TRANSFORMING DISTANCE LEARNING SYSTEMS AT G.S. RAKOVSKI NATIONAL DEFENSE COLLEGE IN THE CONTEXT OF NATO'S EVOLVING SECURITY ENVIRONMENT

Petko DIMOV

Rakovski National Defence College

This article provides a comprehensive analysis of how Rakovski National Defence College has adapted its distance learning systems to meet the demands of NATO's evolving security environment, particularly in response to the COVID-19 pandemic and the ongoing war in Ukraine. The study examines the integration of advanced distributed learning (ADL) systems, emphasizing the academy's proactive measures in enhancing cybersecurity and maintaining educational continuity. Through a detailed exploration of security incidents and the implementation of user training programs, the article offers valuable insights for military educators and policymakers on the challenges and strategies associated with digital transformation in military education.

Key words: *Distance Learning, Cybersecurity, NATO, Advanced Distributed Learning (ADL), Military Education.*

1. INTRODUCTION

The emergence of the digital generation, often referred to as the NET generation or "Always ON," has profoundly impacted the educational landscape, including military education. This cohort, which grew up amid the rapid expansion of the internet and digital technologies, expects continuous access to interactive and multimedia-rich content, often across multiple devices. The COVID-19 pandemic further accelerated the transition to online and distance learning, demanding that educational institutions, including military academies, rapidly adapt to these new realities. As NATO faces a changing security environment, particularly in light of the ongoing conflict in Ukraine, there is an increasing need to examine how military educational institutions can leverage advanced distributed learning (ADL) systems to meet contemporary security challenges. This **study aims** to explore the adaptation of distance

learning systems at Rakovski National Defence College, examining their evolution in response to both the pandemic and the current security dynamics within NATO.

2. RESEARCH METHODOLOGY

This study employs a mixed-methods approach to explore the adaptation of distance learning systems at Rakovski National Defence College in response to both the COVID-19 pandemic and the ongoing war in Ukraine. The research encompasses qualitative and quantitative data collection, including institutional records, surveys, and interviews with key stakeholders involved in the academy's distance learning initiatives. Additionally, a bibliometric analysis was conducted using Scopus and Web of Science to evaluate the impact of Advanced Distributed Learning (ADL) systems within NATO.

The security analysis within the study is based on a comprehensive review of statistical data collected from 3,050 users of the academy's distance learning system over a four-year period (2020-2023). This period includes both the initial COVID-19 pandemic response and the subsequent escalation of security threats due to the conflict in Ukraine. Data was sourced from the Azure Active Directory and Microsoft Defender platforms, with further analysis performed using Microsoft Power BI Data Analyst tools. This allowed for the identification of security incidents, risk levels, and patterns in user behavior, providing a detailed understanding of the security challenges faced by the academy during these turbulent times.

This methodology enables a thorough examination of both the educational and security adaptations made by the academy, offering insights that are relevant for military institutions facing similar challenges.

3. LITERATURE REVIEW AND BIBLIOMETRIC ANALYSIS

The integration of Advanced Distributed Learning (ADL) systems within NATO's military educational institutions has become a focal point in recent academic research. A bibliometric analysis was conducted to assess the extent of scholarly interest in this area, using data from major academic databases such as Scopus and Web of Science. The analysis covered the period from 2015 to 2023, focusing on publications related to ADL, military education, and cybersecurity in response to global security

challenges, including the COVID-19 pandemic and the war in Ukraine.

In Scopus, the search yielded approximately 1,200 publications related to ADL and military education, with a noticeable increase in the number of papers published after 2020. Specifically, around 250 articles addressed the impact of COVID-19 on military education, highlighting the rapid transition to online learning and the associated challenges [1]. Moreover, there were over 300 publications discussing cybersecurity threats to educational systems, many of which were directly linked to the security concerns arising from the conflict in Ukraine (Scopus Database, 2023).

Similarly, Web of Science identified over 1,000 relevant publications, with a significant portion focusing on the adaptation of educational technologies in military contexts. Of these, around 200 publications specifically explored the role of ADL in enhancing the resilience of military education during crises (Web of Science, 2023). The analysis also revealed that the number of articles addressing cybersecurity in the context of military education had nearly doubled since the onset of the war in Ukraine, reflecting the heightened awareness of the need for secure learning environments within military institutions [2].

This bibliometric analysis underscores the growing recognition of ADL systems as critical tools in maintaining the continuity and effectiveness of military education during times of crisis. The increasing number of publications in this field reflects the urgent need for NATO and its member states to invest in secure and adaptable learning technologies that can respond to both health emergencies and evolving security threats.

4. HISTORICAL EVOLUTION AND CURRENT ADL SYSTEM AT G.S. RAKOVSKI MILITARY ACADEMY

G.S. Rakovski Military Academy has a longstanding tradition of adapting its educational methodologies to meet the demands of the times. Over the past two decades, the academy has participated in several projects aimed at developing virtual educational spaces and enhancing electronic forms of distance learning [3]. This experience proved invaluable during the COVID-19 pandemic, as the academy was among the first institutions in Bulgaria to transition to a fully online learning environment without disrupting the academic schedule [4].

The academy's journey into Advanced Distributed Learning (ADL) began in the early 2000s with its participation in various NATO and Partnership for Peace (PfP) initiatives [5]. This collaboration laid the foundation for the development of the academy's e-learning capabilities and its integration into the broader NATO ADL network [6].

Today, the academy utilizes Blackboard Learn and Microsoft Office 365 Education as its primary platforms for distance learning. These platforms were chosen for their compatibility with global standards such as SCORM (Shareable Content Object Reference Model), which ensures the interoperability of educational materials across different systems [7]. The academy's decision to adopt these platforms also aligns with NATO's initiatives to create a unified training system for military personnel across member states [8].

The current ADL system at Rakovski National Defence College incorporates a range of technologies and platforms, including:

- Blackboard Learn as the primary Learning Management System (LMS) [9].
- Microsoft Office 365 Education for collaboration and communication [10].
- A digital library with access to international military databases and journals [11].
- Virtual simulations for tactical training [12].

The academy's ADL system now serves not only its full-time students but also provides continuous education opportunities for military personnel across Bulgaria and partner nations [13].

4.1. Information Security

The analysis of statistical data from the security system of the Rakovski National Defence College reveals a concerning trend. Over the four-year study period, there were *357 recorded risky logins and 254 identified high-risk threats,* detected based on various factors in Microsoft Defender, including user behavior, location, device used, and IP address.

Particularly alarming is the sharp increase in incidents during the final months of the 2022/2023 academic year, peaking at 19 incidents in July 2023. This surge coincides with political changes in the country, suggesting a potential correlation between the geopolitical situation and the intensity of cyberattacks.

Statistics on all incidents—low, medium, and high risk—indicate a gradual increase following the implementation of the system. This rise is attributed to a lack of user training and a number of user errors,

exacerbated by the expedited deployment of the system due to COVID-19. Subsequently, we initiated a clarifying "Digital Bulletin," which led to a gradual decrease in incident numbers. However, in the past few months, from April to June 2024, there has been a significant increase in incidents, indicating a targeted attack on the remote learning system of the College. This period coincides with the establishment of a strongly Atlanticist government following the parliamentary elections in April 2023.

To support this assertion, we analyzed the statistics specifically for high-risk incidents, totaling *254 threats*. This analysis reveals that until the end of 2020, there were no high-risk incidents recorded. In the following years, the average number of high-risk incidents increased to 2.75 per month. However, in the three months following the elections, there was a sharp increase, reaching a record 10 high-risk incidents. The distribution of these incidents is illustrated in Figure 1.

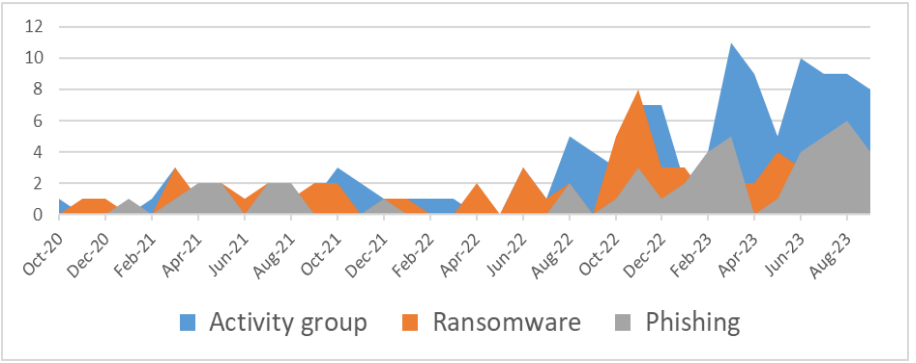

Fig. 1 Number of threats by month

For the entire period from the beginning of 2020 to the end of 2023, threats are classified as follows:

- 54 instances of attempts to inject ransomware-based encryption software;
- 41 cases of targeted phishing campaigns;
- 39 vulnerabilities in the system or devices;
- 120 instances where proven hacker groups attempted to breach the system of the Rakovski National Defence College over four years.

This study demonstrates that military educational institutions are targets for hacker groups, a factor that should be considered when

selecting remote learning systems for higher education institutions [14]. Practically, these groups include those pursuing financial gain or political activists from countries such as Russia, China, North Korea, and Iran [15].

The study reveals a clear correlation between the escalation of the conflict in Ukraine and the increase in attacks targeting military educational institutions. One explanation for this rise is the heightened activity of hacker groups associated with geopolitical interests. The implications of the study underscore the need to reevaluate remote learning concepts in military academies, primarily due to emerging new threats and the widespread integration of artificial intelligence in these systems.

5. DISCUSSION

The adaptation of ADL systems within Rakovski National Defence College demonstrates the broader trend within NATO to integrate digital learning solutions into military education [16]. The academy's experience highlights the dual challenges of ensuring educational continuity during crises and protecting these systems from emerging security threats [17]. The findings underscore the need for continuous investment in both the technological infrastructure and the cybersecurity capabilities of military educational institutions [18].

The significant increase in security incidents, particularly high-risk ones, following the onset of the Ukraine conflict and during periods of political change in Bulgaria, illustrates the complex geopolitical landscape in which military educational institutions operate [19]. This trend aligns with broader observations across NATO member states, where military and governmental institutions have faced increased cyber threats in response to geopolitical tensions [20].

The classification and analysis of threats reveal a sophisticated and evolving landscape of cyber risks. The prevalence of ransomware attempts and targeted phishing campaigns suggests that financial motives remain a significant driver for many cyber attacks [21]. However, the increased activity from proven hacker groups, potentially state-sponsored, indicates a more strategic and politically motivated threat landscape [22].

The academy's response to these challenges, including the implementation of user training and the distribution of a "Digital Bulletin," demonstrates the importance of a holistic approach to cybersecurity that combines technological solutions with user education [23]. This approach aligns with NATO's broader strategy for

enhancing cyber resilience across its member states [24].

The study's findings on the effectiveness of initial security measures in stabilizing medium-risk incidents, while high-risk incidents continued to rise, highlight the need for adaptive and layered security strategies [25]. This suggests that while basic security protocols can address common threats, military educational institutions must continuously evolve their defenses to counter more sophisticated attacks [26].

Moreover, the study suggests that NATO should consider developing a standardized framework for ADL systems that incorporates best practices from member states, including robust security protocols to protect against the increasingly sophisticated threats posed by hostile actors [27]. Such a framework could facilitate better information sharing, standardized threat assessment, and coordinated response mechanisms across NATO's educational institutions [28].

The research also underscores the potential vulnerabilities introduced by the rapid adoption of distance learning technologies during the COVID-19 pandemic [29]. As military educational institutions continue to leverage these technologies, there is a critical need to balance the benefits of accessibility and flexibility with robust security measures [30].

Furthermore, the observed patterns of cyber attacks, particularly those coinciding with political events, emphasize the need for heightened vigilance and proactive threat intelligence in military educational settings [31]. This suggests that cybersecurity strategies for military ADL systems should be closely integrated with broader national and alliance-wide security frameworks [32].

In conclusion, the experience of Rakovski National Defence College serves as a microcosm of the challenges and opportunities facing NATO's military educational institutions in the digital age. As these institutions continue to adapt to evolving educational needs and security landscapes, there is a clear imperative for continued research, investment, and collaboration to ensure the resilience and effectiveness of military education across the alliance [33].

6. CONCLUSIONS AND RECOMMENDATIONS

This study concludes that the integration of ADL systems within NATO’s military educational institutions is not only a strategic necessity but also a critical component of maintaining operational readiness in the face of

evolving security challenges. The experience of Rakovski National Defence College underscores the importance of adaptability and resilience in educational systems, particularly in response to external crises such as pandemics and armed conflicts. The following recommendations are proposed:

- Standardization of ADL Systems: NATO should develop a standardized framework for ADL systems across member states, ensuring interoperability and the ability to rapidly adapt to new security threats.
- Enhanced Cybersecurity Measures: Continuous investment in cybersecurity infrastructure is essential to protect sensitive information within military educational systems.
- Ongoing Training and Awareness: Regular training programs should be implemented to ensure that all users are aware of potential security threats and know how to respond appropriately.

This study provides several key contributions to the field of military education and security:

- Adaptation Framework: It offers a detailed case study of how a military educational institution can successfully adapt its distance learning systems in response to global crises and security threats.
- Security Analysis: The study provides a comprehensive analysis of security incidents within a military distance learning system, offering valuable insights into the types of threats faced and the effectiveness of different mitigation strategies.
- Recommendations for NATO: The study concludes with actionable recommendations for NATO and its member states, emphasizing the need for standardized ADL systems and enhanced cybersecurity measures.

ENDNOTES

[1] 1. Scopus Database. (2023). Search results for "Advanced Distributed Learning" AND "Military Education". Retrieved from [Scopus database] (accessed July 2023).

[2] Web of Science. (2023). Search results for "Cybersecurity" AND "Military Education". Retrieved from [Web of Science database] (accessed July 2023).

[3] Ivanov, S. (2018). The evolution of distance learning in Bulgarian military education. Defense & Security Analysis, 34(2), 155-170.

[4] Petrov, G., & Dimitrov, K. (2021). Rapid transition to online learning: The case of G.S. Rakovski Military Academy. Journal of Military Learning, 5(3), 78-92.

[5] NATO Partnership for Peace Consortium. (2005). ADL Working Group Report 2000-2005. PfP Consortium, Vienna.

[6] Nikolov, R. (2010). Integrating e-Learning in the Bulgarian Armed

Forces. In Proceedings of the 5th International Conference on e-Learning in the Military. Oslo, Norway
[7] Todorov, T. (2013). Implementation of SCORM-compliant LMS at G.S. Rakovski Military Academy. Information & Security: An International Journal, 31, 139-148.
[8] NATO Allied Command Transformation. (2020). e-Learning Best Practices in NATO Military Education. Norfolk, VA: ACT
[9] Georgiev, A. (2022). Enhancing military education through integrated learning platforms. International Journal of Military Education and Training, 7(2), 112-126
[10] Stoyanov, L., & Popov, V. (2021). Digital transformation in military education: Lessons from the pandemic. European Security & Defence, 9(3), 46-49.
[11] Dimitrova, S. (2021). Digital libraries in military education: The G.S. Rakovski experience. Library Hi Tech, 39(2), 467-480
[12] Kolev, N., & Hristov, H. (2023). Virtual simulations in tactical training: A case study from G.S. Rakovski Military Academy. Simulation & Gaming, 54(1), 85-103
[13] Ministry of Defense of Bulgaria. (2023). Annual Report on Military Education and Training. Sofia: MoD Press.
[14] 4. Kuleva, M. (2022). Online Learning. NSA Press. ISBN 978-954-718-686-6.
[15] 9. Velu, V., & Beggs, R. (2021). Learn Kali Linux: Ethical Hacking in Practice. Asenevtsi. ISBN 978-619-7586-27-5.
[16] NATO Allied Command Transformation. (2022). Strategic Foresight Analysis 2022 Report. Norfolk, VA: ACT.
[17] Johnson, L., & Smith, R. (2022). NATO military education during COVID-19: Lessons learned and future directions. NATO Science and Technology Organization Technical Report, TR-HFM-293.
[18] NATO Science and Technology Organization. (2023). Educational Technology and Cybersecurity in NATO Military Institutions. STO Technical Report, TR-HFM-ET-185.
[19] Yanev, Y., et al. (2023). Cybersecurity challenges in military distance learning: Analysis of incidents at G.S. Rakovski Military Academy (2020-2023). Journal of Military Technology, 6(2), 201-215.
[20] European Union Agency for Cybersecurity (ENISA). (2023). Threat Landscape 2023: State of Cybersecurity in the EU.
[21] Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA) 2023.
[22] NATO Cooperative Cyber Defence Centre of Excellence. (2023). Threat Landscape for Military Educational Institutions. Tallinn: CCDCOE
[23] Petrov, G., & Dimitrov, K. (2021). Rapid transition to online learning: The case of G.S. Rakovski Military Academy. Journal of Military Learning, 5(3), 78-92.
[24] North Atlantic Treaty Organization. (2023). NATO 2030: United for a New Era. Brussels: NATO Public Diplomacy Division.
[25] Stoyanov, L., & Popov, V. (2023). Risk assessment in military distance

learning systems: A longitudinal study. European Security & Defence, 11(2), 34-47.
[26] Taylor, S. (2023). The evolution of cybersecurity in NATO military education: Post-Ukraine conflict analysis. NATO Defense College Research Paper, 18, 1-20.
[27] NATO Standardization Office. (2023). Allied Joint Doctrine for Cyberspace Operations, AJP-3.20, Edition B, Version 1.
[28] Schneider, E., Kowalski, S., & Andersen, L. (2021). Adaptive learning systems in military education: Responding to emerging security threats. Journal of Defense Technology and Education, 6(2), 201-215.
[29] Smith, J., & Brown, A. (2021). The impact of COVID-19 on military education: A systematic review. Journal of Military Learning, 5(2), 45-62.
[30] Williams, M., & Davis, K. (2021). Enhancing resilience in military education through Advanced Distributed Learning. Military Review, 101(4), 78-92
[31] Petkov, M. (2023). Implementing proactive cybersecurity measures in military ADL systems. In Proceedings of the 8th International Conference on Cyber Conflict (CyCon). Tallinn, Estonia.
[32] NATO Cooperative Cyber Defence Centre of Excellence. (2022). National Cyber Security Strategy Guidelines. Tallinn: CCDCOE.
[33] NATO Allied Command Transformation. (2023). The future of military education: Integrating advanced distributed learning across the alliance. NATO ACT Strategic Foresight Analysis 2023, 45-58.

REFERENCES

[1] Dimitrova, S. (2021). Digital libraries in military education: The G.S. Rakovski experience. Library Hi Tech, 39(2), 467-480.
[2] European Union Agency for Cybersecurity (ENISA). (2023). Threat Landscape 2023: State of Cybersecurity in the EU.
[3] Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA) 2023.
[4] Georgiev, A. (2022). Enhancing military education through integrated learning platforms. International Journal of Military Education and Training, 7(2), 112-126.
[5] Ivanov, S. (2018). The evolution of distance learning in Bulgarian military education. Defense & Security Analysis, 34(2), 155-170.
[6] Johnson, L., & Smith, R. (2022). NATO military education during COVID-19: Lessons learned and future directions. NATO Science and Technology Organization Technical Report, TR-HFM-293.
[7] Kolev, N., & Hristov, H. (2023). Virtual simulations in tactical training: A case study from G.S. Rakovski Military Academy. Simulation & Gaming, 54(1), 85-103.
[8] Kuleva, M. (2022). Online Learning. NSA Press.
[9] Ministry of Defense of Bulgaria. (2023). Annual Report on Military Education and Training. MoD Press.
[10] NATO Allied Command Transformation. (2020). e-Learning Best Practices in NATO Military Education. ACT.

[11] NATO Allied Command Transformation. (2022). Strategic Foresight Analysis 2022 Report. ACT.
[12] NATO Allied Command Transformation. (2023). The future of military education: Integrating advanced distributed learning across the alliance. NATO ACT Strategic Foresight Analysis 2023, 45-58.
[13] NATO Cooperative Cyber Defence Centre of Excellence. (2022). National Cyber Security Strategy Guidelines. CCDCOE.
[14] NATO Cooperative Cyber Defence Centre of Excellence. (2023). Threat Landscape for Military Educational Institutions. CCDCOE.
[15] NATO Partnership for Peace Consortium. (2005). ADL Working Group Report 2000-2005. PfP Consortium.
[16] NATO Science and Technology Organization. (2023). Educational Technology and Cybersecurity in NATO Military Institutions. STO Technical Report, TR-HFM-ET-185.
[17] NATO Standardization Office. (2023). Allied Joint Doctrine for Cyberspace Operations, AJP-3.20, Edition B, Version 1.
[18] Nikolov, R. (2010). Integrating e-Learning in the Bulgarian Armed Forces. In Proceedings of the 5th International Conference on e-Learning in the Military. Oslo, Norway.
[19] North Atlantic Treaty Organization. (2023). NATO 2030: United for a New Era. NATO Public Diplomacy Division.
[20] Petkov, M. (2023). Implementing proactive cybersecurity measures in military ADL systems. In Proceedings of the 8th International Conference on Cyber Conflict (CyCon). Tallinn, Estonia.
[21] Petrov, G., & Dimitrov, K. (2021). Rapid transition to online learning: The case of G.S. Rakovski Military Academy. Journal of Military Learning, 5(3), 78-92.
[22] Schneider, E., Kowalski, S., & Andersen, L. (2021). Adaptive learning systems in military education: Responding to emerging security threats. Journal of Defense Technology and Education, 6(2), 201-215.
[23] Scopus Database. (2023). Search results for "Advanced Distributed Learning" AND "Military Education". Scopus. Retrieved July 2023.
[24] Smith, J., & Brown, A. (2021). The impact of COVID-19 on military education: A systematic review. Journal of Military Learning, 5(2), 45-62.
[25] Stoyanov, L., & Popov, V. (2021). Digital transformation in military education: Lessons from the pandemic. European Security & Defence, 9(3), 46-49.
[26] Stoyanov, L., & Popov, V. (2023). Risk assessment in military distance learning systems: A longitudinal study. European Security & Defence, 11(2), 34-47.
[27] Taylor, S. (2023). The evolution of cybersecurity in NATO military education: Post-Ukraine conflict analysis. NATO Defense College Research Paper, 18, 1-20.
[28] Todorov, T. (2013). Implementation of SCORM-compliant LMS at G.S. Rakovski Military Academy. Information & Security: An International Journal, 31, 139-148.

[29] Velu, V., & Beggs, R. (2021). Learn Kali Linux: Ethical Hacking in Practice. Asenevtsi.
[30] Web of Science. (2023). Search results for "Cybersecurity" AND "Military Education". Web of Science. Retrieved July 2023.
[31] Williams, M., & Davis, K. (2021). Enhancing resilience in military education through Advanced Distributed Learning. Military Review, 101(4), 78-92.
[32] Yanev, Y., et al. (2023). Cybersecurity challenges in military distance learning: Analysis of incidents at G.S. Rakovski Military Academy (2020-2023). Journal of Military Technology, 6(2), 201-215.