The Emerging Strategic Nexus

Military, Technological, and Cyber Relations Between
China, Russia, Iran, and North Korea



Jeremy Makowski
Cyber Intelligence Expert (Crime, Warfare, Terrorism)

March 2026

Disclaimer **3**
1. Executive Summary **4**
2. Key Findings **5**
3. Analytical Framework **6**
4. Strategic Geopolitical Context of the Emerging Alignment **7**
5. Structural Drivers of Cooperation **8**
5.1 Shared Strategic Opposition to Western Dominance 8
5.2 Complementary Military Capabilities 9
5.3 Sanctions as an Incentive for Economic Cooperation 9
5.4 Growing Cooperation in Defense, Industry, and Technology 10
6. Bilateral Military Relations **11**
6.1 China - Russia 12
6.2 Russia - Iran 13
6.3 Russia - North Korea 14
6.4 China - Iran 15
6.5 China - North Korea 16
6.6 Iran - North Korea 16
7. Technological and Defense-Industrial Cooperation **17**
7.1 🇨🇳 China 18
7.2 🇷🇺 Russia 19
7.3 🇮🇷 Iran 20
7.4 🇰🇵 North Korea 21
8. Cyber Strategy, Capabilities, Operations, and Cooperation **22**
8.1 🇮🇷 Iran 23
8.2 🇨🇳 China 27
8.3 🇷🇺 Russia 31
8.4 🇰🇵 North Korea 36
9. Strategic Implications for International Security **39**
10. Conclusion **41**
11. About the Author **42**
12. References **43**

Disclaimer

This document is made freely available for informational purposes and to support a deeper understanding of the evolving dynamics of relations between China, Russia, Iran, and North Korea.

Reproduction of any part of this document, whether in whole or in part, must include proper attribution to the author and a clear reference to the original source.

Any commercial use of the content, in full or in part, is strictly prohibited without the express written consent of the author.

1. Executive Summary

Over the past two decades, interactions among the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of Korea have evolved from largely transactional exchanges into a more structured pattern of strategic coordination. This alignment does not constitute a formal alliance comparable to NATO or historical bloc structures. However, it increasingly functions as a flexible and adaptive network of cooperation across military, technological, economic, and cyber domains.

This evolution has accelerated significantly since Russia's full-scale invasion of Ukraine in February 2022. Facing sustained military pressure and unprecedented sanctions from the United States, the European Union, and their partners, Russia has expanded its reliance on non-Western actors. In this context, Iran and North Korea have emerged as key providers of military materiel, including unmanned systems and artillery ammunition, while China has played a central role in sustaining economic stability and providing access to dual-use supply chains.

U.S. Department of Defense (DoD) and allied assessments indicate that these interactions are not isolated transactions, but part of a broader pattern of incremental integration under pressure. Rather than forming a unified alliance, these states are developing a distributed system of cooperation that enhances their collective resilience while preserving strategic autonomy.

In parallel, all four states have expanded their cyber capabilities as core instruments of national power. While there is limited public evidence of fully coordinated joint cyber operations, their activities converge in effect, creating a persistent, multi-vector threat environment targeting government, defense, and critical infrastructure networks. This convergence increases operational complexity for defenders, even in the absence of formal coordination.

The concept of a "strategic nexus" provides a more accurate analytical framework than traditional alliance models. It reflects a system of overlapping bilateral relationships, asymmetric dependencies, and selective exchanges of capabilities. China provides industrial scale and technological depth; Russia contributes military expertise and operational experience; Iran offers cost-effective drone and missile capabilities; and North Korea supplies munitions and cyber-enabled financial mechanisms.

This network does not eliminate internal constraints or asymmetries. Cooperation remains uneven, pragmatic, and shaped by national priorities. However, its cumulative effect is strategically significant. It enables sustained military operations under sanctions, facilitates the diffusion of military technologies, and reduces the effectiveness of traditional containment mechanisms.

The primary risk is not immediate alliance formation, but gradual structural consolidation. Over time, this nexus increases the likelihood of overlapping crises across multiple regions, complicates deterrence, and challenges the ability of Western states to manage conflicts within geographically bounded frameworks.

2. Key Findings

- **From Transactional to Structured Alignment:** China, Russia, Iran, and North Korea have moved beyond opportunistic exchanges toward more durable, though still uneven, defense-industrial and strategic cooperation. This remains a loose alignment, not a formal alliance.

- **China-Centered Asymmetric Interdependence:** China serves as the principal economic and industrial enabler within the network, especially through trade scale and dual-use supply capacity, though dependence remains uneven across sectors and partners.

- **Conditional Military-Technical Reciprocity:** Cooperation is increasingly reciprocal but imbalanced: Iran and North Korea provide Russia with munitions, drones, missiles, and personnel support, while Russia appears to provide selective technical and military assistance in return.

- **Parallel Rather Than Integrated Cyber Pressure:** State-linked cyber actors from all four countries sustain pressure on Western government, defense, and infrastructure networks. Their activities converge in effect, but public evidence for fully coordinated joint cyber operations remains limited.

- **Partial but Costly Sanctions Adaptation:** Alternative financial, logistical, and procurement channels reduce some sanctions pressure, but they remain fragmented, less efficient, and dependent on intermediaries.

- **Growing Multi-Theater Security Risk:** The alignment increases the risk of overlapping crises across Europe, the Middle East, and the Indo-Pacific, complicating deterrence and stretching Western planning even without formal escalation coordination.

3. Analytical Framework

Analyzing the relationships among China, Russia, Iran, and North Korea requires a framework that moves beyond traditional alliance models. These states do not operate within a unified command structure, nor do they share binding collective defense obligations. Instead, their interactions are best understood as a strategic nexus: a flexible network of bilateral and selective multilateral relationships driven by converging interests rather than formal commitments. This framework captures three key dimensions of interaction.

The first concerns military relations, including arms transfers, joint exercises, and military-technical cooperation. Available evidence, including U.S. Department of Defense reporting, satellite imagery, and open-source intelligence, indicates a clear expansion of these activities over the past decade, with significant acceleration since 2022. However, the depth and operational relevance of cooperation vary significantly across bilateral pairings.

The second dimension focuses on technological and defense-industrial interaction. Modern military capabilities depend on access to advanced components, manufacturing capacity, and innovation ecosystems. Under conditions of sanctions and export controls, these states have increasingly relied on a combination of domestic production and external procurement networks. This has led to the emergence of distributed supply chains and shared technological pathways, particularly in dual-use sectors.

The third dimension examines cyber capabilities and operations. China, Russia, Iran, and North Korea each maintain advanced cyber programs integrated into broader national security strategies. While public evidence supports patterns of parallel development, indirect facilitation, and shared operational practices, there is limited confirmation of fully coordinated joint operations across all four states. As a result, cyber interaction is best understood as strategic convergence rather than operational integration.

A central feature of this nexus is asymmetry. China possesses the largest industrial and technological base; Russia retains advanced military and nuclear capabilities; Iran specializes in cost-effective asymmetric systems, particularly UAVs and missiles; and North Korea combines missile development with cyber-enabled revenue generation. These asymmetries create incentives for selective cooperation, allowing each actor to compensate for specific weaknesses while leveraging comparative advantages.

External pressure is a key driver of this alignment. Although the scale and nature of constraints differ, all four states face varying degrees of Western sanctions, export controls, or technological restrictions. These pressures do not simply isolate them; instead, they incentivize the development of alternative mechanisms for trade, procurement, and technological exchange.

The strategic significance of this nexus lies in its adaptability. Unlike formal alliances, it does not require political cohesion or institutional integration. Its flexibility allows it to evolve incrementally, making it more difficult to counter through traditional deterrence or containment strategies.

4. Strategic Geopolitical Context of the Emerging Alignment

The strengthening of relations among China, Russia, Iran, and North Korea must be understood within the broader context of the international system's transformation. Since the end of the Cold War, the global order has been largely dominated by the United States, but this balance has begun to change. Over the past two decades, the rise of China as a major economic and military power, the reassertion of Russia as a geopolitical actor, and the growing willingness of regional powers such as Iran to challenge Western influence have significantly altered the global distribution of power. In this evolving geopolitical environment, these four states are increasingly converging around a shared objective: reducing Western strategic dominance and reshaping certain aspects of the international order to better reflect their political and security interests. One of the key factors accelerating this convergence has been the deterioration of diplomatic relations between Russia and Western countries. Tensions increased significantly after Russia’s annexation of Crimea in 2014 and intensified further following the large-scale invasion of Ukraine in February 2022. In response, Western governments imposed severe economic sanctions on Russia.

These sanctions targeted Russian financial institutions' access to advanced technologies, defense industries, and energy exports. As a result, Russia’s access to Western financial markets and high-technology sectors became significantly restricted. Facing growing economic isolation from Western markets, Moscow increasingly turned to non-Western partners for economic, technological, and military cooperation. In this context, Iran has become an important partner for Russia. Having long operated under significant Western sanctions, Iran has developed significant experience in sanctions evasion, defense industrial self-reliance, and asymmetric military capabilities. Beginning in 2022, Russia started deploying large numbers of Iranian-designed Shahed-136 loitering munitions against Ukrainian energy infrastructure.

These drones, which combine relatively low production costs with long operational ranges, have become a central component of Russia's strategy of sustained strikes against critical infrastructure. Russian defense factories later began producing localized versions of these systems, reflecting deeper technological cooperation and growing industrial integration between the two countries.

North Korea has also become an increasingly important partner in Russia's wartime strategy. According to Western intelligence services, Pyongyang has supplied Russia with large quantities of artillery ammunition, including 122 mm and 152 mm shells compatible with Soviet-designed artillery systems widely used by Russian forces in Ukraine. North Korea is also believed to have transferred short-range ballistic missiles that can be used against battlefield targets. These deliveries have allowed Russia to maintain a high tempo of artillery fire along the Ukrainian front lines, where artillery remains a decisive factor in the war of attrition. In return, North Korea is believed to be seeking Russian assistance in several strategic sectors, including satellite technology, missile guidance systems, and potentially the development of nuclear-powered submarines. These exchanges illustrate the increasingly transactional and mutually beneficial nature of military cooperation within this emerging network.

At the same time, the strategic relationship between China and Russia has expanded significantly across multiple domains. Although China has avoided direct military involvement in the war in Ukraine, it has provided substantial economic support that has helped stabilize the Russian economy under sanctions pressure. China has become Russia's largest trading partner, particularly through increased imports of discounted Russian oil and natural gas. This economic cooperation has helped mitigate the impact of Western sanctions and further strengthened the strategic partnership between the two countries.

5. Structural Drivers of Cooperation

5.1 Shared Strategic Opposition to Western Dominance

A central structural driver of cooperation among China, Russia, Iran, and North Korea is their shared perception that the current international system constrains their long-term strategic ambitions. Each of these states views the existing order, characterized by Western economic institutions, U.S. military alliances, and the dominance of Western technological ecosystems, as limiting their ability to exercise political autonomy and regional influence. While their political systems and geopolitical priorities differ, they converge around a common objective: reducing their vulnerability to Western pressure and expanding their strategic freedom of action. Cooperation, therefore, serves as a mechanism to collectively mitigate the effects of diplomatic isolation, economic restrictions, and military containment.

Through diplomatic coordination in international organizations, coordinated messaging on sovereignty and non-interference, and practical collaboration in defense and technology sectors, these states increasingly frame their partnership as a form of strategic balancing against what they perceive as Western structural dominance in global governance.

5.2 Complementary Military Capabilities

Another important driver of this alignment lies in the complementary nature of the four countries' military capabilities and defense-industrial ecosystems. Rather than duplicating capabilities, their cooperation allows each state to compensate for specific weaknesses while leveraging its comparative advantages. China possesses a highly advanced industrial base capable of producing sophisticated electronics, sensors, and large-scale military platforms. Russia maintains extensive expertise in advanced weapons design, including air defense systems, nuclear technologies, and high-end missile systems. Iran has developed cost-effective drone platforms, missile systems, and asymmetric warfare capabilities that are particularly suited for prolonged conflicts and proxy warfare. North Korea, meanwhile, maintains one of the world's largest artillery production capacities and has rapidly advanced its ballistic missile development. When viewed collectively, these capabilities create opportunities for mutually reinforcing exchanges in which industrial capacity, technological expertise, and battlefield-tested systems can be combined to enhance overall military resilience. This complementary structure reduces dependence on Western defense supply chains and strengthens each state's ability to sustain military operations under conditions of international isolation.

5.3 Sanctions as an Incentive for Economic Cooperation

Western sanctions and technological restrictions have played a significant role in shaping patterns of cooperation among these states, although their scope and impact vary considerably across cases. Russia, Iran, and North Korea are subject to extensive sanctions regimes affecting finance, trade, and access to advanced technologies. China, while not subject to comparable comprehensive sanctions, faces targeted export controls, entity designations, and increasingly restrictive access to advanced semiconductor technologies and sensitive industrial inputs.

These pressures have encouraged the development of alternative economic and procurement mechanisms. Reporting from government agencies and sanctions authorities indicates the emergence of networks involving intermediary companies, re-export hubs, and non-dollar financial arrangements designed to mitigate restrictions.

Within this context, cooperation among China, Russia, Iran, and North Korea offers practical pathways to sustain economic and technological exchanges. China's large industrial and commercial ecosystem plays a particularly important role in global supply chains, while Russia and Iran have expanded the use of alternative settlement systems and local currency trade. North Korea, in turn, relies on a combination of covert procurement networks and cyber-enabled revenue generation.

Rather than eliminating interdependence, external pressure has contributed to the gradual formation of parallel mechanisms that support continued interaction, albeit at a higher cost and lower efficiency than pre-sanctions systems.

5.4 Growing Cooperation in Defense, Industry, and Technology

Finally, the convergence of defense-industrial interests has generated new incentives for technological collaboration. As Western export controls limit access to advanced components and manufacturing technologies, these countries have intensified efforts to develop alternative innovation pathways through joint research, technology transfers, and co-production arrangements. Cooperation has been particularly visible in areas such as unmanned aerial systems, missile technologies, and cyber capabilities domains, where relatively modest investments can generate significant strategic effects. For example, drone technology developed by Iran has demonstrated operational effectiveness in modern conflicts, while Russia contributes experience in large-scale military integration and weapons engineering. China provides advanced electronics, industrial manufacturing capacity, and access to complex supply chains, while North Korea contributes expertise in missile testing and rapid weapons iteration.

These interactions create a form of distributed defense innovation in which technological improvements achieved by one partner can be adapted and replicated by others. Over time, this process contributes to the gradual emergence of a loosely interconnected defense-industrial ecosystem capable of sustaining military modernization despite Western states' technological containment efforts.

6. Bilateral Military Relations

The bilateral military relationships linking China, Russia, Iran, and North Korea are not uniform. They differ significantly in depth, visibility, and operational relevance. Some are increasingly institutionalized and publicly demonstrated through joint exercises, coordinated patrols, and formal agreements, while others remain more limited in scope, less visible, or focused on specific forms of military or technical cooperation.

The most developed and operationally significant relationships within this grouping are China-Russia, Russia-Iran, and Russia-North Korea. China and Russia maintain a sustained pattern of joint air and naval operations and strategic coordination, making their military relationship the most visible. Russia and Iran have deepened cooperation in the context of the war in Ukraine, particularly through the transfer and use of Iranian unmanned aerial systems and related technologies. Russia and North Korea have moved further toward an overt defense relationship, including arms transfers and a formal mutual defense agreement signed in 2024.

By contrast, China-Iran, China-North Korea, and Iran-North Korea remain more constrained. China-Iran military cooperation exists but is limited in scale and carefully managed, including occasional joint naval exercises. China-North Korea ties are shaped primarily by political alignment and a longstanding treaty framework, with relatively limited visible joint military activity in recent years. Iran-North Korea relations are difficult to assess due to their opacity; while there are longstanding concerns about past military-technical exchanges, there is limited publicly verified evidence of ongoing structured military cooperation. A key analytical point is that these relationships do not constitute a unified or integrated alliance system. Instead, they form a network of overlapping bilateral ties with distinct strategic purposes. China and Russia emphasize strategic signaling and operational coordination; Russia-Iran and Russia-North Korea ties have become more directly linked to ongoing conflict dynamics; and the remaining relationships operate in narrower or more cautious frameworks (Figure 1).



Figure 1 - Overview of the Military cooperation between China, Russia, Iran and North Korea

6.1 China - Russia

The military relationship between China and Russia stands out as the most substantial and consistently observable among the six cooperation pairings, despite falling short of a formal alliance. In recent years, the two countries have developed a steady pattern of joint operations spanning both naval and air domains. This includes regular naval exercises in the Pacific and surrounding East Asian waters, as well as coordinated strategic bomber patrols. These activities are not sporadic demonstrations, but part of a sustained effort to showcase growing operational coordination across multiple theaters.

In the maritime domain, joint exercises have included live-fire drills and coordinated patrols spanning the South China Sea, the Sea of Japan, and the broader Pacific. The participation of Chinese forces in large-scale Russian exercises further indicates a willingness to operate together beyond strictly bilateral formats. In the air domain, joint bomber patrols, particularly those conducted near Alaska, have extended this cooperation into strategically sensitive regions. These missions remain within international airspace but carry clear signaling value.

The military significance of this relationship lies in its cumulative effect. Repeated exercises enhance coordination at the level of planning, communications, and sequencing, even if the two militaries are not integrated to alliance standards. At the same time, these activities serve a deterrent and signaling function toward the United States and its allies in both Europe and the Indo-Pacific. Importantly, there is still no mutual defense treaty, and China has not participated in Russia's war in Ukraine as a combatant. The relationship is therefore best understood as a high-end strategic partnership with growing operational depth, but not a warfighting alliance.

6.2 Russia - Iran

Russia-Iran military relations have become among the most consequential in practice, primarily because of their direct relevance to ongoing conflict dynamics. The core of the relationship lies in military-technical cooperation, particularly in unmanned aerial systems. U.S. and allied assessments indicate that Iran has supplied Russia with large numbers of one-way attack UAVs, in the style of HESA Shahed 136 Gen 2 (Figure 2) used extensively in Ukraine. These systems have been integrated into Russia's strike campaign against critical infrastructure. Beyond transfers of finished systems, reporting also suggests the development of local production capacity in Russia with Iranian support, indicating a deeper level of industrial and technological interaction.

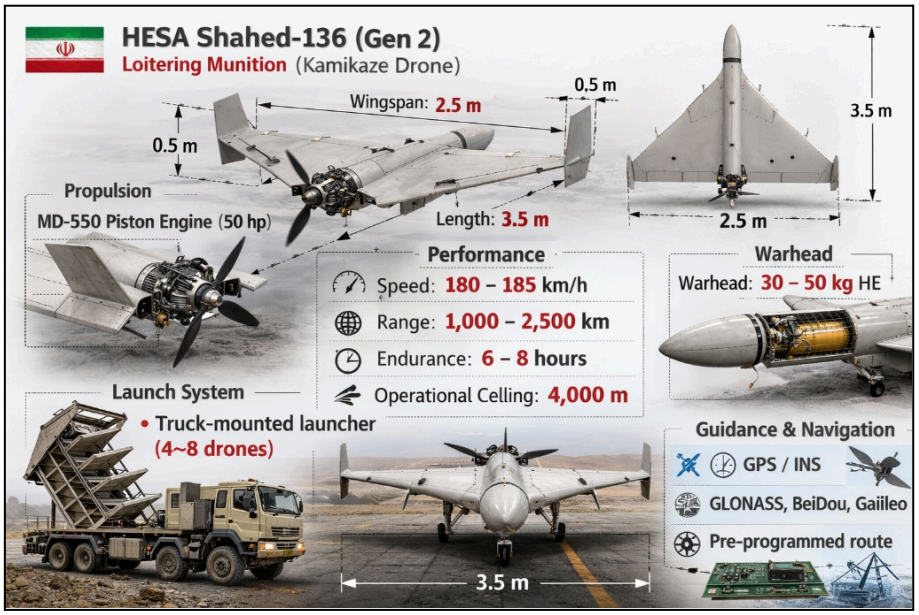


Figure 2 - Overview and specifications of Iranian HESA Shahed 136 Gen 2

In 2016, Russia completed the delivery of S-300PMU-2 "Favorit" surface-to-air missile systems to Iran (Figure 3). Additionally, according to the US Department of Defense, Iran transferred short-range ballistic missiles to Russia in 2024. While several governments publicly confirmed these transfers, some operational details, including deployment patterns and associated systems, remained less clearly established in initial reporting.



Figure 3 - Overview and specifications of Russian S-300PMU-2 "Favorit" surface-to-air missile

What distinguishes this relationship is the combination of battlefield utility and emerging industrial cooperation. Iran is not only a supplier of systems, but also a contributor to Russia's ability to sustain and scale production under sanctions constraints. At the same time, the relationship should not be overstated. As of early 2026, there is no verified open-source evidence that Russia has entered Middle Eastern conflicts militarily on Iran's behalf. The partnership remains highly significant but is primarily defined by wartime support to Russia rather than a broader alliance structure.

6.3 Russia - North Korea

Russia-North Korea military relations have undergone the most dramatic transformation and now represent the closest approximation to a wartime quasi-alliance in this group. The relationship is anchored in a formal treaty signed in 2024, which includes a mutual defense commitment. This marks a clear shift from past decades, when cooperation was more limited and episodic.

Beyond the treaty, the most important development is the scale of North Korea's material support to Russia. Public reporting indicates that Pyongyang has supplied large quantities of artillery ammunition and other military materiel, with estimates suggesting millions of rounds. There is also documented evidence linking North Korean missile systems to strikes in Ukraine, providing rare, concrete confirmation of battlefield use.

The relationship has gone further with reported North Korean military troop deployments to Russia. U.S. and allied officials have stated that North Korean personnel have been trained and deployed in support of Russian operations, marking a significant escalation from indirect support to direct involvement. At the same time, there is evidence that Russia is providing North Korea with military technology and assistance, indicating a reciprocal exchange.

This combination-formal treaty, large-scale arms transfers, missile use, and troop deployment make Russia-North Korea the most operationally consequential and immediate security concern among the six pairings. While some details remain opaque, the available evidence is strong enough to conclude that this is a major and active military relationship with implications for both European and East Asian security.

6.4 China - Iran

China-Iran military relations are real but remain deliberately limited and carefully calibrated. The most visible dimension is maritime cooperation, including joint naval exercises conducted with Russia in the Gulf of Oman. These activities serve a signaling function and reflect shared interests in regional stability and maritime security, particularly in areas linked to energy flows. Beyond exercises, the relationship includes documented concerns regarding procurement networks linked to Iran's missile and UAV programs. Sanctions designations by U.S. authorities have identified entities based in China connected to the supply of dual-use materials and components to Iranian defense-industrial actors. There have also been reports that Iran is seeking to acquire advanced Chinese anti-ship missile systems. As of early 2026, these should be treated as prospective or reported negotiations rather than confirmed transfers.

Overall, China appears to approach military cooperation with Iran cautiously. While Beijing values Iran strategically, particularly for energy security and regional influence, it has avoided deep military integration that could increase the risk of direct confrontation with the United States or its partners. The relationship is therefore best understood as selective and pragmatic rather than alliance-driven.

6.5 China - North Korea

China-North Korea military relations are structurally significant but operationally less visible than other pairings. The two countries are bound by a longstanding treaty that commits them to provide military assistance in the event of an attack. This formal framework gives the relationship enduring importance in any contingency on the Korean Peninsula.

However, current open-source evidence indicates relatively limited observable military cooperation, including joint exercises, deployments, or arms transfers. Instead, the relationship is expressed primarily through political support, economic engagement, and infrastructure development. China continues to play a central role in North Korea's external environment, particularly through trade and connectivity.

The military significance of this relationship lies in its role in deterrence and strategic ambiguity. The existence of the treaty means that any crisis involving North Korea inherently carries the risk of Chinese involvement, even if Beijing prefers to avoid escalation. Compared to North Korea's increasingly active military relationship with Russia, its military engagement with China appears more restrained and less operationally focused

6.6 Iran - North Korea

Iran-North Korea military relations are the least visible but remain important, given their focus on missile and proliferation-related cooperation. The most solid publicly documented evidence comes from United Nations reporting indicating that the two countries have cooperated on long-range missile development, including the transfer of components and the provision of technical support.

This relationship is not characterized by joint exercises, formal treaties, or visible operational coordination. Instead, it is best understood as a long-term, low-visibility exchange centered on missile technology and expertise. Both countries are heavily sanctioned and share incentives to collaborate in ways that bypass international controls.

Recent open-source reports provide fewer concrete details about ongoing transfers compared to earlier periods, and there is no strong public evidence of expanded military cooperation in the 2024-2026 timeframe. Political alignment and rhetorical support exist, including North Korean backing of Iran in the current Middle East crisis, but this does not constitute proof of active military assistance. As a result, Iran-North Korea should be treated as a proliferation-focused relationship with potentially significant long-term implications, but limited visible operational activity.

7. Technological and Defense-Industrial Cooperation

Defense technology and industrial capabilities are a fundamental pillar of modern military power, determining not only the performance of weapons systems but also the sustainability and adaptability of armed forces in conflict situations. In a context increasingly marked by export controls on weapons systems and technological intelligence, sanctions regimes, strategic competition, and access to advanced technologies, access has become both a vulnerability and a lever of influence. States are therefore compelled to find a balance between domestic innovation and external procurement, often operating within complex transnational networks that blur the lines between the civilian and military sectors. Understanding these dynamics is essential for assessing how military capabilities are generated, maintained, and adapted over time (Figure 4).

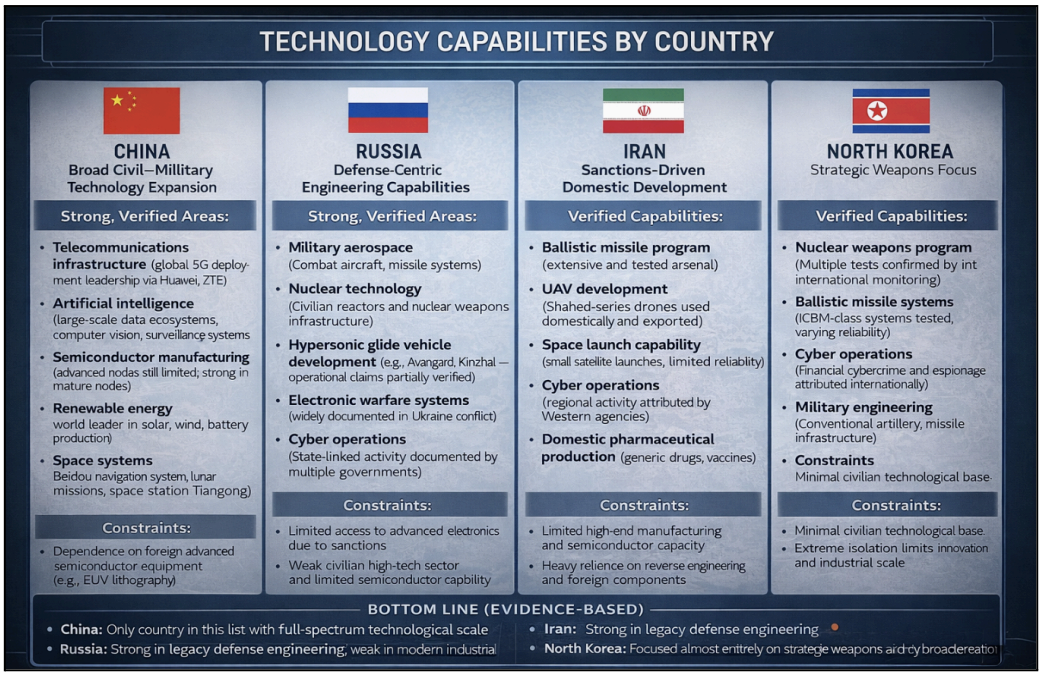


Figure 4 - Overview of the technology capabilities of China, Russia, Iran and North Korea

7.1 🇨🇳 China

Support Networks

China's technological and defense-industrial system is characterized by deep integration between civilian innovation and military requirements, driven by its state-led military-civil fusion strategy. Official U.S. Department of Defense reporting confirms that this approach enables the People's Liberation Army (PLA) to draw from a wide ecosystem of universities, private technology firms, and state-owned enterprises. This integration is particularly visible in high-technology sectors such as microelectronics, artificial intelligence, aerospace engineering, and advanced manufacturing. China's large domestic industrial base reduces reliance on foreign inputs in many areas, although external technology acquisition remains a stated objective in official reporting.

Procurement and Evasion

China itself is not under broad multilateral sanctions, but verified U.S. government actions show that Chinese-based entities have been repeatedly designated for supporting foreign military-industrial programs. Since 2024, U.S. authorities have identified PRC- and Hong Kong-based firms supplying dual-use components, including microelectronics, sensors, and machine tools, to Russia's defense sector. Additionally, U.S. sanctions reporting confirms the involvement of Chinese-based intermediaries in procurement networks linked to Iranian UAV programs and North Korean missile and space activities. These cases demonstrate the role of commercial supply chains and trading companies in facilitating cross-border access to sensitive technologies.

Missiles and Drones

China possesses a highly developed and largely self-sufficient missile and UAV ecosystem. Verified U.S. defense reporting highlights continued advancements in precision-strike capabilities, hypersonic systems, and unmanned platforms.

Technological strengths include:

- Advanced missile guidance and propulsion systems
- Integration of UAVs into joint military operations
- Use of AI and data systems to enhance targeting and autonomy

These capabilities are supported by major state-owned defense companies and a broad domestic R&D infrastructure, reducing dependence on foreign wartime supply.

7.2 🇷🇺 Russia

Support Networks

Russia maintains a significant but constrained defense-industrial base, with verified reliance on both domestic production and foreign-sourced dual-use technologies. Sanctions reporting from the United States and its partners confirms that Russia continues to depend on imported microelectronics, semiconductors, and precision manufacturing equipment for advanced weapons systems. The technological bottleneck is most evident in areas such as high-performance chips, sensors, and CNC machine tools, which are critical for modern missile systems and UAV production.

Procurement and Evasion

Russia has established sophisticated procurement networks to obtain restricted technologies despite international sanctions. Verified reporting from the U.S. Department of the Treasury and the Department of State confirms the systematic use of third-country intermediaries and front companies to facilitate the acquisition of controlled goods. These networks operate across multiple jurisdictions, leveraging legitimate commercial trade channels alongside alternative financial mechanisms to evade detection and compliance controls. Their key characteristics include:

- Reliance on intermediary firms based in jurisdictions with limited or inconsistent sanctions enforcement
- Targeted acquisition of items listed on the Common High Priority List, including microelectronics and integrated circuits
- Use of re-export and transshipment practices to conceal the final military end-users and intended applications

These mechanisms enable continued access to critical technological inputs despite export controls.

Missiles and Drones

Russia continues to produce advanced missile systems and expand UAV capabilities, but verified reporting confirms technological dependence on foreign components. U.S. Treasury actions in 2024 identified networks procuring sensitive electronics for reconnaissance drones and one-way attack UAVs. Additionally, official reporting confirms:

- Cooperation with Iran on the production of Iranian-designed UAVs in Russia
- Continued use of imported microelectronics in missile guidance systems

This indicates that while Russia retains strong design and engineering capabilities, parts of its production chain remain externally dependent.

7.3 🇮🇷 Iran

Support Networks

Iran's defense-industrial system is structured around state-controlled entities, including the Ministry of Defense and Armed Forces Logistics (MODAFL), the Defense Industries Organization, and the Islamic Revolutionary Guard Corps (IRGC). Verified sanctions reporting shows that these entities oversee a distributed network of research, production, and procurement units supporting missile and UAV programs. Technologically, Iran has developed domestic capabilities in areas such as UAV design, propulsion systems, and missile production, but these capabilities rely on externally sourced components and materials.

Procurement and Evasion

Iran relies heavily on international procurement networks to sustain its technological base. Verified U.S. Treasury actions from 2024 to 2026 document networks operating across Asia, the Middle East, and Europe to acquire restricted items. These networks typically focus on:

- Missile precursor chemicals (e.g., oxidizers and propellant inputs)
- UAV components such as engines, navigation systems, and electronics
- Manufacturing equipment and dual-use industrial machinery

Procurement is conducted through front companies, intermediaries, and deceptive shipping practices, as confirmed in multiple sanctions designations.

Missiles and Drones

Iran has established a robust missile and UAV development capability, with verified evidence of ongoing production and technological improvement. However, official reporting confirms continued reliance on imported inputs for key components and materials. Recent U.S. sanctions actions identified procurement of:

- Chemicals used in solid missile propellants
- UAV-related electronics and components

Additionally, verified reporting confirms cooperation with Russia in the financing and production of Iranian-designed one-way attack UAVs, demonstrating the export and scaling of Iranian drone technology.

7.4 🇰🇵 North Korea

Support Networks

North Korea's technological base for missile and WMD programs is supported by a combination of domestic military institutions and international support networks. United Nations reporting confirms that the DPRK uses overseas agents, foreign procurement facilitators, and covert commercial entities to sustain its programs. Due to limited domestic industrial capacity, these external networks play a critical role in acquiring technology, materials, and funding.

Procurement and Evasion

North Korea employs a wide range of verified sanctions evasion techniques to obtain restricted technologies. UN and U.S. reporting consistently identify methods such as the use of front companies, illicit shipping practices, and covert financial activity.

Technological procurement is supported by:

- Cyber operations generating revenue for weapons programs
- Overseas IT worker schemes used to funnel funds
- Foreign-based procurement agents acquiring components for missile and space programs

U.S. sanctions in 2024 and 2026 specifically targeted networks supporting DPRK missile-related procurement.

Missiles and Drones

North Korea continues to advance its ballistic missile capabilities, as consistently confirmed by UN reporting. Its missile program demonstrates ongoing development in propulsion, range, and delivery systems. In the UAV domain, verified information is more limited. Public reporting confirms:

- Testing and display of new unmanned aerial systems
- Establishment of dedicated UAV development structures

However, compared to its missile program, there is less verified information on the scale, performance, and technological maturity of North Korea's drone capabilities.

8. Cyber Strategy, Capabilities, Operations, and Cooperation

China, Russia, Iran, and North Korea have emerged as major actors in the cyber domain, each integrating cyber capabilities into broader national security strategies. Although their operational models and strategic priorities differ, all four states use cyber operations to pursue intelligence collection, disruption, influence, and, in some cases, financial gain.

Their activities span a wide spectrum, including espionage against government and industrial targets, disruption of critical infrastructure, influence operations, and financially motivated cyber campaigns. Over time, these actors have increased both the scale and sophistication of their operations, adapting to evolving technological environments and defensive measures. At the same time, elements of convergence can be observed. These include similarities in tactics, techniques, and procedures; overlapping targeting patterns; and, in some cases, the use of shared infrastructure or permissive operating environments. However, publicly available evidence more strongly supports parallel development, indirect facilitation, and strategic alignment than the existence of fully integrated or coordinated joint cyber operations among all four states (Figure 5).

As a result, the cyber dimension of this nexus is best understood as a loosely connected ecosystem characterized by adaptation, exposure to shared practices, and occasional enabling relationships rather than formalized operational cooperation.



Figure 5 - Overview of China, Russia, Iran, and North Korea cyber activities

8.1 🇮🇷 Iran

Strategic Overview

Iran uses cyber power as an asymmetric instrument of state policy. Its cyber activity is designed less to dominate the digital domain than to generate coercive effects at limited cost: protect the regime, collect intelligence, pressure adversaries, and retaliate below the threshold of open war. In practice, this produces a model centered on espionage, selective disruption, psychological effect, and deniable operations. The core logic is consistency rather than scale: Iran seeks to remain operationally relevant even when under military, economic, or diplomatic pressure.

As of March 2026, the current conflict environment has reinforced that pattern. Following the regional escalation that began on February 28, 2026, U.S. intelligence assessed that Iran-aligned cyber actors were likely to favor low-level but disruptive cyber activity, especially against U.S. and allied networks, while industry reporting identified a surge in state-aligned personas, hacktivist fronts, and coordinated disruptive messaging. This is significant because it shows Iran still prefers cyber effects that are politically usable, deniable, and scalable during a crisis, rather than relying only on high-end destructive operations.

Key Institutions and Operational Structure

The development of cyber agencies in Iran has been a strategic priority over the past two decades, driven by the country's desire to bolster national security, counter external threats, and assert its influence in cyberspace. Following increased cyber vulnerabilities and notable incidents such as the Stuxnet attack, Iran invested heavily in establishing and expanding state-controlled cyber institutions.

Central to this effort are organizations like the Islamic Revolutionary Guard Corps (IRGC) Cyber Command, the Supreme Council of Cyberspace (SCC), and the Passive Defense Organization, each playing a distinct role in shaping policy, conducting cyber operations, and securing digital infrastructure. These institutions reflect Iran’s shift toward a more coordinated and sophisticated approach to cyber power and include the following:

The Islamic Revolutionary Guard Corps (IRGC) is an elite military force fiercely loyal to Iran's Supreme Leader and maintains robust and multifaceted cyber capabilities distributed among its various subdivisions. The IRGC's cyber operations are primarily carried out by specialized units within the Basij Militia and the Qods Force, both of which are implicated in offensive and espionage cyber activities. These units orchestrate cyber intrusions targeting foreign governments, defense industries, academic institutions, and NGOs through techniques such as spear-phishing and sophisticated social engineering campaigns. Notable IRGC-linked cyber intrusion groups include:

- **APT35 (Charming Kitten, TA453, Cobalt Mirage):** A broad cluster of cyber espionage actors conducting targeted operations against diplomatic entities, dissidents, and journalists, using tailored phishing to gather intelligence and conduct influence operations.
- **APT42** is a subgroup of **APT35 t**hat focuses on individuals and organizations involved in policy research, human rights advocacy, and civil society. Its emphasis is on surveilling political opposition and international human rights bodies.
- **Nemesis Kitten:** Operating under contract through Iranian private companies like Afkar System and Najee Technologies, this group executes covert cyber operations supporting IRGC objectives, often engaging in espionage and digital sabotage.
- **Cotton Sandstorm (formerly NEPTUNIUM)**: A sophisticated IRGC-linked threat actor engaged in broad espionage campaigns targeting geopolitical adversaries and critical infrastructure.

Ministry of Intelligence and Security (MOIS) serves as Iran's primary foreign intelligence and internal surveillance agency, reporting directly to the president. Unlike the IRGC, MOIS is noted for a more technically sophisticated approach and a comparatively less ideologically driven operational style. MOIS's cyber activities emphasize targeted intrusions into critical sectors such as energy, telecommunications, maritime infrastructure, and government systems. Its cyber units are linked to several advanced persistent threat (APT) groups that conduct espionage, cyber reconnaissance, and sabotage:

- **MuddyWater:** Known for targeting Middle Eastern governments and telecommunications firms, this group conducts espionage through custom malware and credential theft.
- **OilRig (APT34):** Focuses on the energy sector and government organizations in the Middle East, leveraging phishing campaigns and credential harvesting to extract sensitive information.

- **Hexane:** Engages in cyber reconnaissance and espionage, often targeting telecommunications and infrastructure entities.

While MOIS and IRGC share overlapping mission scopes, MOIS's cyber operations focus more on technical exploitation and intelligence collection than on overt influence or ideological campaigns. The competition between the two agencies occasionally drives innovation and intensity in Iran's cyber warfare efforts.

Furthermore, Iran can count on several active hacktivist groups that, particularly in the current context, openly present themselves as ideologically aligned with the Iranian regime. Among the most important are groups such as Handala Hack Team, FAD Team, APT Iran, and Cyber Islamic Resistance. These groups are particularly active in the claim of launching Denial of Service (DDoS) attacks, hacking databases, and critical infrastructure with varying degrees of success (Figures 6 and 7),

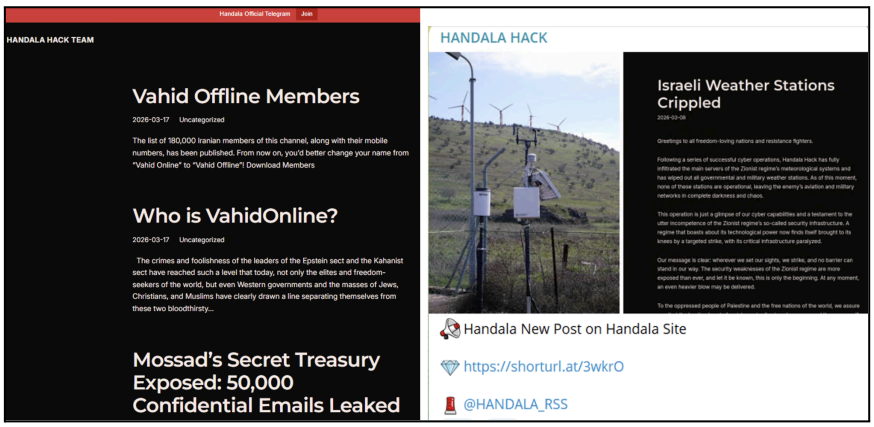


Figure 6 - Iranian Hacking group Handala Hack Team claims on their website and Telegram channel multiple hacking operations against Israeli targets



Figure 7 - A Telegram message from the hacktivist group Cyber Islamic Resistance claiming to launch a series of cyber attacks against what they call "Zionist Regime"

Operational Profile

Iran's most consistent strength is access operations built around people, identity, and weakly defended systems. It regularly combines spear-phishing, credential theft, impersonation, password spraying, cloud compromise, and front organizations. This approach is lower-cost than the Chinese model and less technically elaborate than the best Russian intelligence operations, but it is effective because it is persistent, targeted, and adaptable. Iran has also repeatedly preferred plausible deniability through aliases, fronts, and activist branding, allowing it to shape narratives while avoiding immediate attribution costs.

The latest conflict period also suggests that Iran increasingly treats cyber as part of a broader multi-domain coercion toolkit. The operational value is not only disruption itself, but also timing, symbolism, and psychological pressure. In that sense, Iranian cyber operations are best understood as a force multiplier for crisis behavior: they expand the pressure envelope, complicate response, and create strategic noise around military escalation.

Cooperation

Iran's cooperation with Russia includes elements of technical support and knowledge exchange within the broader defense and intelligence relationship. This includes exposure to Russian-developed surveillance, electronic warfare, and intelligence systems relevant to the development of cyber capabilities.

With China, cooperation is closely tied to infrastructure and technology transfer. Chinese firms have played a significant role in building Iran's telecommunications networks and digital architecture, including components used to monitor and filter internet traffic. This has strengthened Iran's ability to control and secure its domestic information space.

Iran's interaction with North Korea is most clearly observed in overlapping cyber tactics and operations, particularly in financially motivated cyber activity. Both countries have conducted cyber-enabled financial operations targeting cryptocurrency platforms and financial institutions, with documented similarities in tools, techniques, and procedures, indicating shared operational learning and adaptation.

8.2 🇨🇳 China

Strategic Overview

China's cyber strategy is the most systematic, state-integrated, and long-horizon of the four cases. Its purpose is not episodic retaliation, but the steady accumulation of advantage across national security, economic competition, military modernization, and political influence. Cyber operations support that broader architecture by enabling espionage, access persistence, infrastructure mapping, technology acquisition, and information control. China's model is therefore less about dramatic single events and more about durable strategic positioning inside critical systems.

What is most consequential in the current period is the convergence of telecom compromise, critical infrastructure pre-positioning, and global espionage on a scale. Operations associated with the Salt Typhoon and Volt Typhoon show that China is not only interested in collecting information, but also in gaining access at the network core and in sectors with strategic value in a crisis. That makes China's cyber posture more serious than a conventional espionage program: it increasingly blurs the line between intelligence collection and contingency preparation.

Key Institutions and Operational Structure

China's national cyber framework has evolved profoundly over the past two decades, transitioning from fragmented institutional efforts to a highly integrated system that combines military strength, civilian intelligence, and centralized policymaking. This development reflects Beijing's recognition of cyberspace as a critical domain for national security, economic resilience, and geopolitical competition. From early defensive measures to today's sophisticated offensive and intelligence capabilities, China has constructed a layered cyber apparatus involving multiple specialized agencies. These include newly established military units, such as the People's Liberation Army Cyberspace Force, long-standing civilian actors, such as the Ministry of State Security, and central coordinating bodies, such as the Central Cyberspace Affairs Commission. Each plays a distinct but interconnected role within a strategic architecture designed to assert cyber sovereignty, shape global norms, and project digital power. The following sections will examine each of these entities in detail, tracing their origins, functions, and contributions to China's comprehensive cyber strategy.

People's Liberation Army (PLA) Cyberspace Force was established in April 2024, and is the primary military body responsible for China's cyber warfare. Operating under the Central Military Commission, it replaced the former Network Systems Department of the PLA Strategic Support Force. Its responsibilities include offensive cyber operations, network defense, cyber reconnaissance, and integrating electronic warfare into the broader PLA strategy.

- **Offensive Operations Division.** This unit is tasked with launching cyberattacks against foreign military networks and critical infrastructure. It is central to China's ability to disrupt adversarial command systems, gather battlefield intelligence, and execute strategic deterrence in cyberspace.
- **The Cyber Defense Division** is responsible for securing the PLA's information infrastructure. This unit focuses on hardening military networks against intrusions, malware, and data exfiltration attempts. It also develops defensive tools and conducts threat hunting within PLA systems.
- **Cyber Intelligence Division** conducts reconnaissance operations, including cyber surveillance and digital espionage. It collects information on adversary capabilities and supports PLA strategic planning with real-time threat data.
- **The Electronic Warfare Division** integrates cyber capabilities with electronic warfare; this unit targets satellite communications, radar systems, and battlefield sensors to disrupt the enemy's communication systems.
- **PLA Unit 61398 (APT1 / Comment Crew): One of the most extensively documented PLA cyber-espionage** units, conducted large-scale intrusions primarily targeting Western corporations for intellectual property theft.
- **PLA Unit 61486 (APT2 / Putter Panda) engaged** in cyber espionage operations focused on defense, aerospace, and satellite communications sectors.

The Ministry of State Security (MSS) serves as China's civilian intelligence service and oversees the nation's covert cyber-espionage and counterintelligence campaigns. Its cyber operations are primarily conducted through the 13th Bureau and regional cyber units. The MSS maintains deep ties with contractors, universities, and front companies to expand its technical capabilities.

- **13th Bureau (CNITSEC)** is the China Information Technology Security Evaluation Center, which acts as the cyber headquarters within the MSS. Officially responsible for national cybersecurity evaluation, it covertly runs cyber-espionage campaigns, manages malware development, and exploits software vulnerabilities to collect intelligence.
- **Provincial MSS Cyber Units** are distributed across China's provinces and conduct tailored Advanced Persistent Threat (APT) operations. They often focus on regional or sector-specific targets and collaborate with local tech talent or companies under MSS direction.
- **The Chinese National Vulnerability Database (CNNVD)** is administered by CNITSEC. CNNVD is China's equivalent of a national CVE system. However, it has been caught delaying disclosure of vulnerabilities to allow MSS teams time to exploit them in the wild, turning a supposed defense database into an offensive tool.
- **APT10 (Stone Panda / Red Apollo)** conducts large-scale cyber espionage campaigns, notably compromising managed service providers (MSPs) to enable global access to downstream corporate networks and facilitate systematic intellectual property theft
- **APT27 (Emissary Panda/ LuckyMouse)** executes sustained espionage operations targeting government, defense, and critical infrastructure networks, with a focus on long-term access and intelligence collection
- **APT40 (Leviathan/TEMP.Periscope)** Specializes in maritime and geopolitical intelligence collection, targeting naval, shipping, and research entities aligned with South China Sea strategic interests (linked to Hainan MSS)
- **APT41 (Winnti / Double Dragon)** conducts dual-purpose operations combining state-sponsored espionage with financially motivated activity, including supply chain compromises and global intrusions across multiple sectors
- **APT5 (Keyhole Panda)** focuses on telecommunications and satellite sectors, leveraging stealthy, long-term persistence to enable strategic intelligence collection
- **APT15 (Ke3chang / Vixen Panda)** engages in diplomatic and governmental espionage across Europe, Asia, and Africa, emphasizing credential theft and sustained network access

Operational Profile

China's cyber operations are best understood as a three-tier system. The first tier is classic strategic espionage against governments, defense, research, and technology targets. The second is the compromise of telecommunications and core network environments, which provides wide intelligence reach across multiple downstream users and sectors. The third is pre-positioning in critical infrastructure, where access may have intelligence value in peacetime but could also provide options during a crisis or conflict. This layered model is what distinguishes China from the other three states examined here: access is built not simply to steal, but to shape the strategic environment over time.

The January 2026 reporting on compromise of email systems used by staff connected to key U.S. House committees further illustrates the operational logic of Chinese cyber activity: target nodes where policy, oversight, and national security decision-making intersect. This is not opportunistic cybercrime; it is selective access collection aligned with state priorities.

Cooperation

China's cyber cooperation with Russia is formalized through bilateral agreements on information security, including a 2015 cooperation agreement covering information security and cybercrime. This includes exchanges between national computer emergency response teams (CERTs), law enforcement collaboration, and joint exercises under multilateral frameworks such as the SCO. Both countries also coordinate positions in international forums on cyber governance and norms.

With Iran, cooperation is part of a broader long-term strategic partnership. This includes development of telecommunications infrastructure, digital networks, and surveillance technologies by Chinese companies operating in Iran. These activities contribute directly to Iran's domestic cyber capabilities, particularly in monitoring, control, and data management systems.

China's interaction with North Korea includes documented instances of North Korean cyber operations being conducted from Chinese territory or using Chinese infrastructure, particularly in earlier periods. While this does not constitute formal joint operations, it has provided operational access and connectivity that enabled North Korean cyber activity.

8.3 🇷🇺 Russia

Strategic Overview

Russia's cyber strategy remains embedded in the wider doctrine of information confrontation. Cyber is not treated as a self-contained domain, but as one component of a broader state toolkit that includes espionage, sabotage, disinformation, psychological pressure, and operational support to military and intelligence objectives. The Russian model is therefore distinguished less by technical novelty alone than by its integration into a continuous campaign logic: compromise, monitor, shape, disrupt, and exploit. Since the war against Ukraine, Russia's cyber activity has shown a clear operational pattern. It has continued to target Ukraine directly, while also focusing on the wider ecosystem, enabling support for Kyiv, especially logistics providers, technology companies, government institutions, and policy networks in Europe and North America.

This demonstrates that Russian cyber strategy is not confined to battlefield support; it aims to stress the external support architecture around its main geopolitical confrontation.

Key Institutions and Operational Structure

Over the years, Russia has progressively integrated cyber capabilities into its national security framework, recognizing cyberspace as a critical domain for both defense and strategic influence. This integration has involved developing and coordinating specialized institutions and agencies tasked with cyber operations, intelligence gathering, and information warfare. By embedding cyber tools within its broader security apparatus, Russia has enhanced its ability to conduct sophisticated cyberattacks, protect critical infrastructure, and project power in the digital realm. This strategic emphasis reflects a comprehensive approach where cyber activities are tightly interwoven with military, intelligence, and law enforcement functions, making cyber power a central pillar of Russia's national security posture. The following agencies represent the prominent cyber actors in Russia:

Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) is Russia's military intelligence agency and the primary actor behind the country's state-sponsored offensive cyber operations. Operating under the Ministry of Defense, it runs multiple cyber units engaged in espionage, sabotage, and information warfare.

- **APT28/Fancy Bear** specializes in cyber espionage, targeting political organizations, defense ministries, media outlets, and election infrastructure worldwide. This unit is widely believed to have interfered in the 2016 U.S. presidential election and other political events in Europe.
- **Sandworm Team** conducts large-scale, destructive cyber operations. It was behind the NotPetya malware attack in 2017, which caused billions in damages globally, and cyberattacks on Ukraine's power grid. It focuses on cyber warfare capabilities to disrupt critical infrastructure.

The Federal Security Service (FSB) is Russia's principal security agency and successor to the KGB, with wide-ranging responsibilities including counterintelligence, counterterrorism, and surveillance. In the cyber domain, the FSB plays a central role in overseeing and conducting both domestic cyber defense and offensive cyber operations. It operates units specialized in hacking, cyberespionage, and information warfare, often targeting foreign governments, critical infrastructure, and private-sector organizations. The FSB is also responsible for domestic internet surveillance and censorship through programs such as SORM (System of Operative Search Measures), and it enforces compliance with Russia's data localization laws. Internationally, it has been implicated in numerous cyberattacks, including election interference campaigns and operations aimed at disrupting or stealing sensitive information from Western institutions. The following units/groups are linked to FSB cyber operations.

- **Center 16 (Tsentr 16 / Unit 71330)** SIGINT, cyber-espionage support
- **Turla (Snake / Uroburos / Venomous Bear)**
- **Gamaredon (Primitive Bear / Shuckworm / ACTINIUM)**
- **Berserk Bear (Energetic Bear / Dragonfly / Crouching Yeti)**

The Russian Foreign Intelligence Service (SVR) maintains a sophisticated and competent cyber operations division, integral to Russia's broader intelligence and geopolitical strategies. The SVR's cyber capabilities include cyber espionage, advanced persistent threats (APTs), influence operations, and information warfare. Structurally, the SVR operates under a highly secretive, compartmentalized framework, with specialized units dedicated to offensive cyber operations to penetrate foreign government networks, critical infrastructure, and private-sector targets worldwide. These operations are often characterized by custom-developed malware, spear-phishing campaigns, and zero-day exploits to achieve stealthy, long-term access. The SVR's cyber units frequently collaborate with other Russian intelligence and military agencies, such as the GRU (Main Intelligence Directorate), sharing intelligence and operational tactics to maximize impact. Their cyber activities are typically aligned with Russia's strategic interests, including undermining Western political institutions, stealing sensitive technological and military data, and conducting psychological operations to sow discord.

The SVR's ability to integrate cyber tools with traditional intelligence collection makes it a formidable player in the global cyber espionage landscape, consistently adapting its methods in response to evolving cybersecurity defenses. The SVR includes the following cyber units:

- **APT29 / Cozy Bear** is one of the best-known SVR-linked cyber-espionage groups. It is believed to focus on long-term cyber intelligence gathering. This group is known for sophisticated, stealthy intrusion campaigns targeting Western governments, think tanks, and diplomatic entities, often using spear-phishing, malware implants, and zero-day exploits.
- **Information Operations and Influence Units** are not purely cyber. Still, these units work closely with cyber teams to conduct coordinated information warfare, leveraging cyber access to steal and leak sensitive data, amplify disinformation campaigns, and manipulate public opinion.
- **Support and Infrastructure Units** manage the cyber infrastructure that supports operations, such as command-and-control servers, encrypted communications, and secure data exfiltration channels, ensuring operational security and persistence.

Federal Service for Technical and Export Control (FSTEC) is Russia's primary agency for protecting state secrets and critical information infrastructure. It plays a regulatory and enforcement role in cybersecurity policy, focusing on information assurance, secure software certification, and the protection of classified data from foreign technical intelligence. FSTEC issues security requirements for IT products and networks used in government and military settings and mandates compliance through audits and inspections. It also controls the export of cryptographic technologies and dual-use software. While less directly involved in offensive cyber operations, FSTEC contributes to national cyber defense by setting technical standards and working closely with the FSB and other entities to secure state-run information systems.

Institute of Cryptography, Telecommunications and Computer Science (IKSI) is an academic and research institution affiliated with the FSB, tasked with developing advanced capabilities in cryptography, secure communications, and cyber defense technologies. It serves as a training ground for cyber operatives and engineers who go on to work in Russia's intelligence and defense sectors. IKSI conducts cutting-edge research in mathematical algorithms, encryption systems, secure coding, and countermeasures against foreign cyber threats. Its role is strategic and scientific, providing the intellectual and technological foundation for Russia's cyber capabilities.

Additionally, like the Iranian regime, Russia can also count on a number of nationalist hacker groups, such as **NoName057(16)** and **Server Killer**, which are very active in denial-of-service cyberattacks and database hacking, mainly against Western countries (Figures 8 and 9).



Figure 8- Telegram post from the pro Russian Hacking group NoName057(16) or Server Killer, claiming to target Israeli organizations

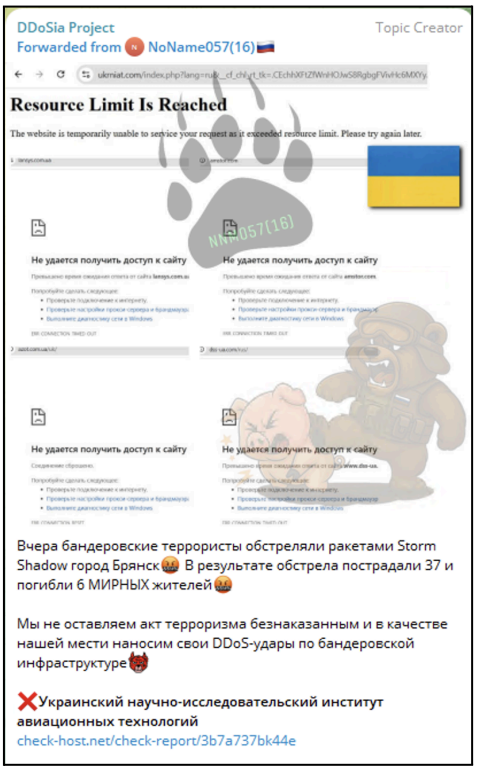


Figure 9 - A Telegram post from the pro-Russian hacking group NoName057(16) claiming the hack of Ukrainian websites

Operational Profile

Russia's cyber activity is best described as campaign-oriented and strategically synchronized. Its operators often pursue long access windows, repeated probing, selective leaks, infrastructure disruption, and influence support rather than one-off attacks for their own sake. The May 2025 joint advisory on GRU targeting of Western logistics entities is particularly revealing: the purpose was not simply espionage, but pressure against the supply architecture supporting Ukraine. That reflects the defining Russian logic of cyber operations in this period: cyber activity is used to erode operational depth, complicate coalition support, and generate friction within the adversary's system.

Russia's continued use of both high-end intelligence tradecraft and noisier disruptive methods also gives it unusual flexibility. It can choose between stealth and spectacle, or combine them, depending on political timing and operational need. That remains one of the defining features of the Russian model in 2026.

Cooperation

In terms of cyber activities, Russia's cooperation with China is primarily institutional and policy-oriented, supported by formal agreements and регуляр engagement between security and law enforcement bodies. Both states conduct joint information security consultations and cooperate through multilateral frameworks such as the Shanghai Cooperation Organisation (SCO), including exercises that incorporate elements of information security and cyber incident response.

With Iran, cyber cooperation is embedded within broader military-technical relations and has evolved alongside its deepening strategic partnership, formalized in 2025. Although most publicly documented collaborations are not explicitly cyber-specific, Russian support in signals intelligence, surveillance technologies, and broader security-sector development has strengthened Iran's cyber and intelligence capabilities. This alignment increasingly extends into the cyber domain, particularly during periods of conflict, with intelligence-sharing and operational coordination reported by multiple security sources. In parallel, pro-Russian hacktivist groups have been observed coordinating with Iran-linked actors in loosely organized campaigns, indicating a blend of state-level alignment and informal collaboration (Figure 10).



Figure 10 - Pro-Russian hacking group Server Killer claiming to join the cyber war against Israel and the US in response to the strike on Iran

Engagement with North Korea reflects a more operational and facilitative dynamic. Documented cases show North Korean cyber operators leveraging Russian infrastructure, including internet routing and hosting services, to conduct operations. This suggests technical enablement and permissive conditions rather than the existence of formal joint cyber units. Overall, Russia's cyber relationships with these states reflect a pragmatic and opportunistic alignment rather than a fully integrated alliance, yet they collectively amplify the scale, reach, and complexity of cyber operations associated with these actors.

8.4 🇰🇵 North Korea

Strategic Overview

North Korea's cyber strategy is the clearest example of a state cyber model directly tied to regime survival, sanctions evasion, and external revenue generation. Cyber operations serve not only as instruments of espionage, coercion, and intelligence collection, but also as practical mechanisms for obtaining foreign currency, acquiring restricted technology, and sustaining the state under prolonged international pressure.

As a result, Pyongyang has developed an unusually flexible system in which cyber espionage, social engineering, cryptocurrency theft, fake employment schemes, and the use of front companies function as interlinked components of a broader revenue and access architecture.

By 2026, the most important feature of the North Korean model will be that it no longer depends primarily on direct hacking. Instead, it increasingly blends network intrusions with fraud, identity deception, illicit remote labor, and laundering mechanisms. This evolution makes its cyber strategy more resilient than a purely theft-based model, because it allows the regime to shift fluidly between criminal, intelligence, and commercial cover activities while preserving deniability and maintaining a steady flow of income and access.

These operations are carried out by elite cyber personnel recruited from some of the country's most prestigious institutions, including Kim Il-sung University and the University of Automation. Selected individuals receive intensive technical and ideological preparation, followed by specialized training both inside North Korea and abroad, particularly in China and Russia, where they gain advanced operational skills and broader exposure to international cyber methods. This combination of centralized state direction, high-end technical training, and operational adaptability has made North Korea one of the most distinctive and durable cyber actors in the world.

Key Institutions and Operational Structure

North Korea's cyber operations are governed by a highly centralized and hierarchical structure, reflecting the tight control of the ruling regime. At the heart of this institutional architecture is the following

The Reconnaissance General Bureau (RGB), serves as the primary agency responsible for overseeing the country's cyber activities. As the main military intelligence arm of the Korean People's Army, the RGB is the central command hub for offensive cyber operations. It reports directly to the State Affairs Commission, chaired by Kim Jong-un, underscoring the strategic importance of cyber warfare at the highest level of North Korea's leadership.

- **RGB, Unit 121** is widely believed to be the most prominent division tasked with executing offensive cyber missions. It plays a leading role in North Korea's cyber warfare efforts and is often implicated in cyberattacks targeting foreign governments, critical infrastructure, and private entities. The unit comprises highly skilled operatives trained to conduct various forms of cyber sabotage and espionage. Several subordinate groups operate under or in close coordination with the RGB.
  Among the most well-known is the Lazarus Group, which has gained international notoriety for its involvement in cyber-espionage and destructive attacks, including the 2014 Sony Pictures hack. The group has been linked to various cyber activities aimed at advancing the regime's political and military objectives.

- **APT38,** which focuses primarily on financial cybercrime. This group is responsible for numerous high-profile bank heists and cyber-enabled thefts aimed at generating hard currency for the North Korean regime. APT38 is known for its sophisticated tactics, including long-term intrusions into banking systems and SWIFT networks.
- **Andariel** is another cyber unit affiliated with North Korea's offensive operations. It focuses on cyber-espionage and attacks specifically targeting South Korea's government and defense sectors. It is believed to operate with a degree of autonomy while remaining within the broader command structure of the RGB.

The Technical Reconnaissance Bureau (TRB) provides signals intelligence (SIGINT) in a supporting role. The TRB operates as part of the broader military intelligence apparatus, contributing electronic surveillance and intelligence-gathering capabilities that complement offensive cyber missions.

The Ministry of State Security (MSS) also contributes to the cyber apparatus by handling internal counterintelligence. Its role primarily focuses on ensuring loyalty within cyber units, preventing defection or unauthorized activity, and securing the internal communications and operations of North Korea's cyber personnel.

Operational Profile

North Korean cyber operations are highly adaptive and strongly shaped by economic necessity. They now span cryptocurrency theft, fake recruiter schemes, malware-laced job processes, fraudulent software development work, data theft, and the acquisition of covert access through outsourced labor channels.

This model gives Pyongyang two advantages: revenue generation without constant reliance on destructive attacks, and access to real corporate environments under a legitimate cover story. It is therefore a more resilient and scalable model than conventional cybercrime alone. The use of AI tools in these schemes, noted by Microsoft in March 2026, also shows that DPRK operators are refining deception rather than radically changing doctrine. AI is being applied to improve impersonation, documentation, communication, and hiring fraud at scale. That is operationally important because it reduces friction in the most human-dependent part of the North Korean model: getting trusted access.

Cooperation

North Korea's cyber cooperation with Russia includes the use of Russian telecommunications infrastructure and hosting services to support cyber operations. This has been documented in cases where North Korean traffic was routed through Russian networks, improving resilience and redundancy.

With China, North Korean cyber actors have historically operated from within Chinese territory, particularly in cities near the border. This operational presence has provided stable internet access, infrastructure, and a permissive environment for conducting cyber activities, including financial operations and espionage. Additionally, North Korea is collaborating with Chinese cybercriminals, especially for money laundering activities.

Interaction with Iran is reflected in similarities in cyber operations, especially in financially driven campaigns. Both countries have targeted cryptocurrency exchanges and financial systems using similar techniques, including malware deployment and social engineering. These parallels indicate convergence in operational practices and capability development.

9. Strategic Implications for International Security

The growing alignment among China, Russia, Iran, and North Korea has significant implications for international security, as it enhances these states' ability to operate under external pressure while challenging existing security frameworks across multiple domains. Although not a formal alliance, this network functions through flexible and overlapping bilateral relationships, making it more adaptable and in some respects, more difficult to counter than traditional alliance structures. Its distributed nature enables simultaneous or sequential pressure across multiple regions, including Europe, the Middle East, and the Indo-Pacific.

One key implication is the gradual reduction in the effectiveness of sanctions and export controls. Rather than fully isolating targeted states, sustained pressure has contributed to the development of alternative trade, procurement, and financial mechanisms. These arrangements do not eliminate constraints, but they can mitigate their impact over time.

A second implication is the diffusion of military capabilities across the network. Transfers of equipment, technical expertise, and industrial support, particularly those linked to the war in Ukraine, demonstrate how cooperation can enhance resilience without requiring full interoperability or integration.

In the cyber domain, the combined activities of these states contribute to a persistent, multi-vector threat environment. Even in the absence of direct coordination, their simultaneous operations increase the complexity of defense by requiring responses to multiple forms of cyber activity across different sectors and regions. More broadly, this alignment increases the interdependence of regional security dynamics. Conflicts are less contained geographically, and developments in one theater can have indirect effects in others. This complicates deterrence and strategic planning, which can no longer be managed solely within regional frameworks. Overall, the strategic challenge is cumulative rather than immediate. The primary risk lies in the gradual strengthening of interconnected relationships that enhance resilience, reduce vulnerability to external pressure, and create more complex security dynamics over time.

10. Conclusion

The relationships between China, Russia, Iran, and North Korea now reflect a durable pattern of coordination that is more structured and strategically relevant than in the past. This is not a formal alliance. There is no unified command, no shared doctrine, and no collective defense commitment. However, these four states are working together in ways that produce tangible effects across military, technological, economic, and cyber domains. The concept of a strategic nexus better captures this reality: a flexible network shaped by shared interests, complementary strengths, and a common willingness to counter Western pressure. This alignment is not accidental. It is driven by clear incentives. Each state benefits from the others' capabilities, whether in industrial production, weapons development, or procurement channels. Sanctions and external constraints have accelerated this process by pushing them toward alternative systems for trade, financing, and military supply. As a result, what were once uneven and largely bilateral relationships have become more interconnected and mutually reinforcing.

At the operational level, the depth of cooperation still varies. China-Russia, Russia-Iran, and Russia-North Korea represent the most significant partnerships, each with a distinct function: strategic coordination, military-technical exchange, and direct support to ongoing conflict. Other relationships remain more limited or selective. This unevenness is not a weakness. It is what allows the nexus to remain adaptable and resilient, avoiding the rigidity and political costs of a formal alliance. The most important development is the emergence of a shared defense-industrial and technological ecosystem. These states are no longer only exchanging equipment. They are enabling each other to sustain production, adapt capabilities, and bypass restrictions. China provides scale, Russia contributes military expertise, Iran advances drone and missile innovation, and North Korea brings both missile development and illicit procurement networks. Together, they reduce the impact of isolation measures and create alternative pathways to maintain and regenerate military power.

Overall, this strategic nexus does not replace traditional alliances, but it does complicate them. Its strength lies in coordination without formal commitment, and in cooperation that is difficult to disrupt through conventional policy tools.

11. About the Author



I am a cyber intelligence expert (Crime, Warfare, Terrorism) with over 15 years of experience across academia, high-tech, military, and law enforcement environments. My core expertise includes intelligence strategy, collection, research, and analysis, with a strong specialization in leading cyber intelligence research initiatives and Cyber HUMINT operations targeting criminal and terrorist activity in cyberspace.

My research interests center on cybercrime, cyberterrorism, and cyber-geopolitical intelligence. Throughout my career, I have trained numerous civilian analysts, military personnel, and law enforcement officers in cyber intelligence research and operational practices, including work in Deep and Dark Web environments, intelligence collection and analysis, and methodological frameworks.

12. References

1. Atlantic Council. (2025). *Digital Autocracy: How China and Russia are Exporting Surveillance*. Atlantic Council Strategy Papers. https://www.atlanticcouncil.org/reports/digital-autocracy-2025/
2. Barnes, J. E., & Sanger, D. E. (2026, March 6). Russia and Iran Forge a Strategic Partnership, Challenging the West. *The New York Times*. https://www.nytimes.com/2026/03/06/us/politics/russia-iran-partnership.html
3. Brookings Institution. (2026, January 12). *How China Reads the 2025 U.S. National Security Strategy: Implications for the CRINK Nexus*. https://www.brookings.edu/articles/how-china-reads-the-2025-u-s-national-security-strategy/
4. Casimir Pulaski Foundation. (2026, January). *The Axis of Upheaval: Russia, PRC, DPRK, and Iran*. Strategic Analysis Series. https://pulaski.pl/en/the-axis-of-upheaval-russia-prc-dprk-and-iran-2/
5. Center for a New American Security (CNAS). (2025). *The Axis of Upheaval: Deepening Military Cooperation Between Russia, China, Iran, and North Korea*. https://www.cnas.org/publications/reports/the-axis-of-upheaval
6. Center for Strategic and International Studies (CSIS). (2025, September 16). *Adversaries and the Future of Competition: Insights from Ukraine and the Middle East*. https://www.csis.org/analysis/chapter-1-adversaries-and-future-competition
7. CISA (Cybersecurity and Infrastructure Security Agency). (2026). *Nation-State Threats: Strategic Assessment of China, Russia, Iran, and North Korea*. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors
8. Council on Foreign Relations (CFR). (2022). *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*. Independent Task Force Report No. 80. https://www.cfr.org/task-force-reports/confronting-reality-in-cyberspace
9. CrowdStrike. (2026). *2026 Global Threat Report: The Emergence of the CRINK Cyber Alliance*. https://www.crowdstrike.com/global-threat-report/
10. DNI (Office of the Director of National Intelligence). (2026, March 14). *Annual Threat Assessment of the U.S. Intelligence Community*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf
11. European Commission. (2025). *White Paper on European Defence Readiness 2030*. Brussels: JOIN(2025) 1 Final.
12. Hodgson, Q., et al. (2019). *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace*. RAND Corporation. https://doi.org/10.7249/rr2961
13. IISS (International Institute for Strategic Studies). (2026, February). *The Military Balance 2026: Global Defence Spending and the CRINK Axis*. https://www.iiss.org/publications/the-military-balance/2026/
14. Kancs, d'Artis. (2024). *European Defence Readiness: A CRINK Scenario Analysis*. arXiv:2501.00058. https://doi.org/10.48550/arxiv.2501.00058
15. Kaya, A., & Aydin, M. (2025). Authoritarian Strategic Alignments in the Ukraine War: Russia, Iran, North Korea, and China. *Journal of Strategic Security*, 18(1), 1–22.

16. Kim, J. H. (2024). North Korea's Pursuit of Coercive Leverage in the Information Age: Expanding Cyber and Counterspace Capabilities. *The Korean Journal of International Studies*, 22(3), 311–335.
17. Mandiant (Google Cloud). (2024). *M-Trends 2024: Special Report on State-Sponsored Operations from the Axis of Autocracies*.
18. Mastro, O. S. (2026). Security ties between autocracies: Insights into authoritarian alignment through the case of China. *European Journal of International Security*. https://doi.org/10.1017/eis.2026.5
19. Microsoft Threat Intelligence. (2025, November). *East Asian Cyber Threats: The Convergence of Chinese and North Korean Tactics*. https://www.microsoft.com/en-us/security/blog/reports/
20. NATO Joint Force Command. (2025). *NATO's Long Cold Front: Countering Russian and Chinese Collaboration in the High North*. https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/
21. NK News. (2025, August). Researchers Identify Chinese Cybercriminal Working for North Korean Threat Group. https://www.nknews.org/2025/08/researchers-identify-chinese-cybercriminal-working-for-north-korean-threat-group/
22. Reddy, S. (2025, December). Breaking the North Korea-Russia Missile Axis. *The Diplomat*. https://thediplomat.com/2025/12/breaking-the-north-korea-russia-missile-axis/
23. Small Wars Journal. (2025, November 26). *Cybersecurity Strategies: China, Russia, North Korea, Iran*. https://smallwarsjournal.com/2025/11/26/cybersecurity-strategies-china-russia-north-korea-iran/
24. The Cyber Express. (2026, March 19). *China Tops the Cyber Threat List: 2026 Annual Threat Assessment Analysis*. https://thecyberexpress.com/china-top-cyber-threat-for-us/
25. Türkiye Today. (2025). NATO Commander Warns of Strategic Coordination Among Russia, China, Iran, and North Korea. https://www.turkiyetoday.com/world/3212763
26. U.S.-China Economic and Security Review Commission (USCC). (2025, November). *Axis of Autocracy: China's Revisionist Ambitions with Russia, Iran, and North Korea*. https://www.uscc.gov/sites/default/files/2025-11/Chapter_3--Axis_of_Autocracy.p