Cyber Defense Strategy: Problems, Conceptual Overview and Formation Mechanisms

Xayyam Nuraliyev
Institute of Information Technology, Baku, Azerbaijan
xeyyam777@gmail.com

***Abstract*— The rapid advancement of information technologies in the modern era has significantly expanded the number and scope of cyber threats, making cybersecurity an essential and integral component of national and organizational security. The primary objective of this study is to analyze the mechanisms of cyber defense formation, identify existing problems, and systematically regulate effective defense approaches. The analysis reveals that cyber defense must not be limited solely to technological measures but must also encompass a normative-legal framework, international cooperation, human resource development, and risk management. The research concludes that cyber defense is directly dependent on the proper assessment of existing risks, the systematic formation of conceptual approaches, and the precise determination of implementation mechanisms. As a result of this research, the problems and mechanisms of modern cyber defense technologies have been investigated and a new conceptual perspective has been introduced.**

Keywords*— *cyber defense; risk management; normative-legal framework; international cooperation; zero trust architecture; conceptual approach.

I. INTRODUCTİON

Cyber defense has become the fifth domain of warfare alongside land, sea, air, and space, and the proliferation of digital infrastructure has rapidly expanded the available attack surface for both state and non-state actors. This reality has become not only a technological problem, but also a normative, governance, and strategic one. As modern states, corporations, and individuals increase their dependence on digital systems, the potential damage from cyberattacks grows proportionally. Research indicates that the global economic cost of cyberattacks will reach $10.5 trillion USD annually by 2025 [1]. This figure clearly demonstrates the importance of recognizing cyber defense as a strategic priority. At the same time, cybersecurity has become a front-line concern not only for technology companies, but also for governments, military structures, financial institutions, and hospitals.

Kotsias et al. [2] note that integrating cyber threat intelligence into commercial organizations is the primary means of closing the asymmetry between attackers and defenders; theoretical frameworks cannot keep pace with the speed of adversarial innovation. The tools used by attackers from AI-based malware to the complex operations of state-sponsored APT (Advanced Persistent Threat) groups are becoming increasingly agile and adaptive. Bridging this gap requires a complex, multi-layered approach; that is, a comprehensive strategy that simultaneously encompasses technical, legal, human, and institutional dimensions.

This paper investigates the cyber defense strategy from three main directions: (1) the primary problems that hinder effective defense, (2) the conceptual frameworks that guide strategic thinking, and (3) the mechanisms for developing coherent cyber defense strategies. The research is based on NIST, CISA, DoD policy documents, as well as scientific articles published on Google Scholar and ResearchGate platforms. The literature review was conducted systematically, with preference given to peer-reviewed articles published in the last five years, as well as normative documents from organizations such as NIST, ISO, the EU, and NATO.

II. KEY PROBLEMS IN CYBER DEFENSE STRATEGY

A. Improper Risk Assessment

The primary prerequisite for effective cyber defense is the proper and systematic assessment of existing risks. However, in practice, a significant portion of organizations either conducts risk assessment superficially or entirely lacks a formalized methodology. This gap is particularly evident in small and medium-sized enterprises, as well as in the state structures of developing countries. Pöyhönen [3] notes that the weakness of international cyber incident response stems precisely from a failure to properly understand the risk landscape. The NIST Cybersecurity Framework (CSF 2.0, 2024) [4] presents risk identification, assessment, and prioritization as the foundational pillars of strategy. Inadequate risk assessment leads both to resource waste and to critical vulnerabilities being overlooked. Therefore, risk assessment must be structured not as a one-time exercise, but as a continuous and dynamic process.

B. Lack of Systematic Conceptual Approaches

The second major problem in cyber defense is the absence of a unified conceptual framework in strategic thinking. Many organizations rely on a reactive approach: response measures are taken after an attack occurs, but a systematic proactive defense architecture is never built. This reactive mentality manifests in various forms: delayed patch management, failure to update incident response plans, or conducting security tests only when required for audits. Wolff [5] warns about the counterproductive effects of defense-in-depth strategies, noting that improperly designed multi-layer defenses can themselves

DOI: 10.25045/cyber.gov.2026.53

create new vulnerabilities. Hasan et al. [6] emphasize that AI-based predictive approaches require a conceptual foundation to replace reactive models. At the root of the problem often lies a low level of cybersecurity literacy at the leadership level — a strategic gap between the board of directors and technical teams.

C. Normative-Legal Gaps

The weakness of the normative-legal framework of cyber defense significantly complicates strategic formation. There is often no harmonization between states regarding definitions of cyberattacks, attribution standards, and response measures. This fragmentation creates legal gaps in cyberspace: an activity considered legal in one country may be considered criminal in another, which significantly complicates international law enforcement. Joubert [7] notes that without a credible attribution mechanism, the credibility of deterrence strategies diminishes. The EU's NIS2 Directive (2022) is assessed as one of the most substantive regional steps aimed at closing this gap. The document sets minimum cybersecurity requirements, incident reporting obligations, and strict sanctions mechanisms for critical infrastructure operators. Nevertheless, such regional frameworks remain uncoordinated on a global scale, and universally accepted international cyber law norms do not yet exist.

D. Human Resources and Personnel Shortage

No matter how advanced the technical solutions are, the human factor continues to remain the weakest link in cyber defense. The 2024 Verizon DBIR report shows that the vast majority of incidents are driven by human error, phishing, and social engineering. According to the ISC2 [8] report, more than 3.5 million cybersecurity positions remain unfilled worldwide; this illustrates how deep the skilled workforce deficit in the sector has become. The shortage is particularly evident in areas requiring high specialization such as threat intelligence, cloud security, and incident response. Zwilling [9] argues that developing universal training curricula for cybersecurity specialists is a strategic necessity. Additionally, continuous professional development programs for existing staff and instilling a cybersecurity culture must be a priority for every organization.

E. Outdated Infrastructure and Technology Gap

The widespread prevalence of outdated information systems in critical infrastructure sectors — energy, water, transportation, healthcare — represents a special source of risk for cyber defense strategy. Many of these systems were built decades ago, designed without consideration of modern cybersecurity standards, and have not been regularly updated. Al-Hamar et al. [10] demonstrate that the integration of IoT networks with critical infrastructure significantly expands the attack surface: every connected device becomes a potential entry point. The convergence of operational technology (OT) with information technology (IT) deepens this vulnerability further. The 2021 Colonial Pipeline attack demonstrated to the entire world how real this risk is. Since modernizing old infrastructure requires large financial investment, in the short term the implementation of compensatory measures — network segmentation, anomaly detection systems — emerges as a strategic priority.

III. CONCEPTUAL OVERVIEW: DEFENSE APPROACHES

A. Risk-Based Conceptual Model

A conceptual model based on the proper assessment of existing risks must form the foundation of a cyber defense strategy. NIST CSF 2.0 (2024) [4] is the most widely accepted example of this model: it offers a structured sequence across the functions of Identify, Protect, Detect, Respond, and Recover. This framework encompasses not only technical measures, but also governance structures, supply chain risks, and third-party relationships. In the 2024 updated version, the "Govern" function was added, emphasizing the incorporation of cybersecurity into the accountability structure at the leadership level. Safitra et al. [1] further develop this framework as an integrative model that combines digital capabilities with resilience, showing that the synthesis of preventive and reactive approaches creates an optimal defense posture.

B. Zero Trust Architecture

Zero Trust Architecture (ZTA) represents the most significant conceptual shift in modern cyber defense. Built on the principle of "never trust, always verify," this model treats every user, device, and traffic flow as a potential threat source; no request is automatically trusted, even if it comes from within the network. This approach fundamentally rejects the classical notion of perimeter defense. NIST SP 800-207 [11] defines the technical foundations of ZTA; the DoD Zero Trust Strategy (2022) [12] mandates the application of this model to state defense structures by 2027. The technical implementation of ZTA encompasses micro-segmentation, multi-factor authentication (MFA), the least privilege principle, and continuous behavioral monitoring. According to the ISC2 [13] report, transitioning to ZTA reduces incidents by more than 80%. Nevertheless, applying ZTA to existing legacy systems creates significant technical and financial challenges, making gradual transition planning necessary.

C. Defense-in-Depth and Cyber Resilience

The Defense-in-Depth (DiD) concept was borrowed from military doctrine but has gained new meaning in the cyber environment: overlapping multi-layered control mechanisms are applied so that the compromise of one layer does not lead to a total breach. A typical DiD architecture forms an ecosystem consisting of network perimeter firewalls, internal segmentation, endpoint protection, email filtering systems, data loss prevention (DLP) tools, and incident response procedures. Recent research shows that DiD and ZTA are not mutually exclusive, but rather complementary [14]: while ZTA centralizes identity verification, DiD multiplies the layers of technical controls. The cyber resilience paradigm shifts attention from preventive defense to recovery capability — even if a system is compromised, maintaining core functionality and the ability to normalize quickly is defined as the primary objective.

D. AI-Based Predictive Approach

The application of artificial intelligence (AI) and machine learning to cyber defense is fundamentally transforming the traditional reactive approach. Hasan et al. [6] demonstrate that AI-based predictive Cyber Threat Intelligence (CTI) identifies behavioral anomalies in real time and significantly shortens response times compared to signature-based methods. The power of AI models stems especially from the correlation of large volumes of log data, network traffic, and endpoint behavior. However, researchers also draw attention to limitations such as the risk of model drift and high false positive rates. Moreover, adversarial actors are in turn using AI to make their attack tools more effective — creating more convincing phishing texts and adaptive malware. This bidirectional dynamic brings to the fore the need for continuous model updates on the defense side and the explainability of AI systems.

IV. Mechanisms for Forming Cyber Defense Strategy

A. Strengthening the Normative-Legal Framework

The formation of effective cyber defense first and foremost requires the precise definition of the normative-legal framework. The U.S. National Cybersecurity Strategy (2023) [15] is assessed as one of the most comprehensive policy documents in this area; the document legally places responsibility for product security on technology companies, transforming the concept of "secure-by-design" into a normative requirement. Raju [16] notes that the weakness of the normative framework makes strategic coordination impossible; Craig and Johnson [17] argue that without a systematic capacity-building framework, the formation of effective national cybersecurity strategies is not possible. Mandatory incident reporting obligations for critical infrastructure operators, minimum cybersecurity certification requirements, and the determination of security criteria in government procurement are important steps toward strengthening the national normative framework.

B. International Cooperation Mechanisms

The transboundary nature of cyber threats makes international cooperation a strategic necessity. The UN Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG) are the primary multilateral platforms for developing norms of state behavior in cyber defense. Pöyhönen [3] emphasizes that the development of international rapid response mechanisms is only possible through close cooperation among governments, the private sector, and academia. Information Sharing and Analysis Centers (ISACs) have proven themselves as an effective institutional mechanism for sharing real-time threat intelligence. Additionally, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) maintains its significance as the primary platform providing doctrine, technical standards, and training opportunities for allied nations.

C. Human Resource Development Mechanisms

Strategy formation mechanisms remain incomplete without addressing the personnel shortage. In a context where more than 3.5 million cybersecurity positions remain unfilled globally, human resource development must be valued as a strategic investment. Catal et al. [18] show that aligning cybersecurity education with international standards significantly enhances global defense capabilities; the NICE (National Initiative for Cybersecurity Education) Framework has been widely recognized as a reference document defining specialty roles, skills, and knowledge areas. Springer Nature [19] evaluates cyber range environments as the most effective mechanism for developing practical skills. Zwilling [9] defines the development of universal training standards as a priority obligation of states.

D. Risk Management Mechanism

Systematic risk management constitutes the operational core of a cyber defense strategy. Risk management encompasses prioritization, the selection of a response strategy (accept, mitigate, transfer, avoid), and the documentation of residual risk. The ISO/IEC 27001 standard, the NIST Risk Management Framework (RMF), and OWASP guidelines define the broadly accepted methodological bases in this field. Davis et al. [20] demonstrate that managing data security in Zero Trust environments through risk-based prioritization yields statistically superior results compared to traditional perimeter-based approaches. The SolarWinds incident demonstrated that through a seemingly trustworthy software update, the networks of thousands of organizations could be simultaneously compromised. In this context, supply chain risk management emerges as an independent strategic domain.

E. Public-Private Sector Partnership

In advanced economies, a large portion of critical infrastructure is managed by the private sector; for this reason, the implementation of a national cyber defense strategy requires strong public-private sector cooperation. CISA plays the central bridging role between the federal government and the private sector; the CIRCIA law, which entered into force in 2022, mandates that critical infrastructure operators report cyber incidents to CISA within 72 hours and ransomware payments within 24 hours. The NITRD Program [21] argues that it is vital for academia, industry, and government to jointly formulate a research agenda so that cyber defense covers the entire ecosystem. For the partnership to be sustained, both sides must make certain concessions — the government must reduce the regulatory burden, while the private sector must increase transparency.

Conclusion

The research concludes that cyber defense is directly dependent on the proper assessment of existing risks, the systematic formation of conceptual approaches, and the precise determination of implementation mechanisms. As a result of the research, the problems and mechanisms of modern cyber

defense technologies have been investigated and a new conceptual perspective has been introduced. Effective cyber defense must integrate normative-legal frameworks, international cooperation mechanisms, human resource development strategies, and systematic risk management into a cohesive whole. The integration of the Zero Trust Architecture, Defense-in-Depth, and cyber resilience paradigms constitutes the optimal conceptual foundation for modern cyber defense strategy.

REFERENCES

1] M. F. Safitra, M. Lubis, and H. Fakhrurroja, “Counterattacking cyber threats: A framework for the future of cybersecurity,” Sustainability, vol. 15, no. 18, p. 13369, 2023. https://doi.org/10.3390/su151813369

[2] J. Kotsias, A. Ahmad, and R. Scheepers, “Adopting and integrating cyber-threat intelligence in a commercial organisation,” European Journal of Information Systems, vol. 32, no. 1, pp. 35–51, 2023. https://doi.org/10.1080/0960085X.2022.2088414

[3] J. Pöyhönen, “International mechanisms for rapid response to cyberattack incidents,” CCDCOE, 2018. https://ccdcoe.org/library/publications/

[4] NIST, Cybersecurity Framework (CSF) 2.0, NIST, 2024. https://doi.org/10.6028/NIST.CSWP.29

[5] J. Wolff, “Perverse effects in defense of computer systems: When more is less,” Journal of Management Information Systems, vol. 33, no. 2, pp. 597–620, 2016. https://doi.org/10.1080/07421222.2016.1205934

[6] K. Hasan et al., “Enhancing proactive cyber defense: A theoretical framework for AI-driven predictive cyber threat intelligence,” RTIC Journal, vol. 5, no. 1, p. 33122, 2024. https://www.rtic-journal.com/download/enhancing-proactive-cyber-defense-a-theoretical-framework-for-ai-driven-predictive-cyber-threat-16176.pdf

[7] V. Joubert, “Getting the essence of cyberspace: A theoretical framework to face cyber threats,” NATO CCDCOE, 2018. https://ccdcoe.org/uploads/2018/10/Joubert-Getting-the-Essence-of-Cyberspace.pdf

[8] ISC2, ISC2 Cybersecurity Workforce Study 2023, 2023. [Online]. https://www.isc2.org/research/workforce-study

[9] M. Zwilling, “Universal training programs for cybersecurity specialists: A global imperative,” Journal of Cybersecurity Education, Research and Practice, 2022. https://digitalcommons.kennesaw.edu/jcerp/–vol2022/-iss1/3/

[10] Y. Al-Hamar et al., “A comprehensive survey on cybersecurity threats and defense mechanisms in IoT networks,” arXiv:2601.00556, 2024. https://arxiv.org/abs/2601.00556

[11] S. Rose et al., NIST SP 800-207: Zero Trust Architecture, NIST, 2020. https://doi.org/10.6028/NIST.SP.800-207

[12] U.S. DoD, DoD Zero Trust Reference Architecture, Version 2.0, 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[13] ISC2, “Enhancing cyber maturity with Zero Trust,” ISC2, 2024. https://www.isc2.org/research/zero-trust

[14] ResearchGate, “Global cybersecurity: Harmonising international standards and cooperation,” 2024. https://www.researchgate.net/publication/382033667

[15] White House, National Cybersecurity Strategy, Washington D.C., 2023. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[16] P. Raju, “Cyber defense as a global challenge,” Global Security Review, vol. 5, no. 2, pp. 33–47, 2022. https://www.researchgate.net/publication/382033667_Global_cybersecurity_Harmonising_international_standards_and_cooperation

[17] A. Craig and R. Johnson, “Building cybersecurity capacity: a framework of analysis for national cybersecurity strategies,” Journal of Cyber Policy, vol. 7, no. 3, pp. 375–398, 2023. https://doi.org/10.1080/23738871.2023.2178318

[18] C. Catal, A. Ozcan, E. Donmez, and A. Kasif, “Analysis of cyber security knowledge gaps based on cyber security body of knowledge,” Education and Information Technologies, vol. 28, no. 2, pp. 1809–1831, 2023. https://doi.org/10.1007/s10639-022-11261-8

[19] Springer Nature, “Cyber range design framework for cybersecurity education,” International Journal of Information Security, 2023. https://doi.org/10.1007/s10207-023-00680-4

[20] P. Davis et al., “Strengthening financial institutions’ data security with blockchain technology and zero trust security,” Meta Heuristic Algorithms for Advanced Distributed Systems, 2024. https://www.researchgate.net/publication/385877700

[21] NITRD Program, Federal Cybersecurity Research and Development Strategic Plan, 2024. https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2024.pdf