Ana Brown

Vulnerabilities in Russian Weapons Systems from Chinese Microelectronics

08, May 2025

Executive Summary

Chronic underinvestment, failed innovation efforts, and a stagnant Research & Development base left Russia increasingly dependent on Chinese components. The war in Ukraine did not create Russia's technological vulnerabilities — it intensified them. Chinese commercial off-the-shelf (COTS) microchips are now widely embedded in Russian weapons systems. While not military-grade, many of these components — especially programmable microcontrollers — pose a credible risk of compromise. Although no direct evidence of sabotage exists, China's likely technical insight into Russian weapons raises the potential for strategic disruption or external control.

Scope Note

The assessment aims to evaluate the extent to which Chinese COTS components are integrated into Russian military hardware and the potential risks this introduces in terms of sabotage, remote access, and geopolitical leverage. It seeks to answer the following key question: To what degree does Russia's reliance on Chinese COTS microelectronics compromise the integrity and security of its weapons systems?

This analysis draws primarily on open-source intelligence, official reporting, and detailed technical and scientific assessments of microelectronic components. These include structural and functional evaluations of recovered chips, examination of firmware programmability, and assessments of vulnerability to remote manipulation or hardware compromise. However, all official Russian and Chinese government databases related to chip exports, imports, and military procurement have been closed or restricted since 2022. Public customs data, defence trade logs, and detailed technical specifications of components are either obfuscated or unavailable.

Key Judgments

I. We assess that Russia's increasing reliance on Chinese-manufactured commercial microelectronics presents a growing strategic vulnerability across a wide range of Russian military systems.

– Russia's domestic microelectronics sector remains underdeveloped. Since 2022, China and Hong Kong have emerged as Russia's principal suppliers of integrated circuits, accounting for nearly 90 percent of shipments during critical periods.

– Numerous Russian military and dual-use systems — including unmanned aerial vehicles, unmanned ground vehicles, and missile guidance and control packages—contain Chinese-origin components. These range from low-complexity circuits to programmable microcontrollers, some of

which likely present a moderate to high risk of firmware compromise or hardware-level manipulation.

II. Based on technical analysis, it is very likely that Chinese commercial microelectronics are susceptible to sabotage, remote disablement, or telemetry subversion. In systems where navigation, guidance, or communication functions rely on these components, targeted disruption is technically feasible, particularly in scenarios involving direct geopolitical conflict.

III. We judge with moderate confidence that China possesses substantial knowledge of Russian military system architecture and may have embedded latent capabilities to disable or manipulate certain platforms.

– While there is no open-source evidence that these vulnerabilities have been activated, the potential strategic risk from embedded backdoors or compromised firmware remains significant. Any exploitation of such capabilities, if it occurred, would almost certainly not be publicly disclosed.

IV. We have low confidence in our ability to assess when or under what circumstances China would attempt to exploit these vulnerabilities to influence or manipulate Russian weapons systems.

– Cyber warfare and compromised electronics are China's preferred tactic, which they have been using for decades to achieve strategic effect while maintaining plausible deniability and avoiding overt escalation.

– In 2012, researchers at the University of Cambridge identified a serious security vulnerability — a hidden backdoor — in a Chinese-manufactured chip used in US military systems, raising concerns about the integrity of foreign-sourced microelectronics.

– The war in Ukraine has made Russia heavily reliant on China for electronics; however, the two states do not maintain a formal alliance. Under current wartime conditions, Russia lacks the capacity and time to thoroughly verify the integrity of all Chinese-supplied components.

V. We judge with low confidence that China would undertake clandestine attacks against the US Homeland via compromised Russian hardware platforms or third-party vectors in the next three to five years; however, based on current geopolitical trajectories, such activity might become more plausible within the next five to ten years.

Russian tech dependence

The war in Ukraine did not create Russia's technological vulnerabilities — it intensified them. Long before the invasion, Russia faced chronic underinvestment in domestic R&D, an inability to meet its own nanotechnology goals, and a growing reliance on Chinese technology. Western sanctions and the collapse of ties with European suppliers only accelerated this dependence.

In 2007, the Russian government established Rusnano, a state-owned enterprise intended to position the country as a global leader in nanotechnology. Despite the support of senior officials and reputable scientists, the initiative failed to meet its ambitious 2011 targets. This was due to a combination of factors: a shortage of technical expertise, weak entrepreneurial culture, inadequate business management skills, and—critically—a lack of domestic nanotechnology production capacity. At the time, the Ministry for Industry and Energy described Russia's nanotech manufacturing capability as being at a "critically low level." Subsequent targets, such as the goal of mass-producing nanotechnologies by 2013, were never realised. Since 2016, Rusnano has hovered on the brink of bankruptcy and has been mired in corruption investigations involving its leadership.

Russia's technological dependency has also increasingly shifted toward China. Between 2013 and 2018, Russian tech imports from the European Union declined significantly, while China's share grew markedly. Russian investment in domestic R&D remained stagnant between 2000 and 2020, consistently hovering just above one percent of GDP[1]—well below global benchmarks—even before the 2022 invasion of Ukraine intensified the Kremlin's emphasis on defence technologies. By 2023, analysts described this shift as Russia losing its strategic flexibility to balance technological dependence between the United States and China, leaving Moscow effectively locked into reliance on the latter.

In 2020, Russian international affairs analyst Danil Bochkov noted that, as a result of Western sanctions and the lack of viable domestic alternatives, Russia was becoming increasingly dependent on Chinese technology for its 5G infrastructure. He warned that this reliance carried espionage risks and that excessive dependence on non-Western systems posed a serious strategic vulnerability.[2]

Huawei — the same company investigated and penalised by the US government for espionage risks, sanctions violations, intellectual property theft, and deception in its global operations, including the illegal sale of surveillance-enabling telecommunications equipment to Iran and North Korea[3] — has made significant inroads in Russia by exploiting the Kremlin's lack of alternative suppliers.[4]

In the hardware sector, Russia's challenges have deepened since the war. The country lacks a robust domestic microelectronics industry. In May 2022, Alexander Kuleshov, head of the Skolkovo Innovation Center, described Russia's tech infrastructure as a "disaster." He noted that essential equipment such as supercomputer boards frequently fail, and many foreign manufacturers have ceased providing repairs, maintenance, or warranty support. In response, Russian intelligence

---

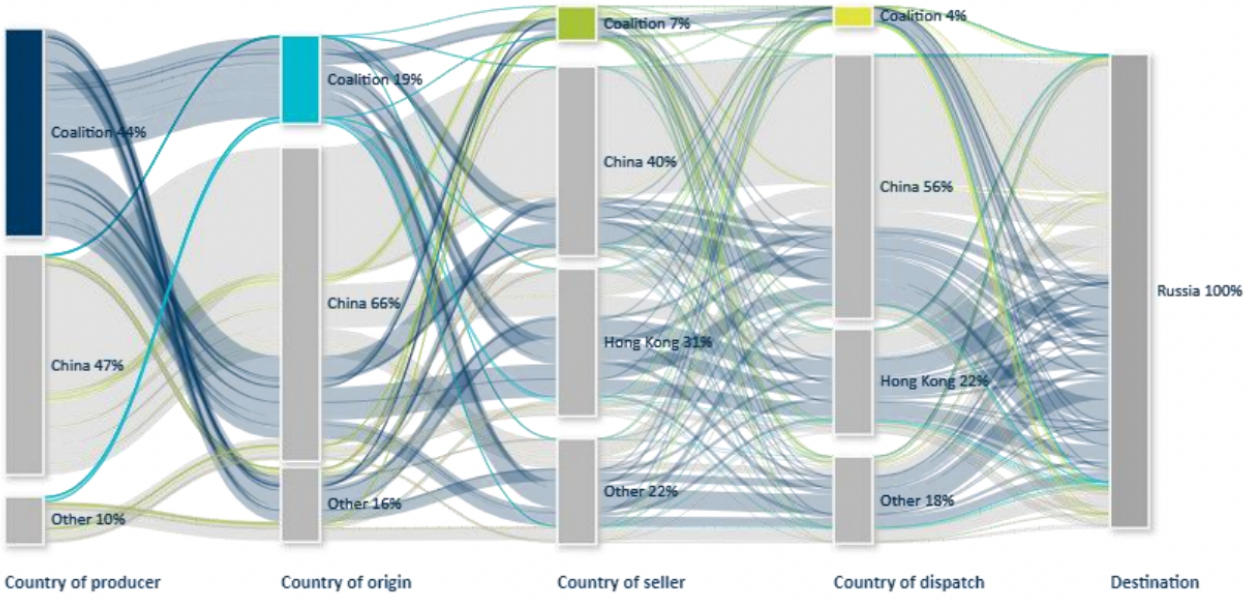
[1] Digital Forensic Research Lab. *Russia's Digital Tech Isolationism*. July 2024 https://dfrlab.org/wp-content/uploads/sites/3/2024/07/AC_CSI_Russias_Digital_Tech_Isolationalism.pdf
[2] Sher, Nathaniel. "China's Bid to Conquer Russia's 5G Market Should Worry the Kremlin." *The Diplomat*, October 28, 2020 https://thediplomat.com/2020/10/chinas-bid-to-conquer-russias-5g-market-should-worry-the-kremlin/
[3] Macaulay, Thomas. "US Assesses Cyber Threat Posed by Chinese Telecom Firms." *The Next Web*, February 8, 2024 https://thenextweb.com/news/us-assesses-cyber-threat-posed-by-chinese-telecom-firms
[4] Digital Forensic Research Lab. *Russia's Digital Tech Isolationism*. Washington, DC: Atlantic Council, July 2024 https://dfrlab.org/wp-content/uploads/sites/3/2024/07/AC_CSI_Russias_Digital_Tech_Isolationalism.pdf

agencies have reportedly circumvented sanctions by sourcing chips through third countries. In some instances, military units have been forced to salvage chips from consumer appliances like refrigerators to meet battlefield needs.[5]

According to the Carnegie Institute, China and Hong Kong accounted for nearly 90% of all global chip exports to Russia between March and December 2022.[6]

A separate analysis by the KSE Institute, based on recovered Russian battlefield equipment, indicates a more nuanced picture: between January and October 2023, China was responsible for 47% of production and 66% of origin points for battlefield goods. While this still highlights China's central role as both a manufacturing base and transit hub, it suggests a slightly reduced share compared to earlier chip-specific data.

Mapping Russia's Imports of Battlefield Goods, January–October 2023



Source: KSE Institute[7]

China has supplied compromised microchips before

In 2012, researchers at Cambridge University discovered a serious security vulnerability — a hidden "backdoor" — in a Chinese-manufactured chip used by the US military. This backdoor could potentially allow external parties to disable or reprogram the chip, even if security protections were active.[8] The chip was reportedly used in critical systems including weapons, nuclear facilities, and public transport infrastructure. The researchers did not reveal the chip's manufacturer or specific

---

[5] Digital Forensic Research Lab. *Russia's Digital Tech Isolationism*. Washington, DC: Atlantic Council, July 2024 https://dfrlab.org/wp-content/uploads/sites/3/2024/07/AC_CSI_Russias_Digital_Tech_Isolationalism.pdf

[6] Stronski, Paul. "Hong Kong's Technology Lifeline to Russia." *Carnegie Endowment for International Peace*, May 16, 2023 https://carnegieendowment.org/research/2023/05/hong-kongs-technology-lifeline-to-russia?lang=en

[7] KSE Institute. *Challenges of Export Controls Enforcement*. Kyiv School of Economics, January 2024 https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf

[8] Skorobogatov, Sergei. *Silicon Scan: A Side-Channel Analysis of the Influence of Trojan Circuits on the Leakage of a Chip*. University of Cambridge, 2012 https://www.cl.cam.ac.uk/~sps32/Silicon_scan_draft.pdf

deployments. Some cybersecurity experts, including from Errata Security, later questioned whether the backdoor was intentionally inserted, suggesting it could have been an accidental feature rather than deliberate sabotage.[9] Regardless, the discovery highlighted serious concerns about the security and integrity of supply chains for sensitive hardware components.

Later in 2012, a Senate Armed Services Committee investigation uncovered counterfeit electronic parts originating from China in critical US military systems, including the Air Force's largest cargo plane, assemblies intended for Special Operations helicopters, and a Navy surveillance plane. Basically, China replicated US microchips using e-waste, compromised them, and sold them back to the United States.[10] The committee's report found that, across 1,800 cases investigated, the total number of suspect counterfeit parts exceeded one million. The year-long investigation, led by Committee Chairman Senator Carl Levin and Ranking Member Senator John McCain, also recorded that the Chinese government denied visas to the Committee staff seeking to travel to mainland China in support of the inquiry.[11]

The reliance of the U.S. military on Chinese-manufactured semiconductors presents serious and escalating national security vulnerabilities. According to the Hudson Institute, this dependence exposes critical defense systems to the risk of cyber infiltration, deliberate malfunction, or system sabotage initiated through compromised hardware components.[12] In a scenario where geopolitical tensions escalate, such vulnerabilities could be exploited by the Chinese government to disable, disrupt, or manipulate military assets at a strategic moment. The threat is particularly acute because compromised semiconductor chips could be inserted deep within supply chains, making them extremely difficult to detect through standard testing or inspections. Moreover, the integration of such components into complex military platforms — including satellites, command and control systems, and advanced weapons — could create latent vulnerabilities that remain dormant until activated.

Wassenaar Arrangement

There are over 500 distinct controlled entries across both the Munitions List and the Dual-Use List in the Wassenaar Arrangement. In theory, any item listed could be compromised, depending on the nature of the technology and the method of attack. However, in practical terms, the greatest vulnerability lies in categories involving electronics, telecommunications, information security, navigation systems, sensors, and aerospace technologies. Items most at risk are concentrated in Category 3 (Electronics), Category 4 (Computers), Category 5 Part 1 (Telecommunications),

---

[9] Macaulay, Thomas. "Researchers Find Vulnerability in Chinese Chips Used by US Army." *The Next Web*, February 9, 2024 https://thenextweb.com/news/researchers-find-vulnerability-in-chinese-chips-used-by-us-army?utm_source=chatgpt.com

[10] U.S. Senate Armed Services Committee. *Counterfeit Electronic Parts in the Department of Defense Supply Chain*. Washington, DC: Government Printing Office, 2012 https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf

[11] U.S. Senate Armed Services Committee. *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain: Report of the Committee on Armed Services, United States Senate*. Washington, DC: Government Printing Office, May 21, 2012 https://www.armed-services.senate.gov/imo/media/doc/SASC-Counterfeit-Electronics-Report-05-21-12.pdf

[12] Williams, Bryan Clark, Dan Patt, and Jack Keane. *Chipping Away: China's Semiconductor Threats to U.S. Military Edge*. Hudson Institute, November 2, 2023 https://www.hudson.org/supply-chains/chipping-away-china-semiconductor-threats-us-military?utm_source=chatgpt.com

Category 5 Part 2 (Information Security), Category 6 (Sensors and Lasers), Category 7 (Navigation and Avionics), and Category 9 (Aerospace and Propulsion).[13]

These categories are susceptible to compromise through various means, including hardware backdoors, firmware tampering, software vulnerabilities, or malicious manufacturing processes such as inserting trojans into hardware. Given the structure of the control lists, it is estimated that approximately 150 to 200 out of the more than 500 specific controlled items are realistically vulnerable to such forms of compromise. This amounts to about 30 to 40 percent of all Wassenaar-controlled positions, with the risk being highest for technologies involving electronics, computing, and critical systems integration.

The Arrangement itself is not legally binding, each participating country commits to implement national legislation and licensing systems to control the export of items listed on the two Wassenaar control lists. Neither Russi nor China are a party to the agreement and Chinese companies are not bound by Wassenaar Arrangement restrictions. China's national export control system is considerably looser than Wassenaar standards, particularly in the regulation of sensitive technologies such as advanced electronics, drones, and cybersecurity equipment. As a result, Chinese firms serve as a loophole by supplying sensitive dual-use goods to Russia, leaving Russia with little choice but to purchase them from China, despite the risk that many of these goods may be compromised.

China and Russia are situational allies

Declaring a “friendship without limits” is characteristic of communist political language. Anthropological linguistics — the study of cultural and linguistic habits — shows that such expressions are common in communist and post-communist discourse, often serving more as ideological signalling than concrete commitment. They did not prevent Russia from invading Georgia, a former Soviet republic, in 2008, nor did they deter its invasion of “brotherly” Ukraine in 2022. Similarly, China’s rhetoric of unity did not stop it from retaking control over Xinjiang, a region historically connected to Soviet Kazakhstan.

Despite the close ties, China and Russia are not allied in the traditional military or political sense. Their joint statement issued on 21 March, 2023 reaffirmed that their relationship is non-aligned, non-confrontational, and not directed against any third party, clearly distinguishing it from Cold War-era alliances.[14]

According to the Chinese state media offers an explanation: first, non-alignment remains a fundamental principle of Chinese diplomacy. This position reflects lessons drawn from China's difficult historical experiences with alliances in the twentieth century and represents a conscious decision to pursue an independent foreign policy, in line with the international trend towards peace and development following the end of the Cold War. Second, the non-aligned character of China-Russia relations is legally codified in the 2001 China-Russia Treaty of Good-Neighborliness and Friendly Cooperation. This treaty rejected traditional models of alliances and confrontation,

---

[13] Wassenaar Arrangement. *List of Dual-Use Goods and Technologies and Munitions List 2023-1*. December 2023 https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf

[14] Xinhua News. “China, Russia Reaffirm Strategic Partnership in Joint Statement.” *Xinhua*, March 22, 2023 http://www.news.cn/world/2023-03/22/c_1211740381.htm

establishing a firm legal and political basis for the distinctive nature of their partnership. Subsequent joint statements, including those issued in 2016 and 2021, have consistently reaffirmed this principle. Third, forming an alliance would contradict the original purpose of the China-Russia relationship: to be good neighbours, good friends, and good partners for mutual benefit. A formal alliance could introduce imbalances, as demonstrated in the US-led alliance systems, where equality among partners is often compromised. Both China and Russia aim to remain independent centres of power within a multipolar world and would resist any arrangement that creates hierarchy. Furthermore, a formal alliance would restrict diplomatic flexibility; for example, if China were bound by such a structure, it would have been unable to maintain neutrality and promote peace talks regarding the Ukraine conflict.[15]

Even The joint statement between Russia and China 2024[16] does not propose forming a formal alliance. On the contrary, it explicitly reaffirms that their relationship is not of a military or political bloc nature. Russia and China describe their relationship as a new model of interaction between major powers, based on principles of non-alignment, mutual respect, equality, and strategic cooperation. Their partnership is intended to promote a multipolar world order rather than create exclusive alliances. The joint statement emphasises that the development of their relationship is guided by their national interests and the broader goal of supporting international stability, rather than targeting or opposing any third party.

As time passes and narratives shift, it is increasingly clear that Russia and China do not share common religious or cultural roots. While the partnership between Russia and China continues to deepen, it remains deliberately distinct from traditional political or military alliances.

China is building capacity

The PRC lacks neither the resources nor the ambition to pursue global dominance. The People's Republic of China has set a strategic goal to surpass the West in artificial intelligence research and development by 2025 and to become the global leader in AI by 2030.[17] AI has been designated a national priority within China's science and technology agenda, with Beijing viewing advancements in AI and autonomy as central to its concept of "intelligentized warfare" — the future of military operations. The PRC considers the integration of military and civilian institutions essential to this effort and has established joint R&D centres, enabling the People's Liberation Army to access cutting-edge AI and robotics technologies developed in the commercial sector.

In 2021, Beijing launched the China Brain Plan, a major national initiative leveraging brain science to drive advances in biotechnology and AI. That same year, Chinese scientists developed a quantum computer capable of outperforming classical high-performance systems on specific tasks. To reduce

---

[15] Xinhua News. "China, Russia Reaffirm Strategic Partnership in Joint Statement." *Xinhua*, March 22, 2023 http://www.news.cn/world/2023-03/22/c_1211740381.htm

[16] Government of the Russian Federation. "Joint Statement of the Russian Federation and the People's Republic of China on Deepening Comprehensive Strategic Partnership." *President of Russia*, March 21, 2023 http://kremlin.ru/supplement/6132

[17] U.S. Department of Defense. *Military and Security Developments Involving the People's Republic of China 2024: Annual Report to Congress*. Washington, DC: Office of the Secretary of Defense, December 18, 2024 https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF

dependence on foreign suppliers, China is also developing its own specialised refrigeration systems required for quantum computing research. Additionally, the PRC has invested over $1 billion in a national quantum laboratory,[18] which, upon completion, is expected to become the world's largest quantum research facility.

While China still depends on foreign technologies for certain critical inputs — particularly advanced semiconductor manufacturing tools and specialised software — its research institutions are actively exploring new materials and architectures for next-generation semiconductor microchips. In parallel, Chinese entities have successfully replicated some foreign technologies, and investigations have revealed the production and circulation of counterfeit chips, including the ones that infiltrated the US defence in 2012.

Military-grade chips vs COTS

Military-grade microchips are specialised components designed to meet stringent standards for durability, reliability, and security in extreme environments such as high radiation, temperature, and vibration. These chips undergo rigorous testing and certification to ensure performance in critical defence applications. Their export is tightly controlled by national regimes to prevent their proliferation to adversaries. Military-grade chips are supposed to be manufactured in secure facilities with strict supply chain oversight to reduce the risk of tampering or compromise.

Commercial Off-The-Shelf (COTS) components refer to readily available hardware or software products designed for general commercial use rather than specialised military or aerospace applications. While COTS parts offer cost efficiency and ease of procurement, they typically lack the ruggedness, security, and reliability standards required for mission-critical defence systems. Their use introduces potential vulnerabilities, especially when sourced from foreign suppliers, as they may be susceptible to tampering, hidden backdoors, or performance failures under extreme conditions.

Nevertheless, COTS components are increasingly used in modern weapons systems due to their cost-effectiveness, availability, and technological advancement. This makes them attractive for integration into a wide range of military platforms, particularly in areas like communication systems, navigation modules, and unmanned aerial vehicles. For example, Russia's Orlan-10 drones have been found to contain COTS microchips and modules sourced from commercial supply chains.[19]

A major vulnerability of COTS components is their susceptibility to remote access and cyber intrusion. Since these parts often lack secure firmware, encryption, or tamper-resistant architecture, they present exploitable entry points for adversaries. Hackers can compromise embedded firmware, insert malicious code during production, or exploit insecure communication protocols. In battlefield systems, this can enable remote disruption, manipulation of guidance or targeting data, or unauthorised telemetry transmission. As COTS use expands, so too does the risk that foreign-made or

---

[18] U.S. Department of Defense. *Military and Security Developments Involving the People's Republic of China 2024: Annual Report to Congress*. Washington, DC: Office of the Secretary of Defense, December 18, 2024 https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF

[19] InformNapalm. "Russian Drone Orlan-10 Consists of Parts Produced in the USA and Other Countries (Photo Evidence)." *InformNapalm*, July 30, 2022 https://informnapalm.org/en/russian-drone-orlan-10-consists-of-parts-produced-in-the-usa-and-other-countries-photo-evidence/?utm_source=chatgpt.com

poorly secured components could be compromised to gain strategic advantage. In fast-moving or resource-constrained conflicts, such as the ongoing war in Ukraine, the reliance on COTS has increased due to limited access to specialised components.

Microchips comparison

Military-grade microchips	Commercial Off-The-Shelf (COTS)
Designed for extreme environments: high radiation, temperature, vibration	Designed for general commercial use; widely used in navigation systems
Should be rigorously tested and certified for security	Limited testing
Manufactured in secure facilities with tight supply chain control	Mass-produced; often sourced from foreign or less secure supply chains
Manufactured in China	Manufactured in China
Likely used in Russian weapons	Definitely used in Russian weapons
Subject to strict international export controls	Limited international export controls
Lower risk of tampering but still possible	High risk of tampering

Application of COTS in Russian weapons

For the purposes of this analysis, it is assumed that Russia retains the capability to independently produce Soviet-era weapons systems, which are currently being depleted in the Russia-Ukraine conflict. Therefore, this assessment focuses exclusively on modern weapons.

Orlan-10 UAV

Russian Orlan-10 unmanned aerial vehicles, for example, have been found to contain Chinese-manufactured microchips, particularly within their navigation and control systems. Analysis of downed Orlan-10 drones revealed components such as the HC4060 2H7A201 and STC 12LE5A32S2 35i—both produced in China—embedded in the GPS tracker module. These microchips play a critical role in the drone's navigation functions, including its interface with Russia's GLONASS satellite system.[20]

In theory, both the HC4060 2H7A201 and the STC 12LE5A32S2 35i microchips could be compromised, although the likelihood and potential impact vary significantly between the two.

The HC4060 2H7A201 is a simple binary counter and timer chip, primarily used to divide frequencies and manage timing functions. Because of its basic design and limited functionality, the risk of embedding malicious features into this chip is very low. However, it is not entirely impossible. A compromised version could be intentionally manufactured with subtle instabilities that might disrupt timing signals, potentially affecting the performance or reliability of a system such as a drone's navigation.

In contrast, the STC 12LE5A32S2 35i is a far more capable microcontroller, based on the Intel 8051 architecture. As a programmable device, it carries a medium to high theoretical risk of compromise. Malicious code, hidden backdoors, or delayed-action sabotage mechanisms could be inserted into its firmware during production. In practice, this could lead to behaviours such as device failure under

[20] InformNapalm. "Russian Drone Orlan-10 Consists of Parts Produced in the USA and Other Countries (Photo Evidence)." *InformNapalm*, July 30, 2022 https://informnapalm.org/en/russian-drone-orlan-10-consists-of-parts-produced-in-the-usa-and-other-countries-photo-evidence/?utm_source=chatgpt.com

certain conditions, geofenced sabotage (causing a system to crash or disable itself in specific locations), or covert data leakage if the microcontroller interfaces with communication systems.

Garpiya-3 (G3)

On September 25, 2024 Reuters reported that Russia has set up a weapons development programme in China aimed at producing long-range attack drones for use in the war against Ukraine. According to two sources from a European intelligence agency and documents reviewed by Reuters, the Russian defence firm IEMZ Kupol—a subsidiary of the state-owned conglomerate Almaz-Antey—has developed and conducted flight tests of a new drone model, the Garpiya-3 (G3), in China with the assistance of local specialists. One of the documents, a report from Kupol to the Russian defence ministry, outlines the project's progress earlier this year.[21]

DLE (Dual-Mode Low Emissions) aircraft engines

DLE engines typically referring to modern gas turbine engines with advanced low-emission combustion systems — do incorporate electronic components, including microchips, as part of their design. These electronics are essential for precise engine control, emissions management, and system diagnostics.

A key feature of modern DLE engines is the integration of a Full Authority Digital Engine Control (FADEC) system. FADEC units rely on microprocessors, memory chips, and various electronic components to continuously monitor and regulate critical engine parameters such as fuel flow, temperature, pressure, and rotational speed. This ensures optimal engine performance while keeping emissions within strict limits.

Additionally, DLE engines are equipped with networks of sensors and embedded electronics to support real-time diagnostics and health monitoring. These systems detect anomalies, track performance trends, and enable predictive maintenance. Since DLE combustion requires finely tuned control of air-fuel mixtures and combustion stages, microchips and digital logic are necessary to manage these functions accurately and efficiently. And all of them come from China.[22]

Vulnerability Assessment of Russian Systems Using Chinese Microelectronics

Model*	Type of Weapon / Technology	Manufacturer	Contains China-manufactured microchips?**	Vulnerability to remote access	Technical means of compromise
Platforma-M	Combat UGV	NITI Progress	Likely	Yes	Telemetry hijack, backdoors, malware injection
Nerekhta	Combat UGV	Degtyaryov Plant and Advanced Research Foundation (ARF)	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path
Soratnik	Combat UGV	Rostec	Likely	Yes	Telemetry hijack, backdoors, malware injection
Kungas	UGV Swarm Concept	Special Engineering Design Bureau	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path
Scarab	Demining UGV, short-range	CET-1	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path

[21] Reuters. "Russia Has Secret War Drones Project in China, Intel Sources Say." *Reuters*, September 25, 2024 https://www.reuters.com/world/russia-has-secret-war-drones-project-china-intel-sources-say-2024-09-25/

[22] Lansing Institute. "China Continues Supplying Russia with Critical Dual-Use Components." *Lansing Institute*, September 24, 2024 https://lansinginstitute.org/2024/09/24/china-continues-supplying-russia-with-critical-dual-use-components/

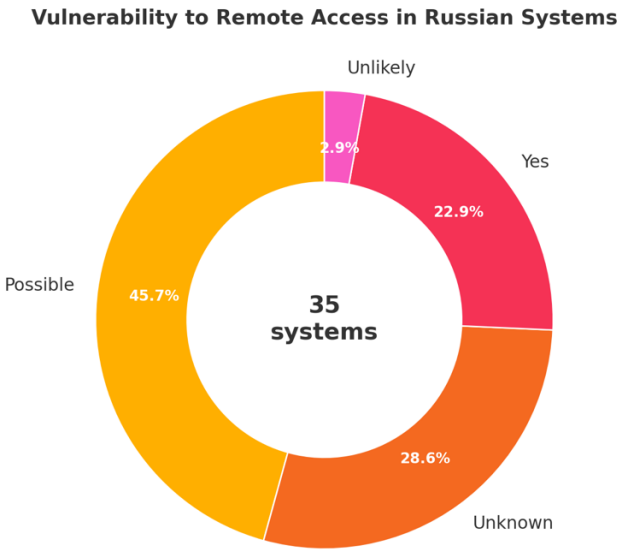
Sphera	Demining UGV, short-range	CET-1	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path
Marker	UGV RDT&E Concept	ARF	Likely	Unknown	Unknown or low-resolution compromise path
Uran-6	Demining UGV, short-range	JSC 766 UPTK (Kalashnikov-Rostec)	Likely	Yes	Telemetry hijack, backdoors, malware injection
Uran-9	Combat UGV	JSC 766 UPTK (Kalashnikov-Rostec)	Likely	Yes	Telemetry hijack, backdoors, malware injection
Uran-14	Firefighting UGV	JSC 766 UPTK (Kalashnikov-Rostec)	Likely	Yes	Telemetry hijack, backdoors, malware injection
Udar	Combat UGV	Rostec	Likely	Yes	Telemetry hijack, backdoors, malware injection
Prohod-1	Heavy Demining UGV	High Precision Weapons JSC	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path
Shturm	Heavy UGV for Urban Combat	Uralvagonozavod	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path
T-14 Armata	Next-Generation MBT (autonomous/semi-autonomous)	Rostec	Likely	Unknown	Unknown or low-resolution compromise path
Nudol system	Ground-based ASAT missile interceptor	JSC Concern VKO Almaz-Antey	Likely	Possible	Targeted EW disruption or spoofing
S-500 system	Air-defence system with potential ASAT	JSC Concern VKO Almaz-Antey	Likely	Possible	Targeted EW disruption or spoofing
Burevestnik (space)	Air-based space launcher	Krasnoarmeysk Scientific Research Institute of Mechanization (KNIIM)	Likely	Unknown	Unknown or low-resolution compromise path
Peresvet	Laser system for satellites/missile blinding	Russian Ministry of Defense	Likely	Unlikely	Vulnerable to optical or electromagnetic countermeasures
Tirada-2	EW system against communication satellites	Central Research Institute of the Ministry of Defense of Russia	Likely	Possible	RF interference spoofing, jamming override
Bylina-MM	EW system for satellite signal disruption	Central Research Institute of the Ministry of Defense of Russia	Likely	Possible	RF interference spoofing, jamming override
Krasukha-4	Radar satellite counter-system	Concern Radio-Electronic Technologies (KRET)	Likely	Possible	RF interference spoofing, jamming override
Divnomorye	Radar satellite counter-system	Concern Radio-Electronic Technologies (KRET)	Likely	Possible	RF interference spoofing, jamming override
Tobol	Satellite protection system	Russian Space Systems (RKS)	Likely	Unknown	Unknown or low-resolution compromise path
Avangard	Hypersonic Glide Vehicle (HGV)	NPO Mashinostroyeniya	Likely	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)
Sarmat	Intercontinental Ballistic Missile (ICBM)	Makeyev Rocket Design Bureau	Likely	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)
Poseidon	Nuclear-Powered UUV	Rubin Design Bureau	Likely	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)
Burevestnik (missile)	Nuclear-Powered Cruise Missile	Novator Design Bureau	Unlikely/Unknown	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)
Kinzhal	Air-Launched Ballistic Missile	Design Bureau of Machine-Building (KBM)	Likely	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)
Tsirkon (Zircon)	Hypersonic Cruise Missile	NPO Mashinostroyeniya	Unlikely/Unknown	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)

Garpiya-3 (G3)	Unmanned Aerial Vehicle	Unknown	Likely	Yes	Telemetry hijack, backdoors, malware injection
DLE30 engines	Aircraft Engine	DLE (China)	Likely	Possible	Engine control manipulation, ECU override
DLE55 aircraft engines	Aircraft Engine	DLE (China)	Likely	Possible	Engine control manipulation, ECU override
DLE60 aircraft engines	Aircraft Engine	DLE (China)	Likely	Possible	Engine control manipulation, ECU override
DLE120 aircraft engines	Aircraft Engine	DLE (China)	Likely	Possible	Engine control manipulation, ECU override
Orlan-10 UAV microchips	UAV Microelectronics	Various (including Chinese suppliers)	Likely	Yes	Telemetry hijack, backdoors, malware injection

* Weapons and technology are composed on the basis of the "Advanced military technology in Russia" report[23]

** Both, military-grade chips and COTS components

The chart below illustrates an assessment of 35 Russian military and dual-use platforms incorporating Chinese-made COTS microelectronics from the table above. Of these, 45.7% were assessed as possibly vulnerable to remote access, reflecting likely exposure through insecure firmware, compromised hardware, or exploitable communication protocols. An additional 22.9% were confirmed to contain components previously identified as remotely accessible or compromised. In contrast, only 2.9% were deemed unlikely to be vulnerable, while 28.6% remain unclassified due to insufficient technical data. The findings suggest that a significant proportion of Russian systems carry embedded cyber risks stemming from their reliance on unverified or foreign-sourced electronics.



[23] Bendett, Samuel, Katarina Kertysova, and Roger McDermott. *Advanced Military Technology in Russia: Capabilities and Implications*. London: Chatham House, September 23, 2021. https://www.chathamhouse.org/sites/default/files/2021-09/2021-09-23-advanced-military-technology-in-russia-bendett-et-al.pdf

Chinese semiconductor manufacturers such as SMIC (Semiconductor Manufacturing International Corporation) and Hua Hong produce microchips in the 28 to 65 nanometre range, which is more than sufficient for many military-grade systems.[24][25] These chips include microcontrollers (MCUs), EEPROM and flash memory, power management ICs, digital signal processors (DSPs), and basic logic chips. Such components are well-suited for supporting functions like inertial navigation, flight control processing, data handling, and telemetry—essential capabilities in missile systems.

While there is no confirmed open-source evidence that Chinese-manufactured chips have been recovered directly from a russian weapons, there is precedent in closely related systems. The Kinzhal missile, for example, shares significant architectural and subsystem similarities with the Iskander-M ballistic missile, which has been documented by Ukrainian and Western investigators to contain Chinese-origin microchips.[26][27] These include components marked with Chinese characters and prefixes, and some reportedly originating from Nanjing-based manufacturers.

Conclusion

There is no publicly available technical information on the specific chips used in Russia's weapons systems. Nor is there accessible data on the types of chips being manufactured by China or transferred through customs and supply chains. Russia's Ministries of Trade, Economy and Federal State Statistics Service (ROSSTAT) have closed access to the relevant databases, and Chinese customs information related to chip exports to Russia is opaque. Information on compromised chips is also absent from the public domain and is unlikely to be disclosed due to the sensitivity of the subject. Additionally, technical research into how dual-use chips may be compromised or exploited remains limited and largely speculative.

Yet. China manufactures a broad range of microchips that are technically suitable and very likely used in Russian missile systems such as Kinzhal and other so-called "super weapons," although these components are not custom-built for military applications. The assertion that Chinese COTS components are integrated into Russia's arsenal is a logical and well-supported inference. However, without verified teardowns of each individual weapon model confirming the presence of Chinese-made components, this remains an informed assumption rather than a confirmed fact.

China likely possesses extensive technical knowledge about Russian weapons systems, potentially including their locations. Given this, there is a possibility that chips supplied by China could be compromised — designed to disable the systems at a strategic moment or even allow external control.

---

[24] SemiWiki Forum. "China Fab Expansion: SMIC and Hua Hong." *SemiWiki*, February 17, 2025 https://semiwiki.com/forum/threads/china-fab-expansion-smic-and-hua-hong.22130/?utm_source=chatgpt.com

[25] DigiTimes. "SMIC, Hua Hong Expand Semiconductor IC Manufacturing Capacity with Equipment Arrivals in 2025." *DigiTimes*, February 17, 2025 https://www.digitimes.com/news/a20250217PD204/smic-hua-hong-semiconductor-ic-manufacturing-capacity-equipment-2025.html?utm_source=chatgpt.com

[26] McBeth, Ryan. "Chinese GPS Chips in Russian Weapons." *Substack*, February 2025 https://ryanmcbeth.substack.com/p/chinese-gps-chips-in-russian-weapons

[27] South China Morning Post. "Ukraine Bans Chinese Firms Accused of Helping Russia Make Missiles." *South China Morning Post*, February 5, 2025 https://www.scmp.com/news/world/russia-central-asia/article/3307132/ukraine-bans-chinese-firms-accused-helping-russia-make-missiles