The Doctrine of Information Security of the Russian Federation

Origins, methods, goals, implementation, effects, and prospective evolution

Tomasz Kamusella

University of St Andrews

A FULLY REFERENCED FACTUAL REPORT

State of evidence as of 21 August 2026

Scope and attribution standard

This report analyses the Russian Federation's formal Information Security Doctrine (2000 and 2016) and the legal, military, technological, diplomatic and information-policy architecture through which its concepts have been implemented. It distinguishes primary Russian policy from external attribution of specific operations. Consistency with the Doctrine is not treated as proof that a particular cyberattack or influence campaign was ordered under a specific doctrinal clause.

> **Core finding.** Russian "information security" is a much broader category than technical cybersecurity. It combines protection of information systems and critical infrastructure with protection of political stability, public consciousness, state narratives, cultural values and information sovereignty, while also treating information capabilities as instruments of strategic competition.

Prepared as a research dossier.

Contents

How to read the references

Bracketed numbers in the report refer to the numbered reference list. Wherever possible, claims about Russian policy use official Russian legal or strategic texts. Operational claims use government attributions, technical reporting, peer-reviewed scholarship or major research institutions. Forecasts are explicitly marked as projections rather than established fact.

Executive summary

The Doctrine of Information Security of the Russian Federation is best understood not as a narrow cybersecurity policy but as the public apex of a much wider state-security conception of the "information sphere." The 2000 Doctrine defined information security in terms that encompassed constitutional rights, information resources and infrastructure, the information industry, state policy communication, mass consciousness, spiritual and cultural values, and protection against external political, economic, military, intelligence and informational pressure. The 2016 Doctrine retained this breadth while giving greater weight to critical information infrastructure, strategic deterrence, technological dependence, foreign information-psychological influence, domestic information technologies and "information sovereignty." [1-3]

Its origins lie in several overlapping developments. Post-Soviet Russia inherited weakened state institutions and acute dependence on foreign information and communications technologies; the Russian military and political elite drew lessons from the media environment of the First Chechen War, which many officials regarded as an "information defeat"; national-security concepts adopted in 1997 and 2000 increasingly securitized information; and Moscow began an international campaign at the United Nations in 1998 to place "international information security" on the global security agenda. These strands converged in the 2000 Doctrine, approved by President Vladimir Putin on 9 September 2000. [1,4-9]

The Doctrine has four persistent strategic logics. First, it is defensive: protect state systems, communications, critical infrastructure, military command, and the confidentiality, integrity and availability of information. Second, it is sovereignist: reduce dependency on foreign technology and external network control, preserve state authority over the national information space, and strengthen domestic production. Third, it is political-cognitive: protect social and political stability, public consciousness, historical narratives and state-defined cultural or "spiritual-moral" values from perceived hostile influence. Fourth, it is competitive and external: develop capabilities for information confrontation, shape foreign audiences, protect Russian narratives abroad and promote international rules that privilege state sovereignty and state control in the information domain. [2-3,10-15]

Implementation has been cumulative rather than confined to one law. It includes data-localization rules; expanded communications-data retention and state access requirements; the 2017 Strategy for the Development of the Information Society; the 2017 critical-information-infrastructure law and GosSOPKA detection/response system; the 2019 "Sovereign Internet" law and centralized traffic-management architecture; the 2021 National Security Strategy and international information-security policy; wartime censorship and foreign-influence legislation adopted after the full-scale invasion of Ukraine; presidential decrees accelerating domestic technology and security requirements in critical infrastructure; and, most recently, the 2026 federal law establishing legal categories for "sovereign" and "national" large foundation AI models. [16-29]

The effects are mixed and should be disaggregated. Russia has built real defensive and coercive capacity: a more centralized apparatus for incident response, control of critical infrastructure, routing and filtering, data localization, surveillance and traffic management. It has also demonstrated significant offensive cyber and information capabilities, including operations attributed by Western governments to Russian military intelligence. At the same time, these capacities have not translated into reliable strategic success. In Ukraine, Russian cyber and information operations produced serious disruption but frequently fell short of pre-war expectations because Ukrainian institutions, private-sector partners and allied support adapted rapidly. [30-39]

Domestically, the same architecture has greatly increased the state's ability to censor and shape the information environment. Independent assessments document blocking, throttling, deep-packet inspection, expansion of registry-based control, pressure on platforms and users, and progressive isolation of parts of the Russian Internet. These outcomes are not accidental side effects alone: they are consistent with the Doctrine's explicit treatment of political stability, public consciousness, "reliable" information, foreign influence and information sovereignty as security objects. Yet they also create costs: centralization introduces single points of failure, regulation and localization raise compliance costs, foreign technology

dependence has not been eliminated, and extensive control can reduce openness, competition and innovation. [31-35,40-42]

Internationally, Russia has pursued an unusually persistent norm-building campaign. From its 1998 UN initiative onward, Moscow has sought recognition of state sovereignty in the information sphere, intergovernmental rather than predominantly private-sector governance, and international legal instruments addressing information and cyber threats. The 2019 decision to negotiate a UN cybercrime convention, initially opposed by many Western states, and the adoption of the UN Convention against Cybercrime in 2024 represent a partial success for the long-term Russian strategy of moving cybersecurity governance toward universal, state-centered UN processes, although the final convention is a negotiated multilateral compromise rather than a Russian instrument. [5-6,43-46]

The most consequential prospective development is the extension of information sovereignty into artificial intelligence. Federal Law No. 243-FZ of 26 July 2026, which enters into force principally on 1 September 2026, authorizes a framework for “sovereign” and “national” large foundation models, links AI policy to technological independence, state security and traditional Russian spiritual-moral values, permits the government to require certain uses of approved domestic models, and provides pathways for state data to support their development. This is not merely an AI industrial policy: it is a plausible next institutional layer of the information-security doctrine, moving from sovereign infrastructure and content governance toward sovereign model behavior. [29]

On present evidence, the most likely trajectory is therefore not complete Russian disconnection from the global Internet. It is a more selective form of controllable connectivity: domestic routing and DNS capacity, centralized filtering, domestic software and hardware mandates in critical sectors, tighter data and platform regulation, legally privileged Russian AI models, and the ability to degrade, throttle or isolate external services during political or military contingencies. This would increase state control and resilience against some external dependencies while also deepening informational closure, technological fragmentation and the risk that security policy becomes an instrument for regulating ordinary knowledge, language and public interpretation. This forecast is assessed as high confidence for continued centralization, medium-high confidence for AI-sovereignty expansion, and medium confidence for any sustained nationwide isolation of RuNet. [18-19,24,28-29,32-34]

Bottom line

The Doctrine has evolved from a 2000 statement of post-Soviet vulnerability into a mature security architecture that treats networks, infrastructure, software, media, cognition, political stability, historical interpretation and international information rules as interlocking components of state power. Its greatest systemic effect is the erosion of a boundary that many Western policies draw between cybersecurity and content: in the Russian framework, both are security domains and both may be governed through state coercive, technical, military, economic and diplomatic instruments.

1. Scope, terminology and evidentiary method

1.1 What the "Doctrine" is - and is not

The 2016 Information Security Doctrine, approved by Presidential Decree No. 646 on 5 December 2016, defines itself as a "system of official views" on securing the Russian Federation's national security in the information sphere. It is a strategic-planning document. It does not function like a criminal code, a procurement plan or an operational military order. Its legal and political significance lies in setting concepts, threat perceptions, national interests and strategic objectives that subsequent laws, decrees, sectoral strategies and agency programs can implement. [2-3]

This distinction is essential for causal analysis. The fact that a later measure - such as traffic filtering, domestic-software mandates or an intelligence cyber operation - is consistent with the Doctrine does not by itself establish that the measure was ordered because of a particular paragraph. The Russian public strategy system is cumulative: national-security strategies, military doctrines, foreign-policy concepts, information-society strategies and sectoral legislation overlap and reinforce one another. Scholars therefore typically analyse the Information Security Doctrine as one element of a broader Russian "information confrontation" and regime-security framework rather than as a single master order. [7,11,14-15]

1.2 "Information security" is broader than cybersecurity

The breadth of the Russian term is visible in the 2016 definition of the information sphere, which encompasses information itself, informatization objects, information systems and websites, communications networks, information technologies, entities involved in producing and processing information, and the mechanisms regulating the resulting social relations. The Doctrine's national interests include not only secure infrastructure and confidential information but also the circulation of reliable information, the presentation of state policy to domestic and foreign audiences, the stability of public and state institutions, and Russian sovereignty in the information space. [2-3]

The 2000 Doctrine was, if anything, still more explicit about public consciousness. It treated threats to constitutional rights and spiritual life, manipulation and disinformation, media dependence, illicit influence on individual, group and public consciousness, and hostile foreign information activities as components of information insecurity. [1]

Western shorthand	Russian doctrinal concept	Practical consequence
Cybersecurity	Information-technical security is one component of a wider information sphere.	Network defence, malware, encryption, routing and critical infrastructure are linked to political and social security.
Strategic communication / influence	Information-psychological effects can be part of "information confrontation."	Narratives, media, public opinion, protest mobilisation and psychological effects may be treated as security matters.
Internet governance	Information sovereignty and state jurisdiction are security objectives.	Network architecture, DNS, platforms, routing and data location become instruments of sovereignty.
Technology policy	Dependence on foreign ICT is a security vulnerability.	Import substitution, domestic software/hardware and state-supported platforms become security policy.
Media / cultural policy	Reliable information, historical memory and values may be framed as security objects.	Content regulation can be justified through national security rather than only ordinary media law.

1.3 Evidence categories used in this report

The report uses an evidence hierarchy because claims about Russian information policy often mix public doctrine, analytic interpretation and attribution of covert operations. Primary Russian legal and strategic sources carry the greatest weight for stated policy. Official foreign-government attributions are used for specific cyber operations but are identified as attributions, allegations or assessments where that is the legal status. Peer-reviewed and major institutional research is used to interpret strategic evolution and implementation. Rights-monitoring organizations are used for observed domestic effects, with their institutional perspective explicitly acknowledged. Forecasts are separated from factual findings.

Evidence class	What it establishes	Examples used
A - Primary Russian state source	Declared doctrine, law, decree, institution, formal objective.	2000/2016 doctrines; 2021 NSS; federal laws; presidential decrees.
B - Official foreign attribution / intergovernmental record	A government or organization's formal attribution or finding.	UK NotPetya attribution; EU KA-SAT declaration; US DOJ indictments.
C - Peer-reviewed / major research institution	Independent interpretation, comparative evidence, strategic assessment.	Carnegie; IISS; Chatham House; NATO Defense College; peer-reviewed studies.
D - Monitoring / rights organization	Documented effects on media, networks, users and civil liberties.	Human Rights Watch; Freedom House.
F - Forecast	Reasoned projection based on law, capability and trajectory; not an established fact.	RuNet scenarios; AI sovereignty; future technical centralization.

2. Origins and evolution of the Doctrine

2.1 Longer antecedents: Soviet information concepts, without assuming direct continuity

Russian information-security thinking did not begin in 2000. Soviet security and military practice had long treated propaganda, deception, “active measures,” psychological influence, counterintelligence and protection of state information as instruments of state competition. Contemporary Russian writers also draw on concepts such as reflexive control and on Soviet/Russian traditions of integrating political and military effects. The institutional and ideological discontinuities of 1991, however, make it misleading to present the 2016 Doctrine as a simple unchanged Soviet doctrine. The safer conclusion is that post-Soviet Russian information strategy reused and recombined older conceptual repertoires within a new technological and political environment. [8,10,14]

2.2 The 1990s: state weakness and the Chechen-war lesson

The immediate post-Soviet environment created a powerful security narrative of vulnerability: fragmented authority, weak state finances, privatized and competitive media, deteriorating military institutions, rapid adoption of foreign ICT and a communication space that the Kremlin did not centrally control. The First Chechen War (1994-1996) became a formative episode. Independent and foreign reporting exposed Russian military failures and civilian casualties, and Russian officials and military commentators often concluded that the state had lost the “information war” even where it retained overwhelming conventional force. Elisabeth Sieca-Kozlowski’s study of military media finds that the second Chechen campaign was accompanied by renewed media control and a restructured military communication apparatus, with measures intensifying in 2000 and culminating in the Information Security Doctrine. [8-9]

This lesson mattered because it fused two problems that liberal-democratic systems often separate: military operational security and domestic narrative control. The Russian answer was not simply better public affairs. It increasingly treated the information environment in which citizens form judgments as a strategic domain in its own right. [7-9]

2.3 National-security concepts and the 1998 UN initiative

The doctrinal process also developed through the broader national-security system. President Boris Yeltsin approved a National Security Concept in 1997; Vladimir Putin replaced it with a revised concept in January 2000, shortly before his election to the presidency. The 2000 Military Doctrine, approved in April, explicitly described state defence as requiring not only military measures but political, diplomatic, economic, social, information and legal means. These documents placed information threats within national-security planning before the dedicated Information Security Doctrine was formally adopted. [6-7]

Russia simultaneously internationalized the issue. In 1998 it introduced a draft resolution at the UN General Assembly on “developments in the field of information and telecommunications in the context of international security.” General Assembly Resolution 53/70, adopted without a vote in December 1998, invited states to inform the Secretary-General about information-security threats, concepts and possible international principles. This marks the beginning of a durable Russian diplomatic project: treating information security not merely as cybercrime or network engineering but as an interstate security problem suitable for UN rule-making. [5-6]

2.4 The 2000 Doctrine: the foundational synthesis

Approved by President Putin on 9 September 2000 as No. Pr-1895, the first Doctrine described itself as the totality of official views on the goals, objectives, principles and basic directions for ensuring information security. It was designed to guide state policy, legal and institutional development, scientific and technical programs and federal target programs. [1]

Its threat catalogue was notably expansive. It included infringements of constitutional rights in the information sphere; threats to the “spiritual revival” of Russia; inadequate state information policy; weakness and foreign dependence of the domestic information industry; hostile foreign political, economic, military and intelligence activity; disinformation about Russia abroad; manipulation of information; illicit

influence on public consciousness; and technical threats to information resources and telecommunications. [1]

The 2000 Doctrine also grouped methods into legal, organizational-technical and economic measures. This tripartite logic survives in practice: law creates state powers and obligations; technical systems make those powers enforceable; budgets, procurement and industrial policy reduce external dependency and build domestic capability. [1]

2.5 2000-2016: from recovery to sovereignty and "information confrontation"

During the following decade, Russian security thinking widened further. The 2011 Ministry of Defence "Conceptual Views" on Armed Forces activity in the information space defined information war as interstate confrontation involving effects on information systems and infrastructure and mass psychological influence designed to destabilize society or coerce decision-making. It presented information-space activity as an integrated combination of intelligence, deception, electronic warfare, communications, automated command-and-control, information work and protection of one's own systems. [10]

The political context also changed. IISS analysis identifies the 2011-2012 Russian protests and the Arab Spring as important drivers of Kremlin concern about digitally enabled mobilization; the Snowden disclosures and the 2013-2014 Euromaidan revolution reinforced fears of foreign access, surveillance and externally assisted political destabilization. After the annexation of Crimea in 2014 and the deterioration of relations with the West, information policy increasingly combined regime security with technological sovereignty and strategic competition. [31]

The 2015 National Security Strategy and 2016 Foreign Policy Concept provided the immediate strategic frame for the revised Doctrine. The Foreign Policy Concept paired defence against information threats with an explicit desire to develop effective means of influencing foreign public opinion, support Russian and Russian-language media abroad, and use modern communications technologies to present Russia's positions. [11-12]

2.6 The 2016 Doctrine: continuity plus modernization

The 2016 Doctrine formally superseded the 2000 text and recast its concepts for a networked and geopolitically confrontational environment. Its national interests included constitutional rights and safe information use; sustainable operation of critical information infrastructure and communications; development of the Russian IT and electronics industries; provision of reliable information on Russian state policy to domestic and international audiences; and participation in an international information-security system that protects Russian sovereignty. [2-3]

Several shifts stand out. "Critical information infrastructure" and strategic resilience are more developed than in 2000. Dependence on foreign information technologies and the competitive weakness of the domestic industry are treated as security vulnerabilities. Foreign information-psychological influence and the use of information technologies to undermine sovereignty, political and social stability and territorial integrity receive sustained attention. The national-defence section calls for improved information security of the Armed Forces and development of forces and means of "information confrontation." [2-3]

Dimension	2000 emphasis	2016 emphasis
Core conception	State, society, individual; content and technical threats.	Same breadth, framed through "information sphere," strategic planning and sovereignty.
Political-cognitive security	Public consciousness, spiritual revival, manipulation, media dependence.	Foreign information-psychological influence, social/political stability, extremist/terrorist use of information.
Infrastructure	Information resources, systems and telecommunications.	Critical information infrastructure, resilient communications and coordinated protection.

Dimension	2000 emphasis	2016 emphasis
Technology	Weakness/foreign dependence of domestic information industry.	Domestic IT/electronics competitiveness, technological independence and reduced foreign dependence.
Military	Information warfare threat; military information systems.	Strategic deterrence, threat forecasting, Armed Forces information security, forces/means of information confrontation.
International	International cooperation and information security.	Russian sovereignty in information space plus international legal mechanisms and strategic stability.

2.7 Post-2016 consolidation: 2021 and 2023

The 2021 National Security Strategy did not replace the Information Security Doctrine; it elevated information security to one of the state's strategic national priorities. It identifies foreign intelligence and influence, cyberattacks, distortion of historical facts, dependence on foreign technologies and outside control of communication infrastructure as threats. It defines the goal as strengthening Russian sovereignty in the information space and directs development of Russian information infrastructure, domestic technologies, Armed Forces information security and forces and means of information confrontation. [18]

A separate 2021 presidential document on state policy in international information security formalized Russia's effort to shape an international legal and institutional order in this domain, with the UN as the principal venue and the Security Council and Foreign Ministry as key coordinators. [19]

The 2023 Foreign Policy Concept, adopted after the full-scale invasion of Ukraine, embeds the same logic in foreign policy. It identifies a secure information space and protection from destructive foreign information-psychological influence as national interests; calls for strengthening Russian sovereignty in the global information space; promotes an international legal regime for information security; and directs the state to disseminate abroad what it regards as truthful information about Russian policy and history, including through Russian media, digital platforms, social networks and diaspora channels. [24]

3. Methods and goals

3.1 The formal goals

The public documents state a set of goals that are partly conventional and partly distinctive. Conventional goals include protecting citizens' information rights, confidentiality, government systems, military command, critical infrastructure, communications and economic activity. Distinctive goals include preserving information sovereignty, constraining foreign influence on public consciousness and political stability, strengthening domestic technology production, controlling dependence on foreign infrastructure and platforms, and ensuring that Russia can communicate its state policy to domestic and foreign audiences. [1-3,18-19,24]

3.2 State and regime security

The Doctrine's language formally protects the "individual, society and the state," but the architecture gives the state a decisive role in defining threats, reliability, sovereignty and destabilizing influence. Carnegie's Gavin Wilde describes this as a "no water's edge" conception: Russian strategic documents frequently treat the distinction between external adversary action and internal political vulnerability as porous. Foreign influence, protest mobilization, media narratives and cyber operations can therefore be placed on a single continuum of threats to state stability. [7]

This helps explain why measures justified as information security can regulate political speech and media activity as well as malware and infrastructure. From the Kremlin's perspective, the common object is the integrity of the state's informational environment. From a liberal rights perspective, the same fusion creates a structural risk that dissent, independent reporting and undesirable interpretation are securitized rather than treated as ordinary pluralism. [2-3,32-35]

3.3 Technological and infrastructure sovereignty

A second goal is the reduction of strategic dependence on foreign hardware, software, cloud services, communications systems and technical standards. The 2016 Doctrine warns that foreign information technologies and the weakness of domestic sectors increase vulnerability. The 2017 Information Society Strategy made domestic infrastructure, Russian ICT production, technological advantage and digital economic development explicit priorities. The 2021 National Security Strategy subsequently called for priority use of Russian technologies and for a resilient Russian segment of the Internet protected from external control. [13,18]

This is both a security and an industrial policy. It aims to preserve continuity under sanctions or conflict, keep sensitive data and control systems under Russian jurisdiction, support domestic vendors and reduce opportunities for foreign intelligence or commercial leverage. Its costs include reduced competition, compatibility constraints, substitution difficulties and the possibility of replacing dependence on Western suppliers with dependence on a narrower domestic or non-Western supplier base. [31,41]

3.4 Information-psychological defence and public consciousness

Russian doctrine expressly treats psychological influence as a security issue. The 2011 military conceptual document, the 2016 Doctrine, the 2021 National Security Strategy and the 2023 Foreign Policy Concept all refer in different forms to hostile influence on society, public opinion or the political order. The state response includes strategic communication, media regulation, counter-propaganda, patriotic and historical narratives, surveillance of extremist content and the legal restriction of information characterized as harmful, false or foreign-directed. [2-3,10,18,24]

The distinctive feature is reciprocity: the same system that seeks to protect Russian audiences from influence also seeks to shape external audiences. The 2016 Foreign Policy Concept called for effective means of influencing opinion abroad, and the 2023 concept requires dissemination of Russian positions and historical interpretations through foreign-facing media and digital networks. Russia's information-security model is therefore defensive and projective at the same time. [12,24]

3.5 Military information confrontation

The military method combines the technical and cognitive sides of information. The 2016 Doctrine directs the state to develop Armed Forces information-security capabilities and forces and means of information confrontation. The 2011 military conceptual views illustrate what this can encompass: intelligence, deception, electronic warfare, communications, command-and-control systems, information work and psychological effects. Recent scholarship describes “informatsionnoe protivoborstvo” as an institutionalized element of Russian grand strategy that integrates cyber-technical and information-psychological methods and can be used below, alongside or during conventional war. [2-3,10,14]

This should not be confused with a claim that every Russian cyber or influence operation is centrally synchronized. Russian agencies have distinct missions and organizational cultures, and public evidence often reveals overlapping or competitive operations. The doctrine provides common strategic vocabulary and priorities; it does not prove perfect whole-of-government command. [14]

3.6 Legal, organizational-technical and economic methods

The 2000 Doctrine’s tripartite method remains analytically useful. Legal methods establish jurisdiction, content rules, data obligations, licensing, liability and procurement requirements. Organizational-technical methods include incident-response centers, state security agencies, filtering equipment, routing control, network monitoring, critical-infrastructure protection and military cyber capabilities. Economic methods include state procurement, localization, subsidies, industrial policy and privileged access to state data or markets. [1,13,16-29]

Method family	Representative instruments	Intended strategic function
Legal-regulatory	Data localization; communications retention; extremist/false-information/foreign-influence laws; platform and user obligations.	Make state control and information-security duties legally enforceable.
Technical-infrastructural	GosSOPKA; TSPU/DPI; national DNS; centralized traffic management; CII security.	Detect attacks, preserve continuity, filter or reroute traffic, reduce external technical leverage.
Military/intelligence	Cyber operations, EW, deception, intelligence, information-psychological operations.	Disrupt adversaries, collect intelligence, shape decisions, support kinetic operations, deter.
Media/information	State media, public diplomacy, external digital platforms, narrative campaigns.	Shape domestic and foreign interpretation and defend state narratives.
Economic-industrial	Import substitution, domestic software/hardware mandates, AI/model support.	Reduce dependence, build sovereign capability, create domestic ecosystems.
Diplomatic-normative	UN resolutions, international information-security policy, cybercrime treaty diplomacy.	Internationalize state-sovereignty principles and constrain unilateral/foreign control.

3.7 International normative strategy

Russia’s international method is not ancillary. Since 1998 it has argued that information and communications technologies can threaten international peace and should be governed through interstate norms and legal instruments. Its preferred concepts stress sovereign equality, state jurisdiction, non-interference and a stronger governmental role in Internet and information-space governance. This agenda reflects genuine concerns about cyber conflict but also aligns with Russia’s domestic preference for state authority over privately operated transnational networks and platforms. [5-6,19,43-46]

4. Implementation: institutions, laws, infrastructure and operations

4.1 Institutional architecture

Implementation is distributed across the presidential administration and Security Council, the Federal Security Service (FSB), Ministry of Defence and military intelligence, Foreign Intelligence Service (SVR), Federal Service for Technical and Export Control (FSTEC), Federal Protective Service, Ministry of Digital Development, Roskomnadzor and its subordinate technical bodies, the Foreign Ministry, prosecutors and courts, state-owned or state-aligned media, and critical-infrastructure operators. The distribution reflects the Doctrine's breadth: no single "information-security ministry" could cover military, intelligence, telecommunications, media, industrial policy, diplomacy and law enforcement. [2-3,13,16-19,31-34]

The Security Council coordinates strategic policy. The FSB has a central role in protecting critical information infrastructure and the GosSOPKA system for detecting, preventing and mitigating computer attacks. FSTEC sets technical-protection requirements. Roskomnadzor regulates communications and media and, under the Sovereign Internet architecture, operates or oversees increasingly centralized technical traffic-control capabilities. The Ministry of Defence and intelligence agencies conduct military and covert activities; the Foreign Ministry leads international information-security diplomacy. [16,19,31-34]

4.2 Data localization and communications access

Federal Law No. 242-FZ of 21 July 2014 established localization requirements for the collection and processing of Russian citizens' personal data, requiring relevant databases to be recorded, systematized, accumulated, stored, clarified and retrieved using databases located in Russia. This reduced some cross-border data exposure while increasing state jurisdiction over data infrastructure and compliance leverage over foreign services. [15]

The 2016 "Yarovaya" legislative package expanded data-retention and assistance obligations for telecommunications and online communications providers. Its implementation required substantial storage capacity and created additional state-access pathways. These measures served counterterrorism and law-enforcement goals but also fit the information-security preference for keeping communications data technically reachable inside the Russian jurisdiction. [16,41]

4.3 The 2017 Information Society Strategy

Presidential Decree No. 203 of 9 May 2017 approved the Strategy for the Development of the Information Society for 2017-2030. It explicitly grounds itself in the National Security Strategy and the Information Security Doctrine. Its priorities include a reliable and high-quality information space, domestic information and communications infrastructure, Russian ICT, the digital economy, technological independence and the development and export of Russian technologies. It is an important bridge from security doctrine to industrial and digital-development policy. [13]

4.4 Critical information infrastructure and GosSOPKA

Federal Law No. 187-FZ of 26 July 2017 created a dedicated legal regime for the security of critical information infrastructure (CII). It covers significant information systems, networks and automated control systems in sectors essential to the economy and state. The law institutionalizes duties to categorize significant facilities, comply with security requirements and cooperate with the state system for detecting, preventing and mitigating computer attacks. [17]

GosSOPKA is designed as a unified, geographically distributed system for detecting and responding to computer attacks and incidents. This is one of the clearest examples of the Doctrine producing conventional defensive capacity. Subsequent amendments and presidential decrees have tightened requirements, particularly after 2022, when sanctions, wartime cyber activity and foreign-technology withdrawal increased concern about continuity and supply-chain risk. [17,20-21,25-27]

4.5 The Sovereign Internet architecture

Federal Law No. 90-FZ of 1 May 2019 amended communications and information legislation to create mechanisms for sustainable operation of the Russian Internet segment during threats to stability, security and integrity. The implementing architecture includes centralized traffic management, technical means for countering threats (TSPU), and a national domain-name system. Officially, these capabilities are resilience mechanisms designed to keep Russian networks operating if external connectivity fails or is disrupted. [47]

In practice, the same infrastructure also increases the state's ability to identify, throttle, reroute and block traffic at scale. Human Rights Watch's 2025 technical and legal review describes TSPU as deep-packet-inspection-capable equipment deployed across providers and managed through Roskomnadzor's subordinate structures, enabling nontransparent centralized filtering and traffic manipulation. Freedom House similarly documents increased blocking and throttling. These are external assessments, but they are consistent with the technical powers created by the law and subordinate regulation. [32-34]

4.6 Post-2021 and wartime acceleration

The 2021 National Security Strategy created a high-level mandate for stronger sovereignty in the information space. After the full-scale invasion of Ukraine in February 2022, implementation accelerated in several dimensions. Presidential Decree No. 166 of 30 March 2022 advanced technological independence and security requirements for critical information infrastructure; Decree No. 250 of 1 May 2022 imposed additional information-security measures on state bodies and strategic organizations. Later amendments continued this trajectory. [18,20-21,25-27]

Content control also expanded. Federal Law No. 32-FZ of 4 March 2022 introduced criminal liability for public dissemination, presented as reliable, of knowingly false information about the Russian Armed Forces and later related state activities. The 2022 law on persons under foreign influence consolidated and broadened the "foreign agent" regime. In 2025, new administrative rules targeted intentional searching for knowingly extremist materials and advertising of circumvention tools. These measures go beyond technical cybersecurity but sit comfortably within a doctrine that treats information-psychological influence, social stability and hostile content as security concerns. [22-23,28]

4.7 Offensive cyber and information activity: implementation by capability, not proof of clause-by-clause orders

Russian state and military-intelligence cyber capabilities demonstrate that information confrontation is operational, not merely rhetorical. Western governments have attributed or alleged multiple major operations to Russian state actors. The United Kingdom assessed that the Russian military was responsible for the 2017 NotPetya attack, which caused global damage far beyond its apparent Ukrainian targets. The European Union attributed the February 2022 KA-SAT/Viasat disruption to the Russian Federation and described it as occurring approximately one hour before the invasion of Ukraine. US prosecutors have charged GRU officers in connection with destructive malware campaigns and attacks on Ukrainian and other targets. [36-39]

These cases show capacity and strategic integration, especially when cyber activity occurs in proximity to military operations. They do not establish that public paragraphs of the Information Security Doctrine constituted the operational authorization for each attack. The correct evidentiary statement is that the operations are consistent with the broader official concept of information confrontation and with national-security priorities to develop such forces and means. [2-3,10,14,36-39]

4.8 Media, strategic communication and external influence

The Russian information-security architecture also supports a wider information ecosystem. The US State Department's 2020 Global Engagement Center report described five mutually reinforcing pillars in Russian disinformation and propaganda activity: official government communications, state-funded global messaging, proxy sources, weaponized social media and cyber-enabled disinformation. That report is a US government assessment rather than a Russian admission, but its categories correspond closely to the doctrine's concern with state information support, external audiences, public opinion and cyber-information integration. [40]

The 2016 and 2023 foreign-policy concepts supply the overt policy dimension. Both call for improved presentation of Russia's positions abroad, support for Russian media or digital channels, and use of modern information technologies. The 2023 document adds stronger emphasis on countering hostile information pressure and communicating Russian interpretations of history. [12,24]

4.9 International rule-making

Russia has implemented the international part of its doctrine through sustained UN diplomacy. The 1998 initiative led to a long-running UN process on information and telecommunications in international security. In 2019, a Russian-backed resolution established an open-ended process to negotiate a comprehensive UN convention on cybercrime, despite significant opposition. The final UN Convention against Cybercrime was adopted by General Assembly Resolution 79/243 in December 2024 and opened for signature in 2025. [5-6,43-46]

The result should be interpreted carefully. The convention is a multilateral compromise negotiated by all participating states, not a codification of Russian doctrine. Nonetheless, its existence confirms that Russia's two-decade strategy of moving important cyber questions into universal, state-centered UN treaty processes achieved a significant institutional objective. [43-46]

4.10 2026: information sovereignty reaches foundation AI models

Federal Law No. 243-FZ of 26 July 2026 represents the newest and potentially most consequential implementation frontier. The law on support for artificial-intelligence technologies creates legal categories for "sovereign" and "national" large foundation models, ties AI development to technological independence, state security and traditional Russian spiritual-moral values, and provides mechanisms for government support and access to state data. It also permits the government to determine cases in which sovereign or national models must be used. The law is enacted but, as of the date of this report, its main provisions have not yet entered into force: the principal commencement date is 1 September 2026, with some provisions later. [29]

The significance is doctrinal rather than merely commercial. Earlier policy sought sovereign networks, domestic data, domestic software and domestic platforms. Foundation models add a new layer: systems that mediate search, summarization, translation, writing and access to knowledge. If implemented broadly, "sovereign AI" can become both an industrial-security instrument and an information-governance instrument, because the state can influence which models are legally privileged, what data they access and what legal/value requirements condition their deployment. [29]

4.11 Implementation timeline at a glance

Year	Instrument / event	Doctrinal significance
1998	Russian UN draft on international information security; UNGA Res. 53/70	Begins durable international effort to treat information security as an interstate security and legal issue. [5-6]
2000	National Security Concept; Military Doctrine; first Information Security Doctrine	Institutionalizes broad information-security concept across state, military, society and technology. [1,7]
2011	MoD "Conceptual Views" for Armed Forces in information space	Operational vocabulary integrating technical and psychological dimensions. [10]
2014	Data localization law	Brings Russian citizens' data and foreign services more firmly under Russian jurisdiction. [15]
2016	Yarovaya package; revised Information Security Doctrine; Foreign Policy Concept	Expands retention/access; modernizes doctrine around CII, sovereignty and foreign influence. [2-3,12,16]

Year	Instrument / event	Doctrinal significance
2017	Information Society Strategy; CII Law No. 187-FZ	Links doctrine to industrial/digital development and critical-infrastructure defence. [13,17]
2019	Sovereign Internet Law No. 90-FZ	Creates legal basis for centralized traffic management and autonomous-resilience mechanisms. [47]
2021	National Security Strategy; international information-security policy	Elevates information sovereignty and information confrontation as strategic priorities. [18-19]
2022	Decrees 166/250; wartime false-information and foreign-influence laws	Accelerates technology security, state-sector controls and content governance during war. [20-23]
2023	Foreign Policy Concept	Integrates information sovereignty, counter-influence and external messaging in foreign policy. [24]
2024-25	CII/decree amendments; search/VPN-related administrative restrictions	Deepens domestic technology requirements and user-level content/circumvention control. [25-28]
2026	Federal Law 243-FZ on AI technologies	Extends sovereignty model toward foundation AI and state-supported “sovereign” models. [29]

5. Effects

5.1 Effect 1: greater state cyber-defence and continuity capacity

The most straightforward positive effect, from a state-security perspective, is the creation of enduring institutions for critical-infrastructure security, cyber incident detection and response, technical standards and continuity planning. The CII regime and GosSOPKA give the state legal and organizational mechanisms to identify significant systems, impose security requirements and coordinate responses. Sovereign-network capabilities can also provide redundancy if external routing or DNS services are disrupted. [17,47]

This defensive logic is not fictitious. Russia is a heavily digitized state exposed to criminal, intelligence and wartime cyber threats. The strategic problem is that defensive resilience and political control often share the same technical means. Equipment capable of rerouting traffic during an external outage can also reroute or block domestic traffic; centralized visibility that helps detect attacks can also facilitate surveillance. The Doctrine's breadth deliberately permits these functions to coexist. [2-3,32-34]

5.2 Effect 2: centralization of the Russian Internet

The cumulative laws and technical systems have shifted RuNet away from the relatively decentralized environment of the 1990s and early 2000s toward an architecture in which the state has stronger leverage over providers, routing, filtering, DNS, data storage and platforms. Human Rights Watch's 2025 review describes a sustained policy of building technical and legal capacity to isolate or centrally control Russian connectivity. Freedom House documents widespread blocking, throttling and platform restrictions. [32-34]

This does not mean that Russia has built a perfectly sealed national intranet. The Russian economy and society continue to depend on transnational infrastructure, software, services and information flows. The more accurate effect is increased "controllability": the state can impose selective degradation, blocking and routing changes with less dependence on voluntary cooperation from each individual provider. [31-34]

5.3 Effect 3: censorship, self-censorship and narrowing information pluralism

The information-security framework has facilitated the treatment of content as a security object. Since 2022, legal restrictions on war reporting, foreign influence, extremist material and circumvention tools have combined with technical filtering and economic pressure on independent media. Rights-monitoring organizations report substantial contraction of online freedom and access to independent information. The causal contribution of the Doctrine cannot be quantified, but its conceptual language - stability, foreign influence, reliable information and information-psychological threats - supplies a coherent security justification for this policy direction. [22-24,28,32-35]

A systemic effect is self-censorship. Where legal categories are broad, penalties serious and network access technically observable, users, media outlets and platforms have incentives to avoid borderline material. This effect is difficult to measure directly but is well established in research on coercive media environments. In doctrinal terms, such behavioral adaptation can be interpreted by the state as greater information stability; from a rights perspective it represents diminished pluralism. [32-35]

5.4 Effect 4: technological localization and its trade-offs

Import substitution and domestic-technology mandates have stimulated Russian software and security vendors and increased incentives to localize data and infrastructure. The approach can reduce some foreign supply-chain and sanctions vulnerabilities, especially in state and critical sectors. [13,20-21,26-27]

The trade-off is that technological sovereignty is costly. IISS has highlighted Russia's longstanding dependence on foreign ICT and the economic burden of attempting to replace globally competitive technologies. Data-retention and filtering mandates impose capital and operating costs on providers. Restrictions on foreign services can reduce competition and access to advanced tools, while centralized systems create high-value targets and potential single points of failure. [31,41]

5.5 Effect 5: substantial offensive capability, but uneven strategic returns

Russia has demonstrated the ability to conduct destructive, disruptive and intelligence cyber operations at scale. NotPetya is an especially important example because its global spillovers showed how an operation aimed at a highly interconnected target environment can impose enormous external costs. The KA-SAT incident showed the ability to combine cyber disruption with the opening phase of a conventional invasion. [36-38]

Strategic effectiveness has nevertheless been uneven. Microsoft's 2022 reporting documented extensive Russian destructive and espionage activity against Ukraine, but also the ability of Ukrainian and allied defenders to rebuild, migrate and protect systems. The UK National Cyber Security Centre concluded that Russian cyber operations had been less decisive than many expected. Chatham House similarly emphasizes Ukrainian resilience, adaptation and the limits of treating cyber or information operations as automatic strategic force multipliers. [30,35,42]

The same lesson applies to influence. Volume, reach and tactical narrative success do not necessarily produce durable political outcomes. Russian information operations can confuse, polarize or exploit existing divisions, yet their effects depend heavily on audience trust, media ecosystems, counter-messaging, local politics and the credibility costs generated by overt aggression. [14,40,42]

5.6 Effect 6: institutional fusion of domestic security and external competition

One of the deepest effects of the Doctrine is organizational and conceptual. Domestic information governance, foreign policy, military information confrontation, counterintelligence, technology policy and cyber defence are treated as parts of one strategic environment. This encourages cross-domain responses: a foreign platform can be viewed simultaneously as a commercial service, an intelligence risk, a channel for political mobilization, a foreign-policy actor and a dependency to be substituted. [2-3,7,14,18-19,24]

The advantage for the state is coherence: different agencies can justify action under a shared security logic. The risk is securitization without clear boundary. Because threats to "public consciousness" or "political stability" are inherently harder to define than malware or an outage, state discretion expands. [1-3,32-35]

5.7 Effect 7: international norm entrepreneurship and partial success

Russia's long campaign has helped ensure that international debates no longer treat cyber questions only as technical or criminal matters. UN processes now address responsible state behavior in cyberspace, and the 2024 UN Convention against Cybercrime created the first comprehensive global treaty in this field. Russia was not alone in producing these outcomes, and many states that disagree with Moscow also favor stronger international law. Yet the trajectory validates Russia's strategic decision in 1998 to use the UN as the principal venue for state-centered information-security diplomacy. [5-6,19,43-46]

The broader normative effect is a persistent contest between governance models. Russia promotes sovereign state authority, non-interference and governmental control over national information space; many Western states emphasize an open, interoperable Internet, multi-stakeholder governance and human-rights constraints on state control. The divide is not absolute, but it increasingly shapes debates on data, platforms, cybercrime, content regulation and AI. [19,24,43-46]

5.8 Effect 8: security policy becomes a framework for historical and cultural governance

The 2000 and 2016 doctrines and later strategies show that Russian information security is concerned with more than current political messaging. References to spiritual-moral values, historical falsification, patriotism and reliable information create a bridge between national security and cultural policy. The 2021 National Security Strategy treats distortion of historical facts and erosion of traditional values as part of the threat environment; the 2023 Foreign Policy Concept instructs the state to communicate Russian interpretations of history abroad. [1,18,24]

The effect is to expand the objects of state security from systems and secrets to interpretation itself. This helps explain why historical memory, language, education and cultural narratives have become increasingly securitized in Russian policy. It also raises the risk that academic or journalistic disagreement can be reclassified as hostile information influence. [18,24,32-35]

5.9 Effects during the war against Ukraine

The war has stress-tested the Doctrine. Russia used cyber intrusion, destructive malware, electronic warfare, state and proxy media, platform manipulation, legal censorship and infrastructure controls alongside conventional force. Western and Ukrainian resilience limited some effects, but the conflict demonstrated the durability of Russia's integrated information-security approach: external operations and internal information control intensified simultaneously. [30,35-40,42]

Internally, war transformed the information-security system from a long-term sovereignty project into an operational wartime control system. Laws adopted after February 2022 sharply increased the risks attached to dissenting descriptions of the war, while technical controls made blocking and throttling more scalable. Externally, Russian campaigns continued to exploit media, proxy sources, social networks and cyber-enabled information tactics. [22-24,28,32-35,40]

5.10 What cannot presently be established

Four limits are important. First, the public Doctrine does not reveal classified operational orders, budgets or target selection. Second, Russian institutions are not perfectly coordinated, so a doctrinally consistent activity may result from agency initiative rather than a centralized Kremlin plan. Third, causal measurement is difficult: economic sanctions, war, technology markets and authoritarian political development also shaped the same outcomes. Fourth, external attributions of cyber operations sometimes rely on intelligence that cannot be publicly disclosed; they should be reported as official assessments rather than treated as judicially proven facts unless courts have established them. [7,14,31,36-39]

6. Potential future effects

This section is prospective. It extrapolates from enacted law, declared strategy and demonstrated capability. It does not claim that every scenario will occur.

6.1 Selective sovereign connectivity rather than permanent total isolation

The highest-confidence forecast is continued expansion of selective control over connectivity. The Sovereign Internet architecture, national DNS, TSPU equipment and recurring legal amendments give the state tools to block, throttle, reroute or restrict external services while keeping economically essential connectivity functioning. A permanent nationwide disconnection would be economically and technically costly; selective isolation during crises is more consistent with the established pattern. [47,31-34]

Future controls may increasingly rely on allowlists, service classification, traffic fingerprinting and centralized instructions to providers rather than traditional URL blocking alone. This would make censorship harder to circumvent and could fragment the experience of the Internet by region, provider, user category or emergency status. This is a medium-high confidence projection based on existing technical direction, not a confirmed future plan. [32-34]

6.2 AI becomes an information-sovereignty layer

The 2026 AI law makes the AI trajectory unusually concrete. If the government uses its new powers broadly, state-approved foundation models could become privileged intermediaries for public administration, critical sectors, education, search, citizen services and enterprise software. Because foundation models synthesize and rank information rather than merely transmit it, this would move information sovereignty from control of networks and databases toward control of computational interpretation. [29]

Potential effects include preferential training on state-controlled or state-provided data; requirements to conform with Russian law and traditional-value policy; reduced access to foreign models in sensitive sectors; development of domestic safety and censorship layers; and the export of Russian sovereign-model infrastructure to partner states. The law enables parts of this architecture but does not determine how extensively the government will use it. Confidence: high that AI sovereignty will become a major policy domain; medium regarding the scale of compulsory model substitution outside state/critical sectors. [29]

6.3 Automated content governance and surveillance

Russia is likely to apply machine learning and generative AI to the same functions already performed by traffic inspection, registries and human monitoring: classification of prohibited material, identification of circumvention services, entity and network analysis, transcription, translation, moderation and prioritization of investigative leads. Such automation could increase the scale and speed of enforcement while also multiplying false positives and reducing transparency. This is a medium-high confidence inference from the combination of existing control systems and the state's AI investment priorities. [18,28-29,32-34]

6.4 Deeper domestic technology substitution in critical sectors

The 2022-2025 decrees and CII amendments indicate sustained pressure to replace foreign software and technical components in strategic systems. Future effects are likely to include narrower approved-vendor lists, domestic security certification, greater state procurement concentration and closer integration of industrial policy with national-security planning. [20-21,25-27]

This can improve control over supply chains and reduce exposure to sanctions or foreign vendor decisions, but it can also lock institutions into less competitive products and generate concentration risk. A sovereign stack is not automatically a secure stack: monocultures can make common vulnerabilities more consequential. [31]

6.5 Information confrontation becomes more AI-assisted and multilingual

The same foundation technologies used defensively can lower the cost of external information operations: automated translation, content generation, audience segmentation, synthetic media, rapid narrative adaptation and large-scale persona management. Russian strategy already treats information-technical and information-psychological tools as complementary. Generative AI increases the productivity of both legitimate public diplomacy and deceptive influence activity. [10,14,24,29,40]

The strategic danger is not that AI creates a wholly new doctrine. It reduces the marginal cost of methods already present in the doctrine: shaping information, exploiting social divisions, supporting military operations, concealing source provenance and extending Russian messaging into many language environments. The evidentiary distinction remains important: capacity and incentive are clear; the exact scale of future state-directed AI influence operations is uncertain. [14,24,29,40]

6.6 Export of a sovereign-information governance model

Russia is likely to continue presenting its model internationally as a defence of sovereign equality against foreign technological domination. Partnerships in the CIS, SCO, BRICS and bilateral relations can facilitate exchange of cyber norms, domestic-platform technologies, data-localization approaches, digital identity systems, filtering capabilities and sovereign-AI models. The 2023 Foreign Policy Concept explicitly supports a common information space with CIS states and wider international cooperation on Russia's preferred information-security principles. [19,24,29]

Adoption by partners will not necessarily reproduce the Russian system wholesale. States differ in capacity, regime type, market structure and relations with China, the United States and Europe. The more plausible effect is modular diffusion: individual elements - data localization, state-centered cybercrime rules, domestic cloud/AI procurement, filtering, platform registration - may travel separately. Confidence: medium. [19,24,43-46]

6.7 A more closed epistemic environment

If network controls, media restrictions, historical-policy rules and sovereign AI reinforce one another, the long-term societal effect could be an increasingly closed epistemic environment in which the state controls not only access to sources but also the AI systems used to search, summarize, translate and compare them. This would be a qualitative change. Traditional censorship removes information; model-level governance can also reorder salience, framing and explanation. [18,24,29,32-35]

Such a system could be resilient against some foreign manipulation while being more vulnerable to domestic epistemic monoculture: errors or political premises embedded in approved sources and models would have fewer independent corrective channels. This is a forecast, not a measured present effect. Confidence: medium-high if sovereign models become widely mandatory; lower if users retain broad access to competing models and foreign information sources. [29,32-35]

6.8 Increased Internet fragmentation and international legal divergence

Continued Russian promotion of cyber sovereignty, combined with similar though not identical policies in other states, can contribute to a more fragmented global Internet. Fragmentation need not mean physical separation. It can result from incompatible data rules, platform obligations, content regimes, identity requirements, encryption policies, AI certification and national routing controls. [19,24,43-46]

The global effect may therefore be competing information jurisdictions rather than a binary "open Internet versus splinternet." Businesses and citizens could face different permissible platforms, models, data flows and content rules depending on national territory. Russia's doctrine is one of the clearest and most mature state-centric versions of this trend. [19,24,29]

6.9 Strategic benefits and strategic liabilities for Russia

Potential effect	Possible strategic benefit to Russia	Possible liability / counter-effect	Confidence

Potential effect	Possible strategic benefit to Russia	Possible liability / counter-effect	Confidence
More centralized RuNet control	Continuity under crisis; rapid blocking/rerouting; reduced external leverage.	Single points of failure; economic friction; circumvention arms race; reduced openness.	High
Domestic CII/software substitution	Less exposure to sanctions/vendor withdrawal; greater supply-chain jurisdiction.	Higher costs; weaker competition; domestic monoculture risk.	High
Sovereign foundation AI	Control of sensitive AI infrastructure/data; domestic industry; policy-compatible models.	Lower model quality if isolated from global ecosystem; politicized outputs; innovation constraints.	Medium-high
AI-assisted information confrontation	Lower cost, higher language coverage, faster production and targeting.	Detection/countermeasures; credibility erosion; adversary uses same technology.	Medium-high
International sovereign-cyber norms	More state authority and room for domestic regulation; coalition-building.	Normative bloc formation; weaker interoperability; rights criticism.	Medium
Tighter content control	Reduced ability of external actors to reach Russian audiences; stronger wartime narrative discipline.	Reduced pluralism, information quality and policy feedback; elite blind spots.	High

6.10 Scenarios to 2030

Scenario	Description	Indicators	Assessment
A. Managed sovereignty - central case	Russia remains globally connected but with centralized technical control, domestic CII stacks, selective blocking and expanding sovereign AI.	Continued TSPU/DNS investment; domestic model procurement; targeted foreign-service restrictions; no permanent national disconnect.	Most likely
B. Wartime enclosure	Major confrontation prompts persistent allowlisting, regional/global gateway restriction and compulsory domestic platforms/models.	Emergency decrees; mass foreign-service blocks; routing centralization; state-sector AI mandates broaden to population services.	Plausible under severe crisis
C. Technological constraint	Economic/technical limits slow substitution and enforcement; foreign/open-source dependencies remain substantial.	Procurement delays; exemptions; weak domestic hardware supply; continued high circumvention and foreign tool usage.	Plausible counter-trend
D. Selective accommodation	Security architecture remains but some restrictions ease to regain investment/technical access.	Regulatory exemptions, interoperability deals, stable foreign-service access, lower censorship intensity.	Less likely absent political change

7. Overall assessment

The Doctrine of Information Security of the Russian Federation is a durable organizing concept rather than a one-time policy document. Its origin can be traced to a post-Soviet security problem: a state that perceived itself as militarily, institutionally and technologically vulnerable in an information environment it did not control. The First Chechen War supplied a salient political-military lesson; the 1998 UN initiative supplied an international strategy; the 2000 Doctrine supplied the first comprehensive state synthesis. [1,5-9]

The 2016 revision marked maturation rather than rupture. The concept of information security retained its cognitive and political content but incorporated the realities of critical infrastructure, network dependence, strategic cyber competition and the domestic technology industry. The 2021 National Security Strategy and 2023 Foreign Policy Concept then made information sovereignty a central national-security and foreign-policy objective. [2-3,18,24]

Implementation has been unusually broad because the doctrine itself is broad. Defensive cyber institutions, data localization, CII security, network control, content law, military cyber capabilities, strategic communication, industrial policy and UN diplomacy are not identical activities; they are connected by a shared assumption that control, resilience and influence in the information sphere are dimensions of sovereignty and national power. [13-29]

The record does not support a simplistic verdict of either “success” or “failure.” Russia has substantially increased domestic state control and defensive capacity; it has demonstrated high-end offensive cyber capability and sustained foreign influence capability; and it has influenced international diplomatic agendas. It has not eliminated foreign technological dependence, created a fully autonomous high-performance digital ecosystem, or reliably converted cyber and information operations into decisive strategic outcomes. Ukraine since 2022 is the clearest demonstration of both Russian capability and its limits. [30-42]

The 2026 AI law suggests the next phase. The doctrinal project began by defining information as a security domain, moved into data and infrastructure sovereignty, and is now extending toward foundation models that interpret and generate information. If implemented at scale, this can make AI governance a direct continuation of Russian information-security policy. The question for the late 2020s is therefore not simply whether Russia can disconnect from the global Internet. It is whether Russia can construct a sufficiently complete sovereign information stack - networks, data, platforms, critical software, security tools and AI models - to remain economically usable while being politically and strategically controllable. [20-29]

Principal judgment

The Doctrine’s most consequential legacy is the institutionalization of a state-security continuum running from server and cable to citizen cognition. That continuum has given Russia a coherent framework for resilience and strategic competition, but it has also normalized the use of security instruments to govern media, historical interpretation, platforms, network access and, prospectively, AI-mediated knowledge.

Appendix A. Evolution of the doctrine, 2000-2026

Policy layer	2000	2016	2021-2023 consolidation	2026 frontier
Threat concept	Foreign political/military/intelligence/information pressure; manipulation; weak domestic industry; attacks on systems.	Foreign info-psychological influence; cyber threats; CII; foreign tech dependence; sovereignty risks.	Foreign interference, distorted history, outside infrastructure control, sanctions/technology vulnerability.	AI dependence and foundation-model sovereignty become explicit industrial/security issues.
Protected object	Individual, society, state; public consciousness; information resources; media/industry.	Information sphere, rights, CII, society/state stability, domestic technology sector.	Sovereign information space, resilient Internet, historical/cultural security, domestic technology.	Domestic/state-approved model ecosystem and training/data infrastructure.
Principal methods	Legal, organizational-technical, economic.	Strategic planning across defence, public security, economy, science/technology and diplomacy.	Centralized network control; CII hardening; import substitution; content law; international policy.	Foundation-model classification, support, data access and potential mandatory use.
External posture	International information security and response to hostile foreign activity.	International legal mechanisms; strategic stability; foreign audience communication.	UN-centered legal regime; counter foreign influence; active external messaging.	Potential export of sovereign AI and model-governance approach.
Core strategic idea	Restore state capacity in a vulnerable information environment.	Secure sovereignty across technical and cognitive information domains.	Integrate sovereignty, wartime security, technology and foreign policy.	Extend sovereignty from infrastructure/content into algorithmic mediation of information.

Appendix B. Detailed implementation timeline

Date	Measure	Area	Effect / significance
17 Dec 1997	National Security Concept (Yeltsin)	Strategic framework	Pre-2000 national-security context for information threats.
2 Nov / 4 Dec 1998	Russian UN draft; UNGA Res. 53/70	Diplomacy	Internationalizes “information security” as a security and norm-making issue. [5-6]
10 Jan 2000	Revised National Security Concept	Strategic framework	Putin-era national-security baseline.
21 Apr 2000	Military Doctrine	Military	Integrates information measures into state/military security. [7]
9 Sep 2000	First Information Security Doctrine	Doctrine	Foundational broad definition spanning systems, society, media, values and foreign pressure. [1]
2011	MoD Conceptual Views on activity in information space	Military	Defines information war and integrated technical/psychological activity. [10]
21 Jul 2014	Federal Law 242-FZ	Data sovereignty	Localization of databases processing Russian citizens’ personal data. [15]
31 Dec 2015	National Security Strategy	Strategy	Immediate basis for 2016 doctrine; stronger confrontation framing. [11]
6 Jul 2016	Federal Law 374-FZ / Yarovaya package	Surveillance/data	Expanded communications retention and assistance obligations. [16]
30 Nov 2016	Foreign Policy Concept	Foreign policy	Links information security with external communication and influence. [12]
5 Dec 2016	Information Security Doctrine, Decree 646	Doctrine	Modern framework: CII, sovereignty, domestic tech, info-psychological threats, information confrontation. [2-3]
9 May 2017	Information Society Strategy, Decree 203	Digital/industrial policy	Connects doctrine to domestic ICT, infrastructure and digital economy. [13]
26 Jul 2017	Federal Law 187-FZ on CII	Cyber defence	Creates CII security regime and GosSOPKA framework. [17]
1 May 2019	Federal Law 90-FZ (“Sovereign Internet”)	Network sovereignty	Central traffic management, resilience mechanisms, national DNS/TSPU architecture. [47]
12 Apr 2021	State policy on international information security, Decree 213	Diplomacy	Formalizes Russian international norm strategy and UN-centered approach. [19]
2 Jul 2021	National Security Strategy, Decree 400	Strategy	Elevates information security and sovereignty; calls for information-confrontation capabilities. [18]
4 Mar 2022	Federal Law 32-FZ	Content / wartime control	Criminalizes specified knowingly false information about Armed Forces/state activity. [22]
30 Mar 2022	Presidential Decree 166	CII/technology	Accelerates technological independence and CII security. [20]

Date	Measure	Area	Effect / significance
1 May 2022	Presidential Decree 250	State-sector security	Additional information-security measures for state/strategic bodies. [21]
14 Jul 2022	Federal Law 255-FZ	Foreign influence	Consolidates legal control of persons considered under foreign influence. [23]
31 Mar 2023	Foreign Policy Concept, Decree 229	Foreign policy	Strengthens information-sovereignty and counter-influence goals. [24]
13 Jun 2024	Decree 500	Security implementation	Amends 2022 information-security measures. [25]
24 Dec 2024	UNGA Res. 79/243	International law	Adopts UN Convention against Cybercrime. [45-46]
7 Apr 2025	Federal Law 58-FZ and Decree 214	CII / technology	Further strengthens transition toward Russian technology in CII. [26-27]
31 Jul 2025	Federal Law 281-FZ	Content/circumvention	Adds administrative rules concerning intentional access to extremist material and circumvention advertising. [28]
26 Jul 2026	Federal Law 243-FZ on AI technologies	AI sovereignty	Creates legal regime for sovereign/national foundation models; main force from 1 Sep 2026. [29]

Appendix C. Claim-evidence matrix

Claim	Evidence	Assessment
Russian information security covers cognitive/content as well as technical security.	2000 and 2016 doctrines; 2011 military conceptual views; 2021 NSS. [1-3,10,18]	Directly established by primary texts.
First Chechen War influenced later state/media information-security policy.	Sieca-Kozlowski; Giles; Carnegie. [7-9]	Strong scholarly support; exact causal weight not quantifiable.
Russia has pursued international information-security norms since 1998.	Russian UN draft, UNGA Res. 53/70; 2021 international policy. [5-6,19]	Directly established.
The doctrine contributed to a centralized, sovereign RuNet architecture.	2016 doctrine; 2017 strategy; 2019 law; HRW/Freedom House implementation studies. [2-3,13,47,32-34]	Strong; specific technical measures also derive from later laws.
The doctrine authorizes every Russian offensive cyber operation.	No public evidence supports clause-by-clause authorization.	Not established; report explicitly rejects this inference.
Russian military intelligence has conducted major destructive cyber operations.	UK/EU attributions; US indictments. [36-39]	Strong official attribution; legal status varies by case.
Russian cyber/information operations have achieved decisive strategic effects in Ukraine.	Microsoft, NCSC and Chatham House show major activity but significant resilience/limits. [30,35,42]	Not supported as a general claim; effects are mixed.
The Russian state can completely isolate RuNet at will without major cost.	Sovereign Internet capacity exists; IISS/HRW document dependencies and constraints. [31-34]	Overstated; selective control is much better evidenced.
Russia is extending information sovereignty into AI foundation models.	Federal Law 243-FZ, July 2026. [29]	Directly established as law; implementation effects are prospective.
Sovereign AI will necessarily produce politically uniform outputs.	No implementation evidence yet; law includes legal/value criteria and state powers. [29]	Plausible risk, not established outcome.

References

[1] Russian Federation, “Information Security Doctrine of the Russian Federation,” approved 9 September 2000, No. Pr-1895. English translation reproduced from the Russian Ministry of Foreign Affairs by Public Intelligence. Source

[2] President of the Russian Federation, Decree No. 646 of 5 December 2016, “On Approval of the Information Security Doctrine of the Russian Federation,” Official Internet Portal of Legal Information. Source

[3] Security Council of the Russian Federation, “Doctrine of Information Security of the Russian Federation” (official English translation), 2016. Source

[4] Elisabeth Sieca-Kozlowski, “From controlling military information to controlling society: the political interests involved in the transformation of the military media under Putin,” Small Wars & Insurgencies 20, no. 2 (2009): 300-318. DOI: 10.1080/09592310902975430. Source

[5] Russian Federation, revised draft resolution A/C.1/53/L.17/Rev.1, “Developments in the field of information and telecommunications in the context of international security,” United Nations, 2 November 1998. Source

[6] United Nations General Assembly, Resolution 53/70, “Developments in the field of information and telecommunications in the context of international security,” 4 December 1998. Source

[7] Gavin Wilde, “No Water’s Edge: Russia’s Information War and Regime Security,” Carnegie Endowment for International Peace, 4 January 2023. Source

[8] Keir Giles, Handbook of Russian Information Warfare, NATO Defense College Research Division, Fellowship Monograph 9, 2016. Source

[9] Sieca-Kozlowski, “From controlling military information to controlling society,” 2009 (see reference 4). Source

[10] Ministry of Defence of the Russian Federation, “Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space,” 2011; English text archived by the National Security Archive. Source

[11] President of the Russian Federation, Decree No. 683 of 31 December 2015, “On the National Security Strategy of the Russian Federation.” Source

[12] President of the Russian Federation, Decree No. 640 of 30 November 2016, “Foreign Policy Concept of the Russian Federation.” Source

[13] President of the Russian Federation, Decree No. 203 of 9 May 2017, “Strategy for the Development of the Information Society in the Russian Federation for 2017-2030.” Source

[14] Karen-Anna Eggen, “A strategy for the weak: the role of information confrontation in Russia’s grand strategy,” Defence Studies (published online 19 September 2025), DOI: 10.1080/14702436.2025.2561639. Source

[15] Federal Law No. 242-FZ of 21 July 2014, amendments concerning processing of personal data in information and telecommunications networks, Official Internet Portal of Legal Information. Source

[16] Federal Law No. 374-FZ of 6 July 2016 (part of the “Yarovaya” package), Official Internet Portal of Legal Information. Source

[17] Federal Law No. 187-FZ of 26 July 2017, “On the Security of Critical Information Infrastructure of the Russian Federation.” Source

[18] President of the Russian Federation, Decree No. 400 of 2 July 2021, “On the National Security Strategy of the Russian Federation.” Source

[19] President of the Russian Federation, Decree No. 213 of 12 April 2021, “Fundamentals of State Policy of the Russian Federation in the Field of International Information Security.” Source

[20] President of the Russian Federation, Decree No. 166 of 30 March 2022, “On Measures to Ensure Technological Independence and Security of Critical Information Infrastructure of the Russian Federation.” Source

[21] President of the Russian Federation, Decree No. 250 of 1 May 2022, “On Additional Measures to Ensure Information Security of the Russian Federation.” Source

[22] Federal Law No. 32-FZ of 4 March 2022, amendments introducing criminal liability for specified false information concerning the Armed Forces and related state activity. Source

[23] Federal Law No. 255-FZ of 14 July 2022, “On Control over the Activities of Persons under Foreign Influence.” Source

[24] President of the Russian Federation, Decree No. 229 of 31 March 2023, “Concept of the Foreign Policy of the Russian Federation.” Source

[25] President of the Russian Federation, Decree No. 500 of 13 June 2024, amending Decree No. 250 of 1 May 2022. Source

[26] Federal Law No. 58-FZ of 7 April 2025, amendments to Federal Law No. 187-FZ on Critical Information Infrastructure. Source

[27] President of the Russian Federation, Decree No. 214 of 7 April 2025, amendments to Decree No. 166 on technological independence and CII security. Source

[28] Federal Law No. 281-FZ of 31 July 2025; see also Kremlin summary of legislation concerning extremist materials and circumvention-tool advertising. Source

[29] Federal Law No. 243-FZ of 26 July 2026, "On Support for the Development of Artificial Intelligence Technologies in the Russian Federation," Rossiyskaya Gazeta, 31 July 2026. Source

[30] Microsoft, "Defending Ukraine: Early Lessons from the Cyber War," Special Report: Ukraine, 2022. Source

[31] International Institute for Strategic Studies (IISS), Cyber Capabilities and National Power: A Net Assessment, chapter on Russia, 2021. Source

[32] Human Rights Watch, "Disrupted, Throttled, and Blocked: State Censorship, Control, and Increasing Isolation of Internet Users in Russia," 30 July 2025. Source

[33] Freedom House, Freedom on the Net 2025: Russia. Source

[34] Freedom House, Freedom on the Net 2024: Russia. Source

[35] UK National Cyber Security Centre, Annual Review 2023, "Case study: Russia." Source

[36] UK Foreign & Commonwealth Office, "Foreign Office Minister condemns Russia for NotPetya attacks," 15 February 2018. Source

[37] Council of the European Union, "Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union," 10 May 2022 (KA-SAT/Viasat). Source

[38] US Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," 19 October 2020. Source

[39] US Department of Justice, "Five Russian GRU Officers and One Civilian Charged for Conspiring to Hack Ukrainian Government," 5 September 2024. Source

[40] US Department of State, Global Engagement Center, Pillars of Russia's Disinformation and Propaganda Ecosystem, 2020; preserved by the US Government Publishing Office. Source

[41] Freedom House, Freedom on the Net 2024: Russia (regulatory, cost and technical-control discussion; see reference 34). Source

[42] Keir Giles, "Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine," Chatham House, December 2023. Source

[43] United Nations General Assembly, Resolution 74/247, "Countering the use of information and communications technologies for criminal purposes," 27 December 2019. Source

[44] United Nations, documentation of the Russian-backed draft leading to Resolution 74/247 and the Ad Hoc Committee process on a cybercrime convention. Source

[45] United Nations General Assembly, Resolution 79/243, "United Nations Convention against Cybercrime," 24 December 2024. Source

[46] United Nations Treaty Collection, United Nations Convention against Cybercrime, treaty status and signature information. Source

[47] Federal Law No. 90-FZ of 1 May 2019, amendments to the Federal Laws "On Communications" and "On Information, Information Technologies and Protection of Information" (commonly known as the Sovereign Internet law). Source

Access note. Web sources were checked for this report on 21 August 2026. Russian official URLs sometimes move between the Kremlin, Government, Security Council and Official Internet Portal of Legal Information; where an official primary text and an accessible translation differ in location, the primary legal identifier (decree or federal-law number and date) is controlling.