

UOT 327

ELGUN TAGHIZADEH

Doctoral student at Baku State University

Orcid: 0000-0002-0514-7808

ElgunTaghizadeh@gmail.com

NEW BOUNDARIES OF INTERNATIONAL SECURITY: CYBER POWER DYNAMICS IN THE DIGITAL AGE

DOI: <https://doi.org/10.36719/2708-065X/108/189-197>

Digital infrastructure and cyberspace have reshaped international security, introducing new threats, actors, and challenges. This paper examines cyber power's role in geopolitics, defense, and economic stability, using cases like WannaCry, Stuxnet, and the Colonial Pipeline attack to illustrate the disruptive potential of cyber operations. It also discusses the dual-use nature of AI and quantum technologies in both defensive and offensive strategies, as well as the impact of disinformation campaigns on political stability. In light of increasing cyber conflict complexity, the study calls for robust cybersecurity governance, international regulatory frameworks, and strategic alliances to enhance resilience in the emerging "Digital Cold War."

Keywords: Cybersecurity, Digital Transformation, International Security, Cybercrime, Disinformation, Critical Infrastructure, State-Sponsored Cyber Operations.

Introduction. Digital transformation, driven by information technologies and the internet, has reshaped international security dynamics. While offering new opportunities, it also introduces significant threats, particularly in cyber warfare and cybersecurity. Increasing digital dependence exposes states to risks such as cyberattacks and information manipulation.

Notable examples include the WannaCry ransomware attack in 2017, which disrupted global sectors, and the Stuxnet virus, which targeted Iran's nuclear program, underscoring cyberspace's impact on security [11]. Moreover, digital transformation heightens risks to economic stability and social cohesion, with disinformation campaigns and social media manipulation influencing public opinion and political processes [31]. International organizations like the UN and EU have initiated cybersecurity regulations and cooperation efforts to address these challenges. Additionally, digitalization is shaping security paradigms, raising concerns over legal and ethical issues, military applications of digital tools, and artificial intelligence's role in security.

As digital transformation reshapes international security, cyber threats have become a critical challenge for states and global institutions. Increasing reliance on digital infrastructure exposes both public and private sectors to sophisticated attacks, threatening economic stability and national security. Cyberattacks exploit vulnerabilities in infrastructure and software, targeting sectors such as finance, healthcare, and government institutions. Common threats include Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, Man-in-the-Middle (MITM) attacks, phishing techniques, ransomware, password breaches, SQL injections, DNS spoofing, and brute-force decryption. The growing sophistication of these threats underscores the need for robust cybersecurity strategies at both national and international [15].

High-profile incidents highlight the strategic significance of cyber capabilities. In 2000, the Department of Defense and NASA were hacked, with NASA's systems disabled for 21 days, resulting in the theft of \$1.7 million worth of software. This case exemplifies how even the most secure institutions are vulnerable and underscores cyber tools' role in geopolitical competition [20].

The WannaCry ransomware attack in May 2017 affected over 200,000 computers in more than 150 countries, disrupting operations and causing significant economic losses. This incident underscores the urgent need for improved cybersecurity [5]. It is also possible to add other examples here:

- Equifax Data Breach: The 2017 cyber-attack is the second largest in recorded history when personal data was stolen. Thus, the personal data of 147.9 million Americans, 15.2 million Britons, and 19,000 Canadians were shared [5].

◉ **The Stuxnet Worm:** In the year 2010, a virus reportedly created by the governments of the U.S. and Israel targeted Iran's nuclear facilities. In particular, it zeroed in on the Natanz facility for uranium enrichment. The issue was an attempt to delay Iran's nuclear program, so the Stuxnet Worm delayed Iran's nuclear program and destroyed its physical structure. Stuxnet is important since it represents new kinds of digital warfare with physical consequences [3].

◉ **Colonial Pipeline Ransomware Attack:** In 2021, Colonial Pipeline was attacked. A ransomware group, going by the name of DarkSide, laid its sights on the largest oil pipeline in the United States, fuel shortages ensued, and both sides of America's east coast were significantly affected. This was not a direct attack on the government but a real attack on its instruments. The same incident was also indicative of the fact that the interaction of the public and private sectors is imperative in the face of cyber threats and it proved once more that the same or even better results may be achieved with armed attacks or explosive munitions using digital means to shape and theorize the reality of the modern era. This can be exemplified both as an offensive strategy and a defensive one [3].

We can add many cyber attacks to this list. The realization is often made by state and non-state actors. The targets can be very different, and the motives that trigger these targets can also look different. Otherwise stated, we can underline economic, political, ideological, psychological and similar motives. At the same time, from the point of view of realization, a person, group, organization and more different structures can be listed here.

Even if we consider the cyber-attacks referred to in the contemporary time as the echo of the "Digital Cold War", we hear the footsteps, poetically speaking. Because let's look at some of the cyber-attacks on state institutions over the last decade, from 2014 to 2024: 1.UK National Health Service, 2.City of Oakland, 3.UK Electoral Commission, 4.Government of Costa Rica, 5.Canada Revenue Agency, 6.Bernalillo County, New Mexico, 7.Pottawatomie County, Kansas, 8.City of Chicago Aviation Department, 9.City of Riviera Beach, Florida, 10.City of Atlanta, 11.City of Baltimore, and others. For example, the number of politically motivated cyber attacks in the United States in the year 2023 was more than 200, out of which 122 fit under the category "Attacks on critical infrastructure targets" [6, p.25]. As seen here, the effects of the digital cold war are already real. It should be noted here that some countries have not been subjected to cyber-attacks because they have not made a rapid transition to digitalization, but this process has slowed down the benefits of digitalization in the long run [4].

Actors of Cyber Attacks. Cyberattacks are carried out by diverse actors-including state-sponsored entities, cybercriminal organizations, hacktivists, terrorist groups, and insiders-each presenting distinct challenges that require tailored cybersecurity strategies.

◉ **State-Sponsored Actors:** Governments leverage cyber capabilities for espionage, disruption, and offensive operations targeting critical infrastructures and institutions [34]. Examples include Russia's involvement in the 2016 U.S. election, China's cyber espionage [28], and North Korea's financial cyber operations, such as the 2016 Bangladesh Bank heist.

◉ **Cybercriminal Organizations:** Driven by financial motives, these groups engage in ransomware, data breaches, and fraud. Notable cases include the Conti ransomware group [13] and REvil, responsible for the 2021 Kaseya attack [2]. Hacktivists: Motivated by ideological or political objectives, hacktivists use tactics like DDoS attacks and data leaks to promote their causes. The decentralized collective Anonymous, for instance, has targeted governments and corporations to expose perceived injustices [16].

◉ **Terrorist Groups:** Although currently limited in their cyber warfare capabilities, terrorist organizations increasingly use digital platforms for recruitment, propaganda, and potentially disruptive attacks [29]. For example, ISIS has exploited encrypted communication channels to further its agenda [27].

◉ **Insider Threats:** Insider risks arise when individuals misuse their authorized access, whether intentionally or through negligence. The Edward Snowden case, which involved the leakage of classified NSA data [17], exemplifies the severe consequences of such breaches.

In the digital age, power dynamics have shifted as state and non-state actors increasingly use information as a strategic asset. Information warfare-defined as the deliberate use of digital tools to manipulate, disrupt, or undermine an adversary's decision-making - extends beyond traditional military tactics to include cyber operations, propaganda, and coordinated media campaigns [23], [34]. For example, during the Ukraine-Russia conflict, both sides employed sophisticated information campaigns to shape international narratives and influence domestic perceptions. By targeting critical infrastructures and public discourse, information warfare blurs the boundaries between peace and conflict, with even minor disruptions in digital communications having significant political and economic consequences.

Disinformation-the intentional spread of false information-shapes public perception and erodes trust in institutions. Social media accelerates its impact, deepening societal polarization and reinforcing biases. During elections, it undermines voter confidence, weakens democratic institutions, and fuels extremism. Additionally, disinformation diminishes the credibility of traditional media, making it harder to maintain an informed public. The convergence of information warfare and disinformation poses significant risks to national and global security. As digital platforms evolve, traditional governance struggles to keep up. Tackling these challenges requires improving digital literacy, strengthening regulations, fostering international cooperation, and developing rapid misinformation responses. With both state and non-state actors exploiting digital vulnerabilities, swift policy action is essential to safeguarding democracy and social stability.

The Impact of Disinformation on Public Opinion. Nowadays, information can seriously determine the future of states. A case in point is the "Cambridge Analytica" scandal. Thus, in 2014, the data of more than 50 million Facebook users was collected and then used in manipulating an election company [10]. We can see fake news and other examples in the continuation of this process. For instance, during the US elections of 2016, fake news, such as "Pope Francis stuns the world, backs Donald Trump for president" gained over 960 thousand interactions on Facebook; "Pizzagate", which received millions of interactions in 2016, "Ireland now officially accepts Trump refugees from America", "WikiLeaks confirms Hillary sold arms to ISIS... Then she dropped another bombshell" are examples of fake news [18].

The above examples demonstrate how disinformation campaigns and social media manipulations can indeed influence public opinions, especially during times of elections. Information warfare is impacting not only the domestic politics of a single country but also the mutual relations of states internationally. For example, activities by Russia in creating political instability in Western countries through troll factories or bot networks have been much debated. That approach was witnessed in most European elections, in the Brexit referendum, and in the US elections in 2016 [36].

Social media accelerates disinformation and propaganda, allowing political actors and states to manipulate public opinion, undermine rivals, and threaten state sovereignty. Information warfare has become a digital weapon, influencing elections, weakening democratic institutions, and destabilizing global security. Addressing these challenges requires international legal frameworks, advanced technological tools, and enhanced media literacy. Additionally, coordinated political manipulation through bot networks and troll factories shapes public discourse. In response, global security efforts now include digital literacy programs, fact-checking mechanisms, and strengthened cybersecurity. Social media companies are enforcing stricter content moderation, while international collaboration expands countermeasures. The key challenge remains balancing security efforts with freedom of expression and political integrity in the digital age.

Cyber war refers to the use of digital technologies by state and non-state actors to conduct offensive operations-such as espionage, sabotage, and assaults on critical systems-that target essential information infrastructures [23]. Unlike traditional military conflicts, cyber warfare is low-cost, asymmetrical, and capable of operating across borders with minimal physical damage [23]. Nye (2010) argues that the emergence of cyber capabilities is reshaping national security by enabling even smaller or technologically agile states to challenge larger military powers through digital vulnerabilities. This evolution creates a complex international security environment, where deterrence and power projection increasingly depend on cyber sophistication alongside conventional military strength. As cyber

weapons proliferate, they further disrupt traditional power balances, necessitating new frameworks for international law and enhanced security cooperation.

Geopolitical Consequences of Cyber Attacks on States. Cyber warfare involves the malicious infiltration of state computer systems to disrupt, disable, or damage them. As digital technologies evolve, cyberattacks have become integral to interstate conflicts, targeting intelligence systems, critical infrastructure, and public order. These attacks threaten national security, economic stability, and public trust, making cyber warfare a key aspect of the Digital Cold War. Actors in this domain include state entities, cyber mercenaries, and hacktivists. A notable example is China's People's Liberation Army Strategic Support Force (CPLASSF), linked to cyber espionage against multiple nations. Operations like "Operation Aurora," attributed to the CPLASSF-affiliated Elderwood Group, exemplify state-sponsored cyber espionage aimed at stealing intellectual property and strategic data, particularly from the U.S.

A highly coordinated cyberattack, involving 34 companies-including Google-highlighted the growing threat of state-sponsored cyber warfare. These attacks, utilizing "Zero-Day" vulnerabilities, allowed hackers to exploit unknown security flaws.

Notably, Chinese-linked hacker groups such as Elderwood Gang and Comment Crew have been tied to major cyber espionage campaigns. Elderwood specializes in targeting second-tier defense suppliers to infiltrate larger U.S. contractors, often using spear-phishing and water hole attacks. In 2010, it carried out "Operation Aurora," breaching Google's security and stealing critical source code. Meanwhile, Comment Crew conducted "Operation ShadyRAT," infiltrating over 72 organizations, including the International Olympic Committee and the United Nations, using Remote Access Tools (RATs). Cybersecurity experts, including Symantec, suggest that these groups operate from China and may have state backing. Reports estimate that Elderwood and Comment Crew account for 90% of economic espionage against U.S. companies, focusing on intellectual property theft and strategic business intelligence. These incidents underscore the increasing role of cyber warfare in global security and economic competition [26]. As a side note, The Atlantic (January 19, 2016) reports that Google left the Chinese market after the 2009 attack [24].

Cyber warfare has evolved significantly over the years, marked by several high-profile incidents. One prominent case is GhostNet, a massive spy network uncovered in 2009 that compromised over a thousand computers in 103 countries, including those of the Dalai Lama's office and various foreign ministries, though the Chinese government denied involvement [22]. Similarly, Night Dragon was a coordinated cyber-attack by Chinese hackers targeting major energy companies in Europe and the United States between 2007 and 2009, affecting more than 70 organizations, including the United Nations and the International Olympic Committee [9]. During the 2008 U.S. presidential elections, hackers infiltrated the computers of both John McCain and Barack Obama, leading to the theft of sensitive information - a breach initially misinterpreted as a virus attack and later attributed to Chinese and Russian actors [7]. Additionally, in 2009, China-based hackers breached the U.S. Joint Strike Fighter Project, compromising sensitive data at a project valued at over \$300 billion [32]. These incidents underscore the evolving nature of cyber warfare and its profound implications for national and international security.

Benjamin Jensen's 2023 Congressional testimony asserts that China "cheated" to achieve its 21st-century goals, a claim that aligns with the strategic vision outlined in the Chinese Communist Party's "Made in China 2025" plan. Jensen argues that AI weapons, capable of performing the work of thousands simultaneously, offer an effective countermeasure against China's substantial human potential, especially given that the United States dominates in quantum computing [1]. He also highlights a significant vulnerability: small businesses, which represent 44% of the U.S. economy, are the least likely to invest in cybersecurity.

The modern cybersecurity landscape increasingly depends on robust cloud security. AI systems require vast datasets and powerful processing capabilities to function effectively, making the protection of data a strategic national security priority. This necessity is underscored by the fact that state-sponsored cyber attackers are actively targeting cloud infrastructures and AI models to steal economic and military secrets, aiming to gain technological and strategic advantages.

In response to these evolving threats, many states have established “cyber armies” within their armed forces. The growth of these digital military units is evident: while only five states maintained cyber armies in 2000, this number rose to over 10 in 2009 and reached 38 by 2018 [19]. These units - often referred to as “Unmanned Armed Forces,” “Cyber Army,” or “National Cyber Defense Unit” - are designed to both defend against cyber threats and project power, marking a shift toward what is increasingly being described as a “digital cold war”.

Moreover, the proliferation of digital espionage, information theft, and attacks on critical infrastructures signals that the digital cold war extends beyond the economic and political spheres into the military domain. In this context, cyber armies and digital defense structures have become indispensable elements of national security policies, influencing military conflicts as well as diplomatic relations in the digital age.

Artificial Intelligence (AI) and quantum technologies are rapidly transforming cyber warfare by reshaping both offensive and defensive strategies. AI enables real-time threat detection, attack analysis, and automated defenses through machine learning, enhancing cybersecurity adaptability. However, AI also introduces new risks, such as adversarial attacks and deepfake-based disinformation [12]. Concurrently, quantum technologies challenge existing encryption standards; quantum computers threaten to break RSA and ECC encryption, accelerating the need for post-quantum cryptography. Conversely, quantum key distribution (QKD) offers enhanced secure communication, as demonstrated by China’s quantum networks [35].

The growing reliance on digital infrastructure has driven states to establish cyber armies as essential components of national defense. Unlike conventional military forces, these cyber units operate in the digital realm, employing sophisticated offensive and defensive operations ranging from espionage to digital sabotage with minimal physical engagement [29]. This shift not only provides plausible deniability but also complicates attribution and accountability, leading to a rise in state-sponsored cyber operations.

Global powers have adopted distinct cyber strategies: the U.S. Cyber Command (USCYBERCOM) utilizes persistent engagement strategies to proactively deter threats; China’s People’s Liberation Army (PLA) Strategic Support Force focuses on cyber espionage and information warfare; and Russia integrates cyber-enabled hybrid warfare into its military doctrine, as seen in its campaigns against Ukraine and other geopolitical adversaries [34]. These developments contribute to what has been termed the “Digital Cold War” state of continuous cyber conflict characterized by espionage, infrastructure attacks, and disinformation campaigns rather than direct military confrontation. In this environment, enhancing cyber resilience and establishing robust international cybersecurity agreements are imperative to prevent escalation and ensure national and global security.

Governments collaborate extensively with cybersecurity firms, highlighting their critical role in national security. For instance, CrowdStrike provides cloud-based antivirus services to the U.S. Department of Justice [14]. This demonstrates the influence of cybersecurity companies. However, their power also carries risks. The 2024 “CrowdStrike Scandal” exemplifies this, where a software failure caused critical systems in airlines, banks, and other organizations to crash, leading to flight cancellations and financial disruptions [30]. Further emphasizing their significance, numerous firms, including Fortinet, Palo Alto Networks, Cloudflare, Cisco, Microsoft, and Amazon, serve as government contractors, reinforcing their integral role in cybersecurity.

State Control, Private Security Companies, and the Protection of Critical Infrastructure. Effective state control and legal frameworks are essential for cybersecurity regulation and national security. While regulations like the GDPR enhance data protection, excessive restrictions may hinder innovation. Private security firms support cyber defense through threat intelligence and incident response, complementing government efforts but requiring stronger oversight. Protecting critical infrastructure - energy, transportation, and healthcare - relies on cybersecurity firms developing tailored solutions and collaborating with governments to ensure resilience and prevent disruptions.

Scientific-Technical Progress and Cybersecurity - New Paradigms and Challenges.

• **AI and Quantum Technologies in Cybersecurity:** Artificial Intelligence (AI) has transformed cybersecurity by enabling advanced threat detection through machine learning, though it remains

vulnerable to adversarial attacks that can lead to misclassification and security breaches [25]. Quantum computing, while offering new opportunities, also threatens traditional encryption methods (e.g., RSA, ECC) and has driven research into quantum-resistant cryptography, intensifying international competition.

• **Digital Transformation and Emerging Cyber Threats:** The rapid adoption of cloud computing and the Internet of Things (IoT) introduces significant vulnerabilities, such as data breaches and large-scale Distributed Denial of Service (DDoS) attacks. Additionally, AI-driven attacks, including deepfakes, challenge information integrity and necessitate robust security protocols and international collaboration [21].

• **Impact on International Security Strategies:** The integration of AI and quantum technologies into the cyber domain requires a fundamental reassessment of national defense policies. Cybersecurity now underpins national security, prompting international alliances to prioritize the development of quantum-safe encryption, the fortification of AI systems, and the establishment of global norms to manage emerging technological risks [23].

Conclusion. The rapid expansion of digital technologies has reshaped international security, introducing both opportunities and unprecedented challenges. Nations must navigate the complexities of cyber warfare, digital disinformation, and evolving cyber threats. State-sponsored cyber operations, cybercrime, and misinformation campaigns emphasize the need for robust cybersecurity policies and international cooperation. Attacks like Stuxnet, WannaCry, and the Colonial Pipeline incident highlight the strategic role of cyber capabilities in modern conflicts. Meanwhile, AI and quantum computing present both security risks and advancements, influencing encryption and defense mechanisms. Disinformation campaigns further disrupt political stability, shaping public opinion and electoral outcomes. As the “Digital Cold War” intensifies, states must enhance cybersecurity governance, strengthen regulatory frameworks, and foster collaboration between public and private entities. The cyber arms race calls for investment in resilient infrastructure, AI-driven threat detection, and quantum-resistant encryption. A coordinated, multilateral approach - uniting governments, international organizations, and private sectors - is essential to ensuring global cybersecurity and stability. Without proactive measures, escalating cyber threats will continue to endanger international security, economic stability, and global peace.

REFERENCES

1. “16 Most Advanced Countries in Quantum Computing,” *Yahoo Finance*, Dec. 06, 2023. Available: <https://finance.yahoo.com/news/16-most-advanced-countries-quantum-131132253.html> [14.02.2025].
2. “Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers | CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, Jul. 12, 2021. Available: <https://www.cisa.gov/news-events/news/kaseya-ransomware-attack-guidance-affected-msps-and-their-customers> [14.02.2025].
3. “The Top 7 Cyberattacks on U.S. Government: A closer look at the evolving landscape of cybersecurity,” *SecurityScorecard*, Jan. 24, 2025. Available: <https://securityscorecard.com/blog/top-cyberattacks-on-us-government> [14.02.2025].
4. “U.S. targeted political cyberattacks 2023,” *Statista*, 2023. Available: <https://www.statista.com/statistics/1428610/us-targeted-political-cyberattacks-by-characteristic/> [14.02.2025].
5. “What is WannaCry? WannaCry Ransomware Attack Case Study,” *Fortinet*. Available: <https://www.fortinet.com/resources/cyberglossary/wannacry-ransomware-attack> [14.02.2025].
6. A. Wolf, “Top Cyber Attacks on Government Agencies | Arctic Wolf,” *Arctic Wolf*, Sep. 19, 2024. Available: <https://arcticwolf.com/resources/blog/notable-cyber-attacks-on-government-agencies> [14.02.2025].
7. ANI, “Business Standard,” 2025. Available: https://www.business-standard.com/article/news-ani/chinese-hacked-obama-mccain-campaigns-say-us-officials-11360700607_1.html [14.02.2025].

8. B. Jensen, "How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy," *www.csis.org*, Oct. 2023, Available: <https://www.csis.org/analysis/how-chinese-communist-party-uses-cyber-espionage-undermine-american-economy> [14.02.2025].
9. Bugcrowd, "Night Dragon Operation," *Bugcrowd*. Available: <https://www.bugcrowd.com/glossary/night-dragon-operation/> [14.02.2025].
10. C. Cadwalladr and E. Graham-Harrison, "Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach," *The Guardian*, Mar. 17, 2018. Available: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> [14.02.2025].
11. D. Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, Feb. 26, 2013. Available: <https://spectrum.ieee.org/the-real-story-of-stuxnet> [14.02.2025].
12. D. M. J. Lazer, M. A. Baum, Y. Benkler and etc., "The Science of Fake News," *Science*, vol. 359, no. 6380, pp. 1094–1096, Mar. 2018, doi: <https://doi.org/10.1126/science.aao2998>.
13. European Cybercrime Centre (Europol), "Ransomware Threat Assessment Report," 2022.
14. ExecutiveGov, "10 Government Cybersecurity Company Contractors," May 08, 2024. Available: <https://executivegov.com/articles/10-cybersecurity-company-contractors/> [14.02.2025].
15. Fortinet, "Top 20 Most Common Types Of Cyber Attacks," *Fortinet*, 2023. Available: <https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks> [14.02.2025].
16. G. Coleman, "Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous", London: Verso, 2014, p. 482.
17. G. Greenwald, "No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State", New York: Metropolitan Books, 2014, p. 272.
18. H. Ritchie, "Read all about it: The biggest fake news stories of 2016," *CNBC*, Dec. 30, 2016. Available: <https://www.cnn.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html> [14.02.2025].
19. J. Blessing, "The Global Spread of Cyber," *CCDCOE*, 2018. p. 23. Available: https://ccdcOE.org/uploads/2021/05/CyCon_2021_Blessing.pdf [14.02.2025].
20. J. Fox, "8 biggest cyberattacks in history | cobalt," *www.cobalt.io*, Oct. 07, 2022. Available: <https://www.cobalt.io/blog/biggest-cybersecurity-attacks-in-history> [14.02.2025].
21. J. Kietzmann, L.W. Lee, I.P. McCarthy, and T.C. Kietzmann, "Deepfakes: Trick or treat?" *Business Horizons*, vol. 63, no. 2, pp. 135-146, 2020.
22. J. Markoff, "Vast Spy System Loots Computers in 103 Countries," *The New York Times*, Mar. 28, 2009. Available: https://www.nytimes.com/2009/03/29/technology/29spy.html?_r=1 [14.02.2025].
23. J.Nye, "Cyber Power Cyber Power," 2010, p.30. Available: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf [14.02.2025].
24. K. Waddell, "Why Google Quit China-and Why It's Heading Back," *The Atlantic*, Jan. 19, 2016. Available: <https://www.theatlantic.com/technology/archive/2016/01/why-google-quit-china-and-why-its-heading-back/424482/> [14.02.2025].
25. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cybersecurity intrusion detection," *Information Sciences*, vol. 380, pp. 18-38, 2016.
26. M. Clayton, "Stealing US business secrets: Experts ID two huge cyber 'gangs' in China," *Christian Science Monitor*, Sep. 14, 2012. Available: <https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China> [14.02.2025].
27. M. Conway, "Deterring Terrorism Online: The Case of ISIS," *Perspectives on Terrorism*, vol. 11, no. 3, pp.1-15, 2017.
28. N. Inkster, *China's Cyber Power*. Routledge, 2018, p. 156.
29. R. A. Clarke and R. Knake, *Cyber War: the Next Threat to National Security and What to Do About It*. New York: Harpercollins E-Books, 2010, p. 320.

30. R.Plummer, "CrowdStrike and Microsoft: What we know about global IT outage," *www.bbc.com*, Jul. 19, 2024. Available: <https://www.bbc.com/news/articles/cp4wnrxqlewo> [14.02.2025].
31. S. Bradshaw and P. Howard, "OII | The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation," *Ox.ac.uk*, 2019. Available: <https://www.oii.ox.ac.uk/news-events/reports/the-global-disinformation-order-2019-global-inventory-of-organised-social-media-manipulation> [14.02.2025].
32. S. Gorman, A. Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *WSJ*, Apr. 21, 2009. Available: <https://www.wsj.com/articles/SB124027491029837401> [14.02.2025].
33. S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, Jan. 2011, doi: <https://doi.org/10.1016/j.jnca.2010.07.006>.
34. T. Rid, *Cyber War Will Not Take Place*. Oxford University Press, 2013, p. 218.
35. Y. Benkler, R. Farris, and H. Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press, 2018. doi: <https://doi.org/10.1093/oso/9780190923624.001.0001>.
36. Z. Zhang, "Study Confirms Influence of Russian Internet 'Trolls' on 2016 Election | Columbia SIPA," *www.sipa.columbia.edu*, Mar. 29, 2022. Available: <https://www.sipa.columbia.edu/news/study-confirms-influence-russian-internet-trolls-2016-election> [14.02.2025].

ELGÜN TAĞIZADƏ

Bakı Dövlət Universitetini doktorantı

BEYNƏLXALQ TƏHLÜKƏSİZLİYİN YENİ SƏRHƏDLƏRİ: RƏQƏMSAL DÖVRDƏ KİBER GÜC DİNAMİKASI

Rəqəmsal infrastruktur və kiber məkan beynəlxalq təhlükəsizliyi yenidən formalaşdıraraq yeni təhdidlər, iştirakçılar və çağırışlar yaradır. Bu məqalə kiber gücün geopolitika, müdafiə və iqtisadi sabitlikdəki rolunu araşdırır və WannaCry, Stuxnet, Colonial Pipeline hücumları kimi nümunələrlə kiber əməliyyatların dağıdıcı potensialını göstərir. Həmçinin, süni intellekt və kvant texnologiyalarının müdafiə və hücum strategiyalarında ikiqat istifadə imkanları və dezinformasiya kampaniyalarının siyasi sabitliyə təsiri müzakirə olunur. Artan kiber münaqişələrin mürəkkəbliyini nəzərə alaraq, tədqiqat yaranan "Rəqəmsal Soyuq Müharibə" şəraitində davamlılığı artırmaq üçün güclü kiber təhlükəsizlik idarəçiliyi, beynəlxalq tənzimləyici çərçivələr və strateji ittifaqların vacibliyini vurğulayır.

Açar sözlər: Kiber təhlükəsizlik, Rəqəmsal transformasiya, Beynəlxalq təhlükəsizlik, Kibercinayətkarlıq, Dezinformasiya, Kritik infrastruktur, Dövlət sponsorlu kiber əməliyyatlar.

ЭЛГУН ТАГИЗАДЕ

Докторант Бакинского государственного университета

НОВЫЕ ГРАНИЦЫ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ: ДИНАМИКА КИБЕРМОЩИ В ЦИФРОВУЮ ЭПОХУ

Цифровая инфраструктура и киберпространство изменили международную безопасность, вводя новые угрозы, участников и вызовы. В данной статье рассматривается роль киберсилы в геополитике, обороне и экономической стабильности, с примерами таких инцидентов, как WannaCry, Stuxnet и атака на Colonial Pipeline, иллюстрирующими разрушительный потенциал киберопераций. Также обсуждается двойственное применение технологий искусственного интеллекта и квантовых вычислений в оборонительных и наступательных стратегиях, а также влияние кампаний дезинформации на политическую стабильность. В условиях растущей сложности киберконфликтов исследование подчеркивает необходимость создания надеж-

ного управления кибербезопасностью, международных нормативных рамок и стратегических альянсов для повышения устойчивости в формирующейся «Цифровой холодной войне».

Ключевые слова: Ключевые слова: Кибербезопасность, Цифровая трансформация, Международная безопасность, Киберпреступность, Дезинформация, Критическая инфраструктура, Кибероперации, спонсируемые государством.

Мəqalənin redaksiyaya daxil olduğu tarix: 14 fevral 2025-ci il.

Мəqalənin çapa qəbul olunma tarixi: 04 mart 2025-ci il.

Rəyçilər: s.e.f.d. Kəram Məmmədov, t.ü.f.d. Məmmədağa Baxışov.
