Issues of RA's Defense Digitalization[1]

Danielyan Gyulnara S.
Quality management system specialist, Aerodynamics CJSC
PhD student at Public administration Academy of RA (Yerevan, RA)
https://orcid.org/0009-0007-4266-0495
gyulnaradanielyan20hk@paara.am

UDC: 330; **EDN:** SRGUJQ
DOI: 10.58587/18292437-2024.4-34
Keywords & phrases: digitalization, defense, Armenia, AI, technology, 4th industrial revolution

ՀՀ պաշտպանության ոլորտի թվային վերափոխման խնդիրները

Դանիելյան Գյուլնարա Ս.
«Աէրոդինամիքս» ՓԲԸ Որակի կառավարման համակարգի մասնագետ
ՀՀ ՊԿԱ ասպիրանտ (Երևան, ՀՀ)

Ամփոփագիր. Մինչ աշխարհը վայելում է չորրորդ արդյունաբերական հեղաշրջման և թվայնացվող աշխարհի առավելությունները, զուգահեռաբար ավելանում են ժամանակակից պաշտպանության ոլորտի թվային վերափոխման խնդիրները, որոնք ենթադրում են դիվերսիֆիկացված հարձակումներ՝ օժտված կրկնվելու մեծ հաճախականությամբ, ինչպես նաև դրանք հաղթահարելու բարդությամբ: Այժմ պետությունների պաշտպանունակությունը մեծապես կախված է թվային տեխնոլոգիաներից և դրանցով պայմանավորված մրցունակության մակարդակից: Արդի ժամանակներում նորագույն տեխնոլոգիաների շնորհիվ, պաշտպանունակության բարձրացումը այլևս հնարավոր է նաև փոքր պետությունների համար՝ այն դեպքում երբ փոքր պետությունները, ընդառաջ գնալով տեխնոլոգիական փոփոխություններին, ամրապնդեն իրենց դիրքը թվային աշխարհում: Հայաստանը, որպես տարածաշրջանային հակամարտություններում ներգրավված երկիր, պետք է անհրաժեշտաբար կայուն քայլեր ձեռնարկի պաշտպանական ոլորտը ժամանակակից սարքավորումներով ամրապնդելու ուղղությամբ և ապահովի հիմք պաշտպանության և անվտանգության հետ կապված ոլորտներում մարդկային կապիտալի զարգացման, պաշտպանական համակարգերի թվայնացման համար: Հոդվածում քննարկվում է Հայաստանի պաշտպանական ոլորտում թվայնացման համալիր նախաձեռնությունների իրականացման միջոցով պաշտպանական ոլորտի օպերատիվ արդյունավետության բարձրացման, ռազմավարական որոշումների բարելավման, կիբերանվտանգության ապահովման հնարավորությունները:
Հանգուցաբառեր և բառակապակցություններ՝ թվայնացում, պաշտպանություն, Հայաստան, տեխնոլոգիա, ԱԲ, 4-րդ արդյունաբերական հեղաշրջում

Проблемы цифровой трансформации оборонной сферы Армении

Даниелян Гюльнара С.
ЗАО "Аэродинамикс" Специалист по системе менеджмента качества
Академия государственного управления РА, аспирант (Ереван, РА)

Аннотация. В то время как мир наслаждается преимуществами четвертой промышленной революции и цифровизации мира, параллельно возникают проблемы цифровой трансформации современного оборонного сектора, связанные с разнообразными атаками, которые могут повторяться с высокой частотой, а также с трудностями их преодоления. Сейчас обороноспособность государств во многом зависит от цифровых технологий и обусловленного ими уровня конкурентоспособности. В наше время, благодаря новейшим технологиям, повышение обороноспособности стало возможным и для малых государств, в то время как малые государства, идя навстречу технологическим изменениям, укрепляют свои позиции в цифровом мире. Армения, как страна, вовлеченная в региональные конфликты, должна предпринять необходимые устойчивые шаги по укреплению оборонного сектора современным оборудованием и обеспечить основу для развития человеческого капитала, цифровизации оборонных систем в сферах, связанных с обороной и безопасностью. В статье обсуждаются возможности повышения оперативной эффективности оборонной сферы, улучшения стратегических решений, обеспечения кибербезопасности посредством реализации комплексных инициатив по цифровизации в оборонной сфере Армении.
Ключевые слова и словосочетания: цифровизация, оборона, Армения, ИИ, технологии, 4-й промышленный переворот

[1] This work was supported by the Higher education and Science Committee of MESCS RA (research project № **23AA-5B013**).

Intoduction

The digitalization process, which is an integral part of the 4th industrial revolution, is an inevitable and irreversible reality that has completely transformed the defense sector. The ultra-fast pace of technological progress has led to the merging of the physical, digital and biological worlds, creating both prospects and potential dangers [**16**]. Digitization processes in the defense sector and automation of some important operations can contribute to the formation of a safer environment, to some extent facilitating at least two of the perhaps most important tasks for states: reducing human losses during military clashes and safer borders. Solving these problems is an urgent problem for Armenia since Armenia has been involved in regional conflicts since independence

To counter the technological race, states (including small states with high levels of poverty, e.g. Armenia) must continuously increase allocations for the digitalization of the defense sector [**14**]. However, unlike the funds spent on the purchase of heavy weaponary, measures aimed at digitalizing the defense sector are justified, since as a result, some of the costs provided for servicing the sector will be significantly reduced. Digitization of the defense sector can reduce bureaucratic costs, optimize logistics, which will lead to savings in total defense sector costs. The use of big data and artificial intelligence in the field of defense can lead to more informed decision-making, thereby optimizing the allocation of resources.Strengthening cybersecurity with the help of digital technologies can reduce the risks associated with cyber attacks, thereby reducing possible financial losses and leakage of military data. Virtual learning environments based on digital technologies can reduce training costs and equipment wear and tear [**6**]. In order to take advantage of these and other advantages of digitalization of the defense sector, a timely and adequate response to changing security challenges established by a clear state policy is required. Approaches to the digitization of the defense sector are based on ideas such as network military operations, investments in artificial intelligence (AI), result orientation, etc. [**1**].

We have used descriptive analysis method considering th available information, reports, research, strategic programs related to digital transformation related to the RA's defense sector.

Literature review

The growing trend of digital transformation and the boundaries expanding every day have aroused the interest of a number of scientists. Heltberg explains the digitization process by its relationship with technological flows, which provide decision makers with optimized knowledge and help in conducting analysis, thereby also contributing to more targeted decision-making [**4**, pp. 220]. Although definitions differ because they emphasize various key aspects of this phenomenon, scientists agree on the positive impact of C4ISR (command, control, communications, computers, intelligence, surveillance and recognition) on the digitization process [**8**, pp. 456-479].

Speaking on the digitalization of the defense sector, Horowitz emphasizes the possibilities of artificial intelligence and the growing importance of cybersecurity in the development of defense sector and international security strategies. His research highlights the impact of digitalization processes on policy and decision-making in the defense sector [**3**].Speaking about the growing role of technology in the defense industry, Winkler notes that the latest digital technologies can lead to dynamic geopolitical changes, create asymmetric threats of hybrid wars and security[**10**]. Attaching particular importance to digital transformations in air defense, Bryant emphasizes that under the influence of hypersonic weapons, UAVs, various aerial reconnaissance and strike weapons, the nature of air warfare has changed significantly [**18**]. Research such as the digitization of the defense industry shows that the wars of modern times have left no alternative to either large or small states. Hoffman [**2**] argues that algorithmic warfare has a revolutionary impact on the defense industry while algorithmic warfare (due to artificial intelligence-based technologies) is also fraught with deadly risks. Matthew's research has shown that whenever algorithms get out of control, catastrophic consequences arise, and when they work flawlessly, they have a huge impact, which humanity could not achieve before [**5**, pp. 919-924]. Algorithmic wars, fraught with deadly risks and massive impact, are a reflection of a new revolution in the military sphere [**2**]. Digital transformation initiatives in NATO and EU member states have a positive impact on resource optimization. European governments emphasize the importance of gradually optimizing digital capabilities in the field of defense and are taking clear steps in this direction[**19**].

Armenia's digitalization strategy for 2021-2025, although it focuses on a development plan aimed at the full development of the country and covering socio-economic spheres [**21**], does not have a clear focus on the digitalization of the defense sector.

Processes and problems of digitization of the defense sector

Digital transformation implies secure, accurate databases and digital platforms obtained simultaneously from multiple sources, accessible and applicable in real time, regardless of the geographical location of the user. Digitalization of

defense allows scaling up the efficiency of the defense sector to achieve [**9**]. Thanks to digital transformation, all data on operational processes, workflow efficiency, quality control and operation planning are available in real time [**7**, pp.1-39] Digital technologies in the defense industry improve logistics systems and supply chains, thereby making the armed forces more flexible and combat-ready.

Such a strategy may involve the development and transfer of the technologies listed below to the defense sector.

Additive manufacturing (additive manufacturing) or 3D printing, the main elements of which are prototyping and mass production. The increase in additional production helps to reduce the cost of manufacturing tools and components, improve design, reduce the time spent on final consumer goods, and increase competitiveness from a technical and commercial point of view [**22**].

Augmented Reality

Augmented reality helps the soldier to better perceive information in the field of view, which reduces the need for training. The mentioned technology is used in practice in night vision goggles (NVG), which can show the exact location of the enemy. The glasses are attached to the helmet in the same way as safety glasses and can work both day and night. virtual, constructive, real-world modeling facilitates the creation of digital duplicates, design and production based on modeling. Modeling can help to "prepare" for future wars.

Big data and analytics

Big data and analysis simplify real-time decision-making and optimal use of resources.

o Descriptive and predictive analysis

o Real-time monitoring:

Cybersecurity issues are becoming more frequent as data and information are such an important resource nowadays that they are sometimes compared to oil. The Internet of Things (IoT), although it has revolutionized cyberspace by connecting billions of devices, has at the same time increased the target for cyberthreat attacks. Every device connected to the Internet of Things can provide cybercriminals with new opportunities to use.

The continuous growth of asymmetric warfare also leads to the functional incompatibility of systems and networks, which entails the integration of data both at rest and during the transmission of information. Therefore, the integration of existing and planned systems is a difficult, long-term and full of potential problems path, especially for a country like Armenia, which is the heir to the post-Soviet conservative defense system. In the fight against the uncertainty arising from technology, countries are allocating funds for research and development work in this area. In other words, even the availability of qualified and qualified specialists is still not enough to move forward in the technological race, it is necessary to create mechanisms through which professionals can conduct joint interdisciplinary research that can also successfully find practical application, from idea to principle of action. Despite the fact that digitalization automates many processes, a complex system still needs **high-quality human capital.**

Thanks to 4.0 industry technologies, aerospace and defense companies have achieved greater success by setting goals to achieve more, but these expectations may not be met due to insufficient **digital literacy** of society, lack of investment and other similar reasons. Sometimes companies have to abandon expensive ideas and choose less effective, but also low-effort ideas. Although digitization of processes helps to save resources, digitized systems are still vulnerable to enemy actions such as counterintelligence, information warfare, surveillance, etc. Digitalization can also help to increase the level of readiness of the Armed Forces, allowing you to get a "general picture" of the military situation and use the information obtained during military operations, both when making tactical and strategic decisions. As a result of the digitization of the defense sector, errors caused by the human factor are gradually minimized, which also makes it possible to reduce human losses on the battlefield. In the digital age, countries must not only be well aware of modern technological advances, but also stay ahead of events in order to be sure of maintaining and improving their "digital positions" at the forefront of innovation.

Armenia's defense sector digitalization issues

The 2020 war showed that Armenia is not ready to wage wars with the effective use of physical and digital technologies. The latest technologies, which include advanced robotics and artificial intelligence, sophisticated sensors, cloud computing technologies, the Internet of Things, data collection and analysis, adaptive/digital manufacturing, have not yet been integrated into the Armenian defense sector, and existing types of weapons are not integrated into a single digital space, Therefore, it is impossible to conduct network-centric warfare without the use of digitization mechanisms. To implement all this, first of all, it is necessary to develop an appropriate strategy, while the RA digitalization strategy [**24**] does not require the digitalization of the defense sector.

The most important step towards the digitization of the defense sector is the resolution of

cybersecurity issues. In 2020, Azerbaijani hacker forums and channels published data and documents from some of the most important government agencies and electronic systems in Armenia, including the Mulberry Groupware electronic document management system used for interdepartmental communication in the Government of Armenia, screenshots/frames of databases. As a result of all this, a number of government websites have been offline for a long time. During the outbreak of the COVID-19 pandemic, an Azerbaijani hacker group managed to publish a database (names, addresses, phone numbers and serial numbers of passports) of approximately 3,000 Armenian citizens infected with COVID-19 [25]. For more information about practical cases of threats, see the article "Armenia Digital Threat Landscape. Civil society and the Media" [**26**], which notes that both government websites and representatives of civil society and journalists are often targeted. The study "Digital security incidents against the Armenian Civil Society in 2019 – 2020" also talks about precedents in the digital space of Armenia [**27**]. The problems in the digital space are not limited to attacks. often seemingly innocent "disinformation" spread through digital technologies and platforms undermines the stability of systems, and fake sermons in war conditions often lead to incorrect orientation. Currently, control over the media is of key importance, and this control is possible only with the help of digital technologies. "Disinformation and misinformation in Armenia confronting the power of false narratives" [28] the study showed that disinformation in war conditions can undermine public trust and interrupt national communication between society, the political elite, and the military, which is also a threat worthy of attention, and is realized precisely in the digital environment.

One of the obstacles to the digitalization of the defense sector is the lack of appropriate technological infrastructure. There are few data processing centers in Armenia [**29**], and the data collection process does not go smoothly. Consequently, it is difficult, if not impossible, to achieve objective solutions using data-driven technologies. Communication between existing data centers is weak and uncoordinated. The geography of the data processing centers is concentrated around Yerevan and the surrounding areas.

It is only in recent years that disciplines such as data science, artificial intelligence, and cybersecurity have begun to be taught in higher education institutions, but given the rapid development of technology with all its consequences, it is necessary, in particular, to conduct some courses and trainings for military personnel, which will be able to reduce the gap in "communication" between technologies to some extent and the staff that manages them.

All these involve the government developing a strategy aimed at digitalizing the defense sector and providing appropriate funds, as a result of which

- Armenia will have increased cybersecurity. The digital protection system will allow Armenia to strengthen its position in the field of cybersecurity, which implies protection from cyber attacks, data leaks, etc.
- Digitalization of the defense sector will provide situational awareness, allowing monitoring and analysis of threats and vulnerabilities in cyberspace in real time. As a result, it will be possible to actively detect and respond to threats, reducing the risk of cybercrime and minimizing their impact on national security.
- Thanks to artificial intelligence, data analysis and optimized communication systems, command and control, intelligence gathering, logistics, decision-making processes will be improved, which will increase the efficiency and effectiveness of the Armenian armed forces.
- The development of digital security capabilities can facilitate cooperation with international partners, including other countries, multinational corporations and cybersecurity alliances. Armenia can use the experience, resources and best practices of global partners to strengthen its position in the field of cybersecurity and contribute to collective defense efforts. All this can lead to the emergence of new economic partners and the diversification of Armenia's foreign market.
- Investments in digital defense can stimulate economic growth and innovation by stimulating the development of science, which will increase Armenia's competitiveness not only in the military, but also in other fields.

Conclusion

Digitalization of the defense industry is currently not a matter of choice, but a necessity. Thanks to the latest technologies, optimization of decision-making processes, the ability to work with a large database, performing automated analysis have reduced the time spent by people on research and the likelihood of error instead, offering ultra-precise and low-cost automated services. For Armenia, the introduction of innovative technologies and digitalization of the military sector can be a breakthrough in the economy.

Engaged in regional conflicts, Armenia, has although faced the most bitter consequences of the lack of a modern arsenal and a non-digital defense sector, is still taking slow steps in the technology race, which promises new dangers. Thanks to the digitalization of the defense sector, Armenia will not

only increase its defense capability, but also become competitive in many other areas.

Reference

1. **Catherine Bucaniec**, "Russian Military to Develop Weapons Using Artificial Intelligence," C4ISRNET, August 17, 2022
2. **Hoffman Frank G**., "Will War's Nature Change in the Seventh Military Revolution? Exploring War's Charcter and Nature", Parameters 47, no. 4 (Winter 2017–2018)
3. **Horowitz Michael C**. *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton University Press, 2010. *JSTOR*, https://doi.org/10.2307/j.ctt7sqwd. Accessed 9 June 2024.
4. **Heltberg Therese,** "'I Cannot Feel Your Print.' How Military Strategic Knowledge Planners Respond to Digitalization," // Journal of Strategy and Management 15, no. 2 (April 2022): 220, https://doi.org/10.1108/JSMA-12-2020-0344
5. **Mathew, A**. The Peril of Artificial Intelligence. In Proceedings of the 2020 Fourth International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 8–10 January 2020; pp. 919–924. https://ieeexplore.ieee.org/document/9171226
6. **Michael Macedonia,** Games, Simulation, and the Military Education Dilemma, The Internet and the University: 2001
7. **Reinhard G., Jesper V., and Stefan S.,** "Industry 4.0: Building the digital enterprise," 2016 Glob. Ind. 4.0 Surv., pp. 1–39, 2016, [Online]. Available: www.pwc.com/industry40
8. **Raska Michael,** "The Sixth RMA Wave: Disruption in Military Affairs?," // Journal of Strategic Studies 44, no. 4 (2021), 456-479
9. **Soare Simona,** Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age, 2023 The International Institute for Strategic Studies
10. **Winkler John D., Timothy Marler, Marek N. Posard, Raphael S. Cohen, and Meagan L. Smith**, 2022, Reflections on Future of Warfare and Implications for Personnel Policies o f t he U.S. department to defense, https://apps.dtic.mil/sti/pdfs/AD1088596.pdf
11. **Yamskov, A. N.** "Ethnic Conflict in the Transcausasus: The Case of Nagorno-Karabakh." // *Theory and Society*, vol. 20, no. 5, 1991, pp. 631–60. *JSTOR*, http://www.jstor.org/stable/657781. Accessed 29 June 2024
12. Army halts IVAS augmented reality goggle project to offer navigation, night vision, artificial intelligence https://www.militaryaerospace.com/sensors/article/14213033/augmented-reality-night-vision-goggles (accessed 20 November, 2023)
13. Army halts IVAS augmented reality goggle project to offer navigation, night vision, artificial intelligence Exploring the Intersection of Big Data and AI: Unlocking Insights and Driving Innovation https://forbytes.com/blog/big-data-and-ai/ (accessed October, 2023)
14. "Chief Digital and Artificial Intelligence Office (CDAO)," CDAO, n. d., accessed March 27, 2023,
15. "Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman, 2013
16. Fourth Industrial Revolution', World Economic Forum, available at https://www.weforum.org/focus/fourth-industrial-revolution, accessed on 25 April 2023
17. "Toward a New Era of Cooperation: How Industrial Digital Platforms Transform Business Models in Industry 4.0," https://www.c4isrnet.com/; and Johannes W. Veile, Marie-Christian Schmidt, and Kai-Ingo Voight, Journal of Business Research 143 (April 2022),
18. Emerging Technologies and the Future of Air Warfare, Raphaël Briant, Translation Michael Storey, In Revue Défense Nationale Issue 11, 2023, pages 105 to 112, https://www.cairn-int.info/journal-revue-defense-nationale-2023-HS11-page-105.htm
19. Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age, https://www.iiss.org/research-paper/2023/08/digitalisation-of-defence--in-nato-and-the-eu/
20. Security sector reform in Armenia, Gagik Avagyan, Duncan Hiscock, 2005
21. 2021-2025 թթ Հայաստանի թվայնացման ռազմավարությունը https://www.e-gov.am/u_files/file/decrees/kar/2021/02/183_1.pdf
22. Why Combine Artificial Intelligence with Additive Manufacturing? https://amfg.ai/2023/11/24/why-combine-artificial-intelligence-with-additive-manufacturing/
23. Rethinking Oil Economy Then and Data Economy Now! https://www.polestarllp.com/blog/yes-data-is-the-new-oil-in-economy
24. Հայաստանի թվայնացման ռազմավարությանը, ռազմավարության միջոցառումների ծրագրին եվ արդյունքային ցուցանիշներին հավանություն տալու մասին https://www.arlis.am/DocumentView.aspx?docID=149957
25. The Cyber Battlefield is Just as Important: Armenia's Cybersecurity https://evnreport.com (contracted link, accessed December 2023)
26. Armenia Digital Threat Landscape: Civil Society & Media REPORTS & SURVEYS November 6, 2023, https://internews.org/resource/armenia-digital-threat-landscape-civil-society-media/
27. Digital security incidents against the Armenian Civil Society in 2019 - 2020 https://mdi.am/wp-content/uploads/2021/02/Digital (contracted link, accessed January, 2024)
28. DISINFORMATION AND MISINFORMATION IN ARMENIA CONFRONTING THE POWER OF FALSE NARRATIVES https://freedomhouse.org/sites/default/files/2021-06/Disinformation-in-Armenia_En-v3.pdf (accessed March 20, 2024)
29. Yerevan Data Center Summary https://www.datacenterjournal.com/data-centers/armenia/yerevan/ (accessed April 7, 2024)

Сдана/Հանձնվել է՝ 07.07.2024
Рецензирована/Գրախոսվել է՝ 14.07.2024
Принята/Ընդունվել է՝ 21.07.2024