REPUBLIC OF AZERBAIJAN

On the rights of the manuscript

ABSTRACT

of the dissertation for the degree of Doctor of Philosophy

SOCIAL AND POLITICAL ASPECTS OF CYBERSECURITY IN THE AGE OF DIGITALISATION

Speciality:	5901.01 – “International Relations”
Field of science:	Political Sciences
Applicant:	**Kamila Famil Jabbarova**

Baku – 2026

The work was performed at the Department of International Relations of the Academy of Public Administration under the President of the Republic of Azerbaijan.

Scientific supervisor: Doctor of Political Sciences, Professor
Elman Xudam Nasirov

Official opponents: Doctor of Political Sciences, Professor
Hijran Kamran Huseynova

Doctor of Philosophy in Political Sciences, Associate Professor
Zumrud Eldar Malikova

Doctor of Philosophy in Political Sciences, Associate Professor
Parvana Telman Mustafazade

Dissertation council FD 2.30 of Supreme Attestation Commission under the President of the Republic of Azerbaijan operating at the Academy of Public Administration under the President of the Republic of Azerbaijan.

Chairman of the Dissertation council: Academician
Urkhan Kazim Alakbarov

Scientific secretary of the Dissertation council: Doctor of Political Sciences, Professor
Sevda Agamirza Aliyeva

Chairman of the scientific seminar: Doctor of Political Sciences, Professor
Elchin Ildirim Ahmadov

GENERAL CHARACTERISTICS OF THE RESEARCH

Background and Significance. The rapid advancement of digital technologies in the twenty-first century has fundamentally reshaped the character of international relations and the architecture of global security. Cyberspace has emerged as a new geopolitical arena in which the strategic interests of states, international organisations, and transnational corporations converge. In this configuration, information resources have come to constitute decisive strategic capital.

The digitalisation of public life has given rise to entirely new forms of conflict, encompassing cyberwarfare, cyber espionage, cyberterrorism, and disinformation campaigns. These phenomena threaten not only critical infrastructure but also the legitimacy of governments, public trust, and the stability of international institutions. Modern conflicts are increasingly developing in a hybrid form that interweaves military, political, economic, and informational instruments. In this context, cybersecurity has become an integral element of national power and diplomacy, and demands comprehensive scholarly examination.

Despite a growing body of research on digital security, the conceptual foundations of cyber threats and cyber warfare remain fragmented. In international relations theory, the realist paradigm frames cyberspace as a new arena for state sovereignty and military power; the liberal approach views it as a platform for legal norms and collective cooperation; constructivist readings treat it as a product of strategic discourse and identity formation. There remains, moreover, a pressing need for a holistic conceptual framework that accounts for the complex interplay of political determinism, technological configuration, and social dynamics within cybersecurity ecosystems-a gap the present dissertation seeks to address.

Artificial intelligence is penetrating political and public life with increasing depth. While it improves governance, it also generates ethical and legal threats including disinformation, manipulation, and privacy violations. Big data analytics now enable the prediction of electoral behaviour and the construction of micro-targeting strategies, shifting cybersecurity beyond the protection of technical infrastructure into the

domain of information security and psychological warfare. Deepfake technologies and generative AI directly undermine electoral integrity and public trust. The Cambridge Analytica scandal during the 2016 US presidential election and the proliferation of deepfakes during India's 2024 general election illustrate the global risks of AI as a tool of political manipulation.

During the 44-Day Patriotic War, the deployment of AI-based tools such as Tavush Bot to achieve information superiority introduced a new paradigm of information warfare. Azerbaijan's Digital Transformation Strategy for 2023–2026 prioritises the application of AI in public administration, foregrounding questions of ethical and transparent AI deployment. The study of the political and social dimensions of AI-driven cyber threats is therefore of particular importance for national security strategy.

This dissertation addresses a subject that has not previously been examined in a comprehensive manner in Azerbaijani political science, and whose systematic treatment remains limited in the broader international literature. Existing scholarship can be grouped into five clusters. The first, including A.S.Arslan, R.O.Keohane, and J.S.Nye,[1] examines cyberspace through the lens of classical IR theory. The second, including L.Alford, G.Bayraktar, and B.Buchanan, focuses on the military and strategic dimensions of cyber operations and interstate conflict. The third, including V.Boulanin, E.Blessing, M.Ashok, and C.Cupać,[2] addresses the role

[1] Arslan, A.S. Neorealist Analysis of Security Dilemma in Cyberspace: A Quantitative Study // Political Theory, – 2024. Version 10: [Electron resource] / URL: https://www.researchgate.net/publication/ 380387742_Neorealist_Analysis_of_Security_Dilemma_in_Cyberspace_A_Quantitative_Study; Keohane, R.O. Power and Interdependence: World Politics in Transition / R.O.Keohane, J.S.Nye. – Boston: Little, Brown, – 1977. – 273 p.; Nye, J.S. Cyber Power / J.S.Nye. – Belfer Center, – 2010. – 28 p.

[2] Boulanin, V. Mapping the Development of Autonomy in Weapon Systems / V.Boulanin, M.Verbruggen // Stockholm International Peace Research Institute (SIPRI), – 2017.; Ashok, M. Ethical framework for Artificial Intelligence and Digital technologies / M.Ashok, R.Madan, A.Joha, U.Sivarajah // International Journal of Information Management, – 2022; Cupać, J. Regulate against the machine: how the EU mitigates AI harm to democracy / J.Cupać, M.Sienknecht // Democratization, – 2024, Vol.31, Issue: 5, – pp.1067–1090.

of AI in security, ethical problems, and legal frameworks. The fourth, including C.Hadnagy and J.Owen,[3] examines manipulation and disinformation in cyberspace. The fifth, including A.Barrinha, S.Arséne,[4] A.Chander, R.Creemers, L.DeNardis, and L.Floridi, investigates internet governance, data nationalism, and global governance models.

Although the technical and legal aspects of cybersecurity have been extensively studied, the socio-political consequences of digitalisation, particularly the balance between individual security and the state's social control functions, require further comprehensive treatment. This dissertation seeks to fill those gaps and to provide a theoretically grounded account of Azerbaijan's cyber-political model in the face of contemporary challenges.

Object and Subject of the Research. Object of research: the general system of the security phenomenon. **Subject of research:** cybersecurity in the age of digitalisation. The **aim** of the dissertation is a comprehensive analysis of the social and political aspects of cybersecurity in the age of digitalisation. To this end, the following **objectives** are pursued:

– To establish the conceptual framework of cybersecurity within political science and its place in the national security architecture;

– To systematise the leading methodological principles and research frameworks applied to the political analysis of cybersecurity;

[3] Hadnagy, C. Social Engineering: The Science of Human Hacking / C.Hadnagy. – Wiley. Canada, – 2018. – 354 p; Owen, J. Psychological Mechanisms in Social Engineering Attacks // EasyChair. – 2024.

[4] Arséne, S. La Chine et le contrôle d'Internet: une cybersouveraineté à multiples facettes // Annuaire français de relations internationales, – 2022, – pp. 959–976; Creemers, R. Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management // Journal of Contemporary China, – 2016, – pp. 85–100; Floridi, L. The fight for digital sovereignty: What it is, and why it matters, especially for the EU // Philosophy & Technology, – 2020, Vol.33, Issue 3 – pp.369–378; Izycki, E. National Cyber Security Strategies in Latin America: Opportunities for Convergence of Interests and Consensus Building, – 2018.

– To examine the cybersecurity challenges of the digital age through the lens of classical and contemporary International Relations theories;

– To investigate the nature of non-kinetic warfare, its driving forces, and its impact on regional security dynamics;

– To analyse the formation of national cybersecurity policy, the concept of digital sovereignty, and international cooperation mechanisms in their interrelation;

– To examine the social engineering phenomenon in its theoretical and practical dimensions, and to map the psychological and behavioural parameters of cybersecurity;

– To argue, drawing on cyber perception theory, for the strategic importance of cognitive resilience in building national digital immunity;

– To assess the state's regulatory role and legal-political responsibility in the application of AI technologies to digital surveillance and cybersecurity;

– To analyse the political and ethical dilemmas generated by AI and autonomous systems, and the fundamental transformations they are producing in the international security environment.

Research Methods. The theoretical foundations of the dissertation draw on the conceptual approaches of scholars who have shaped contemporary models and terminology in international relations, including J.Roozenbeek and S.Van der Linden, R.Jervis, J.S.Nye, L.Kello, K.N.Waltz, H.Morgenthau, B. Buzan, K.Jørgensen, R.Keohane, H.Özdemir, I.Danilin, S.Shekhawat, N.Choucri, F.Kramer, A.Krishnan, J.Snyder, P.Singer, M.Libicki, and V.Güntay.

The methodological base combines materialist dialectics and a systemic approach with the research frameworks developed in Section 1.2. Beyond general methods, the study employs political risk analysis to assess the impact of threats on stability, scenario planning to project digital transformation trends, and case study methodology to examine specific cyber incidents (Table 1).

Table 1

Analytical schema of the main paradigms of international relations and theoretical approaches to cybersecurity

Three Main Paradigms of International Relations	Political Thought Structures	Primary Level of Analysis	Explanatory Elements
Realism	Human groups	Inter-state level	Balance of military power
Rationalism	Rational actors	Individual level	Negotiations, interests
Revolutionism	Critical approach to the capitalist system	Global system level	Structural power and economic dependencies

Source: Compiled by the author on the basis of comparative analyses conducted in Chapter I.

Primary Sources. The normative-legal foundation of the research comprises the Budapest Convention, NATO's Cyber Defence Commitment, the EU's NIS2 Directive and Digital Decade Strategy, and Azerbaijan's Cybersecurity Strategy for 2023–2027 and AI Strategy for 2025–2028. The empirical-analytical base draws on the Global Cybersecurity Index (2025), the National Cyber Power Index (2022), Microsoft's Digital Defence Report (2025), the Tallinn Manual 2.0, and UN reports on responsible state behaviour in cyberspace.

Propositions Submitted for Defence.

New paradigm of sovereignty and international relations

1. The classical model of state sovereignty has undergone transformation from geographic space to the digital domain, giving rise to a 'Digital Westphalian' paradigm in which state boundaries are functionally redefined not merely by geographic coordinates but by algorithmic control and data jurisdiction.

2. The continuity and integrity of the state are secured not only through territorial sovereignty but through critical data maintained in

foreign jurisdictions (cloud units and data embassies), imparting an extraterritorial dimension to the principle of sovereign indivisibility in international law.

3. This dissertation extends the classical DIME model to incorporate epistemic resilience, the capacity to defend shared informational reality against disinformation and synthetic manipulation, as a distinct component of national power. Azerbaijan's hybrid owner-regulator state model is advanced as a corresponding paradigm of digital sovereignty.

Geopolitical dynamics and regional security

1. The classification of regional cyber threats is organised around the profiles of Russia's total digital warfare model and Iran's permanent asymmetric sabotage model, providing the primary analytical framework for assessing the social stability implications of hybrid threats.

2. Azerbaijan's geopolitical position is shaped by cyber transit sovereignty. The Digital Silk Road project confers upon the country normative power status in regional cybersecurity standard-setting, along with attendant strategic advantages.

3. The resilience of the national digital ecosystem under conditions of global internet fragmentation is secured through a hybrid localisation governance model that balances national sovereignty imperatives with international digital circulation.

Cognitive resilience and socio-political stability

1. Cyber awareness has been elevated to the level of cognitive immunity, the first line of national security defence, serving as a strategic filter against manipulation targeting both state institutions and society at large.

2. Social engineering operations target the state's decision-making mechanism at precisely the Orientation stage of the OODA loop, transforming the cyber attribution problem from a technical obstacle into a cognitive one that steers the state towards erroneous geopolitical decisions.

3. Cybersecurity is a strategic resource for preserving state legitimacy and maintaining the social trust index in citizen–state relations.

Artificial Intelligence and the future of governance

1. AI risks divide into a spectrum of rights-based individual harm and systemic-structural harm. Because existing regulatory mechanisms demonstrate institutional inadequacy against systemic threats, liability must be calibrated to the relationship between the scale of harm and the capacity of available regulatory instruments.

2. The integration of AI into governance confers analytical superiority on the executive, thereby shifting the balance of power among branches. Azerbaijan's top-down governance model is assessed as a strategic equilibrium between the imperatives of operational defence and democratic oversight.

Strategic measurement and proactive defence

1. The state's strategic resilience is framed through a multidisciplinary Digital Sovereignty Index (DSI) model grounded in infrastructure, legal framework, innovation, and human capital.

2. National cyber defence is transitioning from a reactive posture to a proactive Cyber Prophylaxis paradigm built on technical vaccination (neutralising threats before system entry) and strategic deterrence through the imposition of economic and political costs on adversaries.

Original Contributions to Knowledge. The dissertation makes original contributions in the following directions: theoretical-conceptual (Digital Westphalian paradigm, algorithmic sovereignty), methodological-analytical (the DSI model; regional threat and AI dual-liability matrices), strategic-doctrinal (AI-driven monocratic executive balance; the cyber prophylaxis model), cognitive-social (cognitive immunity doctrine; defence of the OODA loop Orientation stage), and practical-applied (Azerbaijan's cyber transit capacities; the hybrid state model).

On the conceptual and theoretical framework of cybersecurity:

1. The transition from the classical Westphalian system to the Digital Westphalian model has been conceptualised, and the algorithmic and portable paradigms of state sovereignty have been advanced for the first time. It is argued that the boundaries of the modern state are determined not by geographic coordinates alone, but through algorithmic control and data jurisdiction.

2. The concepts of algorithmic and portable sovereignty have been integrated for the first time into Azerbaijan's national security doctrine within the framework of L. Kello's cyber theories, grounding the argument that the functional existence of the state is secured through both territorial integrity and critical data held in foreign jurisdictions. A conceptual approach to the indivisibility of sovereignty in the context of cloud units is thereby introduced into the international legal literature.

3. The capacity for epistemic resilience, defending shared informational reality in the cognitive domain, has been identified as a component of national power in the digital transformation of the DIME model. Azerbaijan's hybrid state model, synthesising owner and regulator roles, has been empirically classified for the first time.

4. A Hybrid Localisation governance model, striking a strategic balance between national sovereignty imperatives and international data circulation, has been established as a national security priority.

5. The adverse effects of global internet fragmentation on innovation capacity and national sovereignty have been systematised within a unified analytical framework through the factors of protectionism, technical incompatibility, and normative divergence.

On geopolitics, regional dynamics, and state policy:

1. The cyber activity motivations of actors in the regional security complex have been systematised, and a projection matrix for hybrid threats has been constructed using the profiles of Russia's total digital warfare model and Iran's permanent asymmetric sabotage model, underpinning the capacity to anticipate doctrinally derived regional threats within Azerbaijan's cyber defence architecture.

2. Azerbaijan's geopolitical position has been examined for the first time through the paradigm of cyber transit sovereignty, and legal and security oversight mechanisms for data flows transiting Azerbaijani territory have been grounded through a synthesis of classical transit law with data jurisdiction. It is demonstrated that the Digital Silk Road project confers upon Azerbaijan normative power status in regional cyber standard-setting and elevates digital connectivity to a fundamental component of national power.

3. A multidisciplinary DSI model, comprising infrastructure, law, innovation, and human capital, has been developed to measure states' digital resilience and minimise technological dependence. A methodology for measuring state digital power through the synergy of quantitative infrastructure indicators and cyber resilience operational metrics is proposed, and digital sovereignty is for the first time empirically situated at the intersection of individual self-determination and state regulatory capacity.

4. Regional digital infrastructure projects have been reframed for the first time as transitions from the economic to the strategic-political plane, demonstrating that they function as cyberdiplomacy instruments securing strategic autonomy and as primary metrics of the DSI. A Strategic Defence Matrix incorporating specific technological and legal preventive mechanisms alongside the regional threat classification has been developed and its integration into the national security system grounded.

On socio-cognitive aspects and cognitive resilience:

1. Drawing on the conceptual models of R.Jervis, J.Roozenbeek, and S.Van der Linden, the cyber awareness process has been grounded as the cognitive defence line of national security, and a strategic filter mechanism blocking manipulation against asymmetric threats, termed the Cognitive Strategic Defence Doctrine, has been developed.

2. It has been shown that False Flag operations executed with social engineering tools target the state's strategic decision-making at precisely the Orientation stage. A cognitive attribution methodology has been proposed for the first time to address the technical attribution problem, and cyber attacks have been reframed as hybrid instruments generating strategic misperception and constraining foreign policy choices rather than mere technical sabotage.

3. Cybersecurity has been identified as a fundamental strategic element for preserving state legitimacy and the social trust index in citizen – state relations.

On Artificial Intelligence, governance, and future challenges:

1. It has been demonstrated that the integration of AI into decision-making confers information asymmetry and analytical

superiority on the executive, thereby altering the separation of powers. Azerbaijan's top-down AI Strategy governance model has been conceptualised as a rational equilibrium between Santaniello's monocratic executive theory and the imperatives of operational defence against asymmetric threats.

2. Through differential analysis of AI risks, an AI Dual Liability Matrix and an effectiveness threshold of regulation model have been advanced for the first time. Regulation is shown to be effective at the individual level but limited at the systemic-structural level, and the liability paradigm is shifted from subjective culpability to the proportionality of harm to regulatory instruments.

3. A Cyber Prophylaxis Model transitioning national digital infrastructure from a reactive to a proactive paradigm has been advanced. Synthesising M.Smeets's operational costs theory with technical vaccination, it demonstrates the economic inefficiency of attack for the adversary and grounds cyber defence as a form of strategic intelligence.

Theoretical and Practical Significance. The theoretical contribution of the dissertation lies in advancing conceptual frameworks that synthesise classical political theory with digital realities. The transformation of state sovereignty from geographic to technological space is articulated through the Digital Westphalian paradigm, the Algorithmic Control framework, and the concept of Portable Sovereignty. Extending the DIME model to incorporate the incorporation of epistemic resilience, the capacity to defend shared informational reality against disinformation, deepfakes, and synthetic manipulation, enriches national security theory. The DSI and the AI Dual Liability Matrix represent methodological innovations. The analysis of the Orientation stage of the OODA loop contributes to cognitive security theory by transposing the attribution problem onto the cognitive plane.

The practical significance of the research lies in the instruments it offers for national security strategy and public administration. The Regional Threat Matrix, built on the Russian and Iranian models, enables anticipatory identification of the origins and objectives of cyber incidents. Mechanisms for consolidating

Azerbaijan's cyber transit sovereignty and normative power status within the Digital Silk Road framework are set out. The Hybrid Localisation and Cyber Prophylaxis models optimise defence expenditure and operational effectiveness. Applied recommendations are provided for managing the analytical superiority and monocratic executive risks arising from AI integration into governance. In the context of social stability, the cognitive immunity doctrine constitutes a strategic guide for building societal resistance to disinformation and social engineering attacks.

Approbation and Implementation. The principal findings and original contributions of the dissertation have been presented in peer-reviewed articles and conference papers at international and national venues.

Name of the Organization Where the Dissertation was Performed. The work was performed at the Department of International Relations of the Academy of Public Administration under the President of the Republic of Azerbaijan.

The Total Volume of the Dissertation in Characters, with Separate Indication of the Volume of its Structural Sections. The dissertation consists of an introduction, 4 chapters, 11 paragraphs, 7 sub-paragraphs, a conclusion, a list of used literature and abbreviations. The research work includes 28 tables. The introduction consists of 12 pages – 21570 characters, Chapter I consists of 44 pages – 78426 characters, Chapter II consists of 40 pages – 70966 characters, Chapter III consists of 32 pages – 54982 characters, Chapter IV consists of 34 pages – 64075 characters, and the conclusion consists of 6 pages – 10225 characters. The total volume of the dissertation, excluding the list of used literature, is 300244 characters.

MAIN CONTENT OF THE RESEARCH

The **Introduction** establishes the conceptual foundations and scholarly-methodological apparatus of the research. It sets out the background and significance of the topic, reviews the state of the field, delimits the object and subject of research, formulates the aims

and objectives in direct correspondence with the original contributions, structures the theoretical-methodological framework and applied methodology, and discusses the theoretical and practical significance of the findings.

Chapter I, "Conceptual, Theoretical, and Methodological Foundations of the Research", consists of four sections. *Section 1.1, "Analysis of Cybersecurity in Political Context: Conceptual Framework and Methodological Foundations",* traces the process by which the concept of cyberspace has evolved from a technical domain into a central element of global politics and state sovereignty. It is argued that cyber power in contemporary international relations manifests as a dialectical synthesis of the hard and soft power forms in Nye and Keohane's classic typology, and that this synthesis shapes the concept of a comprehensive cyber strategy serving national security interests. The section also analyses legal-diplomatic governance attempts within the frameworks of the UN, NATO, and the Budapest Convention, the inclusive OEWG discussions, and the asymmetric political-strategic dimensions of the digital hegemony competition among great powers.

Section 1.2, "Methodological Principles of the Political Analysis of Cybersecurity and Leading Research Frameworks", structures the multidisciplinary methodological architecture applied to qualitative and quantitative analysis of cybersecurity risks and state strategies. Political risk analysis and strategic assessment methodology are employed to gauge states' institutional preparedness and domestic stability; a five-point risk scale is constructed on the basis of the ITU Global Cybersecurity Index and the Belfer Centre power index. A comparative case study of the national security doctrines of the USA, China, Russia, the EU, and Azerbaijan is conducted, and the empirical-theoretical base is strengthened through optimistic, realistic, and pessimistic scenario modelling (Table 2).

Table 2

Azerbaijan's current standing and dynamics in major international cybersecurity indices

International Index	Current Score / Level	Country Dynamics
ITU GCI 2024	93.76 points (Tier 2)	+4.45 points increase (compared to 2020)

Source: Compiled by the author on the basis of comparative analyses conducted in Chapter I.

Section 1.3, "Cybersecurity Challenges of the Digital Age: Analysis in the Context of Major International Relations Theories", examines at the macro level the phenomenon of digital age security as a product of the exponential growth of information technologies, through the prism of the fundamental paradigms of IR theory. It is shown that the digitalisation wave has transcended classical geographical and military spheres, shifting power projection from physical to virtual platforms and fundamentally altering the pace of interstate interaction. The theoretical case is made for applying different scholarly approaches, namely realism, liberalism, constructivism, role theory, and cyber alliance theory, in hybrid and multidisciplinary combination to account fully for the challenges of the contemporary cyber environment.

Subsection 1.3.1, "Cybersecurity in the Context of Realism and Neo-realism: Balance of Power and National Interests", examines the cybersecurity ecosystem through the principles of anarchy, sovereignty, balance of power, and national interest maximisation. It is shown that, from a neo-realist perspective, the absence of a supreme global regulatory authority leads states to treat cyberspace as a fifth battle domain and deterrence arena, prompting the adoption of cyber sovereignty strategies and hybrid warfare doctrine to minimise technological dependence. The analysis also establishes that the multi-actor structure of cyberspace, the attribution problem, and its asymmetric character mean that the classic state-centric realist power model is partially inadequate in this domain, necessitating complementary frameworks that account for individual rational actors.

Subsection 1.3.2, "Cybersecurity from the Perspective of Liberalism and Neo-liberal Institutionalism: Global Governance and International Cooperation", examines the global security architecture of cyberspace through the propositions of liberalism and neo-liberal institutionalism: mutual dependence, collective security, international organisations, and legal regulation mechanisms. It is argued that the transboundary and asymmetric nature of digital threats pushes states towards multilateral cooperation platforms such as the Budapest Convention and NATO's Cooperative Cyber Defence Centre of Excellence rather than unilateral policies. The section also shows that intense geopolitical competition, information asymmetry, and civil-private sector synergy in the internet ecosystem limit the effective regulatory capacity of international legal institutions, generating institutional crises in the liberal cooperation model.

Subsection 1.3.3, "Constructivism: Identity and the Social Construction of Cyber Threats", analyses the cybersecurity ecosystem through constructivism and the Copenhagen School's securitisation concept, demonstrating that cyber threats are not merely objective technical realities but social constructions produced by strategic discourse, identity, and intersubjective perception. Discursive analysis shows how political actors legitimise emergency governance decisions, data nationalism, and stringent regulatory mechanisms by framing cyber challenges as existential threats. It is argued that the strategic roles states adopt in the international system directly condition their cybersecurity policies and normative behaviour.

Section 1.4, "Micro-Cyber Alliances and New Theoretical-Political Approaches to Cybersecurity", presents the concept of micro-cyber alliances suited to contemporary geopolitical realities and draws the chapter's conclusions. Compared with the bureaucratic latency of traditional military alliances, micro-cyber alliances offer real-time intelligence exchange, functional synergy with private sector actors, and flexible ad hoc cooperation against specific threats. The theory advances existing scholarly thinking that treats cybersecurity as the central pillar of state sovereignty and national security in the digital era.

Chapter II, "Political Dimensions of Cybersecurity: Geopolitics, Conflicts, and State Policy", encompasses three sections. *Section 2.1, "Non-Kinetic Warfare: Digital Dimensions of Geopolitical Competition",* analyses the transformation of modern warfare from physical to digital and cognitive spheres through the lens of non-kinetic warfare. The hybrid threat network formed at the intersection of electronic warfare, information warfare, and cyberwarfare is examined, and it is shown that management of the electromagnetic spectrum and asymmetric cyber operations have become the leading military-strategic instrument of contemporary geopolitical competition (Tables 3, 4).

Table 3

Comparative matrix of non-kinetic domains

Domain	Battlespace	Primary Impact Mechanism	Strategic Objective
Cyber	Digital networks	Malware (APT)	System collapse
Information	Psychological / social	Disinformation and propaganda	Management of public opinion
Electronic	Electromagnetic spectrum	Signal jamming	Technical isolation
Command & Control (C2)	Strategic hierarchy	Interference and manipulation	Paralysis of decision-making

Table 4

Intersecting domains of non-kinetic warfare

Domain	Key Characteristics	Example Actors	Example Operations
Cyber warfare	Digital attacks on networks and infrastructure	States, APTs, hacktivists	Ransomware, attacks on power grids
Information warfare	Manipulation of information and public opinion	States, troll farms, bots	Disinformation, propaganda

Table 4 continuation

Electronic warfare	Disruption of the electromagnetic spectrum	Military, intelligence services	Signal jamming, EMP attacks
Command & Control warfare	Targeting of decision-making systems	States	Breaching C2 systems

Source: Tables compiled by the author on the basis of comparative analyses conducted in Chapter II.

The section also evaluates from a legal-ethical perspective the destructive effects of digital technologies directed at states' sovereign rights, critical infrastructure, and societal resilience, and demonstrates the strategic necessity of closing existing legislative gaps to enable international legal accountability for acts of digital aggression.

Section 2.2, "Geopolitical Driving Forces of Cyberwarfare and Regional Dynamics", analyses the shift in state power measurement from physical territory to the capacity to manage digital networks and data flows, that is, algorithmic sovereignty. It examines how the strategic asymmetry, anonymity, and frictionlessness afforded by cyberspace are driving the transition from conventional power application to non-kinetic warfare and Grey Zone operations. Russia's New Generation Warfare doctrine and the operational mechanics of Advanced Persistent Threats, including Living off the Land, Golden SAML, and cyber-physical sabotage, are mapped in detail.

Regional conflict patterns are classified through distinct models: the Asia-Pacific model centred on US–China competition, code warfare, techno-nationalism, and network fragmentation, including the semiconductor hegemony contest and strategic pre-positioning exemplified by Volt Typhoon; the Middle East model characterised by targeting of energy infrastructure and SCADA systems (Stuxnet, Shamoon); and the Eastern European model of synchronised cyber strikes and kinetic operations in the Ukrainian context. The Russian total cyber-physical warfare model is contrasted with the asymmetric Iranian permanent sabotage-via-

proxies model, and their differences in strategic objectives, technical execution, and target domains are presented in matrix form.

For Azerbaijan, situated at the intersection of regional threat vectors and possessing a complex geopolitical architecture and critical energy infrastructure, the dissertation argues that the transition from reactive defence to a proactive Cyber Prophylaxis Model, informed by the theories of L.Kello and M.Smeets, is a strategic imperative. This model encompasses the hybrid defence of strategic junctions (TANAP, the Port of Baku), the creation of portable sovereignty through Sovereign Cloud and Digital Embassy infrastructure, the deployment of AI-based attribution analytics and deepfake detectors, and the achievement of regional cyber transit sovereignty through the Digital Silk Road project (Table 5).

Section 2.3, "National Cybersecurity Policy: Digital Sovereignty and International Cooperation Frameworks", argues, following Lewis, that cyberdiplomacy has become central to modern foreign policy, and that a state's digital sovereignty is directly proportional to the depth of its participation in international coalitions. Regional cooperation platforms afford medium-power states strategic autonomy through control mechanisms over digital transit corridors. This underpins the geo-economic and geopolitical significance of the Digital Hub and Trans-Caspian Fiber-Optic Cable projects initiated by Azerbaijan, positioning the country as a central regional actor that shapes the regional digital security architecture, secures the Digital Silk Road, and preserves its strategic autonomy.

Table 5

Strategic Defence Matrix for Azerbaijan

Threat Domain	**Model**	**Prophylactic Measure**	**Strategic Objective**
Energy and logistics	Russia (cyber-kinetic)	Redundant offline systems	Nullify the impact of sabotage
State data	East Asia (APT)	Sovereign cloud infrastructure	Protect digital sovereignty

Table 5 continuation

Social stability	Iran / Russia (disinformation)	AI-based deepfake detectors	Protect national unity
Financial sector	Iran (sabotage)	Cross-border cyber insurance plan	Mitigate economic shock

Source: Compiled on the basis of research conducted in Chapter II and the Cyber Prophylaxis Model developed by the author.

According to Lewis in his 3rd paragraph entitled *"National Cybersecurity Policy: Digital Sovereignty and Frameworks for International Cooperation",* cyber diplomacy has become the center of modern foreign policy, and a state's digital sovereignty is directly proportional to its level of participation and influence in international coalitions. Regional cooperation platforms provide middle-power states with the opportunity to gain strategic autonomy through mechanisms of control over digital transit corridors. This conceptual approach scientifically justifies the geo-economic and geopolitical weight of the "Digital Hub" and Trans-Caspian Fiber-Optic Cable projects, initiated by the Republic of Azerbaijan. Thus, Azerbaijan is characterized as a central regional actor that shapes the regional digital security architecture, ensures the security of the digital Silk Road, and protects its strategic autonomy.

The comparative governance models analysed in the section confirms that digital sovereignty is the central pillar of a state's geopolitical survival strategy, and that the relationship between national cybersecurity policy and digital sovereignty is a rapidly evolving symbiosis. While cybersecurity measures are essential for protecting domestic digital infrastructure, they simultaneously create normative barriers against global internet openness and cross-border data flows. Resolving this dialectical tension requires adaptive governance frameworks that balance national autonomy with collective security needs. States must move beyond reactive defence, embrace the whole-of-nation doctrine, and strengthen cyberdiplomacy at the international level. In contemporary geopolitical conditions,

ensuring digital sovereignty has become a strategy for defending national independence, not merely a technical imperative.

The chapter's findings also identify the following priority directions for future policy:

1. Development of unified, standardised DSI metrics for measuring states' digital resilience;

2. Proactive adaptation of AI and 5G/6G technologies to national cyber defence systems without prejudice to network openness and global integration;

3. Updating of international multilateral conventions to close cross-border legal gaps and regulate transnational data flows within the principles of national sovereignty.

The chapter concludes that, while digital sovereignty secures domestic independence, its consequences for global internet fragmentation and the erosion of digital commons are also real. Yet however sophisticated the technological and legal architecture, the effectiveness of any cybersecurity system ultimately depends on the human factor. This methodological observation motivates the next chapter's examination of the human dimension of digital sovereignty: the social engineering threats that can circumvent technical defences, analysed at both the individual and institutional levels.

Chapter III, "Social and Human-Centred Aspects of Cybersecurity", consists of two sections and two subsections. *Section 3.1, "Analysis of Social Engineering: Behavioural and Psychological Dimensions of Cybersecurity",* examines in an interdisciplinary framework the human factor, widely regarded as the most vulnerable element in the cybersecurity ecosystem, and the social engineering mechanisms designed to exploit it. Statistical evidence confirms that 75–95% of successful cyber attacks worldwide originate not from technological vulnerabilities but from the exploitation of human psychology through phishing, pretexting, and deepfake techniques. The section argues that social engineering has evolved from an instrument of individual cybercrime into an asymmetric military-strategic weapon capable of destabilising adversary states, paralysing decision-making mechanisms, and directly threatening state legitimacy.

Subsection 3.1.1, "The Human Factor in Digital Policy: A Strategic Analysis of Social Engineering in the Context of Political Legitimacy and International Security", analyses the strategic role of social engineering in political legitimacy, hybrid warfare, and international security, set against the transformation of cybersecurity from a technocentric to a human-centred paradigm. Karl Popper's warning about utopian social engineering and Robert Jervis's concept of perceptual errors in international politics are projected onto the digital domain; it is argued that cyber actors target the cognitive vulnerabilities and belief systems of diplomatic decision-makers rather than technical infrastructure, thereby generating the risk of unjustified escalation through strategic blindness and erroneous attribution. Drawing on evidence from disinformation operations in the Russia–Ukraine conflict, the HamsaUpdate and MuddyWater cases, and the industrialisation of threats through AI and deepfake technologies, it is shown that protecting national digital sovereignty requires not only technological barriers but also confidence-building measures, the establishment of diplomatic cyber norms, and the strengthening of cognitive resilience as a human firewall at the state – society level.

Subsection 3.1.2, "Artificial Intelligence and Digital Manipulation: Social Engineering in Electoral Processes and the Crisis of Political Legitimacy", examines the transformation of social engineering from individual targeting to mass behavioural manipulation through AI and Big Data, and the legitimacy crises this creates in electoral processes. Machine learning algorithms and micro-targeting are shown to yield candidates a strategic efficiency advantage of around 10–12%, while simultaneously polarising societies through information bubbles and undermining democratic institutions. A comparative analysis of the USA (Cambridge Analytica), France (Macron Leaks), Brazil, Germany, and India traces the trajectories of global digital governance models (Table 6), and Jervis's perceptual error hypotheses are synthesised for the first time with AI's electoral manipulation capabilities, establishing that states face the risk of subjective strategic blindness.

Table 6

Application dynamics of digital technologies in electoral manipulation and their impact on state governance

Election Case / Country	Technology & Model Applied	Statistical Indicator / Effectiveness	Political-Strategic Outcome and Legitimacy Crisis
2012 USA (B. Obama)	Audience analytics and digital behavioural modelling	10–12% efficiency gain in the election campaign	Strategic victory secured by precise targeting of undecided voters
2016 USA (D. Trump)	Big Data analytics, Cambridge Analytica, OCEAN psychometric profiling	Unethical processing of over 50 million individual Facebook profiles	Personalised manipulation targeting voters' fears; alteration of democratic election outcomes
2017 France (E. Macron)	NLP algorithms and real-time social monitoring	Simultaneous semantic analysis of millions of digital opinions	Proactive defence against populist disinformation; defeat of the Macron Leaks cyber operation
2018 Brazil (J.Bolsonaro)	Encrypted messenger (WhatsApp) bots and algorithmic mass broadcasting	Hundreds of thousands of automated digital messages	Creation of information bubbles beyond fact-checking mechanisms; mass opinion manipulation
2021 Germany (Bundestag)	EU normative legal regulation filters	GDPR standards	Establishment of a fundamental legal barrier against political social engineering; protection of digital privacy

Table 6 continuation

2024 India (Parliament)	Generative AI and cloned deepfake tools	Over 80% of political campaigns AI-supported	Erasure of boundaries between reality and fabrication; global emergence of the need for technological filtration systems
Azerbaijan (Digital Model)	G-Cloud (Government Cloud), unified voter registry, centralised Big Data architecture	100% digital registry integration of election infrastructure	Synthesis of technocentric server protection with human-centred cognitive defence; strategic autonomy and construction of a national immune system

Source: Compiled by the author on the basis of comparative analyses conducted in Chapter III.

Section 3.2, "Strategic Analysis of Cognitive Resilience in Cybersecurity: From Perception Theory to the National Digital Immunity System", analyses the transition of the cybersecurity paradigm from narrow technocentric network protection to a human-centred cognitive resilience model, and the mechanisms for constructing a national digital immunity system in light of Robert Jervis's misperception theory. Jervis's automatic perception traps and subjective signal interpretation errors are synthesised for the first time with Roozenbeek and Van der Linden's psychological inoculation methodology, with mathematical modelling demonstrating that simulation-based training reduces individual targeting risk from 32.4% to 5%. It is shown that institutionalising a non-punitive reporting culture within the Budapest Convention's 24/7 contact network and the NIST incident response framework shortens the concealment period for cyber incidents (on average 194 days) and reduces economic losses ($4.5–4.9 million). Drawing on the SCCSS December 2025 statistics, which show blocked malicious

accesses on mail.gov.az rising to 40.8% and 10.1% of cyber attack indicators detected through user reports, it is established that Azerbaijan's Cyber Hygiene, Cyber Summer Schools, and Digital Volunteers projects are building herd immunity and cultivating a proactive human sensor network, together forming the basis of a unified Cognitive Defence Doctrine that constitutes an integral component of national security against asymmetric attacks.

Table 7 systematises in a single hierarchy all the theoretical concepts, legal-practical instruments, and national strategic targets advanced in the section, including the goal of raising IOC indicators to 20% by 2026 to achieve collective herd immunity (Table 7).

Table 7

Azerbaijan's cyber defence indicators (2025)

Defence Level	2025 (December)	Dynamics and Commentary
AzStateNet (Network)	19,168,168 blocks	High effectiveness of perimeter defence
Email (mail.gov.az)	40.8% (2.2 million+ blocks)	Sixfold increase in phishing attacks
Sandbox (analysis)	4,191 malicious documents	Detection of complex trojans
User (IOC request)	10.1%	Success of the Cyber Hygiene project

Source: Compiled by the author on the basis of comparative analyses conducted in Chapter III.

Table 7 systematizes all theoretical concepts, legal and practical instruments and national strategic goals of Azerbaijan (including the goal of bringing IOC indicators to 20%) put forward in a single hierarchy. Analysis of the table shows that anthropological factors have come to the fore in cyber defense. The increase in blockings to 40.8% in the mail.gov.az system indicates that attacks are aimed at human perception, and the fact that IOC appeals account

for 10.1% proves the practical effectiveness of the "psychological vaccination" concept of J. Roozenbeek and S. van der Linden, when personnel, moving from the status of a "weak link", perform the function of a proactive "cognitive firewall". The strategic goal is to ensure collective "herd immunity" by bringing this indicator to 20% by 2026.

Chapter IV, "Artificial Intelligence and Future Challenges in Cybersecurity", consists of two sections and two subsections, and addresses the transformative impact of AI on political power. *Section 4.1, "Governance of Artificial Intelligence in Cybersecurity and Digital Surveillance: The Role of the State and the Liability Dilemma",* investigates the fundamental political questions and regulatory crises generated by the integration of AI into state governance and cyber defence. The process by which legislative, judicial, and media oversight falls behind algorithmic operational speed, producing what the dissertation terms analytical paralysis, is examined. Drawing critically on Santaniello's theory, it is argued that AI concentrates power in the executive in both authoritarian and democratic systems, creating a monocratic executive risk. To address these structural risks, an original dual liability matrix is proposed, constructed along the axes of regulatory effectiveness and scale of harm. The matrix demonstrates that existing international legal frameworks (GDPR, NIS2, the Budapest Convention) are institutionally inadequate against systemic cyber threats located in the high-harm / low-regulation zone, such as deepfake electoral manipulation and attacks on critical infrastructure, and that the diffusion of liability deepens regulatory asymmetry.

Section 4.2, "Political-Ethical Dimensions of AI and Cybersecurity: Autonomous Systems and the Transformation of International Security", analyses the political-ethical paradigms emerging at the intersection of AI and cybersecurity, and the global transformations driven by autonomous military platforms. It is shown that AI technologies are fundamentally altering traditional military-political deterrence and redefining digital sovereignty borders in the virtual sphere. The author argues that the future of digital sovereignty depends not on algorithmic speed but on transparency, ethical

standards, and the preservation of meaningful human oversight in military-political decision-making.

Subsection 4.2.1, "Ethical Paradigms and Conceptual Limitations of AI in the Security Architecture", examines the ethical and technological limitations on the transparent integration of AI into national security systems. The acute decision-making risks generated by the black box problem, encompassing algorithmic bias and opacity of internal computational logic, are mapped. The dual-use paradox, whereby the same technology serves equally for defence and attack, is examined, and it is demonstrated that this paradox accelerates the cyber arms race into a form that is faster and more difficult to regulate under international law than the classical arms race.

Subsection 4.2.2, "Artificial Intelligence in Cyberwarfare: Autonomous Systems, Geopolitical Threats, and Human Rights", examines the existential challenges posed by Autonomous Cyber Weapons to international relations, arguing that human-out-of-the-loop systems break the legal liability chain and enable aggressors to evade political accountability. AI's machine speed is shown to anticipate diplomatic crisis management and generate uncontrolled escalation, while algorithmic systems' inability to satisfy discrimination and proportionality principles undermines International Humanitarian Law. The acceleration of combat tempo beyond human cognitive oversight, the automated detection of zero-day vulnerabilities, and the attribution crisis together render cyber deterrence strategies ineffective and increase global digital inequality. In the regional context, it is argued that false flag operations pose existential risks for medium and small powers like Azerbaijan, grounding the case for Baku's active engagement in international cyber norm-creation. It is concluded that, in the contemporary cyber race environment in which classical geographical buffer zones have lost their significance in the South Caucasus, Azerbaijan's strategic advantage rests not only on conventional military capacity but on sovereign algorithms, autonomous protection of local databases, and absolute cyber resilience.

The **Conclusion** synthesises the research findings and principal conclusions. The conceptual foundations of a modern national security architecture grounded in cloud technologies, algorithmic borders, and cyber transit sovereignty are established. A Cognitive Defence Doctrine is developed through the synthesis of Jervis's perceptual error theory and cognitive inoculation models. The role of AI in electoral manipulation and the resulting legitimacy crises are examined through global case studies, and the effectiveness of the cognitive immunity paradigm in protecting Azerbaijani citizens from manipulation is grounded. The ethical-legal dimensions of AI integration into military and governance systems are addressed, and a strategic recommendation package is advanced for Azerbaijan's ascent to Tier 1 status in global indices, including harmonisation of legislation with NIS2 and GDPR standards, the creation of an AI Ombudsman, an algorithmic transparency registry, a sovereign cloud, and a regional CERT within the APT framework.

The main propositions and original contributions of the dissertation are reflected in the following publications by the candidate:

1. Jabbarova, K.F. Modern aspects of cybersecurity in the world in the context of global threats // – Russia, Tolyatti. Azimuth of Scientific Research: Economics and Management. – 2017. Vol. 6, No. 2 (19). – pp. 323–326.
2. Jabbarova, K.F. The importance of improving cybersecurity organisation mechanisms under modern conditions // – Russia, Bulletin of the Kyrgyz-Russian Slavic University. Political Science. – 2017. Vol. 17, No. 6. – pp. 164–167.
3. Jabbarova, K.F. Current issues in the study and application of international experience in cybersecurity // Counter-Terrorism. Problems of the 21st Century. – 2017. No. 2, – pp. 39–43.
4. Jabbarova, K.F. Key directions and elements of state cybersecurity policy under modern conditions // – Baku: Geostrategiya. – 2017. No. 02(38), – pp. 74–76.
5. Jabbarova, K.F. The importance of cybersecurity under the transformation of national security mechanisms. X

International Conference ‘Exchange of Research Results within International Rapprochement of Scientists’. – Canada, Montreal, – 7 February, – 2017. – pp. 84–89.
6. Jabbarova, K.F. Problems and solutions of cybersecurity in conditions of growing cybercrime // – Baku: Geostrategiya. – 2018. No. 01(43), – pp. 70–72.
7. Jabbarova, K. The Important Aspects of Strengthening the Material and Technical Base of the Cybersecurity System // Theoretical & Applied Science. – USA, Philadelphia. – 2018. Vol. 58. – pp. 154–159.
8. Jabbarova, K. AI and Cybersecurity – New Threats and Opportunities // Pakistan Journal of Life and Social Sciences. – 2024. Vol. 22, No. 2. – pp. 9966–9975.
9. Jabbarova, K. Securing the Future: Integrating AI Safety into Cybersecurity Frameworks // Edelweiss Applied Science and Technology. – 2025. Vol. 9, No. 8. – pp. 1452–1463.
10. Jabbarova, K.F. Analysis of cybersecurity in the context of Realism and Neo-realism theories // Sivilizasiya. Baku Eurasia University. – 2025. No. 2, Vol. 14. – pp. 58–65.
11. Jabbarova, K.F. Cybersecurity and AI governance in digital administration: the role of the state and the liability dilemma // Republican Conference ‘National Priorities of Sustainable Development’. – Baku Eurasia University, – 04 December, – 2025, – pp.123-132.
12. Jabbarova, K. Non-kinetic warfare: digital dimensions of geopolitical competition // 6th Karabakh International Scientific Research Conference. – Shusha, – 23–24 April, – 2026.

The defense will be held on 29 June 2026 at 11.00 the meeting of the Dissertation Council FD 2.30 of Supreme Attestation Commission under the President of the Republic of Azerbaijan operating at Academy of Public Administration under the President of the Republic of Azerbaijan.

Address: AZ 1001, Baku, Lermontov Street, 74.

Dissertation is accessible at the library of the Academy of Public Administration under the President of the Republic of Azerbaijan.

Electronic version of the abstract is available on the official website of Academy of Public Administration under the President of the Republic of Azerbaijan (https://dia.edu.az/).

Abstract was sent to the necessary addresses on 26 May 2026.

Signed for print: 24.04.2026

Paper format: A5

Volume: 44918 characters

Number of hard copies: 20