



Kent Academic Repository

Johansmeyer, Tom and Nurse, Jason R. C. (2026) *The western technology market as Russia's emerging "field of confrontation": the vvolution of strategic thinking, 2013–2023*. Cyber Defense Review, 11 (3). pp. 1-18. ISSN 2474-2120.

Downloaded from

<https://kar.kent.ac.uk/115825/> The University of Kent's Academic Repository KAR

The version of record is available from

<https://doi.org/10.55682/cdr/ja30-77hk>

This document version

Publisher pdf

DOI for this version

Licence for this version

CC BY-NC-ND (Attribution-NonCommercial-NoDerivatives)

Additional information

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in **Title of Journal** , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our [Take Down policy](https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies) (available from <https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies>).

The Western Technology Market as Russia's Emerging "Field of Confrontation": The Evolution of Strategic Thinking, 2013–2023

Tom Johansmeyer^{*1}, Jason R.C. Nurse²

¹Irregular Warfare Initiative, Washington, D.C., USA

²University of Kent, Kent, UK

Dependence on foreign private technology has become an increasingly important consideration in national security strategy. The scale, depth, and pervasiveness of private technology in government operations challenge the ability of states to secure themselves, requiring them to consider the technology sector as an emerging category of stakeholder, with an increasingly significant—and increasingly complex—role. This study examines how Russian strategic thinking on foreign technology dependence evolved between 2013 and 2023 and how the reactions of Western technology companies following Russia's full-scale invasion of Ukraine reinforced this strategic perspective. Drawing on a qualitative analysis of Russian national security, foreign policy, and digital strategy documents, the paper traces the growing characterization of foreign technology dependence as a national security vulnerability and the increasing emphasis placed on technological sovereignty. The findings show that Russian strategic documents progressively framed reliance on Western technology as a source of geopolitical risk, concerns that became more salient following the withdrawal or curtailment of operations by numerous Western technology companies after 2022. Although Russia identified this vulnerability well in advance, its inability to address it left it strategically exposed. These findings contribute to broader discussions on cyber strategy, technological sovereignty, and the role of private technology companies in contemporary national security.

Keywords: cybersecurity, national security strategy, cyber war, economic security, Russia, technology market

* tom.johansmeyer@irregularwarfare.org

Disclaimer: The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.
© 2026 The Author(s), unless otherwise stated. This article is published under the terms of the Creative Commons CC BY-NC-ND 4.0 License (<https://creativecommons.org/licenses/by-nc-nd/4.0/>). Authors retain copyright where applicable.

1 INTRODUCTION

The interplay between the commercial sector and conflict is not new, but the ways in which this relationship is perceived have changed. The interaction between governments and commercial entities has become more challenging (Godfrey 2025), particularly in the technology sector (Gu 2024), as companies become larger and more influential—and as governments rely on their products and services to operate and interact with their citizens and other states. This evolving relationship between the state and the private technology market becomes even more complicated when a state relies on private companies in a rival or adversary state. For example, the U.S. National Cybersecurity Strategy has institutionalized the importance of cyber insurance (Johansmeyer 2024), while government reliance on key defense contractors is well established (Calcara 2024). Similar dependencies exist across many sectors, creating security vulnerabilities that are not easily remedied.

This article examines how Russian strategic thinking regarding dependence on foreign private technology evolved between 2013 and 2023 and what this evolution reveals about the strategic significance of private technology markets in contemporary national security. Specifically, it analyzes how Russian strategic documents framed dependence on foreign technology markets as an emerging national security vulnerability and how this perspective evolved before and after Russia's full-scale invasion of Ukraine in 2022. Although Russian strategy documents consistently identified dependence on foreign technology as a strategic risk, they also reveal the country's limited ability to take decisive action to reduce that dependence.

The consequences of this vulnerability became more tangible following the 2022 invasion of Ukraine, when many Western companies curtailed their operations or support for their products and services in Russia (Yale School of Management 2024). Although the disruption was neither complete nor uniform, these actions transformed a long-recognized strategic concern into an operational reality, disrupting business and government operations in Russia and making tangible a decade of documented concerns.

This article argues that the private technology market—with influence spanning adversarial countries—has become a “field of confrontation” (Douzet and Gery 2021, 108). This expression refers to a strategically contested environment in which states can impose (or experience) security-relevant costs via technology products and services provided by privately owned companies. While the private technology market does not constitute an operational domain in the traditional sense, its central role in government, economic, and societal functions has been shown to constitute a salient security vulnerability for countries relying on systems built and supported by companies headquartered in adversary states. As a result, these companies—of their own accord or under pressure from their relevant regulators and governments—can exert a direct coercive effect.

This article contributes to cyber strategy scholarship by tracing how the Russian Federation has framed the rise of the private technology sector as a growing and strategically significant field of confrontation from 2013 to 2023. It explores how Russia responded to foreign technology company reactions to the 2022 full-scale invasion of Ukraine. Russia relies on technology from a market dominated by its principal adversary (the United States), and it has recognized this problem for more than a decade. While unable to formulate a solution, Russia's reaction to the threat—both before and after the 2022 invasion—provides important insights into how states can navigate their dependence on private technology markets, particularly when they are in foreign (or even adversarial) countries.

2 LITERATURE REVIEW

The increasing reliance of governments on private technology companies has attracted growing attention in cyber strategy and international security scholarship (Mueller 2026; Kramer, Butler, and Teplinsky 2026). Rather than serving solely as commercial providers, technology companies have become strategic actors whose decisions can influence national resilience, military operations, and geopolitical competition.

For the purpose of this study, the *private technology market* refers to hardware, software, and related systems developed and sold by private companies without direction or interference from government bodies—except where governments participate as customers under normal customer relationships. Likewise, government grants or other forms of public assistance do not, by themselves, negate a company's ability to determine its own strategic direction. Throughout this article, the terms *private sector* and *private technology market* are used interchangeably.

The increase in government reliance on the private market—especially in technology (Gu 2024)—has created new forms of strategic vulnerability. This dependence has encouraged more integrated approaches to cybersecurity, including “whole of government” strategies (Committee of Public Accounts 2025; Kramer, Butler, and Teplinsky 2026; Myers 2026), greater reliance on alliances and partnerships to secure access to critical technologies (Johansmeyer, Mott, and Nurse 2024), and recognition that effective engagement with the private sector can itself become a strategic advantage (Mueller 2026).

The strategic advantages possible through collaboration with the private sector, including reliance on the technology market, involve a continuous balancing act. A complex grand negotiation is underway among major technology companies and the governments that use their services, in which the strength of the practical and operational capabilities offered by the private sector is counterbalanced by the government's ability to regulate, control, and otherwise influence the market (Grohman and Barbosa 2026). Governments have sought to exercise this influence through mechanisms such as antitrust enforcement (Hine and Floridi 2026), export controls, and even forced divestiture (Vattikonda and Kelley 2025). Yet these measures rarely produce complete control, reflecting an ongoing negotiation between state authority and private technological power.

Mutual dependence provides at least the appearance of stability, even if those involved in the perpetual negotiation of that stability might believe that the ongoing effort suggests the contrary. The ability to maintain the balance between the private sector and government becomes more complicated, though, as a government's regulatory reach thins. The ability to use legislation (e.g., forced sale) and litigation (e.g., antitrust) provides for direct levers of control by the government, and the more a company's activity is subject to a particular government's legal and regulatory environment, the more control that government has. However, when a company is headquartered in, or derives the bulk of its revenue from, another jurisdiction, those levers become less powerful. This problem is exacerbated when the market on which a government relies is most heavily regulated by its adversaries.

Recent scholarship has framed these challenges through the concepts of digital sovereignty (Grohman and Barbosa 2026; Hine and Floridi 2026; Gu 2024; Pohle and Thiel 2020) and digital decoupling (Mueller 2026). While these perspectives differ in emphasis, they share the recognition that dependence on foreign technology providers may constrain a state's strategic autonomy. Rather than viewing

technology markets solely through an economic lens, this literature highlights their growing importance as instruments of geopolitical competition and national security. The Russian case offers an opportunity to examine how these concerns emerged and evolved within a state's strategic thinking over time. The following section provides the historical context for that evolution.

2.1 Historical Context: The Evolution of Russia's Technology Dependence

Russia (and previously the Soviet Union) has a long history of struggling with its reliance on foreign technology. The Soviet Union's commitment to technology and engineering was substantial, with "tens of thousands of PhDs ... especially in the hard sciences" focused mostly on developing military solutions (McFaul 2018). Despite this investment, Soviet leaders concluded that "it is quicker and cheaper to obtain [technology] from the United States" than to develop comparable capabilities domestically (Bricker 1981, 32). Even when acquired, the Soviet Union found it difficult to integrate foreign technology into existing operations, leading them "to turn increasingly to turnkey factories, relying on foreign firms to design the plant, supervise construction, and install the equipment"—usually with Western financing (CIA 1973).

During this time, the Soviet computer industry was in particularly difficult shape, despite being given "political priority" beginning in 1968 (Gustafson 1981, 75). It was estimated to lag the United States by roughly a decade, with an even larger gap in software than in hardware. It had become clear that the "fear of relying on a potential adversary was one reason for the Soviets' strong desire to minimize dependence on the West for technology and products" (OTA/U.S. Congress 1979, 279). Yet the technological gap left few practical alternatives. Regarding computer systems, the Soviet Union was already in an uncomfortable position of relying on U.S. exports because it was so far behind, and exports to the Soviet Union from the United States and other Western states grew steadily through the 1970s (p. 234).

U.S. policy toward technology exports evolved over the same period, from pre-détente limitations through 1972 (CIA 1973) to a decade of more flexible commercial activity that was paused in 1980, when President Jimmy Carter ordered a "suspension of licensing ... pending a full review of the U.S. government's export control policy" (Gustafson 1981, 1). As the Soviet era drew to a close, U.S. "computer and computer-related exports" again increased, partly in response to the Soviet withdrawal from Afghanistan (U.S. GAO 1990). Export license applications grew accordingly.

The collapse of the Soviet Union did not eliminate Russia's dependence on foreign technology. The reliance on Western technology continued through the 1990s and into the twenty-first century, even when some of that dependence was sustained through widespread software piracy (Sherman 2024b). Until the early days of Russian president Vladimir Putin's first tenure, "Russia's burgeoning internet services and technology sector used Western software and hardware without much question" (Sherman 2024b). As McFaul (2018) observes, the fact that "[n]one of the largest tech companies in the world is Russian" underscores the country's continued dependence on foreign technology. Even in 2016, "[m]ost of the communications equipment and software in Russia is of foreign origin," while the limited domestic production that does exist remains "built almost completely on the basis of foreign components" (Lowry 2021, 67).

Although concerns about technological dependence date back to the Soviet period, Russia increasingly framed this dependence as a national security issue during the late 2000s. Fearing the “internet as a regime security threat ... the Russian government made a concerted push to replace Western hardware and especially software” (Sherman 2024b). By this time, Russia had indeed come to recognize that “[t]echnological innovation is largely taking place beyond the purview of governments,” and that “the rate of innovation is outpacing states” ability to keep abreast of the latest developments and their potential societal impacts,” (Kavanagh 2019). This marked a distinct change from the Soviet era, in which the government presided over technological advancement (although the degree to which this was successful is open to debate, as indicated in OTA/U.S. Congress (1979) and Gustafson (1981). Even in the United States, where private-sector innovation in computing was evident in the 1960s, the level of influence and penetration by the beginning of the twenty-first century was unfathomable thirty years earlier.

Given the nature of the technology sector’s capabilities relative to those of host states—particularly in western markets—mutual dependence has intensified and, indeed, been institutionalized, a development that balances competing influences (CSIS 2023). The private sector drives innovation and growth through its flexible, profit-driven model, while the state can regulate, legislate, exercise purchasing power, and otherwise influence through policy. Taken together, the advantages of the private sector and the state—as well as their mutual interaction—can lead to significant strategic advantages for a country that hosts a mature and well-developed private market, and a country that relies on those companies and their host country becomes disadvantaged (particularly if that host country is an adversary). The problem of economic security arises, leading to the potential for confrontation among adversaries over access to private technology markets.

2.2 Field of Confrontation

Douzet and Gery (2021) describe the cyber domain as a “field of confrontation”—an “object of national security” in which states engage in conflict (metaphorical or otherwise) and in which non-state actors may be engaged. Their framework assumes that states largely determine the extent to which non-state actors participate in this “field”. However, the access that some private technology companies have to state functions challenges this assumption. It may be up to states to “involve non-state actors” in matters of diplomacy and state-level engagement, as noted by the authors, but this view does overlook the fact that states are increasingly reliant on non-state actors for their ability to function, as seen in Russia following the decision of foreign technology companies to withdraw or limit their operations.

Of course, the decision to withdraw is nuanced. On an overarching basis, the decision to leave or limit activity is effectively binary in effect, without regard to what motivates companies to make it. If a company curtails its operations due to subtle government or regulatory pressure, an effort to manage reputational risk, or even to prevent higher or unexpected compliance costs, the effect is the same. However, the strategic implications vary with motivation. When companies are forced (or strongly encouraged) to exit a market due to export controls or sanctions pressure, this represents direct government intervention that can be ascribed to the adversary state rather than to the commercial decisions of non-state actors (in this case, technology companies). Issues such as compliance and reputational risk, not to mention supply chain complexity and the potential for other operational

impacts, sit more squarely with the company itself and thus put the customer state (i.e., the state using this company's technology) in a position of greater direct dependence.

The reliance of states on private companies in this regard, as well as the fact that the use of technology does not necessarily come with significant regulatory control or influence, creates new strategic vulnerabilities and opportunities for interstate competition. The reliance of one state on technological capabilities resident in or regulated by its adversary creates a situation in which that adversary can constrain access to the required technology—or a company, seeking to manage risk, may decide to curtail that access on its own. The result is the possibility that the actions or influence of one state could impede the operations of another (even if it involves implicit pressure that drives a company to make a commercial decision that impacts its customer state). The commercial technology market thus becomes a new “field,” as envisioned by Douzet and Gery (2021), and the depth of confrontation across the state/non-state spectrum may be more profound than originally imagined. This is evident from Russia's concerns about reliance on foreign technology during the Soviet era (OTA/U.S. Congress 1979), which were explicitly renewed in 2014 by the Russian president Vladimir Putin (2014).

The emergence of the private technology market as a field of confrontation is supported by pre-existing Russian security strategy thinking. The Russian concept of “information confrontation” refers broadly to a “clash of national interests and ideas” with adversary states (Hakala and Melnychuk 2021, 5). It covers the wide range of cyber and information domain engagement up through war, although it generally stays below that level (Grise et al. 2022). The use of “confrontation” in Russian strategic thinking (“protivoborstvo”) is intentionally sub-war and implies ‘countering’, which can be seen as a responsive, if not defensive, notion. The result of confrontation over private technology—a “war over the wires rather than in them” (Johansmeyer, Mott, and Nurse 2024, 42)—has become explicit and now requires focused NSS and NCSS attention, which the 2023 US NCSS does for the first time.

The conflict of interest could result in a conflict of action, as the inherent—and now doctrinal (Russian Federation 2023)—advantage enjoyed by the United States could become a flashpoint for cyber engagement. Both the United States and Russia have explicitly identified the commercial technology sector as a strategic issue. The question that remains is whether the commercial technology environment could evolve into a field of confrontation, similar to cyber and space. It would be an unconventional characterization of the technology market—and certainly an expanded notion of what constitutes a field of confrontation. At a minimum, this contested environment—having become vast in scale and importance—clearly adds to the complexity of security strategy.

3 RESEARCH OBJECTIVES

The objective of this study is to examine how Russian strategic thinking regarding dependence on foreign private technology evolved between 2013 and 2023, and how the response of Western technology companies following the 2022 invasion of Ukraine reinforced or challenged our understanding of this dependence. Our research question is: How did Russia conceptualize foreign technology dependence as a national security issue before the 2022 invasion of Ukraine, and how did subsequent events reinforce or reshape that strategic framing?

Russia was chosen for several reasons, the most obvious being that the problems it faces emerged well before 2022 and continue to this day. Following the full-scale invasion of Ukraine, Russia experienced direct and visible pressure through the private technology market, illustrating the uneven ways in which foreign technology companies responded to the conflict. The Russian case demonstrates how complex these dynamics are in practice. While broad arguments can be made about sovereignty, dependence on private markets, and the tension between commercial interests and regulatory pressure, the way these issues unfold involves a range of actors operating under different motivations and constraints. As discussed earlier, states and private technology companies exist in an ongoing relationship of negotiation and mutual influence. The Russian experience provides a clear illustration of these dynamics. Moreover, because Russia identified this vulnerability nearly a decade before it was tested by real-world events, the case offers a unique opportunity to examine how strategic thinking evolved before, during, and after that vulnerability was realized.

4 METHODOLOGY

This article examines Russia's strategic thinking regarding dependence on foreign private technology through the analytical lens of the field of confrontation—an arena of strategic competition that falls short of an operational domain but nevertheless shapes national security.

Our analysis relies on nine public-facing Russian security strategy documents (Table 1), chosen because they collectively document Russia's evolving treatment of dependence on technology companies headquartered in adversary states.¹ We focused on public-facing documents because access to non-public materials is inherently uneven, and questions of authenticity and verifiability may arise. Moreover, differences in purpose and intended audience between public and non-public documents make it difficult to analyze them within a single, coherent framework. Restricting the corpus to public-facing documents, therefore, supports a more focused and internally consistent analysis.

Table 1. Russian strategic documents included in the analysis

Title	Year	Type
Foreign Policy of the Russian Federation	2013	Foreign policy
The Military Doctrine of the Russian Federation	2014	National defense strategy
On the Russian Federation's National Security Strategy	2015	National Security Strategy
Doctrine of Information Security of the Russian Federation	2016	National Cybersecurity Strategy
On the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030	2017	Digitalization strategy
Strategy of Information Society Development in Russia until 2030	2018	Digitalization strategy
Development of AI over the Period Extending up to the Year 2030	2019	AI strategy
On the National Security Strategy of the Russian Federation	2021	National Security Strategy
The Concept of the Foreign Policy of the Russian Federation	2023	Foreign policy

1. The availability of official English-language versions of these documents made it unnecessary to rely on original-language sources. Although additional Russian-language materials were identified, they did not provide substantially different insights into the evolution of Russia's strategic thinking on foreign technology dependence and were therefore not included in the analysis.

The analysis includes Russian security strategy documents from the 2013 Foreign Policy Concept through the 2021 National Security Strategy (NSS), the last such document published before the full-scale invasion of Ukraine. The 2023 Foreign Policy Concept is included to assess how Russia's experience following the withdrawal and restriction of foreign technology companies further shaped its strategic thinking regarding this vulnerability.

This article takes an interpretive approach to security studies (Jorgensen and Phillips 2002), identifying and evaluating themes in Russian security-strategy thinking from 2013 through the period immediately after Russia's full-scale invasion of Ukraine. The authors read the source materials separately to understand the narrative progression of Russian security strategy regarding the emergent vulnerability of its dependence on foreign technology. Themes were identified inductively, although iterative analysis also yielded some deductive results. The authors followed the chronological progression of the documents, tracing the evolving narrative to understand how Russia identified the problem of foreign technology dependence and adapted its strategic response as geopolitical and technological conditions changed. The documents map decisions and their effects, enabling the study of the direct interplay between strategic thinking and lived experience.

The narrative approach and temporal view adopted in this study represent one of several possible interpretations of the documents. The authors recognize that the strategic framing observed in Russian strategy documents may also reflect broader geopolitical tensions, sanctions, technological sovereignty policies, and domestic industrial objectives. These overlapping developments are considered when interpreting the findings.

5 EVOLUTION OF RUSSIAN STRATEGIC THINKING ON FOREIGN TECHNOLOGY DEPENDENCE

The analysis of the strategy documents reviewed reveals a clear evolution in Russian strategic thinking regarding foreign technology dependence from the time the problem was recognized through the invasion and its aftereffects. The documents trace a recurring pattern characterized by a tension between ambition and practicality. Taking a temporal view of the strategy documents shows periods of Russia striving for independence—either to manage its risk or to seek an advantage in the international arena—followed by the recognition that pursuing such objectives would be unlikely to succeed, supported by the realization that using what is already available is far easier than doing it alone. This tension became increasingly pronounced as geopolitical conditions deteriorated and was ultimately tested following the 2022 invasion of Ukraine.

5.1 Recognizing Foreign Technology Dependence as a Strategic Vulnerability (2013-2016)

A baseline for Russia's strategic views of the private technology market as a security vulnerability begins with the 2013 *Foreign Policy of the Russian Federation* (Russian Federation 2013). Although earlier security strategy documents are available, this one comes right at the beginning of a turbulent and transitional period for Russia. This is approximately when Russia's irregular war with Ukraine began—an event that led to nearly a decade of simmering kinetic and digital hostilities before the full-scale invasion in 2022. Russia's 2013 Foreign Policy position focuses on the importance of the "economic interdependence of states" as a "key factor of international stability" (Russian Federation

2013). This position is not controversial and recognizes that trade and other forms of economic engagement can deter physical (and even metaphorical) attacks, given that the attacker would experience potentially significant economic repercussions. Within this context, the 2013 document considers Russia's economic relationship with the United States, implying that mutual economic activity would be stabilizing. Although state NSS documents are typically performative, there was at least an indication in 2013 of a willingness to engage, which is far different from the hostility that increases across Russia's NSS materials through 2021.

The 2013 *Foreign Policy* concept also signaled emerging concerns about the strategic use of technology. It warned that foreign powers could employ technology “and other methods” to “exert political pressure on sovereign states, interfere in their internal affairs, destabilize their political situation, manipulate public opinion” (Russian Federation 2013). This reflects an early recognition that foreign influence could be exercised through technological means, and could occur through channels distinct from those traditionally associated with military and intelligence activity. The same concern appears in the 2014 *Military Doctrine of the Russian Federation*, which calls for developing “a dialogue with interested states on national approaches to confronting military risks and military threats brought about by the extensive use of information and communications technologies for military and political purposes” (Russian Federation 2014). At this stage, Russia's strategic documents still suggested that cooperation and dialogue were possible responses to these emerging risks. However, given the performative nature of national security strategies, such statements should be interpreted cautiously. Indeed, the markedly more confrontational tone adopted in the 2015 *National Security Strategy* suggests that this cooperative framing proved short-lived.

Only two years after the *Foreign Policy Concept*, Russia's 2015 *National Security Strategy* expressed growing dissatisfaction “with its current place in the world” (Oliker 2016; Johansmeyer, Mott, and Nurse 2024). Although this broad statement was not limited to Russia's place in the global technology market, Russia acknowledged that it was “lagging behind other key players in the domain of IT and cyber security” (Sukhankin 2016). This perceived strategic disadvantage shaped its response to the “intensifying confrontation in the global information arena caused by some countries' aspiration to utilize informational and communication technologies to achieve their geopolitical objectives” (Russian Federation 2015).

The clearest indication that Russia understood the strategic security vulnerability it faced is the NSS's explicit call for “reducing critical dependence on foreign technologies” (p. 15). While the strategy identified the problem, it offered little guidance on how to address it. The 2016 *Information Security Doctrine* elevated the issue further, identifying Russia's reliance on “electronic components, software, computers, and telecommunications equipment,” as a condition that made “the socioeconomic development of the Russian Federation dependent on the geopolitical interests of foreign countries” (Russian Federation 2016). The Doctrine consequently called for eliminating dependence on “foreign information technologies and information security” through the development of domestic alternatives.

Together, the 2015 *National Security Strategy* and the 2016 *Information Security Doctrine* mark a clear escalation in Russia's fear of foreign engagement through private technology. Even if performative, the delta from the 2013 baseline is noteworthy: what began in 2013 as a concern over potential foreign influence evolved into an explicit characterization of dependence on foreign technology as a national

security vulnerability. By 2016, Russia's irregular warfare in Ukraine had begun, resulting in some amount of criticism, ostracism, and policy response from the United States, NATO members, and other Western states. This growing concern thus coincided with the deterioration of Russia's relationship with Western states following the onset of the conflict in Ukraine, setting the stage for a strategic search for technological independence.

5.2 Pursuing Technological Sovereignty Through Modernization (2017-2020)

The commercial technology gap Russia sought to close was profound. It was estimated that Russia imported 80-100% of the country's IT equipment, with the software import rate at approximately 75% (Lowry 2021). Companies such as INTEL, AMD, IBM, and Microsoft formed "the basis for the development of the digital economy". Against this backdrop, and in response to the identified technological gap with its adversaries (Sukhankin 2017), the decree *On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030*, ("2017-2030 Decree") sought to achieve technological sovereignty through the development of a competitive domestic technology sector, with the ambitious goal of becoming a global technology leader.

The 2017-2030 Decree was highly influential and became the foundation for subsequent strategic planning. It is indeed repeatedly referenced in later government strategies and decrees. It calls for the provision of "secure and technologically independent software and services" for both private companies of all sizes and government organizations (Russian Federation 2017). The strategy sets an ambitious agenda, with technology independence not limited to system and product creation but also to envisioning a scientific research ecosystem capable of supporting innovation, technological leadership, and, eventually, the "export of Russian information and communication technologies". The *2018 Strategy of Information Society Development in Russia until 2030* largely reinforced these objectives, generally amplifying the points of the 2017-2030 Decree and adding some context (Russian Federation 2018), but without substantially clarifying how they would be implemented.

Contemporary observers questioned the feasibility of these ambitions. Sukhankin's (2017) argued that the 2017 strategy lacked a credible implementation plan. Strategy and analysis documents released between 2017 and 2019 advanced the decree's thinking and introduced more detailed objectives and implementation measures, but they did not translate into meaningful progress toward technological independence. That said, the country began pursuing improvements as part of a focused effort, as suggested by a study from the Institute of the Information Society (2018) in Moscow. Their findings offer a detailed view of Russia's then-current state, objectives, and factors associated with execution. They concluded that Russia remained well behind the world's leading digital economies and acknowledged that this position "is not in sync with the stated political objective of becoming one of the champions of the information society development and the digital economy".

Toward the end of 2019, the rise of artificial intelligence (AI) had begun to inform Russia's strategy on technological independence. The *National Strategy for the Development of Artificial Intelligence Over the Period Extending up to the Year 2030* ("2019 Decree") declared that Russia "must be included in the group of leaders in the global market" for AI capabilities by 2030 (Russian Federation 2019, 12). It stated that "an infrastructure must be created for supporting domestic organizations that engage in activities in the field of AI." This included the construction of "high-performance data processing centers" and the development of a domestic microprocessor market where the products "are not

inferior to their global equivalents as far as speed and energy efficiency”. This objective is emblematic of Russia’s broader strategic concern about the underlying components and other inputs necessary to build the IT equipment and software needed to achieve “technological sovereignty” (p. 8).

Despite increasingly ambitious strategic objectives with renewed commitments to global technology market leadership—revisited every three years by decree—progress remained limited. Achieving genuine technological independence would have required control over complex international supply chains extending from raw materials to advanced semiconductor manufacturing—capabilities that Russia did not possess. As a result, the gap between strategic ambition and practical implementation persisted, setting the stage for the more confrontational tone adopted in the 2021 *National Security Strategy*.

5.3 Last Steps Before the Invasion: Escalation Without Resolution (2021)

The recognition of Russia’s dependence on private technology companies based in adversary states became even more pronounced in the 2021 *National Security Strategy* (Buchanan 2021). What had been framed as a potential risk in 2013 became an explicit accusation eight years later, with the NSS claiming that “transnational corporations” had “aims to achieve a ‘monopoly’ over Internet and information resources” (Russian Federation 2021, 20). It further warned that the “use of foreign information technologies and telecommunications equipment in the Russian Federation increases the vulnerability of Russian information resources”. Compared with the more cautious language of the 2013 *Foreign Policy Concept* and the cooperative tone of the 2014 *Military Doctrine*, the 2021 NSS reflects a markedly more confrontational understanding of foreign technology dependence.

Despite this shift in rhetoric, what did not change from 2013 to 2021 was that the NSS raised the problem but offered no solutions. The strategy again emphasized the “priority use of Russian information technologies and equipment”, yet offered little indication of how technological independence could realistically be achieved. Components and inputs were still sourced from foreign sources (Lowry 2021), and Russia still had not developed its domestic technology market sufficiently to support the NSS’s recommendation. Rather than resolving the underlying vulnerability, the strategy reaffirmed the objective of technological sovereignty while acknowledging, at least implicitly, the difficulty of attaining it. As argued by Johansmeyer, Mott, and Nurse (2025), this framing also allowed Russia to portray itself as strategically disadvantaged by its dependence on technologies controlled by geopolitical rivals.

By 2021, Russia therefore found itself in an increasingly precarious position. It had stated its ambitions for technological sovereignty in increasingly strident terms from 2015 to 2021, developed a strategy to achieve them, and even attempted some implementation. With independence increasingly unlikely, the government sought to solidify its access to foreign technology while at least publicly stating that it was seeking alternatives. This helps explain efforts to require major foreign technology companies to establish offices in Russia before providing digital services (Sky News 2021). Such measures would have increased those companies’ long-term commitment to the Russian market and potentially raised the economic costs of future withdrawal. Coming only three months before the full-scale invasion of Ukraine, these efforts suggest—although they do not prove—that Russia anticipated the possibility of deteriorating relations with Western technology providers and that the sort of diplomatic pressure envisioned as far back as 2013 could materialize.

In many respects, Russia had arrived in 2021 at the same dilemma confronted by the Soviet Union decades earlier. Despite the tens of thousands of scientists the Soviet Union boasted (McFaul 2018), Soviet planners still found it “quicker and cheaper to obtain [technology] from the United States than to develop it in the Soviet Union” (Bricker 1981). Four decades later, when faced with the task of developing a domestic research ecosystem and industry to help the country achieve technological sovereignty, Russia once again decided it was easier to engage with the United States. The vulnerability identified repeatedly in Russia’s strategic documents remained unresolved just months before it would be tested following the invasion of Ukraine. The concerns Russia had about relying on an adversary were about to be realized, with the private technology market becoming part of an expanded field of confrontation.

5.4 After the Invasion: Testing the Vulnerability in Practice (2022-2023)

Russia’s long-standing concerns about dependence on foreign private technology were tested following its 2022 invasion of Ukraine. Shortly after the invasion, Western companies across sectors announced their intentions to exit the Russian market (Sonnenfeld and Tian 2022). Within the technology sector, the responses were mixed. Seven companies scaled back their operations, including Adobe, Okta, and Sabre (Yale School of Management 2026). Fifty-two suspended operations (including Apple, Microsoft, and Nvidia), while thirty-five withdrew entirely. Withdrawal took several forms. Slack exited the market completely, Strava disabled access in Russia, and several companies, including Cisco, IBM, Dell, and HP, either conducted orderly wind-downs or ceased operations.

Company departures did not necessarily mean an immediate loss of access to technology, but rather the beginning of a gradual decline in utility. For example, existing equipment often continued to function, but upgrades, security patches, maintenance, and other services were no longer available, leaving Russian organizations to maintain aging systems themselves and ultimately seek alternatives when replacement became necessary. This also increased exposure to cyber threats from state and non-state cyber actors, as unsupported technologies became more difficult to secure. Consequently, the nature of the disruption varied, and the effects of losing access to foreign technology were unlikely to be immediate; they would accumulate over time. The decision of a technology provider to leave the Russian market, therefore, signaled not an immediate disruption but the beginning of a period of increasing vulnerability.

There have been reports of Russian access to products offered by companies that left the country, including reported increases in iPhone purchases by Russian officials and officials photographed wearing Apple Watches (Gallagher 2024; Corcoran 2025). However, access through unofficial channels complicates procurement, limits upgrade paths, and reduces the long-term utility and stability of technology systems. Some replacement has also come from domestic companies, although China has become an increasingly important supplier (Sherman 2024a), providing both Chinese technology and access to sanctioned or otherwise unavailable Western products (“China Now Supplies 90% of Russia’s Sanctioned Tech Imports – Bloomberg” 2026). Of course, shifting to Chinese technology only perpetuated the problem of foreign dependence (Nardelli 2023), albeit with a trading partner deemed friendlier than the United States.

Russia would benefit from restored access to foreign technology, but after more than four years of disruption, that process could take years. Western markets are unlikely to return to Russia easily.

The economic costs associated with companies' withdrawal in 2022 have been substantial, with the estimated impact across sectors reaching approximately \$200 billion in gross revenues (Stognei 2023). Moreover, if foreign technology companies are unwilling to return to Russia, it is virtually impossible for Russia to 'go it alone' as it had once intended (Buchanan 2021), given the post-invasion 'brain drain' of technology talent (Wachs 2023). Russia, therefore, remains caught between limited access to Western technology and an inability to achieve genuine technological independence.

6 DISCUSSION: LESSONS FROM RUSSIA'S EXPERIENCE

The findings of this study validate many of the concerns expressed in Russia's strategic documents over the previous decade. The vulnerability repeatedly identified between 2013 and 2021 was not eliminated before the invasion; rather, it was tested in practice. Although the effects of the foreign technology market response to Russia's 2022 invasion of Ukraine were ultimately limited (Wellhausen and Zhu 2026), the disruption experienced by Russian government agencies and businesses demonstrates how dependence on foreign private technology can quickly become a strategic liability.

While this may seem like an opportunity to dismiss Russia's security concerns as exaggerated, the situation likely could have been considerably worse. Even if the disruption fell short of a complete severance from foreign technology, the effects on government and commercial operations nevertheless represent a meaningful security problem.

6.1 The Commercial Technology Market as a Field of Confrontation

Private technology has long been a factor in security and conflict (Horowitz 2024). Yet the unique combination of broad adoption and impact, deep integration into government operations, and a pervasive need for systems—even when offered by companies in adversary states—demonstrates that a novel dynamic has emerged. The progression of Russian strategic thinking, combined with the disruptions experienced by Russian business and government operations following changes in how foreign technology companies engaged with the Russian market after the 2022 invasion (Wellhausen and Zhu 2026), supports the interpretation of the commercial technology market as an emerging field of confrontation. The case demonstrates that access to privately owned technological capabilities has become a matter of national security rather than a simple commercial exchange.

In the cyber environment, one can credibly claim that the commercial technology market itself has become at least part of an expanded field of confrontation. The struggle to access and ensure the availability of the technology systems on which governments rely opens a new form of economic and cyber conflict to be understood and managed. Unlike in traditional military confrontation, influence in this space is exercised through commercial relationships, software maintenance, cloud services, supply chains, and access to privately owned technological capabilities, rather than through direct state control alone.

The private technology sector has become a powerful economic and operational force for businesses and government organizations around the world, and their dependence on a relatively small cohort of companies (Lowry 2021) illustrates the security problem, especially for adversaries of the countries where those companies are domiciled. In particular, the largest technology companies tend to be based in (and largely regulated by) the United States, which puts Russia in the position of relying on systems

that can be influenced, even indirectly, by its principal adversary. This is not to say that the U.S. control of the systems that private companies sell to Russia is absolute; there are points of friction between companies and regulators, as well as governments more broadly. For Russia, though, the vulnerability is considerable, as its strategy documents have consistently recognized since at least 2013.

6.2 The Limits of Technological Sovereignty

More broadly, this study reveals how a security vulnerability identified well in advance can be actualized in a relatively short period of time. More vexing, however, is that this type of vulnerability is notoriously difficult to remedy, particularly when the objective is technological self-reliance rather than maintaining an orderly, albeit strained, relationship with one's adversaries.

What Russia has shown, more broadly, is that there are limited means to manage the risks associated with foreign technology dependence. Developing a domestic industry capable of producing competitive alternatives is time-consuming and costly, and even where it is possible, questions remain regarding its economic viability compared with continued imports. Diversifying technology partners may reduce the risk of any single supplier state having disproportionate control or influence (e.g., the United States relative to Russia), but it does not eliminate dependence; it merely redistributes the associated risks. Eliminating the risk altogether may therefore be unrealistic, although it can be managed to varying degrees.

6.3 Implications Beyond Russia

Russia's lessons are applicable well beyond its own case. Although its exposure was particularly significant in 2022, because of the commercial strength of adversary states, many countries rely heavily on imported commercial technology and are beginning to recognize the strategic implications of that dependence. Discussions across the United Kingdom and Europe regarding reliance on U.S. technology exports (Bambridge 2026; Ryan 2026) illustrate that these concerns extend beyond Russia. There may not be an easy way to eliminate the risk of access to foreign technology, but the problem must be recognized in security strategy, with mitigation efforts where possible.

At the same time, the Russian case demonstrates that complete technological isolation is difficult to impose. The notion of entirely severing Russia's access to foreign technology proved unrealistic given the alternative channels through which technology continued to flow. Nevertheless, the decisions made by foreign technology companies were consequential. Even where access was only partially restricted, company withdrawals signaled the beginning of an extended period of technological degradation and demonstrated how vulnerable governments and businesses can become when critical systems depend on foreign commercial providers.

The Russian case also illustrates an important characteristic of the commercial technology market as a field of confrontation. Unlike traditional domains of conflict, its boundaries are diffuse, with influence more prevalent than direct control, and underlying market dynamics—both legal and informal—impeding the clear alignment and decision-making that facilitate strategic planning. This is reflected in Russia's evolving assessment of foreign technology dependence and in the subsequent realization of that vulnerability after the 2022 invasion, albeit with more limited consequences than initially anticipated.

7 CONCLUSION

The evolution of the private technology market as a field of confrontation should not come as a surprise. Our study demonstrates that Russia consistently viewed dependence on foreign private technology as a strategic vulnerability and that this concern evolved from an abstract policy objective into an operational reality following the 2022 invasion of Ukraine. Despite recognizing a major dependency on its principal adversary, Russia was unable to take meaningful action to mitigate this perceived security problem. With the loss of technology talent following the 2022 invasion, Russia seems further from boosting its domestic capabilities than it was even before the 2017-2030 Decree.

Russia's experience suggests that technological dependence cannot realistically be eliminated. Building domestic alternatives is costly, time-intensive, and may never fully replace globally competitive commercial ecosystems. The only way forward, it seems, is to figure out how to live with the risk—to recognize it explicitly within national security strategy and develop mechanisms to manage disruption when access to critical technologies becomes constrained.

Given that the problem for Russia (and other countries) is only partially resolvable at best, there is a clear research opportunity to examine the emergence of the private technology market as a field of confrontation. The first, from Russia's adversaries' perspective, involves the potential to more formally weaponize this market dynamic. As the withdrawal from the Russian market unfolded, it was clear that Russia would retain partial access to some technologies and find workarounds for others (e.g., through China). An open question is whether action by U.S. regulators and other government officials would have led to a faster, more complete withdrawal from the market, including enforcement measures to prevent the ongoing use of unsupported technology products. Even the prospect of such encouragement from governments could be used to compel an adversary's behavior, and there is an open question as to whether heightened intent and execution discipline could expose Russia to greater disruption.

Conversely, more research could be conducted on the use of technology market advantages as a de-escalatory capability (Healey and Jervis 2020). Related to the notion of compelling behavior, communicating clear market leadership and discussing potential consequences could become a diplomatic capability used to prevent (or at least mitigate the risk of) conflict. Finally, there is the opportunity to explore the implications of foreign technology dependence and the tangible implications of their withdrawal from a country. While exact calculations may be difficult, estimation is certainly possible, particularly for listed companies that have to disclose financial performance periodically. Thus, there is data available to indicate the potential disruption from a cessation of foreign technology access, which could be used for weaponization or de-escalation.

The commercial technology market powers businesses and governments; it keeps economies functioning. The companies behind these systems have become large, global, and influential. As a result, they are more capable than ever of wielding meaningful influence among states. As the Russian case illustrates, a country could be exposed to security threats as a result of commercial decision-making—particularly if that decision-making is influenced by a country's adversaries. Understanding how commercial technology markets shape competition, coercion, resilience, and conflict, therefore, represents an increasingly important challenge for both researchers and policymakers.

ABOUT THE AUTHORS

Dr. Tom Johansmeyer is the co-head of the Economic and Legal Warfare project at the Irregular Warfare Initiative. He recently completed his PhD in international conflict analysis at the University of Kent, where he researched how the economic security implications of the hyperbolization of cyber war risk. For his MA in global diplomacy at SOAS, University of London, he researched the relationship between natural disasters and political violence. Tom's research interests are largely centered on the economic implications of extreme events — across natural and manmade disasters — from which he draws on his extensive reinsurance industry experience, both as a broker in Bermuda market (at present) and previously as the head of PCS at insurance industry analytics firm Verisk. Tom served in the U.S. Army in the late 1990s as a personnel services specialist, mostly in Warrior Country in South Korea.

Dr. Jason R. C. Nurse is a Reader (Associate Professor) in Cyber Security in the Institute of Cyber Security for Society (iCSS) School of Computing at the University of Kent, UK. He also holds the roles of Visiting Fellow in Defence & Security at Cranfield University, UK and Associate Fellow at the Royal United Services Institute for Defence and Security Studies (RUSI). He received his PhD from the University of Warwick, UK, and did his PostDoc at the University of Oxford. His research interests include cyber resilience, security risk management, security culture, cyber insurance, corporate communications and cyber security, and insider threat. Jason was selected as a Rising Star for his research into cybersecurity, as a part of the UK's Engineering and Physical Sciences Research Council's Recognising Inspirational Scientists and Engineers (RISE) awards campaign. Dr. Nurse has published almost 200 peer-reviewed articles in internationally recognised security journals and conferences, and he is a professional member of the British Computing Society.

REFERENCES

- Bambridge, Joseph. 2026. "British Lawmakers Warn of "Glaring Risks" in Relying on US Tech." *Politico* (April 22, 2026). <https://www.politico.eu/article/uk-british-lawmakers-demand-transparency-over-us-tech-dependence/>.
- Bricker, Rodney P. G. 1981. *U.S. Technology Transfer to the Soviet Union: A Dilemma*. Air War College. <https://apps.dtic.mil/sti/tr/pdf/ADA107313.pdf>.
- Buchanan, Elizabeth. 2021. "Russia's 2021 National Security Strategy: Cool Change Forecasted for the Polar Regions." *RUSI Commentary* (July 14, 2021). <https://rusi.org/explore-our-research/publications/commentary/russias-2021-national-security-strategy-cool-change-forecasted-polar-regions>.
- Calcara, Antonio. 2024. "Governments and Markets in the Digital Age." *International Studies Review* 26 (1): 1–10. <https://doi.org/10.1093/isr/viae007>.
- CIA (Central Intelligence Agency). 1973. *Intelligence Report: Transfer of Technology from the United States to the USSR: Problems and Prospects*. https://www.cia.gov/readingroom/docs/DOC_0000316270.pdf.
- Committee of Public Accounts. 2025. *Government Cyber Resilience: Twenty-Fourth Report of Session 2024–25*. House of Commons. <https://committees.parliament.uk/publications/47734/documents/249527/default/>.
- Corcoran, Jason. 2025. "How Putin Turned Against Tech and "Strangled" Russia's Silicon Dreams." *The Moscow Times* (June 3, 2025). <https://www.themoscowtimes.com/2025/06/03/how-putin-turned-against-tech-and-strangled-russias-silicon-dreams-a89316>.
- CSIS (Center for Strategic and International Studies). 2023. "The Biden–Harris Administration's National Cybersecurity Strategy," March 2, 2023. <https://www.csis.org/analysis/biden-harris-administrations-national-cybersecurity-strategy>.
- Douzet, Frederick, and Aude Gery. 2021. "Cyberspace Is Used, First and Foremost, to Wage Wars: Proliferation, Security and Stability in Cyberspace." *Journal of Cyber Policy* 6 (1): 96–113. <https://doi.org/10.1080/23738871.2021.1937253>.
- Gallagher, William. 2024. "Russian Officials Buy Four Times More iPhones after Ban." *AppleInsider* (October 21, 2024). <https://appleinsider.com/articles/24/10/21/russian-officials-buy-four-times-more-iphones-after-ban>.
- Godfrey, J. T. 2025. "What Is the Current Relationship Between Business and Government? Q&A with Professor Norm Bishara." *Michigan Ross Faculty News and Research* (June 25, 2025). <https://michiganross.umich.edu/news/what-current-relationship-between-business-and-government-qa-professor-norm-bishara>.
- Grise, Michelle, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna U. Holynska. 2022. *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation*. RAND Corporation.
- Grohman, Rafael, and Alexandre C. Barbosa. 2026. "Sovereignty-as-a-Service: How Big Tech Companies Co-opt and Redefine Digital Sovereignty." *Media, Culture & Society* 48 (2): 416–424. <https://doi.org/10.1177/01634437251395003>.

- Gu, Hongfei. 2024. "Data, Big Tech, and the New Concept of Sovereignty." *Journal of Chinese Political Science* 29:591–612. <https://doi.org/10.1007/s11366-023-09855-1>.
- Gustafson, Thane. 1981. *Selling the Russians the Rope? Soviet Technology Policy and U.S. Export Controls*. RAND Corporation. <https://www.rand.org/content/dam/rand/pubs/reports/2008/R2649.pdf>.
- Hakala, Janne, and Jazlyn Melnychuk. 2021. *Russia's Strategy in Cyberspace*. Riga: NATO Cooperative Cyber Defence Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf.
- Healey, Jason, and Robert Jervis. 2020. "The Escalation Inversion and Other Oddities of Situational Cyber Stability." *Texas National Security Review* 3 (4): 30–53. <https://doi.org/10.26153/tsw/10962>.
- Hine, Emmie, and Luciano Floridi. 2026. "The Impact of Modern Big Tech Antitrust on Digital Sovereignty." *Digital Society* 5 (8): 7–27. <https://doi.org/10.1007/s44206-026-00249-3>.
- Horowitz, Jonathan. 2024. "The Business of Battle: The Role of Private Tech in Conflict." *Lawfare* (September 17, 2024). <https://www.lawfaremedia.org/article/the-business-of-battle--the-role-of-private-tech-in-conflict>.
- Institute of the Information Society. 2018. *Digital Economy Country Assessment for Russia*. Moscow: Institute of the Information Society, May. <https://iis.ru/wp-content/uploads/2020/12/DECARussia2018eng.pdf>.
- Johansmeyer, Tom. 2024. "If Cyber Is Uninsurable, the United States Has a Major Strategy Problem." *Journal of Risk Management and Insurance* 28 (2): 1–19. <https://jrmi.au.edu/index.php/jrmi/article/view/291/190>.
- Johansmeyer, Tom, Gareth Mott, and Jason R. C. Nurse. 2024. "Cyber Strategy in Practice: The Evolution of US, Russian and Ukrainian National Cyber Security Strategies through the Experience of War." *The RUSI Journal* 169 (3): 40–51. <https://doi.org/10.1080/03071847.2024.2377544>.
- Johansmeyer, Tom, Gareth Mott, and Jason R. C. Nurse. 2025. "Invisible Lines, Visible Impact: How Territorial Security Influences Russian Cyber Security Strategy." *The RUSI Journal* 170 (1): 20–31. <https://doi.org/10.1080/03071847.2025.2458143>.
- Jorgensen, Marianne, and Louise Phillips. 2002. *Discourse Analysis as Theory and Method*. London: Sage Publications.
- Kavanagh, Camino. 2019. *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?* Carnegie Endowment for International Peace, August 28, 2019. <https://carnegieendowment.org/research/2019/08/new-tech-new-threats-and-new-governance-challenges-an-opportunity-to-craft-smarter-responses>.
- Kramer, Franklin D., Robert J. Butler, and Melanie Teplinsky. 2026. "A Blueprint for Military-Industrial Partnership: Shared Risk and Unified Cyber Security." *The Cyber Defense Review* 11 (2). <https://doi.org/10.55682/cdr/4511708>.
- Lowry, Anna. 2021. "Russia's Digital Economy Program: An Effective Strategy for Digital Transformation?" In *The Palgrave Handbook of Digital Russia Studies*, edited by D. Gritsenko, M. Wijermars, and M. Kopotev. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-42855-6_4.
- McFaul, Michael. 2018. "The Missed Opportunity of Technological Breakthrough in Putin's Russia." *Hoover Institution* (October 3, 2018). <https://www.hoover.org/research/missed-opportunity-technological-breakthrough-putins-russia>.
- Mueller, Milton. 2026. "Cyber Defense in an Interdependent World: A Critique of Digital Decoupling." *Cyber Defense Review* 11 (2): 1–6. <https://doi.org/10.55682/cdr/pkjc-f4fh>.
- Myers, Ross A. 2026. "Embracing a Whole-of-Nation Approach to the 2026 National Cybersecurity Strategy Inspired by the Manhattan Project." *The Cyber Defense Review* 11 (2). <https://doi.org/10.55682/cdr/71d4-414p>.
- Nardelli, Alberto. 2023. "Russian Memo Said War Leaves Moscow Too Reliant on Chinese Tech." *Bloomberg* (April 19, 2023). <https://www.bloomberg.com/news/articles/2023-04-19/russia-china-worries-set-out-in-private-memo-on-tech-risk>.
- Oliker, Olga. 2016. "Unpacking Russia's New National Security Strategy." *Center for Strategic and International Studies* (January 7, 2016). <https://www.csis.org/analysis/unpacking-russias-new-national-security-strategy>.
- OTA/U.S. Congress (Office of Technology Assessment and U.S. Congress). 1979. *Technology and East–West Trade*. Office of Technology Assessment, November. https://digital.library.unt.edu/ark:/67531/metadc39412/m2/1/high_res_d/7918.pdf.
- Pohle, Julia, and Thorsten Thiel. 2020. "Digital Sovereignty." *Internet Policy Review* 9 (4): 1–19. <https://doi.org/10.14763/2020.4.1532>.
- Putin, Vladimir. 2014. "Presidential Address to the Federal Assembly." President of Russia, December 4, 2014. <http://en.kremlin.ru/events/president/news/47173>.
- Russian Federation. 2013. "Foreign Policy of the Russian Federation." Russian Embassy in China, February 12, 2013. https://beijing.mid.ru/en/countries/rossiya/kontseptsiya_vneshney_politiki_rossii/.
- Russian Federation. 2014. *The Military Doctrine of the Russian Federation*. Approved by the President of the Russian Federation, No. Pr.-2976. English translation, December 25, 2014. Accessed July 30, 2026. https://rusmilsec.blog/wp-content/uploads/2021/08/mildoc_rf_2014_eng.pdf.
- Russian Federation. 2015. "On the Russian Federation's National Security Strategy," December 31, 2015. <https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf>.

The Western Technology Market as Russia's Emerging "Field of Confrontation"

- Russian Federation. 2016. "Doctrine of Information Security of the Russian Federation," December 5, 2016. http://www.scrf.gov.ru/security/information/DIB_eng/.
- Russian Federation. 2017. "On the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030." President of Russia. Original title: " 2017–2030 ", May 9, 2017. <http://kremlin.ru/acts/bank/41919/page/1>.
- Russian Federation. 2018. "Strategy of Information Society Development in Russia until 2030." Committee on International Affairs of the Duma, August 12, 2018. <https://interkomitet.com/foreign-policy/basic-documents/strategy-of-information-society-development-in-russia-until-2030/>.
- Russian Federation. 2019. "Development of Artificial Intelligence over the Period Extending up to the Year 2030," October 10, 2019. <https://cset.georgetown.edu/wp-content/uploads/Decree-of-the-President-of-the-Russian-Federation-on-the-Development-of-Artificial-Intelligence-in-the-Russian-Federation-.pdf>.
- Russian Federation. 2021. "On the National Security Strategy of the Russian Federation," July 2, 2021. https://rusmilsec.blog/wp-content/uploads/2021/08/nss_rf_2021_eng_.pdf.
- Russian Federation. 2023. "The Concept of the Foreign Policy of the Russian Federation," March 31, 2023. https://mid.ru/en/foreign_policy/fundamental_documents/1860586/.
- Ryan, Johnny. 2026. "Europeans Are Dangerously Reliant on US Tech. Now Is a Good Time to Build Our Own." *The Guardian* (February 17, 2026). <https://www.theguardian.com/commentisfree/2026/feb/17/europeans-are-dangerously-reliant-on-us-tech-now-is-a-good-time-to-build-our-own>.
- Sherman, Justin. 2024a. "Russia's Becoming More Digitally Isolated—and Dependent on China." *Council on Foreign Relations* (August 12, 2024). <https://www.cfr.org/articles/russias-becoming-more-digitally-isolated-and-dependent-china>.
- Sherman, Justin. 2024b. *Russia's Digital Tech Isolationism: Domestic Innovation, Digital Fragmentation, and the Kremlin's Push to Replace Western Digital Technology*. Atlantic Council, July. https://dfrlab.org/wp-content/uploads/sites/3/2024/07/AC_CSI_Russias_Digital_Tech_Isolationism.pdf.
- Sky News. 2021. "Russia Demands Foreign Tech Companies Open Offices in the Country or Face Sanctions." *Yahoo! News* (November 24, 2021). <https://uk.news.yahoo.com/russia-demands-foreign-tech-companies-105800408.html>.
- Sonnenfeld, Jeffrey, and Steven Tian. 2022. "Some of the Biggest Brands Are Leaving Russia. Others Just Can't Quit Putin. Here's a List." *The New York Times* (April 7, 2022). <https://www.nytimes.com/interactive/2022/04/07/opinion/companies-ukraine-boycott.html>.
- Stognei, Anastasia. 2023. "Billions of Dollars in Western Profits Trapped in Russia." *Financial Times* (September 18, 2023). <https://www.ft.com/content/fb0ab6e1-ab45-438e-b9a1-1bc352645647>.
- Sukhankin, Sergey. 2016. "Russia's New Information Security Doctrine: Fencing Russia from the "Outside World"?" *Eurasia Daily Monitor* 13, no. 198 (December 16, 2016). <https://jamestown.org/russias-new-information-security-doctrine-fencing-russia-outside-world/>.
- Sukhankin, Sergey. 2017. "Russia Adopts New Strategy for Development of Information Society." *Eurasia Daily Monitor* 14, no. 66 (May 16, 2017). <https://jamestown.org/russia-adopts-new-strategy-development-information-society/>.
- "China Now Supplies 90% of Russia's Sanctioned Tech Imports – Bloomberg." 2026. *The Moscow Times* (May 1, 2026). <https://www.themoscowtimes.com/2026/05/01/china-now-supplies-90-of-russias-sanctioned-tech-imports-bloomberg-a92662>.
- U.S. GAO (United States General Accounting Office). 1990. *Export Controls: U.S. Policies and Procedures Regarding the Soviet Union*. United States General Accounting Office. <https://www.gao.gov/assets/nsiad-90-185fs.pdf>.
- Vattikonda, Niharika, and Benjamin Kelley. 2025. "The D.C. Circuit Court's TikTok Ban Decision, Explained." *Lawfare* (January 9, 2025). <https://www.lawfaremedia.org/article/the-d.-c.-circuit-court's-tiktok-ban-decision--explained>.
- Wachs, Johannes. 2023. "Digital Traces of Brain Drain: Developers during the Russian Invasion of Ukraine." *EPJ Data Science* 12 (14): 1–18. <https://doi.org/10.1140/epjds/s13688-023-00389-3>.
- Wellhausen, Rachel, and Boliang Zhu. 2026. "Exiting Russia." *American Political Science Review*, 1–18. <https://doi.org/10.1017/S000305542610152X>.
- Yale School of Management. 2024. "Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain." Chief Executive Leadership Institute, January 28, 2024. <https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain>.
- Yale School of Management. 2026. "Yale CELI List of Companies Leaving and Staying in Russia." Chief Executive Leadership Institute, May 3, 2026. <https://www.yalerussianbusinessretreat.com/>.

Received 4 August 2025; Revised 17 July 2026; Accepted 20 July 2026