































CRIMINALITY

CRIMINAL MARKETS

PEOPLE

Human trafficking in Russia is a complex and entrenched market, involving multiple actors, including mafia-style groups, criminal networks, private-sector actors and stateembedded figures. Victims are trafficked both into and out of the country, with forced labour and sexual exploitation being the most prevalent forms. Despite the presence of anti-trafficking laws, enforcement remains inconsistent, and corruption within law enforcement and border control officials worsens the issue. Forced labour is particularly prevalent in industries such as construction, agriculture and domestic work, with victims primarily originating from Central Asia and South East Asia. Within Russia, 'working houses' operate as sites of forced labour, where individuals, often recruited under false pretences, are exploited without compensation. Additionally, there are also reports of individuals being trafficked into Russia from Europe and Africa, further complicating the transnational nature of the issue. The ongoing conflict in Ukraine has intensified human trafficking concerns, with reports indicating that thousands of Ukrainian children have been relocated to Russia under questionable circumstances.

Human smuggling networks function on a considerable scale, with both domestic and foreign participants aiding irregular migration across Russia's borders. Criminal networks, private-sector actors and state-embedded figures exploit legal loopholes to smuggle individuals into and out of the country. Russia has been accused of facilitating irregular migration into the EU, with Belarus also playing a role in orchestrating migration crises along European borders. Official figures indicate that deportations and expulsions of irregular migrants have surged, reflecting the extent of undocumented migration. Corruption within Russia's immigration processes is pervasive, with reports of bribes being exchanged for work permits and visas, particularly among migrants from Central Asia. On the other hand, the war against Ukraine has prompted significant emigration from Russia, resulting in hundreds of thousands of Russian citizens leaving the country since February 2022. While most migration occurs through legal channels, some individuals resort to illegal methods to enter other countries, such as Georgia, Armenia, Türkiye and Central Asian countries.

Extortion and protection racketeering remain prevalent, with organized crime groups targeting businesses and demanding payments in exchange for protection. High-profile cases of extortion involving mafia-style groups demonstrate the systemic nature of the issue. Some businesses are compelled to incorporate political figures

into their ownership structures as a means of protection. The illicit market for extortion and protection racketeering has a detrimental effect on legitimate sectors, particularly small businesses, entrepreneurs and investors.

TRADE

The arms trafficking market in Russia is extensive, involving both domestic and transnational criminal networks. Underground workshops modify and produce illicit weapons, with smuggling routes extending to Europe, West Asia and Africa. Corrupt officials within law enforcement and the government facilitate the movement of these illegal arms. The ongoing conflict in Ukraine has intensified this market, with reports indicating that arms are being smuggled from military zones into Russia for resale. Russia's formal arms exports have suffered due to international sanctions, prompting criminal networks to expand the illicit arms trade. Additionally, clandestine deals with sanctioned states, such as Iran, have increased despite these restrictions.

The trade in counterfeit goods remains widespread, with varying degrees of social acceptability, and it affects industries such as pharmaceuticals, clothing and electronics. The legalization of parallel imports in 2022 has blurred the distinction between legal and illicit markets, resulting in an increase in counterfeit products. Reports indicate that counterfeit alcohol alone accounts for billions in lost revenue. The demand for counterfeit luxury goods has surged following the withdrawal of Western brands from the Russian market. Amid the conflict with Ukraine, Russian consumers are increasingly turning to counterfeit goods, particularly from Asia, to satisfy their demand for luxury items. Türkiye has thus become a key hub for importing counterfeit goods into Russia, capitalizing on strengthened trade relations between the two countries. Furthermore, counterfeit tobacco products dominate the illegal nicotine market, which is estimated to constitute a significant portion of overall tobacco sales.

Illicit trade in excise goods, particularly alcohol and tobacco, continues to flourish, with established smuggling networks. Online platforms and retail distributors contribute to the illegal distribution of these products, resulting in significant tax revenue losses. Reports indicate that illicit nicotine-containing liquids are increasingly being distributed without regulatory oversight. Furthermore, a substantial portion of the illegal alcohol and tobacco products entering Russia is believed to originate from countries within the Eurasian Economic Union, including Armenia, Belarus, Kazakhstan and Kyrgyzstan. Furthermore, despite corporate boycotts, alcohol brands continue to reach the Russian market through parallel imports via countries like China and Türkiye.



ENVIRONMENT

Russia's vast forest resources position it as a major player in the global timber market, with substantial domestic production and consumption. The illicit timber trade is also widespread and frequent. Criminal networks and corrupt forestry officials enable these activities by using fraudulent documentation to transport illegally harvested timber. The EU's ban on Russian timber imports has led to an increase in exports routed through Central Asia, allowing Russian timber to circumvent sanctions before entering European markets.

Fauna crimes encompass the illegal hunting and trafficking of protected species, including tigers, elk and rare birds. Smuggling networks, often linked to foreign actors, facilitate the transportation of animal products, such as skins and caviar, to international markets. Corrupt officials within wildlife agencies have been implicated in issuing fraudulent permits that enable this illicit trade. Destination countries for smuggled wildlife products include China and Western Asia, where the demand for exotic animal derivatives remains high.

Non-renewable resource crimes, particularly the smuggling of oil, gas and precious metals, have escalated due to geopolitical tensions. Russia has developed a fleet of tankers to circumvent international sanctions on oil exports, employing deceptive shipping practices, including disabling automatic identification systems, conducting ship-to-ship transfers and re-exporting through third countries. Türkiye has emerged as a crucial hub for rerouting Russian oil to Europe, while countries like India and China have become major buyers of Russian oil, complicating enforcement efforts. Reports indicate that illegal gold and amber mining operations are linked to organized crime groups, with smuggled minerals being routed through intermediary countries such as the UAE. These activities provide critical revenue streams, including funding for Russian military operations.

DRUGS

The heroin trade in Russia remains significant despite geopolitical shifts. Trafficking routes have evolved, with Tajik criminal networks continuing to play a key role in mid-level heroin distribution. The darknet has emerged as a primary marketplace for heroin transactions, with Russia's digital drug economy surpassing traditional street-level markets in revenue. The conflict in Ukraine has disrupted established trafficking routes, prompting criminal networks to adapt their supply chains.

The cocaine trade has expanded, with seizures indicating Russia's role as both a transit and destination country. Large shipments of cocaine have been intercepted at Russian ports, reflecting the increased use of the country as a waypoint in international smuggling operations. The high cost of cocaine restricts domestic consumption to elite circles; however, the market is growing as new trafficking routes emerge.

The cannabis market is thriving, supported by both domestic production and international smuggling networks that cater to consumers. Cannabis ranks as the second most popular drug sold on Russia's darknet platforms, following mephedrone. A significant quantity of cannabis is cultivated domestically in a network of makeshift factories, with darknet platforms and shops providing the essential knowledge, equipment and seeds to local producers. These platforms subsequently purchase the harvested crops to sell them on the darknet, thereby establishing a self-sustaining underground market for cannabis in the country.

The synthetic drug trade is expanding rapidly, with law enforcement agencies dismantling several large-scale production facilities. Darknet markets play a crucial role in the sale of synthetic drugs, with Russia emerging as a significant hub for online drug trafficking. The ongoing war in Ukraine has led to an increased use of synthetic stimulants, such as amphetamines, mephedrone, alpha-PVP and barbiturates among combatants, reflecting broader trends in wartime drug consumption. Major online platforms now oversee much of this trade, adapting to Russia's growing economic isolation.

CYBER-DEPENDENT CRIMES

Russia is a major hub for cybercrime, with both independent and state-sponsored actors engaging in sophisticated cyberattacks. Ransomware operations orchestrated by Russian cybercriminals frequently target international corporations, financial institutions and government entities, often causing widespread economic and operational disruptions. Cybercriminal groups with ties to Russian intelligence services have conducted cyberespionage campaigns targeting critical infrastructure in the US, Europe and Ukraine. The Russian cybercrime ecosystem is highly transnational, characterized by collaborations between cybercriminal syndicates and state-affiliated threat actors. This nexus facilitates complex cyber operations, including large-scale data breaches, hacking schemes and advanced persistent threats. The illicit cyber market in Russia fuels global conflicts, particularly in the context of the ongoing war in Ukraine, where Russian-linked cybercriminals have executed ransomware attacks, disrupted essential services and stolen sensitive data from Ukrainian institutions. These cyberattacks aim to destabilize national security, erode trust in institutions and amplify geopolitical tensions. Russia's cybercrime infrastructure remains one of the most expansive and technically advanced globally, with its reach extending far beyond national borders.

FINANCIAL CRIMES

Financial crime in Russia is deeply entrenched, driven by systemic corruption, large-scale embezzlement, tax evasion and fraudulent schemes. High-profile cases involving government officials and influential business figures underscore the pervasive nature of illicit financial activities. Ponzi schemes and investment fraud have seen a significant rise in recent



years, with social media platforms serving as primary tools for deception. Fraudsters often employ sophisticated tactics, including social engineering, pyramid schemes and identity theft, to extract funds from unsuspecting victims. The Russia–Ukraine war has further exacerbated financial cybercrime, leading to a sharp increase in phishing attacks originating from Russia. Reports indicate that Russian-based phishing operations targeting European and US businesses have surged eightfold since the conflict began, posing a major cybersecurity and financial threat on an international scale.

CRIMINAL ACTORS

Russia's criminal landscape remains heavily influenced by mafia-style groups, particularly the 'thieves-in-law,' a highly structured organization with deep historical roots. Operating under a collective identity rather than named factions, they maintain a hierarchical structure led by recognized figures and follow a strict code of conduct marked by tattoos and rituals. Despite relatively small numbers, they wield significant influence over criminal enterprises in Russia and abroad. Their activities include extortion, drug trafficking, financial crimes, money laundering and the illicit trade of high-value goods, often in collaboration with international networks. They levy 'taxes' on businesses and control organized crime in prisons. Furthermore, they have established global networks in financial crimes and illicit trade, with their influence extending beyond Russia. Although law enforcement has targeted them, their ability to adapt and integrate into legitimate businesses complicates these efforts.

Other organizations, such as the Solntsevskaya and Tambovskaya groups, which possess increasingly decentralized and flexible structures, dominate various segments of the criminal underworld, ranging from narcotics distribution to extortion. Some of these syndicates have successfully integrated into Russia's legal economy, using legitimate businesses as fronts for illicit activities. Domestic criminal networks in Russia generally operate as well-organized groups with fluid structures, enabling them to adapt to market demands and evade law enforcement efforts. Prominent cybercriminal organizations, including FROZENBARENTS and FROZENLAKE, have been linked to sophisticated cyberattacks targeting the energy, defence and financial sectors, particularly in Ukraine. These groups employ phishing campaigns, data theft and hack-and-leak operations, often coordinating their efforts with broader strategic interests.

State-embedded actors play a critical role in Russia's organized crime ecosystem, where corruption is deeply entrenched at multiple levels of governance. From local law enforcement to high-ranking political figures, state officials frequently engage in criminal activities, leveraging their positions for financial gain and protection from prosecution. Corruption manifests in various forms, including bribery, embezzlement and abuse of authority, allowing state actors to extract resources and manipulate law enforcement mechanisms to their advantage. Notably, reports highlight instances of

senior officials protecting criminal enterprises in exchange for financial kickbacks. Some government agencies are directly compromised, enabling large-scale corruption networks to thrive. Russian intelligence agencies have also been linked to organized crime, utilizing criminal networks for state-sanctioned operations, such as sanctions evasion, cyberattacks and covert financial transactions. The increasing fusion of state and criminal actors has blurred the lines between legitimate governance and illicit enterprise, with many criminal organizations operating under the implicit protection of political elites.

Foreign criminal actors play a notable role in Russia's organized crime landscape, with groups from Central Asia, Georgia, Serbia, China and Vietnam engaged in a variety of illicit activities. Central Asian criminal groups, particularly from Kyrgyzstan, Uzbekistan and Tajikistan, dominate segments of the drug trade, including the trafficking of synthetic drugs in major urban centres. Georgian networks are active in extortion and cannabis trafficking, while Serbian groups maintain a stronghold in the arms trade. Chinese and Vietnamese criminal organizations operate extensively in the Russian Far East, controlling markets for counterfeit goods, illegal mining, timber smuggling and labour trafficking. These groups have established close ties with Russian criminal actors, facilitating crossborder smuggling and illicit trade networks that extend into Europe and Asia. Although Russian law enforcement has attempted to curb foreign criminal influence, many of these groups continue to operate with relative impunity due to corruption and political complicity.

Organized crime in Russia is deeply intertwined with the private sector, particularly in industries susceptible to financial manipulation, such as real estate, retail and finance. Criminal groups use legitimate businesses as fronts for money laundering, with shell companies and offshore accounts playing a central role in concealing illicit funds. The construction, hospitality and entertainment sectors are particularly vulnerable to criminal infiltration due to weak regulatory oversight. Oligarchs and politically connected business elites are instrumental in facilitating financial crimes, leveraging their wealth and connections to secure favourable government contracts and evade regulatory scrutiny. These individuals maintain extensive offshore holdings, enabling large-scale tax evasion and money laundering operations. Their close ties to Russian political elites allow them to operate with relative impunity, often benefiting from state-backed financial schemes that protect them from legal scrutiny. Many of Russia's wealthiest individuals hold assets offshore, evading domestic taxes and channelling funds through international financial systems. Furthermore, private-sector actors engaged in government contracts frequently exploit corruption networks to secure favourable deals, often at the expense of public funds. Although some efforts have been made to regulate these sectors, entrenched corruption and weak enforcement mechanisms continue to facilitate the deep integration of organized crime into Russia's economy.



RESILIENCE

LEADERSHIP AND GOVERNANCE

The Russian government has taken steps to combat organized crime by establishing interdepartmental working groups and coordinating with law enforcement agencies. However, these measures have faced widespread criticism due to allegations of collusion between the government and criminal networks. The prioritization of suppressing political dissent over tackling organized crime, particularly in the context of the ongoing war in Ukraine, has further undermined these efforts. The death of Alexei Navalny while in prison in 2024 underscored the repression faced by opposition figures and heightened concerns regarding state involvement in criminal activities. The operations of the Wagner Group exemplify the intersection of organized crime and state interests. Following the death of its former leader, Yevgeny Prigozhin, the group has continued to operate under the Russian National Guard (Rosgvardia), raising concerns about state affiliations with paramilitary groups engaged in illicit activities. Reports also indicate that migrants, particularly ethnic minorities and newly naturalized Russian citizens, have been subjected to forced military recruitment, further exposing vulnerabilities in governance and human rights protections. Additionally, Russia's alleged state-sponsored cyber activities, including cyber warfare and espionage, complicate regulatory and enforcement efforts. International scrutiny of Russia's ties to organized crime has intensified, particularly due to its involvement in conflicts such as the war in Ukraine. Western sanctions have targeted financial networks linked to criminal enterprises, while the economic strain from these measures has fuelled internal instability. The International Criminal Court has issued arrest warrants for Russian officials implicated in the forced deportation of Ukrainian children, further highlighting the intersection of criminal activities and state policies.

Efforts to enhance transparency and accountability in Russia have been significantly undermined by systemic corruption and political interference. The presidential decision to exempt government officials, particularly those involved in the conflict in Ukraine, from disclosing their assets has raised concerns that anti-corruption measures are designed to protect political elites rather than combat illicit financial flows. The government has also restricted the activities of independent oversight organizations, labelling groups as 'undesirable organizations.' Although technical measures, such as e-payment systems, have been introduced, access to government spending data remains severely limited, with only 60% of expenditures being publicly disclosed. Increased secrecy in procurement processes and the closure of the land cadastre to public access have further hindered efforts to increase transparency. The role of the Russian judicial system in combating corruption remains highly compromised. While high-profile corruption cases may suggest an official crackdown on financial crimes, reports indicate that enforcement has been selective, often targeting political opponents rather than addressing systemic corruption. Russia's state corporatism enables politically connected individuals to benefit from government contracts while ensuring impunity for illicit financial activities.

Russia has ratified several international agreements aimed at combating organized crime, including treaties that address financial crimes, drug trafficking and money laundering. However, its adherence to these agreements has been called into question, particularly due to its involvement in transnational criminal activities and conflicts, such as those in Ukraine and Syria. Allegations of human rights abuses and violations of international law further undermine Russia's standing in global law enforcement cooperation. Despite being a signatory to multiple extradition treaties, Russia has been accused of manipulating the extradition process for political purposes, targeting activists and opposition figures rather than focusing on suspects involved in organized crime. The country's cooperation with international law enforcement agencies, such as INTERPOL and Europol, has significantly deteriorated due to geopolitical tensions, especially with Western nations. Nevertheless, Russia has continued to strengthen its ties with countries in the Asia-Pacific region, the West Asia, Africa and Latin America, engaging in security agreements and law enforcement partnerships that align with its strategic interests.

Russia's legal framework encompasses provisions aimed at combating various forms of organized crime, including drug trafficking, arms trafficking, fraud, money laundering and terrorism. Although legislative reforms have been implemented to enhance prosecutions against criminal organizations, the political climate has increasingly influenced the enforcement of these laws. Recent amendments that criminalize participation in organized crime meetings seek to mitigate illicit activities; however, selective enforcement remains a concern, as authorities tend to prioritize cases that align with state interests. Furthermore, existing laws permitting construction in wildlife reserves and the exploitation of natural resources have raised concerns regarding the state's potential complicity in environmental crimes. Additionally, there has been a noticeable tolerance for cybercriminal groups operating within Russia, with these entities reportedly serving the state's interests in cyber warfare. Likewise, counterfeit goods are tolerated to ease the impact of scarcity and isolation on the population.



CRIMINAL JUSTICE AND SECURITY

Russia's judicial system includes specialized units tasked with prosecuting organized crime cases. However, political interference and corruption have a severe impact on judicial independence. Judges' career advancements are often tied to their compliance with the directives of political elites, and courts are frequently used to target political dissidents rather than genuine criminal enterprises. Pressure on independent lawyers and the judiciary's handling of highprofile cases raise further concerns about independence. Additionally, the quality of legal education, especially outside major cities, affects the judiciary's effectiveness. The penitentiary system is deeply flawed, characterized by overcrowding, human rights abuses and pervasive corruption within prisons. Organized crime networks continue to exert control over various aspects of the prison system, facilitating illicit activities behind bars. The mistreatment of political prisoners has garnered widespread international condemnation. Reports of extrajudicial violence, human rights abuses and mistreatment in custody highlight challenges to the systemic issues within the justice system. Russia's law enforcement agencies, including the Federal Security Service, the Federal Protective Service and the Ministry of Internal Affairs, possess extensive resources to combat organized crime. However, personnel shortages, political interference and a focus on suppressing dissent rather than addressing criminal activities have hindered their effectiveness. Reports of corruption among law enforcement officials, including the extortion of migrants, further exacerbate public distrust. Furthermore, reports of extrajudicial violence, human rights abuses and a lack of accountability further undermine the credibility of the law enforcement system and significantly impact public trust in these agencies.

Territorial integrity continues to be a significant challenge, especially in light of the ongoing war in Ukraine. The vastness of Russia's borders, coupled with the state's inability to maintain effective control, has enabled illicit trafficking. Additionally, geopolitical tensions have complicated efforts to secure these borders. Resource constraints and the expansiveness of the border pose additional significant challenges to surveillance and enforcement. Moreover, corruption among border control personnel undermines the effectiveness of enforcement mechanisms. In the cyber domain, the conflict between Russia and the West has escalated since the invasion of Ukraine, with Russia increasingly becoming a target rather than merely a source of attacks. What began as reciprocal DDoS campaigns has evolved into more innovative and sustained operations against Russia, leveraging crowdsourced tools and hacktivist efforts that have exposed sensitive data and disrupted systems. Although DDoS attacks have limited strategic impact, Ukraine's IT Army has effectively countered Russian cyberattacks on critical infrastructure, significantly undermining the integrity of Russia's cyberspace.

ECONOMIC AND FINANCIAL ENVIRONMENT

Russia has established an anti-money laundering (AML) framework, with the Federal Financial Monitoring Service (Rosfinmonitoring) serving as the primary authority overseeing financial investigations. However, systemic corruption and political interference have undermined the effectiveness of these measures. Russia's suspension from the Financial Action Task Force in 2023, a consequence of its war in Ukraine, raises concerns that efforts to uphold international AML standards may be compromised.

The country's economic regulatory environment is hindered by corruption, state interference and restrictive business conditions. Organized crime continues to exploit vulnerabilities in financial regulations, particularly in money laundering and smuggling activities. Sanctions imposed by western nations have prompted Russia to seek alternative financial channels, including informal economic networks and transactions with sanctioned states, to mitigate economic restrictions.

CIVIL SOCIETY AND SOCIAL PROTECTION

Support for victims of organized crime, particularly human trafficking, remains inadequate in Russia. The absence of a comprehensive legislative and administrative framework has left many trafficking victims vulnerable to deportation or prosecution. Victims are often not identified at the outset of investigations, allowing trafficking to remain largely undetected. Even when victims are recognized, protection measures are insufficient, lacking substantial assistance, security provisions and long-term support. NGOs play a critical role in providing services to victims, but increasing government restrictions and funding shortages have severely weakened their capacity. While there are efforts to address drug addiction through prevention programs and rehabilitation initiatives, the stigma surrounding drug use remains pervasive. Crime victims also face significant barriers in accessing support services due to societal prejudices, bureaucratic inefficiencies and inconsistent legal protections.

Efforts to combat organized crime in Russia remain inadequate, particularly concerning human trafficking and drug-related offences. The criminalization of assistance to smuggled individuals has exacerbated vulnerabilities, making it challenging for humanitarian organizations to operate effectively. Furthermore, the government lacked both a designated lead agency to coordinate anti-trafficking efforts and a body to monitor or assess its performance. Public awareness campaigns aimed at preventing organized crime are limited, with government initiatives primarily focused on law enforcement rather than proactive community engagement. Although the Ministry of Internal Affairs has reported progress in reducing criminal markets, corruption and resource shortages continue to hinder a meaningful impact. Key areas such as community outreach, social



intervention and whistle-blower protection remain largely overlooked. Furthermore, local communities typically do not view the fight against organized crime as a collective responsibility unless they are directly affected.

Civil society organizations and independent media in Russia operate under severe restrictions. Journalists and activists investigating organized crime and corruption frequently face harassment, imprisonment or forced exile. The government has expanded its use of 'foreign agent' laws to target NGOs and media outlets, effectively curbing independent oversight efforts. In addition to state repression, independent journalists and media organizations encounter threats and intimidation from organized crime groups, further constraining their ability to report freely. Attacks on journalists, media institutions and civil society activists by both state and non-state actors remain widespread, fostering a climate of fear and self-censorship. Despite these challenges, some organizations continue to provide victim support services, albeit under growing pressure and significant operational risks. The government maintains control over all national television networks, as well as many print and radio outlets and a substantial portion of the media advertising market, either directly or through state-owned enterprises and affiliated business elites. A small number of independent media platforms persist, primarily operating online and headquartered outside of Russia.

This summary was funded in part by a grant from the United States Department of State. The opinions, findings and conclusions stated herein are those of the authors and do not necessarily reflect those of the United States Department of State.

