RAIS Journal for Social Sciences | Vol. 10, No. 1, 2026
ISSN 2574-0245 (Print) | ISSN 2574-1179 (Online) | DOI:10.5281/zenodo.19661757

Digitalization of Reserve Management in NATO/EU: Record-Keeping, Call-Up, Distributed Training, and Cyber Risks

Elena-Adriana Brumaru

PhD Candidate, Military Academy of the Armed Forces "Alexandru cel Bun," Republic of Moldova
brumaruelenaadriana03@gmail.com

Abstract: Military reserve management is undergoing a structural transformation driven by accelerated digitalization and interoperability requirements within NATO and the European Union. This article critically examines reserve personnel record-keeping and mobilization architectures, distributed training models based on the Live-Virtual-Constructive (LVC) paradigm, and cyber risks specific to digital reserve management platforms. By comparing centralized and federated data management models, the paper identifies opportunities to reduce force generation cycle times while highlighting vulnerabilities associated with digitalization, including the compromise of databases containing reservists' personal information and denial-of-service attacks during critical call-up periods. The analytical framework integrates European legal requirements (GDPR, NIS2) with NATO standards (STANAGs) and proposes a governance model oriented toward resilience and operational continuity. The conclusions offer eight prioritized recommendations for strategic, technical, and operational decision-makers.

Keywords: Reserve Management, Military Digitalization, NATO Interoperability, Distributed Training, Cybersecurity, GDPR, Operational Resilience

1. Introduction

The digital transformation of armed forces is no longer a strategic option, but an operational necessity. In a context where NATO and the European Union face an increasingly complex security environment—marked by hybrid conflicts, pressures on the eastern borders, and persistent cyber threats—the capacity to generate force rapidly, efficiently, and interoperably becomes an essential indicator of alliance credibility. In this equation, military reserves play a crucial, yet often underestimated, role (Szvircsev Tresch, 2019).

Reserve management—personnel record-keeping, call-up, training, and distributed readiness—has remained, in many NATO and EU member states, anchored in bureaucratic paradigms inherited from the Cold War era. Paper files, telephone call-ups, and exclusively in-person training still constitute the norm in some European armies, despite political commitments to modernization. This situation creates a dangerous asymmetry between the ambition declared at NATO summits and the actual mobilization capacity at the national level (NATO, 2022).

Digitalization promises to compress the force generation cycle—that critical interval between the political decision to activate reserves and the moment when reserve units become operational. An integrated digital system can reduce this cycle from weeks to days, through automated call-up, instantaneous verification of availability and qualifications, and facilitation of remote training (Lasconjarias & Larsen, 2015). However, digitalization is not

without risks. The centralization of reservists' personal data on digital platforms creates attractive targets for state and non-state adversaries, while dependence on digital infrastructures introduces vulnerabilities that can be exploited precisely at moments of maximum tension (Libicki, 2009).

This article aims to analyze this tension between opportunity and risk, structuring the inquiry into three complementary sections. The first section examines reserve management architectures, comparing centralized and federated models and discussing data interoperability standards. The second section addresses distributed training and readiness, with emphasis on the Live-Virtual-Constructive (LVC) paradigm and the operational limitations of these models. The third section deals with security and governance, analyzing specific cyber risks and proposing a data protection and operational continuity framework.

The relevance of the topic is amplified by the recent lessons of the conflict in Ukraine, where the rapid mobilization of reserves proved a determining factor in the state's capacity for resistance. The Ukrainian experience demonstrated that states investing in digital record-keeping and call-up systems can activate significant reserves within a compressed timeframe, while those relying on manual procedures risk disorganization and critical delays. This lesson has redefined the urgency of digitalization in many NATO and EU member states, transforming a technical concern into a strategic priority (Fiott, 2018).

The methodological approach combines critical review of the specialized literature with conceptual analysis and the proposal of architectural models. The sources used include official NATO and EU documents, technical standards (STANAGs, ISO), European legal frameworks (GDPR, NIS2), peer-reviewed articles, and defense think-tank reports. The analysis maintains a clear distinction between public data and the author's interpretations, respecting the rigor of academic research applied to the security domain (Buzan et al., 1998).

2. Reserve Management Architectures: Record-keeping, Mobilization, Data Interoperability

2.1 Architectural Models: Centralized versus Federated

The management of reservist records in NATO states oscillates between two fundamental architectural paradigms. The centralized model presupposes a single database, administered at the national level, which concentrates all information regarding reserve personnel: identification data, military qualifications, health status, availability, and training history. This model, adopted in one form or another by states such as Estonia and Finland, offers the advantages of data integrity and query speed, but presents a single point of failure: the compromise of the central database would expose the entire reserve force (Jermalavicius et al. 2018).

The federated model, by contrast, distributes data across multiple institutional nodes - service branches, regional commands, reserve units, which retain autonomy over their own datasets, but share a common metadata layer through standardized interfaces. This model, closer to the practice of federal states such as Germany or Belgium, offers superior resilience to attacks, but introduces significant challenges in data synchronization and consistency (Bundesministerium der Verteidigung, 2016).

A third, hybrid approach combines a central metadata registry with distributed repositories of detailed data. The central registry maintains an index of reservists with essential attributes (rank, military specialty, availability status), while sensitive data (medical, security) remains in local nodes. This architecture reduces the attack surface of the central component and complies with the data minimization principle imposed by GDPR (European Parliament and Council of the EU, 2016).

The choice of architectural model is not merely a technical decision; it reflects deep political and institutional trade-offs. States with a centralist tradition in military administration will naturally gravitate toward centralized models, while federal structures will favor distribution. What matters is that the decision be informed by an explicit risk assessment, and not merely by institutional inertia. Moreover, whichever model is chosen, the interoperability layer must be designed from the outset to facilitate data exchange with allies, rather than added later as an extension (Lasconjarias & Larsen, 2015).

Comparing the three models shows that there is no universally optimal solution for managing reservist records in NATO countries, but only different options for balancing administrative efficiency, cybersecurity and institutional coherence. The centralized model offers high speed and data integrity, but concentrates risk in a single point of vulnerability, as illustrated by the experience of countries such as Estonia and Finland. The federated model, practiced in forms similar to Germany or Belgium, increases resilience by distributing data, but complicates synchronization and maintaining information consistency. The hybrid approach appears to be a functional compromise, reducing the attack surface of the central core and aligning with the data minimization principles imposed by the European Union through the GDPR framework. Ultimately, the choice of architecture is not purely technical, but reflects the administrative culture, the structure of the state and the tolerance for risk. The optimal decision must be based on an explicit strategic assessment of vulnerabilities and the integration of allied interoperability requirements during the design phase, not on simple institutional continuities.

2.2 Data Standards and Interoperability

Within the NATO context, personnel data interoperability is based on a network of standardization agreements (STANAGs) that define common formats for information exchange. STANAG 2287, for example, establishes personnel strength reporting procedures, but was not originally designed for integrated digital environments. Adaptation to the digital era requires the adoption of structured data formats such as XML or JSON, with metadata schemas compliant with NATO Federated Mission Networking (FMN) standards (NATO, 2023a).

At the European Union level, the European Interoperability Framework (EIF) provides guiding principles for data exchange between public administrations, principles also applicable to the defense domain. Concrete implementation requires defining a minimum metadata set for reservist records, which should include: an interoperable unique identifier, military rank (according to the NATO rank table), primary military occupational specialty (MOS code), date of last medical certification, security clearance level, and availability status (European Commission, 2017).

The proposed format should comply with the ISO 8601 standard for calendar dates, ISO 3166 for country codes, and adopt a semantic model based on military ontologies such as JC3IEDM (Joint C3 Information Exchange Data Model), which enables structured querying of personnel information in a multinational environment (NATO, 2019).

An often-neglected aspect in discussions about interoperability is that of semantic governance. It is not enough for data to be in the same technical format; they must carry the same meaning across different national contexts. The concept of "available reservist," for example, varies significantly between a conscription-based system (such as Finland's) and a volunteer-based one (such as the United Kingdom's). Semantic harmonization requires the development of a common controlled vocabulary, validated by national experts and mapped onto existing national taxonomies. Without this harmonization, technical interoperability remains superficial - systems can exchange data, but cannot correctly interpret them in an operational context (European Commission, 2017).

The analysis highlights that interoperability of personnel records within NATO and the European Union cannot be reduced to the simple technical compatibility of data formats. Although standardization agreements such as NATO STANAG 2287 provide a common framework for reporting personnel, they need to be adapted to today's digital realities by using structured formats (XML, JSON) and by aligning with architectures such as Federated Mission Networking (FMN). In parallel, the principles of the European Union, reflected in the European Interoperability Framework (EIF), indicate the need for a standardized minimum set of metadata and the use of established international standards (ISO 8601, ISO 3166), as well as robust semantic models, such as JC3IEDM, to ensure the coherence of data querying in a multinational environment. However, the critical element identified is semantic governance. Without a harmonization of meanings—through a common controlled vocabulary and mapping between national taxonomies—interoperability remains formal, not functional. Structural differences between national systems, such as those in Finland and the United Kingdom, demonstrate that the same label can hide distinct operational realities. Genuine interoperability therefore requires the simultaneous integration of three levels: technical (formats and standards), semantic (shared meaning) and institutional (validation and governance). Only a coordinated approach to these dimensions can transform data exchange from an administrative exercise into an effective operational tool.

2.3 Mobilization Flows and Digital Call-Up

The digital call-up of reservists involves a chain of processes that begins with the political decision to activate and concludes with the physical reporting of the reservist to the designated unit. In a digitalized system, this chain can be partially automated: the system identifies eligible reservists based on operational criteria (specialty, distance from the assembly point, valid medical status), transmits notifications through multiple channels (mobile application, SMS, e-mail), and collects participation confirmation in real time (Ringsmose & Ryning, 2017).

The critical element of digital call-up is the resilience of communication channels. A coordinated cyberattack on national telecommunications infrastructure during the call-up period could paralyze the process. Therefore, the call-up architecture must include redundant channels: in addition to primary digital channels, it is essential to maintain backup procedures based on radio networks or personal call-up chains at the local level, following the Finnish model (Ministry of Defence Finland, 2021). Mobilization time thus becomes a measurable indicator of the digital maturity of the reserve system. The strategic objective should be to reduce the average call-up time from 72 hours to under 24 hours for priority categories of reservists, an objective achievable only through a coherent integration of record-keeping, communication, and validation systems (Fiott, 2018).

Therefore, we can say that the digital conscription of reservists involves a chain of processes that starts with the political decision to activate and ends with the physical presentation of the reservist at the designated unit. In a digitalized system, this chain can be partially automated: the system identifies eligible reservists based on operational criteria (specialty, distance from the assembly point, valid medical condition), sends notifications through multiple channels (mobile application, SMS, email), and collects confirmation of participation in real time (Ringsmose & Ryning, 2017). The critical element of digital conscription is the resilience of communication channels. A coordinated cyber attack on the national telecommunications infrastructure during the conscription period could paralyze the process. Therefore, the conscription architecture must include redundant channels: in addition to primary digital channels, it is necessary to maintain reserve procedures based on radio networks or personal conscription chains at the local level, following the Finnish model (Ministry of Defence Finland, 2021). Mobilization time thus becomes a measurable

indicator of the digital maturity of the reserve system. The strategic objective should be to reduce the average call-up time from 72 hours to under 24 hours for priority categories of reservists, an objective achievable only through a coherent integration of record-keeping, communication and validation systems (Fiott, 2018).

3. Distributed Training and Readiness: Models, Validation, Operational Limitations

3.1 Distributed Training Concepts and the LVC Paradigm

Distributed training represents a paradigm through which reservists can maintain and develop military competencies without being physically present at a training facility, using communication and simulation technologies accessible remotely. Within NATO, the reference model for distributed training is the LVC paradigm, which integrates three components: training in a real environment (Live), with physical equipment and personnel; virtual simulation (Virtual), in which personnel operate simulated systems; and constructive simulation (Constructive), in which both forces and the environment are computer-generated (NATO 2023b). For reservists, the virtual and constructive components are particularly relevant, as they enable training outside concentrated training periods. A reserve logistics officer, for example, can work through transport planning scenarios in a constructive environment accessible online, maintaining their skills without traveling to a garrison. NATO has recognized this potential through the Connected Education and Training Directive, which encourages the use of digital platforms for individual and collective training (NATO Allied Command Transformation, 2020).

The integration of the three LVC components into a coherent training environment remains, however, one of the most complex technical challenges. Each component operates with different protocols, different levels of fidelity, and different bandwidth requirements. Temporal and spatial synchronization between a Live exercise at a training range, a virtual simulation on an artillery simulator, and a constructive simulation of troop movements at the brigade level requires sophisticated middleware infrastructure and rigorous interoperability standards. Nevertheless, for individual or small-group training of reservists, the virtual and constructive components can be used independently, with more accessible technical requirements (Cayirci, 2013).

Thus, distributed training, based on the LVC paradigm promoted by NATO, represents a strategic solution for maintaining the skills of reservists in an increasingly digitalized and dispersed operational environment. For this category of personnel, the Virtual and Constructive components offer a major advantage: flexibility, accessibility and continuity of training outside concentrated training periods, reducing logistical costs and mobility constraints. However, the full integration of the three LVC dimensions into a unified ecosystem remains a complex technical challenge, involving advanced synchronization, strict interoperability and high-performance middleware infrastructure. From this perspective, the gradual application—independently using the virtual and constructive components for individual or small group training—appears as a pragmatic and sustainable option for reservists. In essence, distributed training does not completely replace training in a real environment, but complements and amplifies it, transforming technological availability into a force multiplier for the military reserve.

3.2 Simulation Technologies and Training Platforms

Distributed training platforms range from sophisticated tactical simulation systems, such as the Joint Multinational Simulation Center (JMSC), to web-based applications for individual training, such as Learning Management System (LMS) platforms. For reservists, pragmatic options include: e-learning modules for doctrine updates, serious games for developing

tactical thinking, virtual staff exercises via videoconference, and constructive simulation scenarios accessible through a secured VPN (Page and Smith 2018).

The technical interoperability of simulation platforms is governed by the IEEE 1516 standard (High Level Architecture [HLA]), which allows the connection of different simulators into a common federation. However, implementing HLA in the context of reservist training encounters practical difficulties: subscription costs, the technical complexity of integration, and the need for stable bandwidth, which not all reservists have at home (Cayirci, 2013).

3.3 Competency Validation and Certification

A fundamental challenge of distributed training remains validation: how can competency acquired through remote training be credibly demonstrated? Current NATO certification models rely predominantly on evaluation in a physical environment (Combat Readiness Evaluation [CREVAL]), which creates a discrepancy between digital training and the mechanisms for its recognition (NATO, 2016).

A partial solution lies in the development of digital competency frameworks specific to reservists, which correlate learning objectives with measurable indicators in the virtual environment. The digital competency portfolio, based on the e-CF (European e-Competence Framework) standard, could be adapted to include military competencies validated through simulated exercises. This would require: clear definition of performance objectives for each specialty, instrumentation of simulation scenarios with automated performance indicators, and the establishment of a crediting system that partially equates distributed training with physical attendance at training courses (European Commission, 2019).

3.4 Operational Limitations

Distributed training cannot fully replace physical training. Competencies such as live firing, operations in a CBRN (chemical, biological, radiological, nuclear) environment, armored vehicle maneuvering, or first aid procedures under fire require physical presence and real equipment. Therefore, the optimal model is a blended one, in which distributed training covers the cognitive and procedural component, while concentrated training periods are dedicated exclusively to practical competencies (Sabin, 2015).

The logistics of distributed training also present challenges. Reservists have unequal access to digital infrastructure: variable bandwidth, personal devices with different capabilities, and different levels of digital competency. These disparities can create a "digital divide" within the reserve force, where urban units have access to advanced training, while rural units remain exclusively dependent on traditional methods (Wither, 2020).

Testing and certification must, therefore, include minimum technical accessibility standards and provide compensatory mechanisms for reservists who cannot access distributed platforms. The practical recommendation is that each member state establish a guaranteed minimum digital configuration (terminal, connectivity, multifactor authentication) for its reservists, modeled on the digital inclusion projects of the European Commission (European Commission, 2021).

Distributed training offers a flexible and cost-effective solution for maintaining reservists' cognitive and procedural skills, ranging from advanced simulation centers such as the Joint Multinational Simulation Center to accessible LMS-based e-learning platforms. While interoperability standards like IEEE 1516 (HLA) enable technical integration, practical constraints-costs, complexity, and unequal bandwidth access - limit full implementation at the reservist level. A major gap persists between digital training and formal recognition mechanisms, as current certification models such as NATO CREVAL

remain primarily oriented toward physical evaluation. Developing digital competency frameworks aligned with the European Commission e-CF standard could partially bridge this divide.

Ultimately, distributed training cannot replace hands-on preparation for physically intensive tasks. The optimal approach is a blended model, combining remote cognitive training with concentrated in-person practical sessions, while ensuring minimum digital access standards to prevent the emergence of a structural digital divide within reserve forces.

4. Security and Governance: Data Protection, Cyber Risks, Continuity

4.1 Legal Requirements: GDPR and NIS2

Digital reserve management platforms process sensitive personal data: identification information, medical data, institutional affiliations, home addresses, and security clearances. The General Data Protection Regulation (GDPR) mandates, through Articles 5 and 25, the principles of data minimization and protection by design (privacy by design), which oblige military system developers to collect and store only the data strictly necessary for the defined purpose (European Parliament and Council of the EU, 2016).

The NIS2 Directive, which entered into force in 2023, extends cybersecurity obligations to essential sectors, including public administration and, implicitly, defense structures. Member states are required to designate essential entities, establish incident reporting requirements, and impose cyber risk management measures. For reserve management platforms, NIS2 implies mandatory periodic security audits, incident notification within 24 hours, and the implementation of technical measures proportionate to the risk. The tension between GDPR requirements and the operational needs of defense is real. Article 23 of the GDPR allows the restriction of certain data subject rights for national security purposes, but the application of this exception varies significantly among member states, creating a fragmented legal landscape that complicates interoperability (Rojszczak, 2020).

4.2 Governance Model for Reserve Management Platforms

A robust governance model must integrate three dimensions: legal compliance, technical security, and operational continuity. At the organizational level, it is recommended to appoint a Data Protection Officer (DPO) dedicated to reserve personnel systems, distinct from the general DPO of the Ministry of Defense, given the specificity of the data processed. From the NATO perspective, the governance framework must be compatible with the NATO Cyber Defence Pledge (2016) and with the NATO Cyber Security Policy, updated at the Madrid Summit in 2022. This entails: data classification according to NATO security levels, role-based access control (RBAC), complete audit logging of data access, and logical separation of production, testing, and disaster recovery environments (NATO, 2022). The proposed model structures governance at three levels: the strategic level (national and allied policies, legal framework, risk tolerance); the operational level (incident management procedures, continuity plans, cyber exercises); the technical level (security configuration, continuous monitoring, patch and vulnerability management). Each level must have clearly defined responsibilities and upward reporting mechanisms (Kerttunen & Tikk, 2020).

An essential element of governance is the cycle of audit and continuous improvement. Reserve management platforms must be subjected to periodic security assessments, in accordance with the ISO 27001 standard for information security management systems, as well as regular penetration tests conducted by specialized teams. The results of these assessments must feed into a structured risk management process that

prioritizes vulnerability remediation according to the potential impact on mobilization capacity. This risk-based approach is more effective than mechanical compliance with checklists, as it allows the allocation of limited resources toward the protection of the most critical functionalities (Klimburg, 2012).

4.3 Cyber Risk Scenarios and Mitigation Measures

The analysis of cyber risks specific to reserve management platforms reveals several critical scenarios. The first and most severe scenario is the compromise of the database containing reservists' personal information. An adversary who gains access to these data can identify military reserve personnel, their home addresses, specialties, and individual vulnerabilities, facilitating influence operations, blackmail, or physical targeting (Rid 2020).

The second scenario involves denial-of-service (DDoS) attacks on call-up platforms during critical mobilization periods. A DDoS attack well-synchronized with a security crisis could delay call-up by hours or days, with potentially devastating operational consequences. Mitigation measures include: geographic distribution of call-up infrastructure, the use of content delivery networks (CDN), and the maintenance of alternative call-up channels (Pernik, 2018).

The third scenario targets the manipulation of record data without detection. A sophisticated adversary could subtly modify data - for example, altering availability status or qualifications - in order to degrade mobilization capacity without triggering alerts. Countermeasures require: implementation of cryptographic integrity of records (blockchain or hash-chains), periodic data consistency audits, and anomaly detection mechanisms based on artificial intelligence (Smeets, 2022).

4.4 Operational Continuity

The Business Continuity Plan (BCP) for reserve management platforms must ensure the minimum functioning of the system even under conditions of a major cyberattack or extensive technical failure. Essential components include: offline backups of critical databases, periodically updated and stored in protected facilities; predefined manual call-up procedures, practiced annually; emergency communication systems independent of the primary digital infrastructure; and an alternate command center for managing personnel crises (Klimburg, 2012).

Periodic cyber exercises, such as those conducted within the Locked Shields exercise organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), must be expanded to include scenarios specifically targeting reserve management platforms. These exercises should test both the technical resilience of systems and the capacity of personnel to switch to manual procedures in a timely manner (CCDCOE, 2023).

Last but not least, the human dimension of operational continuity must not be neglected. Personnel responsible for operating reserve management platforms must be regularly trained in emergency procedures, including the transition from digital systems to manual procedures. This dual competency - digital and analog - is essential for the real resilience of the system, beyond the technical resilience of the infrastructure. Consequently, continuing professional development programs for reserve management personnel must include dedicated modules on cyber crisis management and operations under conditions of digital degradation (Smeets, 2022).

5. Conclusions

The digitalization of reserve management within the NATO/EU space represents a strategic imperative that, when implemented coherently, can fundamentally transform force generation capacity. However, this transformation must be managed with an acute

awareness of the risks it introduces, from cyber vulnerabilities to legal fragmentation and digital access disparities.

The analysis conducted in this study has revealed a recurring tension between the benefits of digitalization - speed, interoperability, efficiency - and the associated risks: data centralization creates strategic targets, dependence on digital infrastructures introduces vulnerabilities, and the digital gap among reservists threatens equity of access to training. Managing this tension requires a balanced approach, grounded in the principle of resilience: systems must be designed not only for optimal performance, but also for graceful degradation under conditions of attack or failure. Based on the analysis conducted, the following eight recommendations are formulated, grouped at three levels:

At the strategic level:

1. Adoption, at the level of the NATO Military Committee, of a minimum standard for the digitalization of reservist records, with a five-year implementation deadline, to ensure personnel data interoperability among member states.

2. Explicit integration of the cybersecurity of reserve management platforms into national defense planning cycles and NATO capability assessments.

3. Harmonization of the interpretation of GDPR exceptions for national security purposes, through common guidance at the EU level, to facilitate the exchange of reserve data in a multinational context.

At the technical level:

4. Development of a minimum set of interoperable methods for reservist record-keeping, compatible with FMN and JC3IEDM, adopted through a dedicated STANAG.

5. Implementation of cryptographic integrity for record entries, through hash-chains or other integrity assurance mechanisms, for the detection of subtle manipulations.

6. Establishment of a guaranteed minimum digital configuration for each reservist (terminal, connectivity, multifactor authentication), as a precondition for distributed training.

At the operational level:

7. Annual testing of digital call-up procedures, including scenarios of digital infrastructure failure with switching to manual procedures, within the framework of national and allied exercises.

8. Inclusion of attack scenarios targeting reserve management platforms in NATO (Locked Shields, Cyber Coalition) and EU cyber exercises, for testing resilience under realistic conditions.

These recommendations do not exhaust the issue, but offer a structured starting point for a transformation that otherwise risks being driven by institutional inertia or commercial pressures, rather than by a coherent security vision.

References

Bundesministerium der Verteidigung. (2016). *Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr.* BMVg.

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis.* Lynne Rienner Publishers.

Cayirci, E. (2013). Modeling and Simulation as a Cloud Service: A Survey. *Proceedings of the 2013 Winter Simulation Conference,* 389-400. https://ieeexplore.ieee.org/document/6721436

CCDCOE. (2023). *Locked Shields 2023: After Action Report.* NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/exercises/locked-shields/

European Commission. (2017). *European Interoperability Framework - Implementation Strategy.* COM(2017) 134 final. https://ec.europa.eu/isa2/eif

European Commission. (2019). *European e-Competence Framework (e-CF) - Version 4.0.* Publications Office of the EU. https://ecompetences.eu/

European Commission. (2021). *2030 Digital Compass: The European Way for the Digital Decade.* COM(2021) 118 final.

European Parliament and Council of the EU. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (GDPR).* Official Journal of the EU L 119.

European Parliament and Council of the EU. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2).* Official Journal of the EU L 333.

Fiott, D. (2018). EU Defence Capability Development: Plans, Priorities, Projects. Chaillot Paper 148. EU Institute for Security Studies.

Jermalavicius, T., Praks, H., Stoicescu, K., & Pernik, P. (2018). *Comprehensive Defence in the Baltic States: Reservists and Volunteers.* International Centre for Defence and Security.

Kerttunen, M., & Tikk, E. (2020). Cyber Security Governance in the European Union. *Cyber Policy Institute Working Paper.* https://cypolicy.com/

Klimburg, A. (2012). *National Cyber Security Framework Manual.* NATO CCD COE Publications.

Lasconjarias, G., & Larsen, J. A. (Eds.). (2015). *NATO's Response to Hybrid Threats. Forum Paper 24.* NATO Defense College.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar.* Santa Monica: RAND Corporation. DOI: 10.7249/MG877.

Ministry of Defence, Finland. (2021). *Finland's Defence Report 2021.* Helsinki: Finnish Government. https://julkaisut.valtioneuvosto.fi/

NATO Allied Command Transformation. (2020). *Framework for Future Alliance Operations.* ACT. https://www.act.nato.int/

NATO. (2016). *Bi-SC Directive 075-007 on Education, Training, Exercise and Evaluation.* Mons: SHAPE.

NATO. (2019). *JC3IEDM - Joint C3 Information Exchange Data Model, Edition 3.1.4.* Bruxelles: NATO Consultation, Command and Control Agency.

NATO. (2022) *Strategic Concept.* NATO Public Diplomacy Division. https://www.nato.int/strategic-concept/

NATO. (2023a). *Federated Mission Networking Implementation Plan, Version 5.0.* Allied Command Transformation.

NATO. (2023b). *Connected Education and Training - Concept Paper.* Allied Command Transformation.

Page, E. H., & Smith, R. (2018). Introduction to Military Training Principles and Practices. *Proceedings of the Interservice/Industry Training, Simulation and Education Conference* (I/ITSEC).

Pernik, P. (2018). *Preparing for Cyber Conflict: Case Studies of Cyber Command.* International Centre for Defence and Security.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux.

Ringsmose, J., & Ryning, S. (2017). Now for the Hard Part: NATO's Strategic Adaptation to Russia. *Survival* 59 (3): 129-146. https://doi.org/10.1080/00396338.2017.1325603

Rojszczak, M. (2020). GDPR and National Security Exceptions. *Computer Law & Security Review* 36: 105381. DOI: 10.1016/j.clsr.2019.105381.

Sabin, P. (2015). Wargaming in Military History. In J. Ferris & E. Mawdsley (Eds.), *The Cambridge History of the Second World War* (pp. 386-404). Cambridge University Press.

Smeets, M. (2022). *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force.* Oxford University Press.

Szvircsev Tresch, T. (2019). Reserve Forces in European Countries. In S. Biscop & R. Whitman (Eds.), *Routledge Handbook of European Security* (pp. 245-260). Routledge.

Wither, J. K. (2020). Back to the Future? Nordic Total Defence Concepts. *Defence Studies* 20 (1): 61-81. https://doi.org/10.1080/14702436.2020.1718498.