin in November 2023, to bring together decision-makers across the political, military and technical levels [15].

However, as of today, there is no NATO AJP specifically addressing cybersecurity. Relevant definitions in the field do, however, exist. The NATO Doctrine about Cyber Operation identified the cyberspace as "The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data." [16]. Directly related is the definition of Cyber Security (or cybersecurity), described as "The application of security measures for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation." [16]. In the context of NATO publications, cybersecurity has also been defined as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification or exploitation" [17].

In AJP-3.20, the Alliance identified four main categories of malicious actors -or threat actors- that can undermine cyber activities and take advantage of eventual gaps in the realm of cyber security. Those actors and their characteristics are presented in the table below [2]:

Table 1: categories of cyber threat actors and their characteristics according to NATO AJP-3.20.

Threat actor	Characteristics
State actors	Adversaries that may conduct terrorist, espionage, subversive, sabotage, organised crime or other malicious kinds of activities. Such activities may be conducted by State bodies/formally affiliate institutions both below the threshold and during an open armed conflict.
Non-state actors	Even though formally classified as independent entities, non-state actors could be exploited by (and their actions attributed to) States to conduct offensive cyber activities, especially when the expertise and/or technological means are limited at State level.
Criminals	Criminal groups conduct malicious cyber activities mainly to gain wealth and fame. They are not necessarily politically motivated and rarely impact military activities, even though the difference with non-state actors could be non-existent from the technical capabilities' perspective.
Insiders	Personnel disgruntled, corrupt, or affiliated to an adversary could try to cause harm to the Alliance through relatively cheap cyber methods, infiltrating the defences from the inside. Sometimes threat actors can access elaborate cyber security systems by exploiting an insider who is not aware but ignores certain cyber security measures.

As the Alliance hold responsibility for the cyber security of its own networks and IT infrastructure, and not for the ones of its Members, in 2003 the NATO Computer Incident Response Capability (NCIRC) was established to protect NATO's own networks by providing centralised and round-the-clock cyber defence support to various NATO sites. However, in the context of NCIRC, a Rapid Reaction Teams can be deployed to support the protection of NATO or Allied networks [18]. An additional push for the provision of NATO-centred cyber operational support came in 2021 In September 2021, with the appointment of the first Chief Information Officer (CIO) to "facilitate the integration, alignment and cohesion of ICT systems NATO-wide" [15]. The last development in this sense comes from the Virtual Cyber Incident Support Capability (VCISC), launched after the July 2023 NATO Summit in Vilnius to support national mitigation efforts in response to significant malicious cyber activities.

That being said, in the end are the States that are responsible for the cyber security measures to be taken internally. That means that it is States' responsibility to ensure that its organisations and representatives are acting in compliance with recognised international standards (i.e., the ones redacted by the International Organization for Standardization (ISO) in collaboration with the International Electrotechnical Commission

[2] NATO AJP-3.20, as assessed in the framework of the research conducted by the authors in the context of NATO RTG NMSG-HFM-354.

(IEC) on Cybersecurity), such as ISO/IEC 27001 dealing with Information Security Management Systems (ISMS). Among the international standards to be applied at national level is also the European General Data Protection Regulation (GDPR) that, in the context of CBRN XR training scenarios shall be strictly followed by all EU countries. To conclude, it should be noted how cybersecurity measures are not necessarily limited to preventing -and responding to- external attacks. The measures to be set up include proper handling of personal and sensitive data, trainings and scenarios' data, and all kind of information transferred from/to the XR headsets from/to the cloud, workstation or other data storage location.

3. DATA AND CYBER SECURITY RISKS TO BE TAKEN INTO ACCOUNT WHEN DESIGNING A CBRN XR/VR SCENARIO

XR/VR scenario development, particularly in the CBRN area, calls for particular attention to data and cybersecurity threats. For the purpose of this paper, the risks have been identified in the following categories: 1) hardware; 2) software; and 3) network. Each of these risks, clearly presents unique challenges and potential vulnerabilities that are in most cases intertwined. In the context of EU funded projects, there is a strong demand to pay attention to data and cybersecurity concerns. The European Union requires all projects developed with EU funds, to comply with existing EU regulations. This includes the purchase of hardware produced and software developed in the EU. Even if derogations are possible, the need protect sensitive data, ensure compliance with stringent privacy regulations, enhance cybersecurity, and reduce dependency on non-EU technologies is more and more required. Even though it is still possible to conduct tests and equipment which is not produced in the EU, additional care should be exercised to ensure that products are not counterfeited or tampered, as this will pose additional vulnerabilities and potentially compromise the security of the entire system.

Concerning hardware risks when developing a VR scenario, the difference between wired and wireless solutions comes into play, as it influences the whole architecture. In principle, wired solutions -i.e., those connected to supporting hardware via a physical cable- mitigate the risk of external access to the system at the cost of introducing physical limitations for the movement of trainees. On the other hand, wireless solutions have a positive impact on mobility but must take into account a wider spectrum of cyber risks, including eavesdropping[3] [19], interference, and unauthorized access. Implementing robust encryption protocols for wireless communication is thus essential to mitigate these risks.

Software security in VR scenario development is related to different factors. Among those, the encryption of installed files constitutes a security measure to protect the sensitive data and content within the scenarios. In fact, in the event of loss or theft of the physical headset solution or related equipment, encryption ensures that unauthorized access to potentially restricted information is prevented. Additionally, when using commercial off-the-shelf headsets, interactions with pre-existing software must be taken into account, particularly when third party software is installed by default. This is because malicious software could exploit these interactions to gain unauthorized access or control over the system, propagating the infection to several connected devices or by silently acting as a backdoor for the transmission of data to the outside. In that regard, thorough testing and validation of the software ecosystem are necessary to ensure a secure interaction. If those security measures are especially true for scenarios developed by using actual classified data (for example, by realistically designing a particular effect of a WMD, but also characteristics and proprieties of materials and ballistic data of weapons and weapons systems), it must be highlighted that even when operating in a scenario setting that does not entail classified information for its development, the procedures undertaken by the trainees may be sensitive.

[3] "An attack in which an attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the claimant".

However, in terms of software measures, the XR/VR training platforms should also possess high standards for the safeguard of data (both personal and related to the intended use) generated by the system. Regarding the first category, as defined by Article 4(13), (14) and (15), and Article 9 and Recitals (51) to (56) of the EU GDPR [20], personal data include a specific category, known as sensitive data, that entails i.e., data revealing ethnic origin, political opinions, philosophical beliefs, but also biometric data. The latter (including, i.e., fingerprint verification and iris scanning) are particularly sensitive in the military context, as it could be used to access restricted security areas and devices. The GDPR also put emphasis on key matters such as the consent of the subject for the collection and storage of data, and the removal, deletion, and processing of the data. A feasible way to protect personal data include the pseudonymisation process - that is, replacing any information which could be used to identify an individual with a pseudonym- or the anonymisation of data -in which the information is stored in such a way that the individual is not or no longer identifiable and is no longer considered personal data-. However, the anonymisation process does not fall under GDPR regulations. When considering the second category -that is, data generated by the system during its intended use- the presence of an After-Action Report (AAR) automated system (that automatically register inputs and actions from the trainee and collect them to provide overall feedback on the training) must be carefully evaluated and assessed in terms of data protection issues. The reason is that, even though the AAR may not refer to a recognisable individual (thanks to pseudonymisation or anonymisation processes described above), the aggregated data coming from multiple training sessions potentially involving hundreds if not thousands of trainees may reveal gaps in training and capabilities of NATO MS.

Finally, when developing a scenario requiring internet connection to function properly, multiple risks related to networks' proprieties are to be taken into account; of particular concern for military activities and training are malicious or involuntary upload and transfer of information to third parties. The risks of the use of an intranet network are strictly related to those of an internet one, but somewhat limited by the need for a malicious actor to be in close proximity to the physical location where the training is occurring. An offline version indeed reduces drastically these risks but requires the whole setting to be offline.

4. SOLUTIONS ADOPTED BY FONDAZIONE SAFE IN THE CONTEXT OF EU AND NATO RTG SPONSORED ACTIVITIES TO MITIGATE THE RISKS.

In addressing the delineated risk categories, SAFE and its partners resorted to mitigation strategies during the development, testing, and finalization phases of the activities it implemented. Those strategies both came from previous experience and the need to address certain shortcomings and gaps with creative solutions that are much simpler and cheaper to implement compared to otherwise technically complicated IT-related ones.

Starting from the hardware risks, during the internal development of a CBRN VR training scenario to be used at SAFE Testing & Training Calvarina facility, comprehensive analyses were conducted by the team of developers, ensuring the integrity of headsets thus excluding that the headset had been tampered. Additionally, to mitigate theft or loss, each headset was safeguarded by a password/gesture protection mechanism that requires hard reset for removal, hence making the headset data secure. Safe storage and transportation of the device from/to SAFE HQ is also exercised, with the components of the system being located in a dedicated office that can be securely locked.

In the context of the same initiative on the software front, the scenario was developed with dual configurations, encompassing encrypted or non-encrypted options. To access the scenario, users are prompted to input a password, which can be modified periodically to enhance security. Furthermore, the scenario was architected within an encrypted environment, reinforcing computer security through threefold level of security: BIOS password, encrypted hard drive, and a complex password for computer access. In the event of loss or theft, the system supports a remote lock feature. However, those measures alone may not be sufficient in every circumstance. In fact, as a general rule, when dealing with classified information transmitting unencrypted data over third-party services not on-premises is legally forbidden. This has an effect on the use of XR and streaming platform for the CBRN training. As an example, NVIDIA CloudXR is a provider of VR streaming via the cloud. CloudXR streams VR information unencrypted directly to VR devices. Therefore, if the VR image or audio contains classified information, it will flow uncontrolled to other connected locations. For this reason, cloud storage shall not be considered an ideal solution, with the necessary resources running in local on dedicated devices to be the preferred one.

When it comes to the generation of After-Action Report in the scenario internally developed at SAFE, they comply with the anonymisation of data, considering that the system does not require personal data to function (even when operating as intranet-connected device instead of stand-alone mode). If needed to, the tag/identifier of a trainee can be either stored on a separate device with no association dataset wise or registered physically on a list that can be later securely stored as to comply with personal data protection guidelines. This solution can be applied to any scenario that requires this kind of feature with minimal technical strain.

The need to produce AAR compliant with cyber and data security also emerged in the context of NATO MSG-HFM-354 activities on the “Study, Design, Building and Deployment of a CBRN XR Training Platform”. The automatic generation of AARs to evaluate the performance of trainees (even simultaneously) without overburdening trainers is seen as an extremely strong point in favour of this kind of solutions, however security constraints must be kept in mind. Possible solutions discussed in the context of the RTG include designing a part of the reference scenario (which involves a written reporting procedure) integrating an extended reality component in which a physical sheet of paper is recognised by the system. The trainee is then able to fill-in the module (using a conventional pen or pencil, just like the real-life procedure would entail) and completing the reporting without any kind of data registered by the system. The evaluation of this specific task undertaken by the trainee is then evaluated by a human instructor, so that a potential aggregation of data containing systematic shortcomings in this phase of the training is not registered and does not generate a classified data.

Finally, when it comes to network measures, the scenario developed by SAFE was tailored to operate across different network environments, including internet connectivity for multiplayer engagement with the ability for remote players to participate, intranet for localized multiplayer interaction, and an offline mode for single player use. Even though the use of the former is not to be preferred for the reasons discussed above, there is nonetheless the possibility to execute the scenario on trusted internet networks, ensuring compliance with prescribed physical conditions, such as physical limits surrounding the network (thus not being identifiable from outside) and, ideally, to work on hidden networks hence further improving the security architecture. The intranet mode, which is currently the one preferred at SAFE Testing & Training area, operates wirelessly while avoiding internet connectivity, with all data traffic being solely between the headsets connected and a dedicated laptop. The fact that the Calvarina Testing & Training area is located in a remote location greatly increases protection against attacks that require the malicious actor to be in close proximity to access the network. Finally, to avoid connecting to unknown networks, the use of the offline solution is not only encouraged but also the only approved one when the headset containing the CBRN VR training scenario is transported to be presented in the context of workshops, conferences, and meeting with potential end-users. In that way, even relatively simple cyber-protection measures such as password-protected headsets and password required to access the scenario are considered sufficient.

5. CONCLUSIONS

In this work, a list of fundamental concerns regarding cyber and data protection in the context of the development of a XR/VR training scenario, together with some solutions implemented by Fondazione SAFE in the context of different activities, were presented. To do so, an overview of the contemporary evolution regarding the use of XR/VR systems in the military context was presented, together with relevant NATO cybersecurity guidelines and various elements to be assessed in terms of hardware, software, and network. Both technical elements and creative solutions to meet the guidelines in terms of cyber and data security were presented, based on the direct experience of Fondazione SAFE during the implementation of different activities. Amongthe solutions, while the ones related to the hardware are somewhat more intuitive and more feasible to achieve (i.e., protecting the devices and running programmes with proper encryption, also guaranteeing that storage and transportation can satisfy adequate levels of security), the ones related to software need to take into account factors that may not be immediately recognisable. In fact, even when the scenario per se does not contain sensitive data to simulate certain events, the procedures undertaken by trainees might be, thus requiring appropriate level of protection. Furthermore, the generation of automatic After-Action Reports (AARs), a feature that brings a considerable added value to the whole XR/VR training concept, must comply with data and cybersecurity guidelines in order not to expose any personal information or -when taking into account aggregated data- potential flaws and gaps in the actual training procedures. Regarding the former, anonymisation of data seems to be a good solution; however, for the latter, non-creating relevant aggregated data in the first place might be the most suitable solution both from a security and technical point of view. In order to do so, some elements bound to be evaluated can be gathered via physical forms (i.e., paper-based modules) that the VR system is programmed not to recognise. Finally, regarding the network environment, the best solutions in terms of security remain the one able to operate completely offline. Despite entailing several limitations (that in the case of a system capable of offering multiplayer capabilities shall be carefully evaluated), it constitutes the only setup that can be considered immune from network-related cyber threats.

6. REFERENCES

[1] Elsa B. Kania, Ian B. McCaslin, *The PLA's evolving outlook on urban warfare: learning, training, and implications for taiwan, in military learning and the future of war series*, Institute for the Study of War, April 2022, https://www.understandingwar.org/report/pla%E2%80%99s-evolving-outlook-urban-warfare-learning-training-and-implications-taiwan (Accessed September 2023).

[2] See, among others, J.A. Booth, *The Use of Virtual and Augmented Realities in Air Force Training*, Air Command and Staff College - Distance Learning, 29 Apr 2019. https://apps.dtic.mil/sti/pdfs/AD1107328.pdf (Accessed August 2023).

[3] Capt. A. Rasmussen, *AFSOC embraces extended reality to enhance readiness*, in Beale Air Force base website, Oct 5, 2023. https://www.beale.af.mil/News/Article-Display/Article/3549539/afsoc-embraces-extended-reality-to-enhance-readiness/ (Accessed October 2023).

[4] J. Judson, *BAE Debuts 'See Through' Armored Vehicle System in US*, in Defense News website, Oct 14, 2015. https://www.defensenews.com/digital-show-dailies/ausa/2015/10/14/bae-debuts-see-through-armored-vehicle-system-in-us/ (Accessed August 2023).

[5] Kelley M. Sayler, *Military Applications of Extended Reality*, Congressional Research Service (CRS), Updated May 2022 https://sgp.fas.org/crs/natsec/IF12010.pdf (Accessed August 2023).

[6] See, among others, Keith B. Alexander, Jamil N. Jaffer, *Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition*, in Georgetown Journal of International Affairs, vol. 19, 2018, pp. 51–66. JSTOR, http://www.jstor.org/stable/26567527. (Accessed August 2023).

[7] A. Roque, *Course correction: US Army renegotiating USD22 billion IVAS contract, eyeing path for different form factor*, 9 Nov 2022, in Janes.com. https://www.janes.com/defence-news/news-detail/course-correction-us-army-renegotiating-usd22-billion-ivas-contract-eyeing-path-for-different-form-factor (Accessed August 2023).

[8] Boyce, Michael & Thomson, Robert & Cartwright, Joel & Feltner, David & Stainrod, Cortnee & Flynn, Jeremy & Ackermann, Christian & Emezie, John & Amburn, Charles & Rovira, Ericka. (2022). *Enhancing Military Training Using Extended Reality*: *A Study of Military Tactics Comprehension*. In Frontiers in Virtual Reality. 3. 754627. 10.3389/frvir.2022.754627.

[9] Livingston et al., *Military Applications of Augmented Reality*, in Handbook of Augmented Reality, 2011, https://apps.dtic.mil/sti/pdfs/ADA638065.pdf (Accessed August 2023).

[10] NATO 2020. NATO standard: AJP-3.20: Allied Joint Doctrine for Cyberspace Operations. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (Accessed August 2023).

[11] *NATO Cyber Defence* (para. 70-71), Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016. https://www.nato.int/cps/en/natohq/official_texts_133171.htm?selectedLocale=en (Accessed August 2023).

[12] *Comprehensive Cyber Defence Policy* (para. 32), Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, 14 June 2021. https://www.nato.int/cps/en/natohq/news_185000.htm#32_(Accessed August 2023).

[13] NATO 2022 Strategic Concept Adopted by Heads of State and Government at the NATO Summit in Madrid 29 June 2022 (available online).

[14] Cyber Defence Pledge, NATO Press Release (2016) 124, 8 July 2016 https://www.nato.int/cps/su/natohq/official_texts_133177.htm (Accessed August 2023).

[15] *Cyber defence*, in NATO website https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed August 2023).

[16] NATO 2020. NATO standard: *AJP-3.20: Allied Joint Doctrine for Cyberspace Operations*, *Terms and definitions*. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (Accessed August 2023).

[17] Sean S. Costigan, Michael A. Hennessy (edited by), NATO, 2016. *Cybersecurity - A Generic Reference Curriculum*. p.15. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-curriculum.pdf (Accessed August 2023).

[18] Alexander Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication, p.181, Tallinn 2012, https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf (accessed August 2023).

[19] Paul A. Grassi Michael E. Garcia James L. Fenton, *Digital Identity Guidelines*, NIST Special Publication 800-63-3: https://doi.org/10.6028/NIST.SP.800-63-3 (Accessed Sept 2023).

[20] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).