The Impact of Darknet and Dark Web Environments on Cyber Sovereignty

Agshin Pashayev[1], Samed Dursunov[2]
[1,2] Institute of Information Technology, Baku, Azerbaijan
[1]pasayev_aqsin@mail.ru, [2]samed.dursunov@gmail.com

***Abstract*— In the context of digital transformation, the concept of state sovereignty is acquiring new dimensions, with the notion of cyber sovereignty becoming increasingly prominent. The borderless nature of the Internet and its distributed network architecture enable the rapid transmission of information beyond national boundaries, thereby reducing the effectiveness of traditional state control mechanisms. This study analyzes the Internet environment across three layers Surface Web, Deep Web, and Darknet and examines their impact on cyber sovereignty. The findings indicate that these technological characteristics complicate legal regulation and increase risks related to information security, including disinformation, manipulation, cyberattacks, and cyber threats. Consequently, the issue of cyber sovereignty requires a comprehensive approach that integrates legal, technological, and international cooperation frameworks.**

Keywords*— *cyber sovereignty; cybersecurity; Darknet; Deep Web; anonymous networks; cryptography; digital sovereignty; information security.

I. INTRODUCTİON

Information and communication technologies (ICT) have driven a profound transformation of social, economic, and political processes on a global scale. The Internet infrastructure has evolved into the principal communication platform of modern society, playing a critical role across a wide spectrum of domains from public administration to economic activity. At the same time, the global and borderless nature of the Internet environment has introduced new challenges for national security policies of states [1].

In Azerbaijan, the development of network technologies and digital infrastructure has closely followed these global trends. The country's increasing integration into global digital networks has made the issues of information security and cyber sovereignty particularly relevant at the national policy level [2].

One of the widely employed concepts in contemporary security discourse is that of cyber sovereignty. This concept encompasses a state's capacity to exercise legal and technological control over its digital infrastructure, information flows, and cyberspace. However, the distributed architecture of the Internet, the transboundary movement of data, and the dominant position of international technology platforms complicate the practical implementation of this concept [3,4].

The concept of cyber sovereignty is closely linked to questions of digital self-determination, wherein states seek to define and enforce the legal norms that govern their national cyberspace. This includes not only the control of physical infrastructure but also the ability to regulate digital content, protect critical data assets, and respond to external cyber threats in a timely and effective manner [3,4].

In recent years, the expansion of Darknet and Dark Web environments has necessitated the development of new approaches within national cybersecurity strategies. Due to their inherent characteristics such as anonymous communication, multilayered cryptographic mechanisms, and decentralized network structures these environments require more sophisticated technical and legal frameworks for effective governance and monitoring [5,6].

II. THE PROBLEM OF CYBER SOVEREİGNTY İN THE DİGİTAL SPACE

One of the fundamental characteristics of the Internet environment is its reliance on a distributed network architecture. The Internet is a global communication system that lacks a centralized governing authority and has emerged through the interconnection of thousands of autonomous networks. This structure operates on the basis of the following technological principles:

- TCP/IP protocols;
- a packet-switched data transmission model.

Within the packet-switched model, data are segmented into smaller units (packets) and transmitted across the network via multiple routing paths. These data packets traverse the network infrastructures of different countries, with their routes dynamically adjusted in real time through routing mechanisms. While this feature enhances the resilience and flexibility of the Internet, it simultaneously constrains the ability of states to exercise comprehensive control over information flows.

From the perspective of cyber sovereignty, one of the key challenges lies in the regulation of cross-border data flows. Information resources created or hosted in one country may be distributed through servers located in other jurisdictions. This significantly complicates the enforcement of national legislation and the implementation of legal regulatory frameworks [7].

The jurisdictional ambiguity inherent in cross-border digital activity creates a significant gap between the theoretical scope of national law and its practical enforceability. When

DOI: 10.25045/cyber.gov.2026.40

cybercriminal activities originate from servers hosted in jurisdictions with differing or absent legal frameworks, states face substantial obstacles in pursuing prosecution and accountability [7].

Moreover, the growing influence of global technology companies within the digital ecosystem exerts a considerable impact on state information policies. As social networks and international platforms manage vast volumes of data and communication flows, the regulation of their activities has become an essential component of the cyber sovereignty agenda [8,9].

III. THE DEVELOPMENT AND IMPLİCATİONS OF CRYPTOGRAPHİC TECHNOLOGİES

Cryptography plays a pivotal role in ensuring the security of digital communication systems. Modern Internet infrastructure relies on a variety of cryptographic protocols to safeguard the confidentiality and integrity of data.

The widespread application of cryptographic methods is essential for maintaining information security within the digital environment. In this context, the following technologies are extensively utilized:

- Tor and I2P – enable the transmission of network traffic through multilayered encryption mechanisms, thereby preserving user anonymity;
- VPN and proxy services – allow data flows to be routed through alternative pathways, enhancing privacy and access flexibility;
- Cryptocurrencies and blockchain technologies – ensure the security of financial transactions through cryptographic algorithms;
- End-to-End encryption – guarantees that data can only be accessed by the communicating parties, namely the sender and the intended recipient [10].

Nevertheless, the proliferation of anonymous communication technologies may pose certain challenges for law enforcement agencies. In some instances, these technologies can be exploited to conceal cybercriminal activities and facilitate illicit operations. Therefore, achieving an appropriate balance between privacy and security remains a critical objective within cybersecurity policy frameworks [3].

From a policy standpoint, the dual-use nature of cryptographic technologies poses a dilemma for regulatory authorities. While strong encryption protects citizens' rights and secures sensitive communications, the same mechanisms can shield malicious actors from detection. Effective cybersecurity governance must therefore address this tension through nuanced legal frameworks rather than blanket restrictions on cryptographic tools [3,11].

IV. STRUCTURAL LEVELS OF THE INTERNET ENVIRONMENT

The Internet environment can be categorized into several fundamental layers based on its functional characteristics (Figure 1). These layers include:

- Surface Web – the publicly accessible segment of the Internet, comprising web resources indexed by search engines. This layer is used daily by the vast majority of users and represents the most visible part of the online ecosystem.
- Deep Web – a segment of the Internet that is not indexed by search engines but includes legitimate and functional online services. This layer encompasses banking systems, email services, academic databases, and corporate information systems. The Deep Web constitutes the largest portion of the overall Internet infrastructure.
- Darknet – an environment that operates through specialized software and anonymous network protocols. Within this layer, both user and server anonymity are ensured through advanced technological mechanisms, and access is not possible via standard web browsers [5].

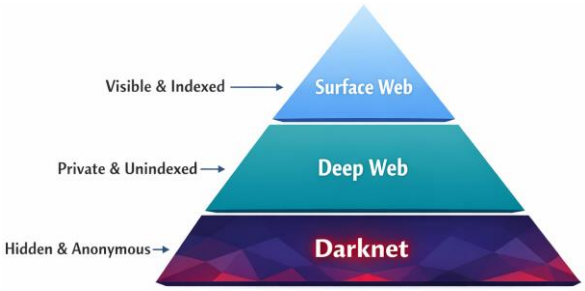

Figure 1. Structural layers of the internet environment

V. TECHNOLOGİCAL CHARACTERİSTİCS OF THE DARKNET AND DARK WEB ENVİRONMENT

From a technological perspective, the Darknet is based on a parallel network model that operates on top of the existing Internet infrastructure. While it utilizes the conventional TCP/IP framework, it incorporates alternative protocols and advanced encryption mechanisms [5,10].

One of the core technologies underlying the Darknet is the principle of onion routing. Within this model, data packets are transmitted through multiple intermediary nodes, with separate layers of encryption being decrypted at each stage. As a result, no single network node can fully determine both the origin and the final destination of the transmitted data (Figure 2) [6,10].

The Dark Web, in turn, represents the web-based environment operating on Darknet infrastructure. Resources within this environment function through alternative domain systems, such as .onion, and are accessible exclusively via anonymous networks [6].

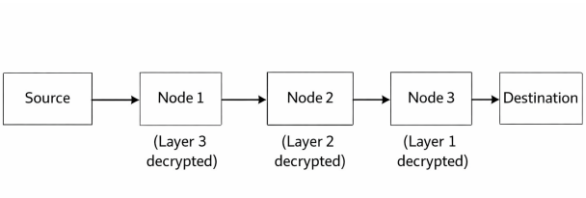

Figure 2. Onion routing mechanism

Anonymity is not only a defining characteristic of this environment but also a critical technological element that ensures its resilience and continuity.

The Tor network, as one of the primary access gateways to the Dark Web, currently comprises thousands of relay nodes distributed across numerous countries. This geographic dispersion makes it technically infeasible to disable the network through action against any single point, further reinforcing its resistance to state-level intervention and content control [6,10].

VI. Threats Posed by the Darknet Environment

In certain cases, the Darknet environment may be exploited for cybercriminal activities. Instances such as the dissemination of malicious software, the emergence of illicit marketplaces, and the provision of illegal services have been observed within this domain [12].

Furthermore, radical groups and terrorist organizations may utilize anonymous communication channels to exchange information. For individual users, risks include data breaches and the unauthorized circulation of personal information [13].

For these reasons, the Darknet environment presents significant challenges not only from a technological standpoint but also in terms of legal regulation and national security [3,7].

Research indicates that a notable proportion of Darknet activity is associated with cybercrime ecosystems, including the trade of stolen credentials, exploits, and ransomware-as-a-service offerings. Hacker forums operating on Dark Web infrastructure serve as coordination platforms where threat actors share tools, exchange intelligence, and recruit participants for targeted attacks against both private and governmental entities [12,13].

Technological Response Models of States

Different states adopt diverse approaches to addressing cybersecurity challenges. For example, China regulates information flows through the "Great Firewall" system, which is based on extensive Internet control mechanisms. This system employs technologies such as IP blocking, DNS filtering, and traffic analysis [14].

The European Union adopts an approach grounded in legal and institutional mechanisms in the field of cybersecurity. In this context, the NIS2 Directive (Network and Information Security Directive 2) aims to establish unified cybersecurity standards across member states [11].

Estonia, on the other hand, implements a model based on a digital state framework, placing particular emphasis on cybersecurity through electronic identification systems and robust national digital infrastructures [4,14].

Azerbaijan, in alignment with broader regional trends, has formalized its approach to information and cybersecurity through the adoption of the State Strategy on Information Security and Cybersecurity for 2023–2027. This strategic document defines national priorities for the protection of critical information infrastructure, the development of cybersecurity competencies, and the promotion of international cooperation in the digital domain [14].

These diverse national approaches underscore the absence of a universally accepted model for cyber governance. International cooperation, information sharing between national cybersecurity agencies, and the development of harmonized legal standards remain essential components of any effective global response to the challenges posed by the Darknet and anonymous network environments [3,11].

Conclusion

The analysis demonstrates that the Darknet and Dark Web environments constitute complex components of the broader digital security ecosystem. While they expand the possibilities for anonymity and privacy, they simultaneously introduce new challenges to state cyber sovereignty policies [5,6].

The distributed architecture of the Darknet, its layered encryption mechanisms, and its global node infrastructure enable it to function as a technologically resilient and adaptive system. Consequently, the complete restriction or elimination of this environment is considered impractical [10].

Looking ahead, the development of cybersecurity strategies should be based not solely on control mechanisms but also on a balanced approach. Such an approach must integrate the protection of user privacy, the strengthening of international cooperation, and the implementation of innovative technological solutions [3,4].

For states such as Azerbaijan, this balanced approach is particularly relevant given the country's ongoing digital transformation and its strategic positioning at the intersection of European and Asian digital corridors. Strengthening national cybersecurity capacity while engaging actively in international frameworks will be essential to effectively address the evolving threat landscape associated with Darknet and Dark Web environments [2,14].

References

[1] G. Pashayeva, "Emergence and development stages of informatics in Azerbaijan," Problems of Information Society, vol. 15, no. 1, pp. 72–85, 2024.Available:https://www.researchgate.net/publication/378092909_Emergence_and_development_stages_of_informatics_in_Azerbaijan

[2] R. Alakbarov and G. Pashayeva, "Emergence and Development of Network Technologies in Azerbaijan," pp. 251–265, 2024. [Online]. Available:https://www.researchgate.net/publication/391063497_AZRBAYCANDA_SBK_TEXNOLOGIYALARININ_MEYDANA_GLMSI_V_INKISAFI

[3] H.Cora and E. H. Mikail, "Cybersecurity, Sovereignty, and International Law: Normative Challenges in the Digital Age," vol. 23, e234381, 2026. Available:https://revista.domhelder.edu.br/index.php/veredas/article/view/4381/27026

[4] I. K. Kwentoa, “Cybersecurity in Digital Sovereignty: Protecting National Digital Ecosystems against Foreign Cyber Infiltration in the Age of Decentralized Technology,” Journal of Next-Generation Research 5.0, vol. 1, no. 4, pp. 1–22, May–Jun. 2025. Available: https://jngr5.com/jngr/article/view/130/127

[5] M. Coşar, “Siber Dünyanın Karanlık Yüzü: Deepweb ve Darknet,” Journal of Management Theory and Practices Research, vol. 3, no. 1, pp. 58–71, 2022. Available: https://dergipark.org.tr/en/download/article-file/3118937

[6] E. Jardine, “The Dark Web Dilemma: Tor, Anonymity and Online Policing,” 2015, pp. 1–24. [Online]. Available: https://www.cigionline.org/publications/dark-web-dilemma-tor-anonymity-and-online-policing/

[7] R. K. Shaikh, R. Anjum, and A. Barkat, “Cyber-Security Beyond Borders: Unraveling Cross-Jurisdictional Legal Complexities in Cyberspace,” Advance Social Science Archive Journal, vol. 5, no. 1, pp. 334–352, Jan.–Mar. 2026. Available: https://assajournal.com/index.php/36/article/view/1312/1959

[8] B. Nabiyev, K. Dashdamirova, “About the technological and cyber security aspects of ensuring the heterogeneous usage policy of the Internet environment,” in Proc. ITTA 2024, Baku, Azerbaijan, 2024, pp. 1–12. Available: https://itta.cyber.az/2024/papers/33.pdf

[9] R. Alquliyev, B. Nabiyev, and K. Dashdamirova, “Cyber Threats and Their Intellectual Analysis Issues in the Context of Technological Challenges of the IV Industrial Revolution,” in Proc. 2023 IEEE 17th International Conference on Application of Information and Communication Technologies (AICT), Oct. 2023. doi: 10.1109/AICT59525.2023.10313154

[10] Tor Project, “Tor Network Size Statistics,” Tor Metrics, Available: https://metrics.torproject.org/

[11] European Union Agency for Cybersecurity (ENISA), “Cybersecurity and Resilience of Smart Systems,” 2022. [Online]. Available: https://www.enisa.europa.eu/publications

[12] K. Thomas et al., “Investigating Cybercrime Markets on the Dark Web,” in Proc. IEEE Symposium on Security and Privacy, pp. 171–186 ,2015. [Online]. Available: https://ieeexplore.ieee.org/document/7163025

[13] M. Almukaynizi, A. Grimm, E. Nunes, J. Shakarian, and P. Shakarian, “Predicting Cyber Threats through Hacker Social Networks in Darkweb and Deepweb Forums,” in Proc. CSS 2017, Santa Fe, NM, USA, Oct. 2017, Article No.: 12, pp. 1–7. Available: https://dl.acm.org/doi/epdf/10.1145/3145574.3145590

[14] “Strategy of the Republic of Azerbaijan on information security and cyber security for 2023-2027” Aug. 28, 2023. [Online]. Available: https://president.az/az/articles/view/60949