The Dark Web and Cyber Sovereignty: Risks to States and Defense Mechanisms

Anar Suvarov
Azerbaijan State Oil and Industry University, Baku, Azerbaijan
info@asoiu.edu.az

Abstract— This article explores the role of the Dark Web in modern cyberthreats and its effect on cybersovereignty. It analyzes cybercrime markets, cybercrime as a service, and key risks to states, such as data breaches and ransomware. The article also discusses defense mechanisms, including threat intelligence and dark web monitoring. The findings emphasize the significance of proactive cybersecurity approaches to protect national security.

Keywords— Dark Web; Cyber Sovereignty; Cybercrime; Threat Intelligence; National Security.

I. INTRODUCTİON

The term "cyberspace" still does not have a globally accepted definition, although it is sometimes used interchangeably with the concept of the Internet or the digital virtual world. Several definitions have emerged from well-known organizations such as the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Russian-American Cybersecurity Summit, etc. (East-West Institute and the Institute of Information Security of Moscow State University). According to the US Department of Defense (Dictionary of Military and Related Terms of the Department of Defense, 2010), cyberspace is "a global area consisting of an interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and integrated processors and controllers, in the information environment". On the other hand, the Russian-American Cybersecurity Summit describes cyberspace as "an electronic medium in which information is created, transmitted, received, stored, processed, and deleted." Both definitions indicate that cyberspace encompasses the combination of internet and telecommunications technologies that enable the recording, storage, retrieval, and transmission of information. Krippendorff (2010) further supports this notion, claiming that "cyberspace emerges from the collective human capacity to express the possibilities in which technological artifacts are designed, utilized, and conceptualized." By comparison, Gibson (1984) highlights the anthropological dimension of cyberspace, describing it as an "iceberg of social change" approaching post-industrial culture. This emphasizes how cyberspace introduces new cultural behaviors to human enterprises and, consequently, transforms human experience by offering new viewpoints [1].

Cyber sovereignty - the extension of state sovereignty into cyberspace, affirms a country's right to manage, control, and regulate its data, digital content, and internet infrastructure within its borders. This represents a shift from a free, global internet to a decentralized, local system that emphasizes autonomy in terms of digital infrastructure, security, and regulations. The concept of cyber sovereignty originates from internet governance and typically denotes the capacity of governments to establish and enforce regulations in cyberspace via state authority. Bruce Schneier, a leading voice in internet governance, defines it as governments' efforts to control segments of the internet within their national borders [2]. The 2017 Tallinn Manual 2.0 is a key work that examines how existing international legal norms apply to cyberspace [3]. Discussions about cyber sovereignty often involve international law concepts such as intervention, use of force, due process, and state responsibility. On the other hand, the relation between data and territory challenges traditional presumptions of international law. As Fleur Johns claims, these developments represent a "reconfiguration of territory in international law," shifting focus from physical boundaries to issues of data access and technical capabilities [4].

A subset of the Deep Web(all parts of the internet that are not indexed by standard search engines like Google, Bing, or Yahoo), the Dark Web is distinguished by its anonymity and links to illicit activity. Because it runs on encrypted networks, both website owners and users can remain anonymous. Of these networks, Tor (The Onion Router) is the most well-known.

The Dark Web is infamous for housing illicit markets for the trafficking of guns, drugs, counterfeit money, and hacking services, but it also acts as a safe harbor for journalists, activists, and whistleblowers working under repressive governments. They can speak freely here without worrying about retribution. Based on the fact that the Dark Web is not indexed by mainstream search engines, accessing it needs specialized software, such as the Tor browser, and familiarity with particular URLs. The Dark Web is resolutely hidden and requires specialized equipment to gain access, but the surface web and the Deep Web, which are used by the majority of users regularly - include unindexed sections like private databases and password-protected websites. While these solutions offer privacy and security by anonymizing users' internet activity, they also put users in danger of fraud, phishing, and malware. The Dark Web has a complex function in the internet ecosystem, providing safeguards for privacy and freedom of expression with serious threats, despite its dangers and connections to illegitimate activity. It's critical to enter the Dark Web carefully, mindfully, and with knowledge of the benefits and drawbacks [5].

State sovereignty and national security are seriously threatened by the Dark Web. By utilizing advanced encryption

DOI: 10.25045/cyber.gov.2026.17

technology and onion routing, this platform establishes a "stateless" environment in which normal legal jurisdictions are not relevant. This setting makes it possible for hackers and non-state actors to fight asymmetrically across national boundaries against vital infrastructure [6]. In particular, the development of the "Cybercrime as a Service" (CaaS) model facilitates the trade in "zero-day" vulnerabilities and stolen official credentials that can cause a threat to state energy grids, financial systems, and defense institutions. Additionally, the Dark Web establishes advantageous conditions for anonymous transactions that evade taxes, money laundering through separated cryptocurrencies, and the spread of extremist propaganda that stimulates domestic radicalization. As a result, this concealed network undermines the state's monopoly on the legal use of force and economic control, and forces governments to face a difficult choice between national security and digital privacy [7].

II. FORMATİON OF THE DARK WEB ECONOMY

The Dark Web economy is an illegal digital market system accessed through special software (e.g. Tor), based on user anonymity and cryptocurrency payments. This economy is built on the uncontrolled trade of seized data, prohibited goods, and cybercriminal services (hacking, ransomware, etc.).

As much as they depend on markets, cybercriminals also rely on legal enterprises. Both the computing capabilities and targets of cybercriminals differ from each other. Specialization is enabled by criminal software markets; a computer programmer can create malware and sell it without being involved in the specifics of cybercrime activities. By giving inexperienced cybercriminals all the resources and assistance they need to perform their crimes, criminal software markets also decrease the level of technical expertise needed to enter the realm of cybercrime. According to McAfee (2013) and Sood and Enbody (2013), these markets enable criminals to create new hacking tools, hire and retain personnel, acquire the necessary skills, and disperse the spoils of crime among several organizations. Examples of platforms where criminal software and illegal services are bought and sold include Evolution, HPC, and Rescator. Evolution is a marketplace where malware, credit card information, DDoS attacks, and compromised accounts are sold. HPC is a forum for Russian-speaking hackers and a platform where they trade their services, including hacking tools. Rescator is an online marketplace focused primarily on selling stolen credit card information [8].

Cybercrime as a Service (CaaS) means a criminal economy where cybercrime is organized on an industrial scale and malicious tools, services, and permissions are sold on a subscription model. Within this model, RaaS (Ransomware as a Service), PhaaS (Phishing as a Service), DDoS services, malware, and artificial intelligence-based fraud tools are widespread. It is estimated that CaaS will cost the global economy an estimated 10.5 trillion USD annually in 2025, which clearly demonstrates its scale and level of threat. This model allows for the expansion of criminal activities by making high-level cyber attacks more accessible [9].

III. RİSKS TO THE STATE

Risks to the state means the threats posed by cyberattacks and illegal activities to state institutions, national security, critical infrastructure, and citizen data. These risks mainly present themselves in the form of data leaks, unauthorized access to critical systems, and ransomware attacks, and can result in serious economic, social, and security consequences.

In 2015, a cyberattack on the U.S. Office of Personnel Management (OPM) database caused the theft of personal and security clearance information for approximately 22 million federal employees and their dependents. The information included social security numbers, dates of birth, addresses, and even 5.6 million fingerprints, a breach of one of the government's most sensitive forms of security clearance. The government's classification of the incident as a large-scale data loss underscores the serious risks such breaches pose to national security, intelligence, and the personal safety of citizens [10].

According to information published by Brinztech Threat Intelligence in 2025, it was found out that illegal access rights to the systems of a company operating in the Polish energy sector were being sold on dark web platforms. By selling this access, the attacker claimed to have extensive control over the company's internal systems, which had the potential to ruin energy supplies, weaken economic stability, and pose serious risks to national security. This incident once again shows how dangerous cyber threats against critical infrastructure facilities are in terms of state security [11].

Ransomware attacks almost always result in data theft. Data exfiltration, which leads up to file encryption, was used in 96% of attacks in 2025, causing more damage to the enterprise. Since data theft is more harmful to the brand and more subject to regulations, data exfiltration contributed to a significant increase in breach costs. Globally, data breaches cost an average of $4.44 million in 2025, while healthcare data breaches cost $7.42 million. With 22% of reported attacks, the healthcare industry remained the most targeted industry by ransomware gangs in 2025. Except education, which saw a 13% year-on-year decrease in the number of attacks, other sectors experienced an increase in attacks in 2025 [12].

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issued a major security advisory on October 9, 2025, citing a sharp increase in ransomware attacks targeting healthcare facilities in the United States. Over the past ninety days alone, more than 350 hospitals and healthcare facilities have been affected by a coordinated campaign, a 400% increase in attacks compared to the same period in 2024. The attacks have also resulted in significant disruptions to patient care, including the cancellation of elective surgeries, referrals to emergency rooms, and the unavailability of vital medical records. It has been described by federal officials as "the most severe healthcare cybersecurity crisis in U.S. history." Healthcare facilities in Massachusetts have been particularly targeted, including several hospitals in the Boston area [13].

IV. DEFENSE MECHANİSMS İN THE CONTEXT OF CYBER SOVEREİGNTY

In the context of cyber sovereignty, defense mechanisms encompass the strategies and measures that states apply to protect national security, critical infrastructure, and information independence in the digital environment. These mechanisms are mostly based on timely threat detection, monitoring of the dark web, and coordinated cybersecurity methods at the national level.

Threat intelligence refers to the systematic collection and processing of information about cyber incidents for the purpose of timely detection, analysis, and prevention of cyber threats. This method allows government agencies to predict potential attacks in advance, assess risks, and enhance national cybersecurity strategies. In modern times, threat intelligence is considered one of the main pillars of effective cyber defense [14].

Dark Web Monitoring and Analysis has become an integral part of modern cybersecurity strategies. Tracking illegal activities on the Dark Web, such as data breaches, credit card data leaks, financial fraud, and targeting of critical infrastructure, allows for early detection and prevention of cyber threats at the state level. This approach plays a major role in proactive threat detection, risk assessment, and prevention of digital crimes, ultimately strengthening the state's national security resilience [15].

In the 21st century, with the increasing role of digital systems in public administration, energy, transportation, and other areas, cybersecurity has become a national security problem. Azerbaijan is performing modern defense measures at the national level to protect critical infrastructure systems and state resources against external cyberattacks and is working on preventive approaches to prevent cyberthreats. Measures such as cyberattack simulations, vulnerability detection, and information exchange between state structures are being carried out within the country, which serves to improve digital sovereignty. These strategies have become an integral part of ensuring digital independence and protecting national security for Azerbaijan [16].

CONCLUSİON

The scientific and practical importance of this study is that it comprehensively analyzes the issues of protecting state sovereignty and protecting critical systems in the digital environment in the context of the role of the Dark Web, cybercrime models and modern threats. Anonymous and uncontrolled environments such as the Dark Web establish favorable conditions for attacks against state databases, personal data and critical infrastructure systems, which leads to serious risks to national security. The establishment of threat intelligence systems for states, Dark Web monitoring and the implementation of coordinated cybersecurity measures at the national level play an important role in strengthening digital sovereignty, and the development of these approaches helps to protect the information independence of states.

According to the recommendations, state and cybersecurity agencies should strengthen proactive defense strategies, invest in systems that ensure early detection of threats in the Dark Web and other concealed digital environments, and develop national and international cooperation. At the same time, it is important to make the human factor more sustainable through professional personnel training and training programs in the field of cybersecurity, expand public-private sector partnerships, and organize information exchange mechanisms more effectively. Such measures will not only respond to current threats, but also allow for more agile combat with future changes in the cyber environment.

REFRENCES

[1] U. Mbanaso and E. S. Dandaura, "The Cyberspace: Redefining a New World." [Online]. Available: https://www.researchgate.net/publication/-280101879_The_Cyberspace_Redefining_A_New_World

[2] B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, NY, USA: W. W. Norton & Company, 2015, p. 134. [Online]. Available: https://archive.org/details/datagoliathhidde0000schn/page/n9/mode/1up

[3] M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, U.K.: Cambridge University Press, 2017. [Online]. Available: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf

[4] F. Johns, "Data territories: Changing architectures of association in international law," in *Netherlands Yearbook of International Law*, vol. 47, 2016, p. 109. [Online]. Available: https://www.researchgate.net/-publication/345000383_Data_Territories_Changing_Architectures_of_Association_in_International_Law

[5] S. Z. Drissi, "The Dark Web," Jul. 2024. [Online]. Available: https://www.researchgate.net/publication/382306203_The_Dark_Web

[6] D. Moore and T. Rid, "Cryptopolitik and the darknet," *Survival*, vol. 58, no. 1, pp. 7–38, 2016, doi: 10.1080/00396338.2016.1142085.

[7] M. Chertoff and T. Simon, "The impact of the dark web on internet governance," Centre for International Governance Innovation, 2015. [Online]. Available: https://www.cigionline.org/static/documents/gcig_paper_no6.pdf

[8] M. Gad, "Crimeware marketplaces and their facilitating technologies," 2014. [Online]. Available: https://scispace.com/pdf/crimeware-marketplaces-and-their-facilitating-technologies-1v2y2vfbv3.pdf

[9] M. Khalil, "Cybercrime-as-a-service: Market size and growth," 2025. [Online]. Available: https://deepstrike.io/blog/cybercrime-as-a-service-statistics-2025

[10] J. Chaffetz, "The OPM data breach: How the government jeopardized our national security for more than a generation," Sep. 7, 2016. [Online]. Available: https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

[11] Brinztech Threat Intelligence, "Unauthorized access sale detected for a Polish energy company," 2025. [Online]. Available: https://www.brinztech.com/breach-alerts/brinztech-alert-unauthorized-access-sale-detected-for-a-polish-energy-company/

[12] HIPAA Journal, "Healthcare most targeted sector 2025 ransomware." [Online]. Available: https://www.hipaajournal.com/healthcare-most-targeted-sector-2025-ransomware/

[13] "Healthcare ransomware attacks surge 400% in US – hospitals under siege as FBI issues critical security alert." [Online]. Available: https://cyberupdates365.com/healthcare-ransomware-attacks-surge-400-percent-fbi-alert/

[14] MSP Dark Intel, "Threat intelligence: The strategic backbone of modern cyber defense," *Medium*, 2025. [Online]. Available: https://medium.com/@mspdarkintel/threat-intelligence-the-strategic-backbone-of-modern-cyber-defense-5da1381b4da4

[15] Cyber Security Council, "Dark web – A strategic shield for national security," 2025. [Online]. Available: https://www.cybersecurity.councilgov.us/2025/08/24/dark-web-a-strategic-shield-for-national-security/

[16] Baku Network, "Cyber sovereignty in the 21st century: How Azerbaijan is building a digital shield," 2025. [Online]. Available: https://www.bakunetwork.org/en/news/analytics/14672