GEOSTRATEGY OF DIGITAL THREATS

UDC: [004.056:005.21]:[32.019.5+327.8]
DOI: https://doi.org/10.53486/tids2025.28

SERGEY BAZHENOV
Science Horizons Foundation, Russia
sbazhenov@mail.ru
ORCID ID: 0000-0001-7593-0526

ELENA BAZHENOVA
Southern Federal University, Russia
eubazhenova@sfedu.ru
ORCID ID: 0000-0001-8253-5073

DMITRY ABROSIMOV
Southern Federal University, Russia
dabrosimov@sfedu.ru
ORCID ID: 0000-0002-5278-6581

Abstract. This article examines the transformation of digital threats into instruments of geostrategy, positioning cyberspace as a critical "*fifth domain*" of global power competition. Through a systematic analysis of the evolution, actors, tactics, and impacts of state-sponsored and non-state cyber operations, the study reveals how digital threats have shifted from technical disruptions to core elements of national security strategy. Key findings indicate: (1) *Geopolitical drivers*, including inter- state rivalry, technological dependency, and asymmetric advantages, fuel the weaponization of cyberspace; (2) *State and non-state actors* (e.g., cyber powers like the U.S., China, Russia; proxy groups; criminal syndicates) exploit tactics such as APTs, critical infrastructure sabotage, disinformation, and ransomware to achieve strategic goals; (3) *Systemic consequences* include the erosion of strategic stability, blurring of war/peace thresholds ("*gray zone*" conflicts), vulnerabilities in critical infrastructure, and challenges to international law and norms; (4) Regulatory fragmentation persists, with voluntary norms (UN GGE) lacking enforcement, while states prioritize national resilience, offensive cyber capabilities, and coalitional deterrence. The study concludes that digital threats now constitute a central destabilizing factor in international relations, demanding urgent multilateral cooperation to establish binding rules, foster trust, and invest in next-generation security technologies (AI, post-quantum cryptography). Without a paradigm shift toward collaborative governance, persistent cyber competition risks systemic global instability.

Keywords: geostrategy, digital threats, cybersecurity, international security, hybrid conflicts, cyber resilience, deterrence, cyberspace governance.

JEL Classification: F52, O33, H56, K24

INTRODUCTION

The modern geopolitical space is undergoing radical transformation under the influence of digitalization. Cyberspace, having evolved from a technical environment into a strategic domain, has become an arena for interstate rivalry, a tool of hybrid conflicts, and a source of existential challenges to national security. The intensification of cyberattacks on critical infrastructure (energy, transport, healthcare), large-scale disinformation campaigns, state espionage, and the activities of transnational cybercriminal groups underscore the need for a comprehensive analysis of digital threats in the

context of global geostrategy. The absence of universally accepted international regulatory norms and the problem of attribution exacerbate escalation risks, making the study of their geopolitical dimension imperative for the theory and practice of international security.

The goal of this study is to identify the essence of the driving forces and strategic consequences of digital threats as a factor in contemporary geopolitics.

To achieve this goal, the following tasks are proposed:

- Define the conceptual apparatus ("*geostrategy of digital threats*", "*cybergeopolitics*").
- Analyze the evolution of digital threats from technical incidents to an instrument of state policy.
- Classify key actors (states, non-state structures) and their strategic motives.
- Investigate tactical and technical instruments for implementing geostrategies in cyberspace.
- Assess the impact of digital threats on the stability of the international system and national security.
- Analyze challenges for legal regulation and existing response strategies.

MAIN CONTENT

The evolution of digital threats in a geostrategic context. The phenomenon of digital threats has undergone a qualitative transformation: from initially sporadic acts of technical vandalism and criminal activity, they have evolved into one of the key instruments of state policy and geostrategic rivalry *(Rozhkov, 2023).* Understanding this evolution is necessary for comprehending their contemporary role in the global security system.

From technical incidents to an instrument of state policy. The origins of digital threats lie in the 1970s-1980s, when they were predominantly technical-criminal or ideological-protest in nature ("hacktivism"). The first viruses (e.g., Brain, 1986) and network worms (Morris Worm, 1988) demonstrated infrastructure vulnerabilities but lacked systematic political or strategic subtext. The 1990s saw a sharp increase in *cybercrime*, motivated by economic gain, highlighting the vulnerability of the emerging digital space to abuse. A turning point was the beginning of the 21st century, when nation-states realized the strategic potential of cyberspace:

1. *State cyber espionage.* Cyberspace became a primary field for collecting intelligence data (political, military, economic, scientific-technical). Operations such as *Titan Rain* (target – US government structures, mid-2000s) or *Aurora* (target – US corporations, 2009) demonstrated the scale and sophistication of state digital information collection programs, often attributed to China. The goal was not merely disrupting systems but long-term, covert extraction of strategically important data.
2. *Cyber operations as an instrument of power politics.* The 2007 incident in Estonia (massive DDoS attacks on government and financial institutions, linked to Russia) became one of the first examples of using digital attacks to exert *political pressure* on a sovereign state. This marked a shift toward perceiving cyberattacks as tools of *coercion and destabilization* in international relations.
3. *Sabotage of critical infrastructure.* The attack on Iranian nuclear facilities using the *Stuxnet* worm (discovered in 2010, attributed to a joint US-Israel development) became an unprecedented example of *cyber-physical impact* leading to physical destruction of industrial equipment. This proved the fundamental possibility of using cyberspace to inflict *strategic damage*

comparable to the effect of traditional weapons but with lower risk of direct confrontation and greater attribution complexity.

4. *Integration into hybrid wars.* The armed conflict in eastern Ukraine (since 2014) vividly demonstrated the model of *hybrid warfare*, where cyberattacks (on energy systems, media, government institutions – e.g., the attack on the power grid in 2015 and 2016) became an integral component alongside information campaigns, actions of irregular forces, and political pressure. Cyberspace transformed into one of the theaters of military operations.
5. *Weapons of Mass Disruption (WMD).* The 2017 *NotPetya* ransomware attack (initially targeting Ukraine but causing global collapse), attributed to Russia, went beyond military or political goals, inflicting multibillion-dollar damage to businesses worldwide. This highlighted the *transnational nature and cascading effects* of modern digital threats, their ability to paralyze global supply chains and economies.

Main driving factors of the geostrategization of digital threats. The transformation of digital threats into a geostrategic instrument is driven by a complex of interrelated factors *(Khorunov, 2025):*

1. *Intensification of geopolitical competition.* The return of "*great power rivalry*" logic (especially between the US, China, and Russia) created an environment where the pursuit of advantage and deterrence of adversaries extended to cyberspace. Digital operations became an element of *strategic deterrence, demonstration of force, and weakening of competitors* without direct military confrontation.
2. *Technological revolution and its strategic significance.* The development of key technologies sharply raised the stakes:
   - *Proliferation of the Internet of Things (IoT):* Multiple new vulnerable entry points into critical infrastructure (smart grids, industrial control systems – ICS/SCADA).
   - *Adoption of 5G:* Increased speed and reduced latency create new opportunities but also new attack vectors; the struggle for dominance in 5G standards (Huawei vs. the West) itself became a geostrategic issue.
   - *Artificial Intelligence (AI) and Machine Learning (ML):* Automation of attacks (rapid vulnerability discovery, creation of adaptive malware), enhanced capabilities for big data analysis for espionage and disinformation. The race for AI leadership is directly linked to the future military-strategic balance *(Masloboev and Tsygichko, 2025).*
   - *Quantum computing (prospectively):* Threat to break modern crypto algorithms, undermining the foundations of digital security and trust.
3. *Critical dependency of societies and economies on digital infrastructure.* Pervasive digitalization of government administration, financial systems, healthcare, transport, and energy made them *high-priority targets.* A successful attack on such infrastructure can cause damage comparable to a traditional military strike, paralyzing the functioning of an entire state.
4. *Pursuit of asymmetric advantages.* Cyberspace provides a relatively inexpensive and highly effective way for states less powerful in traditional military terms (DPRK, Iran) or non-state actors to challenge stronger opponents. *Low entry barriers* (compared to creating nuclear weapons or modern armies) and *high profitability* of attacks contribute to their proliferation.
5. *Reduced risk of direct escalation and complexity of attribution.* Relative anonymity of actions in cyberspace and technical difficulties in unambiguously identifying the source of an attack *(attribution problem)* allow states to conduct aggressive operations while remaining below the

threshold that could provoke a traditional military response. This creates an attractive *"gray zone"* for achieving strategic goals.

6. *Information-psychological dimension.* Digital platforms (social media) have become powerful tools for waging *information wars,* spreading disinformation, manipulating public opinion, interfering in elections, and destabilizing societies from within. This allows influencing political processes in other countries, undermining trust in institutions, and creating social tension as an integral part of geostrategic pressure.

Key actors and their geostrategic motives. The landscape of digital threats is characterized by a multiplicity and heterogeneity of actors, whose goals, capabilities, and strategies differ significantly *(Bazhenova, 2024).* Understanding their motivation and role in the geostrategic context is necessary for adequate risk assessment and developing effective responses. This section offers a classification of key actors based on their nature, capabilities, and predominant strategic motives.

Nation-States: Main drivers of geostrategy in cyberspace. States remain the most resource-intensive and influential actors, whose actions in cyberspace are directly linked to their global or regional strategic ambitions. They can be conditionally differentiated by capability level and priorities:

1. "Cyber Powers" (Tier-1 Cyber Powers):
   - *USA.* Possesses the most developed offensive and defensive cyber capabilities (US Cyber Command). *Motives:* Maintaining global technological and military leadership; protecting critical infrastructure and national security; deterring adversaries (concept of "Defend Forward"); economic espionage (officially denied in favor of defense/intelligence); promoting a liberal world order and norms in cyberspace. *Key document:* National Cyber Strategy (emphasizes active defense and deterrence).
   - *China.* Demonstrates rapid growth in cyber power, closely integrated with the civilian technology sector and military modernization (PLA Strategic Support Force). *Motives:* Ensuring national security and stability of the ruling regime; industrial-scale

   economic espionage to accelerate technological development ("military-civil fusion"); strengthening regional dominance; control over the information space ("*cyber sovereignty*"); preparation for potential future conflicts (including Taiwan scenario). *Key document:* National Security Strategy (emphasis on "network power").
   - *Russia.* Actively uses cyber operations as an element of "non-linear" and hybrid warfare, often through proxy groups. *Motives:* Strengthening regional influence and sphere of interest (post-Soviet space); destabilizing and undermining trust within Western societies and institutions; exerting political pressure on opponents; collecting intelligence; protecting the state from internal and external threats. *Key document:* Military Doctrine of the Russian Federation (cyberspace as a domain of military operations).
   - *European Union.* Focuses on cyber defense, resilience, and developing a regulatory framework. *Motives:* Protecting the single digital market and critical infrastructure; promoting a rules-based order in cyberspace; reducing dependence on non-European technologies; coordinating responses to cross-border threats (through ENISA and solidarity mechanisms). *Key document:* EU Cybersecurity Strategy.
2. *Others (Israel, United Kingdom).* Possess high offensive capabilities. *Israel's Motives:* Survival in a complex region, preemptive deterrence of threats (especially from Iran),

technological leadership. *UK's Motives:* Maintaining global influence, protecting interests within Five Eyes, countering state threats (NCSC, Offensive Cyber). "Active Players" (Tier-2/3 Cyber Powers):

- *Iran:* Significantly increased cyber capabilities, often as a tool of asymmetric response to sanctions and isolation. *Motives:* Regional deterrence (against Saudi Arabia, Israel, USA); destabilizing opponents; ideological struggle; intelligence gathering; financing (cybercrime as a source of income for proxy groups). Known for attacks on the financial sector and infrastructure (Shamoon).
- *DPRK (North Korea):* Uses cyber operations as a vital source of financing due to harsh sanctions and to demonstrate strength. *Motives:* Financing nuclear and missile programs (large-scale bank theft campaigns, cryptocurrency attacks); collecting strategic intelligence; demonstrating technological capabilities and deterrence (attacks on media, infrastructure of South Korea). Groups (Lazarus) are highly aggressive.
- *Others (India, Pakistan, Vietnam, Turkey, etc.):* Building capabilities, often in the context of regional confrontations. *Motives:* Counterintelligence, protection from neighbors, economic espionage, prestige.

Non-State Actors: Eroding the state monopoly on force. These actors operate with varying degrees of autonomy from states, complicating attribution and the threat landscape:

1. *Transnational Cybercriminal Groups:*
   - *Motive:* Exclusively financial gain (extortion, data theft, fraud, access sales). *Tactics:* Ransomware-as-a-Service (RaaS), phishing, vulnerability exploitation. *Examples:* Conti, REvil, LockBit. *Geostrategic Significance:* Inflict colossal economic damage globally; paralyze critical services (healthcare – attack on HSE Ireland, Colonial Pipeline); can be unwittingly or intentionally used by states as proxies or cover ("plausible deniability"). Growing professionalization and specialization (initial access brokers).
2. *Hacktivist Groups:*
   - *Motive:* Political protest, ideological struggle, social or environmental causes. *Tactics:* DDoS attacks, defacements, data leaks. *Examples:* Anonymous, Killnet. *Geostrategic Significance:* Can be used by states to destabilize opponents under the guise of "civilian initiative"; amplify information noise, complicating detection of state operations; create social tension. Often their impact is more symbolic than strategic.
3. *Cyber Units of Non-State Armed Groups and Terrorist Organizations:*
   - *Motive:* Propaganda, recruitment, financing, intimidation, destabilizing target states. *Tactics:* Primitive website attacks, use of social media, phishing. *Examples:* ISIS (Islamic State), cyber units of separatist groups. *Geostrategic Significance:* Currently possess limited capabilities but represent a growing threat; their actions can provoke interstate conflicts; require international law enforcement cooperation.
4. *State Proxy Groups (State-Sponsored Advanced Persistent Threat - APT Groups):*
   - *Status:* Exist in a "gray zone" – formally non-state but closely linked to state intelligence services or military (funding, cover, tool transfer). *Motives:* Performing tasks the state wants to keep in the shadows (espionage, sabotage, disinformation), ensuring "plausible deniability". *Examples:* APT28 (Fancy Bear, Russia), APT29 (Cozy Bear, Russia), APT41 (Winnti, China - mix of espionage and crime), Lazarus Group (DPRK).

Geostrategic Significance: Key tool for states to conduct operations in the "gray zone"; complicate attribution and hinder responses; lower the threshold for using cyber force.

Private Sector: Object, subject, and capability provider. The role of the private sector is multifaceted:

- *Primary target of attacks:* Corporations own and operate most critical infrastructure and store valuable data (PII, intellectual property).
- *Key technology and service provider:* Companies develop and implement technologies shaping the threat and defense landscape (cloud, IoT, AI, security systems). States depend on their products and expertise.
- *Actor shaping threats:* Technology giants possess unprecedented data volume and influence over information flows, becoming a geopolitical factor in itself (struggle for digital sovereignty, Big Tech regulation). Cybersecurity companies (sometimes with unclear ties) develop and sell tools that can be used offensively (e.g., exploits, spyware - NSO Group).
- *Public-Private Partnership (PPP):* The need for threat intelligence sharing and coordinated responses makes state-business interaction critical but often problematic due to trust, confidentiality, and liability issues.

Tactics and instruments of the geostrategy of digital threats. The implementation of geostrategic goals in cyberspace is carried out through a diverse and constantly evolving arsenal of tactics and instruments. Their choice is determined by the actor's tasks (espionage, sabotage, destabilization, coercion), their capability level, desired degree of stealth, and calculation of consequences *(Matyashova, 2023).* This section systematizes key methods used by state and non-state actors to achieve strategic effect.

Cyber Espionage: The invisible war for information. Essence: Targeted, covert collection of confidential information of a political, military, economic, scientific-technical, and diplomatic nature.

- *Tools and methods:*
  - *Advanced Persistent Threats (APT):* Long-term (months, years), targeted, and sophisticated operations, often conducted by state or proxy groups. Use zero-day vulnerability chains, targeted spear phishing, complex remote access malware (RATs).
  - *Supply Chain Compromise:* Compromising legitimate products during development or distribution to implant backdoors (example: *SolarWinds Orion (2020),* attributed to Russia, affected US government structures and corporations).
  - *Credential Theft:* Using phishing, exploits, leaked password databases to gain access to protected systems.
  - *Passive Traffic Interception:* Monitoring unencrypted or weakly encrypted communications.
- *Geostrategic Goal:* Gaining long-term competitive advantage (military plans, technologies, negotiation positions), monitoring adversary intentions, assessing vulnerabilities. The most common form of state activity in cyberspace.

Sabotage and Destruction (Cyber Sabotage/Destruction): Inflicting material damage and disruption. Essence: Physical damage or disabling of critical infrastructure, destruction of data, disruption of key systems.

- *Tools and methods:*

- *Cyber-Physical Attacks:* Targeted impact on industrial control systems (ICS/SCADA), leading to physical consequences. Example: *Stuxnet (2010)* – destruction of centrifuges in Iran.
- *Wiper Attacks:* Malware that irreversibly erases data and damages boot systems (example: *NotPetya (2017),* attributed to Russia, caused billion-dollar damage globally; *Shamoon,* attributed to Iran).
- *Denial-of-Service (DDoS) Attacks:* Overloading target systems with requests, causing unavailability (often temporary but can cause severe damage, especially to financial or media resources). Scaled using botnets.
- *Data Manipulation:* Subtly altering information (e.g., in energy grid management systems, financial reports) to covertly undermine trust or cause wrong decisions.

- *Geostrategic Goal:* Inflicting direct damage on the adversary (economic, military), demonstrating power and capabilities, deterrence, destabilizing a state or region, escalating conflict below the threshold of open military confrontation.

Destabilization and Undermining Trust: Information-Psychological Operations (IPOs). Essence: Using digital platforms to manipulate public opinion, spread disinformation (fake news), propaganda, incite social discord, and undermine trust in institutions.

- *Tools and methods:*
  - *Targeted Social Media Campaigns:* Creating fake accounts and communities ("bot farms," "trolls"), mass boosting, using micro-targeting to spread narratives. *Example:* Election interference (USA-2016, other countries).
  - *Hack-and-Leak:* Compromising and selectively publishing confidential information to discredit political figures, parties, or organizations (example: *Operation "DCLeaks," DNC Hack,* attributed to Russia).
  - *Disinformation via Fake Media and Deepfakes:* Creating and disseminating false content mimicking authoritative sources or real people.
  - *Attacks on Independent Media and Platforms:* DDoS attacks, hacks to suppress critical voices.
- *Geostrategic Goal:* Weakening political opponents from within, polarizing society, undermining the legitimacy of elections and democratic processes, creating a favorable environment for external influence, diverting attention from other operations.

Cyber Extortion (Ransomware) as a tool of coercion and financing. Essence: Encrypting data or threatening its publication to demand ransom.

- *Tools and methods:*
  - *Targeted Attacks on Critical Infrastructure:* Hospital networks (HSE Ireland, 2021), pipelines (Colonial Pipeline, 2021), municipalities, large corporations. Use sophisticated penetration methods (exploits, buying access).
  - *Ransomware-as-a-Service (RaaS) Model:* Cybercriminal groups provide platforms and malware to "*renters*" for a share of the ransom, drastically increasing the scale of the threat.
  - *Double and Triple Extortion:* Besides encrypting data, threatening its publication (double) and launching DDoS attacks against the victim (triple).

- *Geostrategic Goal (for states/proxies):*
  - *Financing:* For states under sanctions (DPRK) or proxy groups.
  - *Destabilization and Coercion:* Targeting critical infrastructure of an adversary to cause chaos and exert political pressure (often under the cover of criminal activity for "plausible deniability").
  - *Inflicting Economic Damage.*

Supply Chain Attacks: The domino effect. Essence: Compromising legitimate software, hardware, or update services during early stages of development or distribution, allowing the attacker to access all users of the compromised product.

- *Tools and methods:* Introducing vulnerabilities or backdoors into source code, compromising update servers, replacing legitimate libraries.
- *Examples: SolarWinds Orion (2020), attack on Kaseya VSA (2021, REvil), CCleaner compromise (2017).*
- *Geostrategic Goal:* Achieving widespread impact with relatively low effort; penetrating well-protected networks through trusted suppliers; inflicting mass damage on the adversary's economy and infrastructure; demonstrating penetration capabilities into global networks.

Exploitation of Zero-Day Vulnerabilities and Managed Hacking Services. Essence:

- *Zero-Day:* Using a previously unknown vulnerability in software/hardware for which there is no patch. Extremely valuable and expensive tool.
- *Managed Services:* Hiring specialized cyber contractors (commercial companies, hacker collectives) by a state or group to conduct specific operations.
- *Geostrategic Goal:* Ensuring maximum stealth and effectiveness for high-value operations (espionage, sabotage); accessing maximally protected targets; outsourcing operations to reduce risks and ensure denial.

Regulation challenges and response strategies. The complexity, cross-border nature, and rapid evolution of digital threats used for geostrategic purposes create significant difficulties for developing and implementing effective regulatory mechanisms. Response strategies of states and the international community are constantly evolving, trying to adapt to the dynamic threat but facing fundamental political, legal, and technical obstacles *(Romashkina, 2020).* This section analyzes key regulatory challenges and the spectrum of emerging responses at national and international levels.

Challenges of International Law and Diplomacy

1. *Applicability of Existing Law:*
   - *Use of Force and Self-Defense (UN Charter, Art. 2(4) and 51):* Ongoing debates about when a cyberattack reaches the threshold of "*use of force*" or "*armed attack*". States hold different positions: some (US, allies) allow Art. 51 application to large- scale destructive attacks on critical infrastructure, others (Russia, China) insist on a higher threshold, close to traditional armed attack, fearing legitimization of "*preemptive*" strikes.
   - *International Humanitarian Law (IHL):* Difficulties in applying principles of proportionality, distinction, and precaution to cyber operations during armed conflict. Defining the status of cyber combatants and civilian objects in cyberspace remains contentious.

- *State Sovereignty and Non-Intervention:* Lack of consensus on which actions in cyberspace (espionage, DDoS, disinformation) violate the sovereignty of the target state and the principle of non-interference in internal affairs. Positions range from broad interpretation (any unauthorized interference) to narrow (only actions causing significant damage or coercion).

2. *State Responsibility:*
   - *For Actions of Non-State Actors:* To what extent is a state responsible for cyberattacks originating from its territory if it "*knew or should have known*" about them but did not take measures? The principle of "*due diligence*" is recognized by many but its practical application and evidentiary base are complex.
   - *For Actions of Proxy Groups:* The problem of establishing and proving actual state control over such groups to apply norms of international legal responsibility.
3. *Formation of Norms of Responsible Behavior:*
   - *Multilateral Efforts (UN):* Work by Groups of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG) led to the recognition of 11 norms of responsible state behavior (UNGGE reports 2015, 2021; OEWG final report 2021). These include: commitment to cooperate, not to intentionally damage critical infrastructure, promote stability, respect human rights, combat cybercrime, report vulnerabilities, not use civilian infrastructure for attacks, not use ICT to interfere in internal affairs, respect supply chains, not damage emergency response infrastructures, protect key digital infrastructure objects.
   - *Problems:* Norms are *voluntary, non-binding*. There are no mechanisms for verifying compliance or enforcing implementation. *Deep disagreements* persist over their interpretation, especially regarding the use of force, sovereignty, human rights, and the state's role in internet governance. Uncertainty about whether specific operations (disinformation, espionage) violate these norms.
   - *Role of Regional Organizations:* OSCE (confidence-building measures), NATO (application of Art. 5 to cyberattacks – decisions 2014, 2016), ASEAN, OAS – develop regional norms and cooperation mechanisms, but their effectiveness is limited by geography and political will of participants.
4. *Bilateral Channels and Confidence-Building Measures:* Establishing "*red lines*" and hotlines between major powers (US-Russia, US-China) to prevent escalation and manage crises. However, their sustainability is subject to fluctuations in political relations (e.g., freezing of US- Russia dialogue after attacks).

National and Coalitional Response Strategies. In the absence of a reliable international legal regime, states focus on national and coalitional measures, combining defense, deterrence, and offensive capabilities:

1. *Strengthening Cyber Resilience:*
   - *Priority:* Protecting critical infrastructure (CI) through mandatory security standards (e.g., NIS2 Directive in EU, CISA initiatives in US).
   - *Measures:* Accelerated vulnerability identification and patching, network segmentation, backups, regular penetration testing (pentesting), preparation of incident response plans (IRP) and disaster recovery plans (DRP).

- *Public-Private Partnership (PPP):* Creating Information Sharing and Analysis Centers (ISACs), joint exercises (e.g., Cyber Europe), incentivizing business security investments.

2. *Cyber Deterrence Strategies:*
   - *Deterrence by Denial:* Increasing costs for the attacker by strengthening defenses, making a successful attack unlikely or too expensive. The main focus for most states.
   - *Deterrence by Punishment:* Threat of inflicting unacceptable damage on the attacker in response. Requires:
     - *Offensive Cyber Capabilities:* Developing capabilities for conducting retaliatory or preemptive cyber operations (e.g., USCYBERCOM, NCSC Offensive Cyber, equivalents in other countries).
     - *Employment Doctrines:* Clearly defining thresholds, targets, and rules for employing offensive cyber and non-cyber means (sanctions, counterintelligence, military) in response to cyberattacks. The US "*Defend Forward*" doctrine emphasizes proactive actions outside own networks to identify and neutralize threats before they materialize.
     - *Challenges:* Attribution problems, risk of escalation, difficulty signaling intentions without compromising secrecy, ethical and legal questions.
   - *Deterrence by Engagement:* Diplomacy, norm creation, international cooperation to reduce motives for attack and increase costs for violating them.
3. *Active Defense and Response Operations:*
   - *Within National Law:* Actions to disrupt attacker infrastructures (e.g., "cleaning" botnets), returning stolen data, deactivating malware on own networks. Often requires expanding mandates of intelligence services and military.
   - *Legal and Ethical Boundaries:* Risk of violating other states' sovereignty, collateral damage, escalation.
4. *Deterrence and Coercion Diplomacy:*
   - *Public Attribution:* Publicizing evidence of state or group involvement in attacks (e.g., joint statements by Five Eyes countries, EU) to impose political costs and stigmatization.
   - *Coalition Pressure:* Coordinated sanctions (economic, diplomatic, personal) against state sponsors, hackers, and associated structures.
   - *Criminal Prosecution:* International arrest warrants (Interpol), joint law enforcement operations (e.g., against ransomware groups).
5. *Investing in the Future:*
   - *Personnel and R&D:* Mass training of cybersecurity specialists, funding research in AI for security, post-quantum cryptography, secure architectures (Zero Trust).
   - *Global Technology Regulation:* Efforts to establish security standards for IoT, critical components (chips, software), managing risks associated with AI.

Promising Directions and Enduring Challenges

1. *Role of Artificial Intelligence:* AI revolutionizes both attack (automation, adaptability, generation of targeted phishing/deepfakes) and defense (threat analysis, anomaly detection, response automation). The race in this area will be a key factor in the future balance of power *(Masloboev and Tsygichko, 2025).*
2. *Quantum Threat:* The development of quantum computing creates an existential threat to

modern cryptographic algorithms underlying digital security. Urgent investments in post-quantum cryptography (PQC) and system migration are needed *(Arrykova, Ashirov, Guvandzhov and Churiev, 2025).*

3. *Data Governance and Digital Sovereignty:* The struggle for control over data, information flows, and technological standards will intensify, generating new regulatory conflicts (GDPR, data localization laws, Big Tech regulation).
4. *"Gray Zone" and Attribution:* Will remain the main challenges. Technologies (AI, blockchain for information storage) may partially help, but political will for transparency and cooperation remains decisive.
5. *Need for Inclusive Dialogue:* Effective regulation requires involvement not only of states but also the private sector, technical community, and civil society. Multilateral platforms (UN, IGF) must become more effective.

CONCLUSIONS

The conducted analysis allows us to conclude that digital threats have evolved from technical incidents into a key instrument of contemporary geostrategy. Cyberspace has become a full-fledged "fifth domain" of global rivalry, where states and non-state actors realize their long-term goals of security, influence, and power. *Key findings:*

1. *Threat Transformation:* The geostrategic significance of digital threats is driven by intensifying geopolitical competition, the critical dependence of societies on digital infrastructure, and the pursuit of asymmetric advantages. Tactics (APT, espionage, sabotage, disinformation, ransomware, supply chain attacks) directly serve the strategic goals of actors.
2. *Systemic Challenges:* The geostrategy of digital threats generates fundamental risks:
   - *National Level:* Blurring lines between war and peace ("gray zone"), vulnerability of critical infrastructure, crisis of deterrence models, intractable dilemma of attribution and response.
   - *International Level:* Erosion of strategic stability, militarization of cyberspace, undermining of trust, maladaptation of international law, deadlock in forming effective behavioral norms.
   - *Global Level:* Colossal economic losses, threats to supply chains, undermining social cohesion and democratic processes.
3. *Regulation Deadlocks:* Lack of consensus on applying international law and the voluntary nature of UN norms limit their effectiveness. The response shifts toward national and coalitional strategies combining:
   - Strengthening cyber resilience (resilience).
   - Deterrence through denial and punishment (deterrence), including developing offensive capabilities.
   - Pressure diplomacy (sanctions, public attribution).
   - Investments in technology (AI, post-quantum cryptography) and personnel.
4. *Permanent Cyber Competition:* Despite efforts, the world is moving along a trajectory of continuous cyber competition with high risks of escalation and destabilization. Breakthrough technologies (AI, quantum computing) simultaneously amplify both threats and defense means, exacerbating the race.

Digital threats have ceased to be a peripheral challenge, becoming a central, system-forming factor in contemporary geopolitics, defining state vulnerability, the fragility of the international system, and the contours of future conflicts. Overcoming their destabilizing impact requires not only technological solutions and forceful deterrence strategies but, first and foremost, an unprecedented level of international trust, political will to overcome geopolitical differences, and the development of specific, enforceable rules of responsible behavior in cyberspace. Without this breakthrough, the world is doomed to a permanent "gray zone" of digital confrontation with unpredictable consequences for global security and stability.

REFERENCES

1. Arrykova, G.K., Ashirov, I.G., Guvandzhov A. and Churiev, M.M., 2025. Quantum Technologies in Data Security: From Theory to Reality. *Science and Worldview, 1* (45), 283-288.
2. Bazhenova, E.Yu., 2024. *Geo-economics: textbook* / E. Yu. Bazhenova, Southern Federal University. Rostov- on-Don; Taganrog: Southern Federal University Press, 344 p.
3. Masloboev, A.V. and Tsygichko, V.N, 2025. Analysis of Trends in the Influence of Artificial Intelligence on Geopolitics and Security: New Challenges and Threats of Digital Transformation. *Reliability and Quality of Complex Systems, 1* (49), 126-135. doi: 10.21685/2307-4205-2025-1-16
4. Matyashova, D.O., 2023. The Place of Digital Threats in the Modern Concept of Human Security. *Power, 31* (3), 144-150.
5. Rozhkov, E.V., 2023. Development of Digital Technologies (Opportunities and Threats) (at the Regional Level). *Forum of Young Scientists, 4* (80), 86-100.
6. Romashkina, N., 2020. The Problem of International Information Security in the UN. *World Economy and International Relations, 12(*64). 25-32.
7. Khorunov, E.K., 2025. International Cooperation in the Field of Cybersecurity. *Bulletin of Science, 3* (1 (82)), 513-524.