



CENTER FOR
THE STUDY OF
DEMOCRACY

A wide-angle photograph of the Moscow skyline at dusk. The foreground shows the Kremlin's towers and walls, illuminated with warm lights. The middle ground is filled with a dense urban landscape of various buildings. The background features a cluster of modern, glass skyscrapers, some of which are lit up, contrasting with the darkening sky. The overall color palette is dominated by blues, greys, and the warm oranges and yellows of the city lights.

Shadow Fusions

The Convergence of Criminal Networks and
the Russian State

Shadow Fusions

**The Convergence of Criminal Networks
and the Russian State**



As Europe confronts the return of large-scale warfare on the continent, it also faces a more covert and insidious threat: Russia’s strategic use of criminal networks as a tool of hybrid warfare. Criminal groups are no longer operating on the margins—they are embedded into the Kremlin’s foreign policy to conduct sabotage, evade sanctions, and erode societal cohesion. This criminal-state alliance, rooted in Soviet-era practices and reinforced under Putin’s regime reflects a deliberate model of statecraft that merges intelligence services, oligarchs, and transnational crime networks to achieve geopolitical objectives and achieving hybrid warfare aims.

This report explores how actors like these weaken democratic institutions from within, exploiting legal grey zones and undermining public trust. Europe can no longer afford to ignore this hybrid threat. A unified, intelligence-driven response is urgently needed to defend its democratic foundations.

Authors:

Ryan McLaren, Analyst, Security Program & Democracy Shield Task Force, Center for the Study of Democracy

Elena Clemente Fito, Analyst, Geoeconomics Program, Center for the Study of Democracy

Atanas Rusev, Director, Security Program, Center for the Study of Democracy

Editorial Board:

Dr. Ognian Shentov

Ruslan Stefanov

Dr. Todor Galev



This work is licensed under the [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Cover photo: Canva

ISBN: 978-954-477-533-9

2025, Center for the Study of Democracy

CONTENT

EXECUTIVE SUMMARY	3
INTRODUCTION	6
ORGANISED CRIME AS WARFARE	10
PUTIN'S WAR ON THE WEST	14
THE KREMLIN'S CRIMINALS	21
Mercenaries, Bikers and Little Green Men	21
Smugglers and Sanctions Evaders	28
The Cybercriminals	37
Disposable Hoodlums: Espionage, Assassinations and Active Measures	41
The People Smugglers	45
Donbasionisation: Annexation and Buffer-Zones	47
An Army of Criminals	51
THE AUTHORITARIAN AXIS AND CRIMINAL NETWORKS	53
COMINTERN TO CRIMINTERN	58
Roads to a Response	59

LIST OF FIGURES

Figure 1.	The Kremlin’s Hard Power Mix	8
Figure 2.	The ‘European Headquarters’ of the Night Wolves, located in Dolna Krupa, Slovakia.....	24
Figure 3.	The Ermakov Smuggling Network	31
Figure 4.	A Ship-to-Ship Transfer of Russia-made Oil Products to the US.....	36
Figure 5.	The Kremlin’s Shadow War on Europe	44

LIST OF BOXES

Box 1.	The Night Wolves	23
Box 2.	North Korea’s Criminal Statecraft	32
Box 3.	Greek Ship-to-Ship Transfers.....	34
Box 4.	Telegram Recruitment.....	42
Box 5.	Belarus’ Role in Weaponising Migration	46
Box 6.	The Hongmen Network	54

EXECUTIVE SUMMARY

As Europe grapples with the return of large-scale war on the continent, a parallel, less visible conflict is being waged in the shadows: one that directly threatens the internal stability and security of the European Union. The Russian state has increasingly weaponised crime as an instrument of hybrid warfare against the West, fusing the power of organised criminal networks with state power.

Rooted in Soviet-era traditions and perfected under Putin's authoritarian rule this state-criminal fusion empowers actors like the Wagner Group, the Night Wolves, 'disposable' local street gangsters and oligarch-linked smugglers to execute state objectives. Their operations span illicit financing, arms trafficking, cyberattacks, people smuggling, and influence campaigns, amongst others. Criminal groups are no longer peripheral actors; they have become core components of Russia's foreign policy apparatus. Organised crime has thus moved beyond being a law enforcement issue, and it is now a frontline strategic weapon undermining the cohesion and security of European democracies.

With the return of geopolitical competition, this fusion has naturally evolved into a global, state-supported ecosystem. Kremlin-controlled oligarchs use front companies and shadow supply chains to procure sensitive technologies like microchips for Putin's war efforts, circumventing Western export controls. European complicity – through banks, energy companies, and maritime operators – further facilitates these efforts. Ports in Greece, financial firms in the UK, Netherlands and France, and corporate structures in Serbia and the UAE, for example, have all served as key nodes in these criminal laundering and smuggling networks.

Kremlin-linked criminal actors have also infiltrated the European civil space. Sharp power tools, like Russian nationalist motorcycle gangs, promote Russian narratives under the guise of cultural outreach, while private military firms/mercenaries engage in resource extraction in Africa to fund Russian influence operations and weaponise migration flows. This integration of criminal enterprise with foreign policy enables Russia to project power abroad while exploiting institutional and legal vulnerabilities at home.

This model produces a "double-destabilizing effect": eroding rule of law while amplifying Russian influence externally, without direct military confrontation. The goal is not just to evade sanctions or generate profit – it is to destabilise democracies from within. In this sense, Russia's criminal-state fusion represents a form of asymmetric warfare that targets the political fabric of its adversaries as much as their physical security.

Organised crime is thus no longer a law enforcement issue alone. It is a matter of urgent international security. To defend its democratic institutions and societal resilience, European democracies must recognise the true nature of the threat they face: a hostile state using criminal networks as a proxy force in

a protracted hybrid warfare. Grasping the magnitude of this threat is the first step toward an effective response.

Key Findings

- The Kremlin's **strategic embrace of criminal networks** has been enhanced under Putin by absorbing and weaponising it. Criminal groups are functional arms of the state, engaging in illicit activities like smuggling, extortion, and money laundering in exchange for political protection and state contracts. Russia has applied lessons learned from the fragmentation of Yugoslavia in regions like Donbas and Crimea, where criminal groups secure territory, supply logistics, and shape local political orders. These practices also represent a continuation of Soviet-era tactics, where criminal actors were routinely co-opted to advance state objectives and support strategic operations. These cases demonstrate the interconnection between war economies, state capture, and institutionalised corruption, and how they have been adapted to the current globalised financial and security environment.
- Russia's **hybrid warfare tactics are carefully calibrated** to avoid triggering a direct NATO response, relying on deniable actors and unconventional methods. These include cyberattacks, political interference, and sabotage executed by mercenaries, hackers, and criminal proxies. Hybrid methods also extend into the economic domain, where Russia exploits global finance, trade networks, and regulatory loopholes to bypass sanctions and procure critical goods. This blend of covert aggression and systemic exploitation allows Russia to apply sustained pressure on the West while maintaining plausible deniability.
- **Organised crime is now a hybrid warfare tool**, not just a law enforcement issue. The Kremlin uses criminal actors, including biker gangs like the Night Wolves, mercenaries such as the Wagner Group, and in tandem with criminal networks, to achieve strategic objectives in conflict zones and Western democracies alike. Europe's defence, law enforcement and political institutions must recognise and confront Russia's use of organised crime as a weapon of hybrid warfare. The Kremlin's integration of criminal networks into its foreign policy represents a deliberate strategy to destabilise the West from within – through sabotage, illicit finance, smuggling, and influence operations. **Acknowledging this threat explicitly** is the foundation for any effective response. Russia being labelled as the orchestrator of these actions will focus public discourse, prioritise law enforcement focus, and ensure the allocation of proper resources.
- **Sanctions evasion through criminal networks** has become essential to sustaining Russia's war economy. Oligarchs and criminal entrepreneurs use front companies (*'panamas'*) and smuggling networks to procure critical materials such as microchips, thus blunting the effectiveness of Western export controls and enabling continued aggression. In addition, European actors have been complicit – knowingly or not – in Russia's circumvention efforts. Financial institutions, energy firms, and maritime shipping

companies across the EU have facilitated the laundering of Russian oil and money, despite new sanctions legislation. Criminal methods such as ship-tracking manipulation and shell companies have proven highly effective.

- **A unified and intelligence-led response is essential to counter these hybrid threats.** Fragmentation between national agencies, and between counterintelligence and organised crime units undermines Europe's ability to act decisively. The EU must strengthen inter-agency and cross-border intelligence sharing, particularly through expanding the powers and coordination of bodies like the Single Intelligence Analysis Capacity (SIAC), the European Defence Agency, Eurojust and Europol. A dedicated EU Foreign Influence Task Force and improved cooperation across the EU's security architecture would close current gaps in preparedness. Closer cooperation with NATO on countering hybrid warfare should also play a role.
- **Targeting financial networks and supply chains** will disrupt the Kremlin's shadow alliances. Russian oligarchs and criminal proxies rely on covert financial flows, front companies, and third-country intermediaries to sustain both the war economy and internal influence operations. Europe must establish a centralised financial intelligence analysis framework that oversees sanctions enforcement and stricter export controls, amongst others. This financial intelligence sharing could be done through a strengthened and expanded Anti-Money Laundering Authority, EU Financial Intelligence Units (FIUs) Platform and European Public Prosecutor's Office, equipped with enhanced mandates and resources.

Special attention must be paid to smuggling hubs in places like the UAE, Serbia, and Belarus. Cracking down on these economic lifelines will severely hamper Russia's ability to wage a hybrid war. Additionally, the West more broadly should exert more pressure on third countries like Georgia, Kazakhstan and other post-Soviet states who hide and launder Russian money, whilst Europe should also scrutinise states like Turkey and China who help Russia evade sanctions on its fuel.

INTRODUCTION

Europe is currently seeing the return of large-scale conventional conflict on the continent for the first time since 1945, and, whilst the frontline trenches, artillery craters and drone strikes remain limited to the fields and cities of Ukraine, the remainder of the continent has not escaped untouched. Polish shopping malls and English warehouses are being torched, submarine cables in the Baltic and Irish Seas have been cut and critical infrastructure across the EU continues to be the target of cyberattacks. As Putin himself sees it, **Russia is at war with 'the collective West'**, and the EU is a legitimate target.¹ Europe's institutions have begun to wake up to the Kremlin's full-scale hybrid warfare campaign. The instrumentalisation of criminal networks as a hybrid warfare tactic has now been recognised as an emerging threat in the recently adopted new *Internal Security Strategy*, stating that "(h)ostile foreign states and state-sponsored actors seek to infiltrate and disrupt our critical infrastructure and supply chains, to steal sensitive data and position themselves for maximum disruption in the future. They use crime as a service and criminals as proxies,"² like gig economy workers. Europol too has identified the threat posed by "those orchestrating hybrid threats" in their most recent EU Serious and Organised Crime Threat Assessment report.³ Similarly, the recent 'Niinistö Report' which assessed the challenges facing the EU and suggested how to enhance Europe's civilian and defence preparedness and readiness also acknowledged the threat posed by this emerging criminal trend.⁴

Despite recent statements, Europe and her allies remain unprepared for this intersection between **the criminal and the state that operates in the grey zone between war and peace.**⁵

Though Russia's armed forces are primarily tied up in Ukraine, the Kremlin has nonetheless dramatically intensified its war on the collective West. In his hybrid war on Europe, Putin has utilised proxies as a means of compensating for redirected manpower and material. In an 'eye-catching' shift, **the Russian state has overwhelmingly turned to criminal networks for its foreign policy objectives.**⁶ These criminal proxies have been used to generate may-

¹ "Our armed forces ... are fighting on the line of contact that is over 1,000 kilometres long, fighting not only against neo-Nazi units but actually the entire military machine of the collective West." Putin, V., "Address by the President of the Russian Federation", *Office of the President of Russia*, September 21, 2022.

² European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy*, COM(2025) 148 Final, 1, Strasbourg, April 1, 2025.

³ Europol, *European Union Serious and Organised Crime Threat Assessment - The Changing DNA of Serious and Organised Crime*, Publications Office of the European Union, Luxembourg, 2025, p. 6.

⁴ Niinistö, S., *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, Report by Special Adviser to the President of the European Commission, November 26, 2024, p. 43.

⁵ Triplett, H., "The US is Already Losing the Next War," *The National Interest*, June 16, 2025.

⁶ McCallum, K., "Director General Ken McCallum gives latest threat update" [Speech], MI5 Security Service, *Counter Terrorism Operations Center*, October 8, 2024.

hem across Europe: assisting the Kremlin evade Western-imposed sanctions, helping annex territories, and conducting espionage and acts of arson and sabotage across Europe and the United States, amongst others. For instance, most of the examples hinted at above have been attributed to members of organised criminal groups working on behalf of the Kremlin.

This weaponisation of criminal networks for foreign policy aim has many names, and its definition has been widely debated. Yet, whatever term is most appropriate, *geocriminality*, *criminal statecraft*, *crimintern* or *state-sponsored crime*, for instance, the phenomenon represents a serious and pressing threat to the security of Europe. The changing nature of serious and organised crime, **primarily its adoption as a hybrid threat and sharp power tool**, has a ‘double destabilising effect’ on the EU and its Member States – impacting the ‘very foundations of the EU and its society.’⁷ It undermines the licit economy, threatening the safety and security of society internally, which increasingly aligns with the external goals of foreign powers who wish to destabilise and disrupt.⁸ As Thomas Haldenwang, the head of the German domestic intelligence agency states, “Russia is using the entire toolbox, from influencing political discussions to cyber-attacks on critical infrastructure to sabotage on a significant scale.”^{9, 10}

Whether it is the official EU line or not, and whether its policymakers “like it or not...” Europe must realise it is “in direct confrontation with Russia,”¹¹ and action must be taken. If concrete, intelligence-led, effective response is to be led, the collective West must first understand the nature of the threat and know ‘the beast.’¹²

However eye-catching and topical this changing DNA of organised crime as a hybrid threat and sharp power tool may be, though, the phenomenon is also not new. The Russian state, in its various guises, has long exploited criminal elements to compensate for its material handicaps against Western adversaries. Criminal actors contributed to the Soviet Union’s “active measures” (which would now be understood as state-organised crimes)¹³ abroad, whilst domestic organised criminals helped the State fill market shelves and supply the security services with black cash for operational funds.¹⁴ By examining Russia’s use of organised crime as a tool of statecraft through its recent

⁷ Europol, *European Union Serious and Organised Crime Threat Assessment - The Changing DNA of Serious and Organised Crime*, 2025.

⁸ Europol, *European Union Serious and Organised Crime Threat Assessment - The Changing DNA of Serious and Organised Crime*, 2025.

⁹ Thomas Haldenwang; cited in Kayali, L. et al., “Europe is under attack from Russia. Why isn’t it fighting back?”, *Politico*, November 25, 2024.

¹⁰ Shentov, O., Stefanov, R., and Vladimirov, M., *The Kremlin Playbook in Europe*, Sofia: Center for the Study of Democracy, 2020.

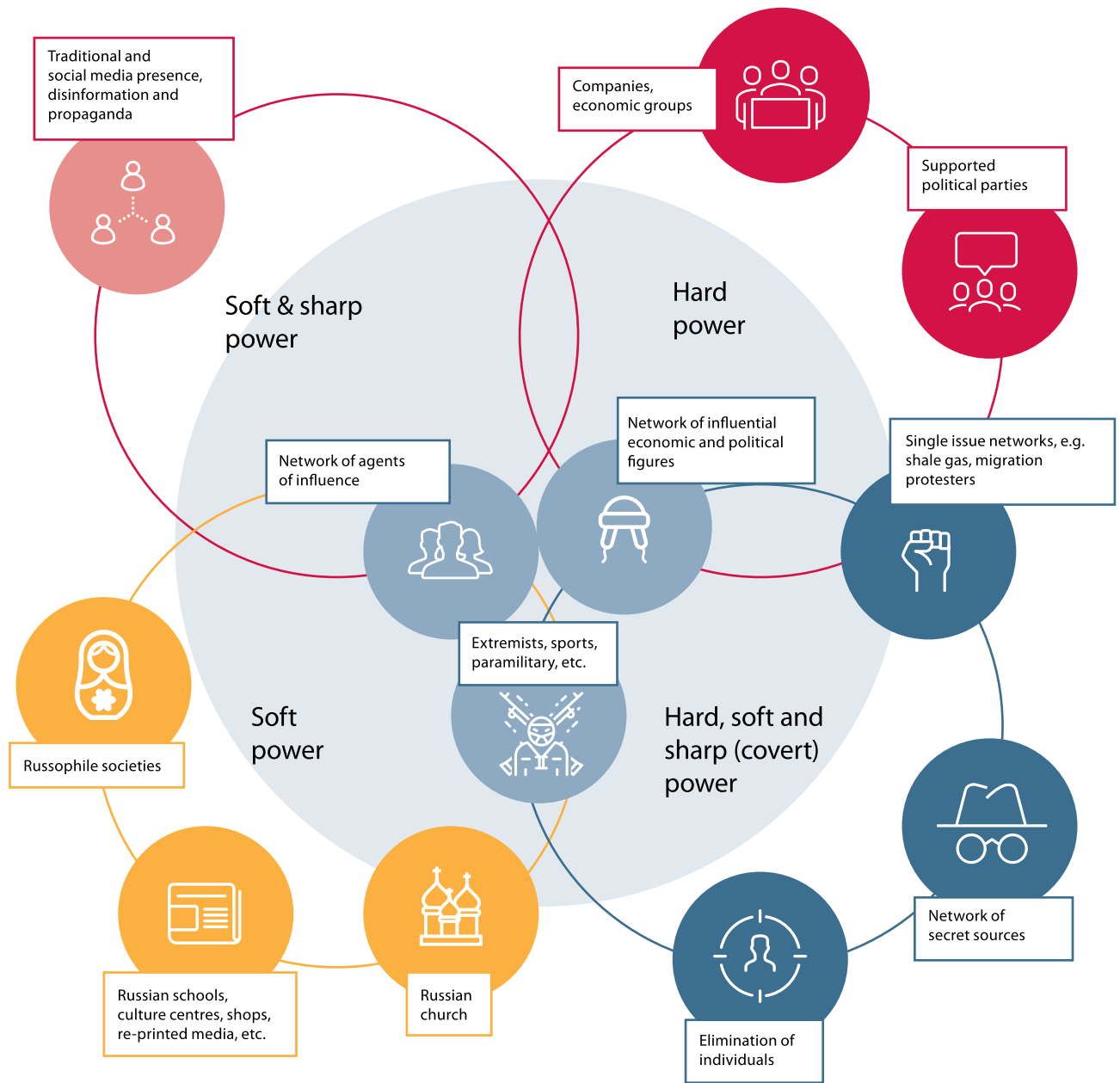
¹¹ Bruno Kahl, President of the German foreign intelligence agency (BND), cited in DW: “Germany: Spy Chiefs Warn of Increasing Russian Threat”, *Deutsche Welle*, October 14, 2024.

¹² Galeotti, M., *Gangsters at War: Russia’s use of organised crime as an instrument of statecraft*, Geneva: Global Initiative Against Transnational Organised Crime, 2024.

¹³ Chambliss, W.J., “Power, politics, and crime”, Boulder, CO: Westview, 1999; Chambliss, W.J., State-organised crime - The American Society of Criminology: 1988 Presidential Address, *Criminology* 27(2), 184, 1989.

¹⁴ Belton, C., *Putin’s People: How the KGB Took Back Russia and Then Took on the West*, HarperCollins, 2020.

Figure 1. The Kremlin's Hard Power Mix



Source: Shentov, O., Stefanov, R. and Vladimirov, M., *The Kremlin Playbook in Europe*, Sofia: Center for the Study of Democracy, 2020, p.14.

history, as well as Putin's ready embrace of the criminal underworld, several patterns emerge and a clearer sense of the threat posed by the Kremlin's crim-intern may be arrived at.

Furthermore, the Kremlin's utilisation of criminal networks for its foreign policy aims has clear parallels with the latest major conflict on European soil. Following the collapse of Yugoslavia in the early 1990s and the resulting international arms embargo imposed on the region,¹⁵ wartime smuggling and arms trafficking, often conducted with the tacit approval or direct involvement of state actors, became vital components of the war economy. As post-communist states struggled with economic instability amid the broader collapse of state institutions following the collapse of the Soviet Union, criminal groups expanded their influence, blurring the lines between political elites, security services, and organised crime. These state's reliance on 'smuggling for survival' during the conflict provided organised crime with fertile soil to spread its deep roots – roots that continue to plague the region to this day. The historical experience of this major conflict will hold lessons for Europe today that will only grow in relevance, particularly as it seeks to navigate the post-war transition.

Putin's Russia does not have a monopoly on the use of crime as a tool of statecraft. Other cash-strapped pariah states or fellow adversaries of the West have also relied on criminal acts as a means of achieving foreign policy goals. The use of crime by member states of the 'Authoritarian Axis' is explored for a comprehensive understanding of the threat facing the Western security alliance.

¹⁵ Hajdinjak, M., *Smuggling in Southeast Europe: The Yugoslav Wars and the Development of Regional Criminal Networks in the Balkans*, Sofia: Center for the Study of Democracy, 2002.

ORGANISED CRIME AS WARFARE

Today's geopolitical arena is characterised by a complex interplay of state influence, extending beyond traditional military and economic might. Organised crime, traditionally understood as centralised enterprises engaged in illegal activity **primarily motivated for profit**, has evolved significantly in its transnational dimensions. This organised crime is now utilised by state actors like Russia to achieve their strategic geopolitical objectives.

Since its attempted *coup de main* in Ukraine, Russia has attempted to reshape the world order, using all assets at its disposal. At the core of Russia's war on the West is the amalgamation of hard, soft and sharp power instruments through state capture in Russia itself. The Kremlin, like China, has gradually removed the boundary between the public and the private sector, capturing the Russian economy using security services and control over the media, as shall be explored in further detail.

Aware of its material limitations compared to the West, and still wary of triggering Article 5 – therefore triggering a full-scale war with the combined forces of NATO - the Kremlin has reverted to hybrid warfare tactics and its sharp power reservoirs. This hybrid war is conducted broadly to both punish the West for its support of Ukraine and deter further support in future and contributes to an attempt to rebuild a Russian empire.

These hybrid operations take on several forms, but their means focus mostly on **psychological operations, coercion, and deterrence to advance its foreign policy goals**. These actions aim to influence public opinion, divide NATO allies, and undermine Western democratic norms while staying below the threshold that would trigger Article 5. Russia leverages criminal groups, NGOs, commercial entities, and proxies to maintain deniability, making attribution, and thereby response, difficult.¹⁶ These operations are low-cost and often executed remotely or through intermediaries. However, outsourcing to criminal or untrained actors reduces operational professionalism and creates strategic risks, such as agency loss or unintended escalation.¹⁷ Yet, despite these drawbacks, the Kremlin continues to rely heavily on **organised criminal networks, positioned at the pinnacle of its hybrid warfare campaign**. They are key instruments of its sharp power strategy, exploiting their reach, deniability, and capacity **to operate in legal and political grey zones**.

The Wagner Group, for instance, exemplify this status of functioning in legal and political grey zones. Their operations exemplify a "kleptocratic ecosystem" where criminal states, militarised criminals, and profiteers mutually reinforce each other. The Russian state funds Wagner, which then extracts

¹⁶ Conley, H.A., et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, D.C.: Center for Strategic & International Studies, 2016.

¹⁷ Jones, S.G., *Russia's Shadow War Against the West*, Washington, D.C: Center for Strategic and International Studies; CSIS Briefs, 2025.

resources, and these resources, in turn, fund other illicit activities and state goals, with proceeds laundered through global financial systems. This creates a **circular, self-sustaining mechanism**, making countering the threat significantly more complex as it requires disrupting the entire interconnected web of state sponsorship, resource exploitation, and financial laundering, rather than just individual components.

Among these evolving forms of power, *sharp power* has emerged as a particularly insidious approach employed by authoritarian states like Russia. Authoritarian influence efforts in young and vulnerable democracies have been described as “sharp” in the sense that they **pierce, penetrate, or perforate the information and political environments in the targeted countries**. These regimes are not necessarily seeking to “win hearts and minds,” the common frame of reference for “soft power” efforts, but they are seeking to influence their target audiences by manipulating or distorting the internal environment, including the information that reaches them.^{18,19} Proxies with criminal links, such as the Night Wolves Motorcycle Club, serve as messengers for pro-Kremlin propaganda in European countries through events like “Victory Roads.”

The Kremlin’s cannibalisation of the Russian state has left almost every aspect of Russian society bending to the will of Putin: from petty thieves to the oligarch class. The *manual regime* in combination with the sharp power of the Russian state not only encapsulates what Russia’s strategy is internationally but also reflects Putin’s deeper objective of shaping and manipulating domestic perspectives and outlooks within Russia itself. The use of these tactics is akin to the Soviet “active measures,” and follow the nature of hybrid threats.²⁰ These include disinformation campaigns, propaganda, forgeries, front organizations, and support for foreign authoritarian movements.²¹

The Kremlin’s broader geopolitical gains have been shaped by the traditionally-weaponised organised criminal networks that the state has curated. Long aware of the material imbalance between the Soviet Union and its Western adversaries, the Kremlin has long utilised crime and criminals for the growth of their strategic aims. Such growth has been fuelled by **strategic corruption**, which deliberately pursues geopolitical interests by states through corrupt means. The Kremlin weaponises corrupt practices as a tenet of its foreign policy, aiming for geopolitical goals besides private benefits.²² This blurring of traditional criminal and political motivations complicates efforts by conventional law enforcement agencies, which typically focus on financial crime and local criminal organisations, to effectively counter these groups.

¹⁸ National Endowment for Democracy (NED), ‘*Sharp Power: Rising Authoritarian Influence*’ cited in *The Kremlin Playbook in Southeast Europe*, Sofia: CSD, 2020.

¹⁹ Stefanov, R., and Vladimirov, M., *The Kremlin Playbook in Southeast Europe: Economic Influence and Sharp Power*, Sofia: Center for the Study of Democracy, 2020.

²⁰ Novossiolova, T. and Georgiev, G., *Disinformation in the Kremlin’s Toolkit of Influence: Training Guidance for Scoping the Threat to the Norms and Institutions*, Sofia: Center for the Study of Democracy, 2022.

²¹ Novossiolova and Georgiev, *Disinformation in the Kremlin’s Toolkit of Influence*, Sofia: CSD, 2022.

²² Sabev, M., Georgiev, G. and McLaren, R., *Safeguarding the Foundations: Strengthening Civil Security in Bulgaria, Montenegro, North Macedonia and Serbia*, Sofia: Center for the Study of Democracy, 2024.

The expansion of Russian organised crime into the West's politics and financial infrastructure has been facilitated by certain countries' jurisdictions' secrecy. Such examples could be the British Virgin Islands, the Cayman Islands, or Cyprus.²³ Russian shell entities, including those in Cyprus, are often layered in an intricate black-cash network that conceals the identity of the ultimate beneficial owners. Nominee and bearer shares can be used in tandem with shell entities to optimise concealment. Accountants, lawyers, as well as trust and company service providers facilitate and promote the abuse of shell entities by lawbreakers.²⁴ Access to these jurisdictions helps Russia continue business as usual, specifically evading sanctions in their investment strategies, financial transactions, and tax optimisation. These murky structures have become the backbone of organised crime networks since they facilitate the legitimate integration of illicit flows into the economy, while the funds that have infiltrated the West provide operational funds for influence campaigns and operations against Russia's adversaries.²⁵

As was the case during the Soviet Union, organised crime networks are instrumental in providing Russia with access to restricted goods, such as advanced electronics for its military, and facilitating money laundering and illegal financial flows. The criminal groups have long served as sources of "black cash" for various operations.²⁶ The so-called *kremligarchs*, Russia's business elite cajoled by Putin, are not independent entrepreneurs but rather political and economic '**custodians of Kremlin assets**' ('holders,' not owners) and 'agents against the West'.^{27,28} Their wealth and security are contingent on loyalty to Putin; hence, their enterprises thrive through state contracts and alignment with Kremlin interests. These individuals leverage their access to billions of dollars and extensive connections to exploit vulnerabilities in global financial systems, furthering Moscow's objectives.²⁹

The union between the *kremligarchs* and the incentives of illicit financial flows leads to a **nexus of state capture and strategic corruption**.³⁰ All these facets of the Russian state converge to exert geopolitical pressure, most effectively by entrenching themselves within strategic sectors such as energy, infrastructure, telecommunications, and finance. Despite a decline in trade and corporate footprint due to sanctions and falling oil prices, Russia retains high impact through opaque ownership structures and targeted acquisitions. This often occurs via rigged privatizations and offshore investments. Russian state-owned banks like Sberbank and VTB play a central role in expanding this influence, using debt leverage and distressed asset takeovers to entrench

²³ Shentov, Stefanov, and Vladimirov, *The Kremlin Playbook in Europe*, Sofia: CSD, 2020.

²⁴ Pacini, C., W. Hopwood, G. Young and J. Crain, 'The role of shell entities in fraud and other financial crimes', *Managerial Auditing Journal*, Vol. 34, no. 3, 2019, pp. 247-267 in *The Kremlin Playbook in Europe*, Sofia: CSD, 2020.

²⁵ Vladimirov, M., Rueda Orejarena, G. and Osipova, D., *Global Reach: The Kremlin Playbook in Latin America*, Sofia: Center for the Study of Democracy, 2024.

²⁶ Rusev, A., et al., *Financing of Organised Crime*, Sofia: Center for the Study of Democracy, 2015.

²⁷ Zaslavskiy, I., *Sanctioned Kleptocracy: How Putin's kremligarchs have survived the war—and even prospered*, Washington: Atlantic Council Eurasia Center, 2025.

²⁸ Belton, *Putin's People: How the KGB Took Back Russia and Then Took On the West*, 2020.

²⁹ Conley, et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, D.C.: CSIS; 2016.

³⁰ Pretrova, V., *Cash is King: Impact of the Ukraine war on illicit financial flows in South Eastern Europe*, Sofia: Center for the Study of Democracy, 2023.

Moscow-aligned networks. Russia's deployment of organised crime, strategic corruption, and state capture is not a fragmented set of tactics but a deeply integrated and mutually reinforcing approach to **sharp power projection**.³¹

These networks, comprising local oligarchs and political intermediaries, secure Kremlin interests by distorting markets, resisting energy diversification, and perpetuating dependency on Russian resources. Through this strategy, Moscow transforms economic ties into enduring political leverage, undermining institutional independence and EU integration efforts in the region.³² Organised crime therefore has been a key tool for Russia in expanding its geopolitical presence, particularly within countries that have certain affinity to its regime, such as Bulgaria, Hungary or Serbia. These *Trojan horses* in different spheres allow Russian influence to slip through, continuing to destabilise parts of Western society and create divisions, thus achieving the Kremlin's hybrid war and sharp power objectives.

³¹ Sabev, Georgiev, and McLaren, *Safeguarding the Foundations*, Sofia: CSD, 2024.

³² Conley, et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, D.C.: CSIS, 2016.

PUTIN'S WAR ON THE WEST

Upon assuming power in 2000, Vladimir Putin vowed to crack down on crime and corruption. However, rather than eliminating criminal networks, he **consolidated** and **centralised** them under Kremlin control. As president, he established a **new social contract with organised crime**: in exchange for political loyalty and service to the state, criminal networks could operate without state interference, provided they maintained order and contributed to state interests. This approach allowed Russia's criminal elite to expand their reach globally, adapting from the brute-force methods of the *vory* to the more sophisticated business-driven model of the *avtoritety*. These groups embedded themselves in strategic economic hubs worldwide – major port cities, financial centres, and locations with large Russian diaspora communities – using money laundering, illicit trade, and financial manipulation as tools of influence. As the European Union expanded to include several Eastern and Central European countries, Russian organised crime would identify vast, new opportunities for creating wealth, particularly through new forms of cross-border crime.³³

Putin's administration used criminal networks to **enforce political control, enrich elites, and advance Russia's foreign policy objectives**. The oligarchs who benefited from criminal privatisation were incorporated into the Kremlin's power structure, becoming key players in Russia's **state-capture model**.³⁴ These developments mirror **Soviet-era practices**, where criminal groups operated under state oversight to serve broader strategic goals.

Indeed, Russian organised crime has long been intertwined with state structures, dating back to the early Tsarist period.³⁵ Under successive regimes, the state has utilised criminal groups for economic, political, and military purposes. Throughout Soviet history, criminal groups evolved alongside state institutions, adapting to political and economic shifts. The Stalinist period saw the *Vory v Zakone* (Thieves-in-Law) dominate the prison system, forming a criminal subculture in Gulags.³⁶ These groups smuggled goods, bribed officials, and acted as intermediaries between the state and illicit economies. Penal battalions famously fought in the Soviet army during the Second World War. Following Stalin's death and the Khrushchev-era prison amnesties, many former *vory* reintegrated into society, strengthening their ties with corrupt Communist Party officials.³⁷

³³ Siegel, D., "Russian Organised Crime in Europe", - In P.C. van Duyne, D. Siegel, G.A. Antonopoulos, A.H. Harvey, K. von Lampe (Eds.). *Criminal Defiance in Europe and Beyond: From Organised Crime to Crime-Terror Nexus* (pp. 51-76). Eleven International Publishing, 2020; Siegel, D., "Mobile banditry. East and Central European itinerant criminal groups in the Netherlands", The Hague: Eleven International publishing, 2014.

³⁴ Sabev, Georgiev, and McLaren, *Safeguarding the Foundations*, Sofia: CSD, 2024.

³⁵ Galeotti, M., *The Vory; Russia's Super Mafia*, New Heaven: Yale University Press, 2018, p. 9.

³⁶ Galeotti, *The Vory; Russia's Super Mafia*, 2018, p. 36.

³⁷ Shelley, L., Post-Soviet Organised Crime: Implications for Economic, Social and Political Development, *Demokratizatsiya* 2(3), 1995, pp. 341-358.

By the Soviet 'Era of Stagnation' under Brezhnev (1964-1982), organised crime had become embedded within the Soviet system, particularly in the shadow economy. The fiscal stagnation that defined Brezhnev's rule that drove citizens to look elsewhere for goods ensured organised crime networks would benefit enormously. Corruption flourished as criminal syndicates collaborated with Soviet bureaucrats to distribute scarce goods, circumvent economic restrictions, and smuggle resources. By the 1973 oil crisis, the Soviet State's reliance on criminal networks and offshore financial operations had become deeply entrenched, with the KGB playing a pivotal role in managing illicit funds and intelligence operations.^{38,39,40} This collusion between state security and organised crime laid the groundwork for the power structures that would later define post-Soviet Russia, where security elites and criminal networks merged into a new ruling class.⁴¹

The KGB's foreign intelligence networks played a vital role in the managing of illicit funds bound for abroad, specifically to pay European companies who clandestinely worked with the Soviets to provide dual-use equipment (such as Fiat, Merloni, Olivetti, Siemens and Thyssen⁴² Their primary roles in this regard involved the handling and transferring of physical illicit cash to these organisations or to front businesses, and selling off Soviet commodities through these fronts at the world market rate, gaining vast profits in the process. Funds such as these were also used to finance KGB operations throughout Europe, and was known as '**black cash.**' Black cash funded the Soviet campaigns of active measures - *aktivnye meropriyatiya* – throughout the international arena of the Cold War. These active measures became increasingly central to the KGB's mandate abroad following Yuri Andropov's elevation to leader of the Soviet Union, the first former head of the KGB to become general secretary.^{43, 44} The technique of utilising agents-saboteurs to carry out high-risk operations to undermine the West and demoralise public support and unity would leave a lasting blueprint for a revanchist Russia decades later.⁴⁵

With the introduction of Perestroika and Glasnost under Gorbachev, the Soviet economy was partially liberalised, with KGB operatives and criminal networks exploiting economic reforms to amass wealth and power. The sudden emergence of private businesses, or kooperativniki, created lucrative opportunities for organised crime, allowing gangsters to infiltrate these newly legalised private cooperatives, using them as fronts for established protection rackets, extortion schemes, money laundering, and wealth accumulation.

³⁸ Kaufmann, R., "The End of Cheap Oil: Economic, Social, and Political Change in the US and Former Soviet Union", *Energies*, 2014.

³⁹ Dawisha, K., *Putin's Kleptocracy: Who Owns Russia?*, Simon & Schuster, 2014, p. 15.

⁴⁰ Belton, *Putin's People: How the KGB Took Back Russia and Then Took On the West*, 2020.

⁴¹ Shelley, L., *Contemporary Russian Organised Crime: Embedded in Russian Society* - In: *Organised Crime in Europe. Studies Of Organised Crime*, edited Finaut, C., and Paoli, L., pp. 563-584, Dordrecht: Springer vol 4, 2004.

⁴² Belton, *Putin's People: How the KGB Took Back Russia and Then Took On the West*, 2020.

⁴³ Anh Tuan, B., "Soviet 'Active Measures'", *The Washington Times*, December 1, 1982; retrieved from CIA Reading Room, 2010.

⁴⁴ Andrew, C. and Mitrokhin, V., *The Mitrokhin Archive: The KGB in Europe and the West*, Penguin, 2000, p. 316.

⁴⁵ Richterova, D., "The Long Shadow of Soviet Sabotage Doctrine?," *War on the Rocks*, August 19, 2024.

KGB operatives, leveraging their own corrupt networks, also moved into these emerging markets, controlling entry and facilitating illicit financial flows.

The Soviet Union's impending collapse prompted KGB elites to funnel vast amounts of capital into offshore accounts rather than support a crumbling regime.⁴⁶ Among the disillusioned operatives watching these events unfold was a young KGB officer stationed in Dresden – Vladimir Putin – who, like many of his peers, saw Gorbachev's reforms as a dangerous betrayal of Soviet stability, and Andropov's offensive blueprint as an inspiration.

Vladimir Putin campaigned for President largely on a platform of crime-busting and anti-corruption. This platform was supported by his track record of ridding the streets of St. Petersburg of the most visible gang-related bloodshed and by tackling the food shortages gripping the city. The President would use language of *the vory* and honour a thief's code, and reach a mutually beneficial arrangement with the criminal underworld, secretly condoning their operations whilst calling on their skills and abilities when he required. Similarly, Putin reached kleptocratic deals with the oligarchs that allowed them to maintain most of their influence, wealth and power, in return for unadulterated loyalty and support when needed.⁴⁷ In this sense, these oligarchs, such as Abramovich, Kerimov, Rotenberg and Kovalchuk, for instance, are merely 'holders' and custodians of Kremlin wealth, not owners in their own right. These are kept in check by the President through the weaponisation of the State's legal system. This monopolistic political-business-criminal elite, the '**Chekist oligarchy**,' controls almost every societal structure in the Russian Federation today – including the criminal.⁴⁸ The 'grand bargain' reached by Putin and the oligarchic class was similar to that offered to Russia's criminal class: organised criminals were permitted to continue operations, on Putin's terms, provided they performed their duty when required.

For all the increased visibility of the new interconnected organised crime groups that became the Russian criminal state, the importance of ex-KGB agents in this nexus had been kept mostly under wraps. This connection was most pronounced in St. Petersburg, largely owing to its harbour and status as Russia's gateway to the West, and the corresponding opportunities for smuggling. As the Russian Federation's developed its market economy, the city would become the 'ground zero' for the alliance between former KGB officers and organised crime that was to dominate Russia.⁴⁹ In his role as deputy mayor, Putin was accused of having encouraged the activities of the city's underworld for his private gain – especially the work of the *Tambovskaya* group.⁵⁰ Notable examples of his connection with organised crime can be found in the details surrounding the notorious criminal privatization of the port of St. Petersburg and the Baltic Shipping Company, the purchasing of the San Trust alcohol distillery, and the attempted privatization of the Hotel Astoria.⁵¹

⁴⁶ Hosaka, S., *Chekists Penetrate the Transition Economy: The KGB's Self-Reforms during Perestroika*, *Problems of Post-Communism* 70(4), pp. 427–438, 2022.

⁴⁷ Burrough, B., "The Kremlin's Long Shadow," *Vanity Fair*, April 7, 2007.

⁴⁸ This approach mirrors that of Xi Jinping's 'United Front' strategy, which mobilises Chinese citizens, wherever they are in the world, to contribute to increasing China's influence in the world. Like in Russia, this also includes the criminal class. This shall be expanded on below. Tan, R. and Wu, P.L., "Chinese association accused of mixing crime and patriotism as it serves Beijing," *The Washington Post*, June 24, 2025.

⁴⁹ Belton, *Putin's People: How the KGB took back Russia and then took on the West*, 2020.

⁵⁰ Dawisha, *Putin's Kleptocracy: Who Owns Russia?*, 2014, pp. 128–41.

⁵¹ Dawisha, *Putin's Kleptocracy: Who Owns Russia?*, 2014, pp. 128–41.

Simultaneously, as Putin and his ex-KGB allies were consolidating the reins of power and increasing their ties to organised crime, the tattooed, old-school gangsters of the *vorovskoi mir* began to fade away, replaced by a new generation of criminal businessmen known as *avtoritety* ('authorities').⁵² These authorities, dressed in fine (smuggled) Italian suits and driving expensive (smuggled) Western cars abandoned the trades the *vory* excelled at, such as drug smuggling and prostitution, and instead prioritised legitimising their activities by manipulating the political environment.⁵³ With the assistance of the corrupted Soviet government executives from decades prior and the KGB men holding the money and access to the illegal structures and transnational corporations, these *avtoritety* quickly leapt on the newly privatised assets to seize profitable economic spheres. In return for assistance in entering this market, as these reservists reputedly lacked entrepreneurial experience and the necessary connections, the ex-KGB operatives and active reservists would use targeted violence on the opponents of their newly-found patrons. By doing so, these partners would control market entry, market share and border control whilst building Russian capitalism. "Thus were born, it is estimated, most of Russia's oligarchs and commercial banks."⁵⁴

This '**violent entrepreneurship**'⁵⁵ resulted in, essentially, a reversal of the traditional relationship between organised crime and the state: "gangsters and black-market entrepreneurs became dominant, with security officers desperate for their pay and patronage."⁵⁶ And, in contrast to what is commonly assumed of Russia's nexus between the state and organised crime, the former was not corrupted by the latter. Instead, organised crime simply became the state.⁵⁷ The fusing of the active reservists of the KGB, now left in limbo since the dismantling of the agency, with organised criminals and corrupt former Soviet bureaucrats was to have a profound impact on the criminal state that is Russia. These groups would combine their professional knowledge and networks to turn their new capitalist venture international. Foreign companies and new banks would begin to be used to cover their operations, as well as the source of their capital. New economic ventures in the former Soviet space would gradually take off, in part to shape foreign politics and exert economic influence.⁵⁸ This would later serve as an important tool for state capture. As President Boris Yeltsin declared, by 1994 Russia was already becoming a 'superpower of crime.'

⁵² Varese, F., *The Russian Mafia*, Oxford: Oxford University Press, 2001, p. 167.

⁵³ Galeotti, M., The Russian 'Mafiya': Consolidation and Globalisation *Global Crime* 6(1), 2004.; Shelley, Post-Soviet Organised Crime: Implications for Economic, Social and Political Development. *Demokratizatsiya* 2(3), 1994, pp. 341-358.

⁵⁴ Dawisha, *Putin's Kleptocracy: Who Owns Russia?*, 2014, pp. 128-41.

⁵⁵ "Violent entrepreneurship can be defined as a set of organisational decisions and action strategies enabling the conversion of organised force (or organised violence) into money or other market resources on a permanent basis." Volkov, V., "Violent Entrepreneurship in Post-Communist Russia", *Europe-Asia Studies*, 51(5), 1999, pp. 741-754.

⁵⁶ Galeotti, *Gangsters at War: Russia's use of organised crime as an instrument of statecraft*, GI-TOC, 2024.

⁵⁷ Cheloukhine, S., "The roots of Russian organised crime: from old-fashioned professionals to the organised criminal groups of today", *Crime Law & Social Change* 50, 2008, pp. 353-374.

⁵⁸ Cheloukhine, "The roots of Russian organised crime: from old-fashioned professionals to the organised criminal groups of today", *Crime Law & Social Change* 50, 2008, pp. 353-374.

Indeed, the violent entrepreneurs went international. Soviet ex-KGB agents and former elites throughout several other post-socialist countries in Central and Eastern Europe countries maintained power through extensive privatisation and embezzlement of state enterprises. These were orchestrated by predatory criminal networks, known as “thugs”/“*nutri*.”^{59,60} As states struggled with economic instability amid the broader collapse of state institutions following the dissolution, criminal groups expanded their influence, blurring the lines between political elites, security services, and organised crime. They tended to set up shop on key nodes on supply chains and routes for illicit goods and services, such as major port cities or border towns like Stockholm or Thessaloniki. Alternatively, major cities with either significant financial sectors, like London, or established Russian communities, like Sofia or Cyprus, developed as hubs for money laundering.^{61,62}

The international move was in part driven by the fear of a return to Communism, and the need to secure their revenue streams if they lost their main sources of income. Once there, these mafiosos searched for new money-making opportunities. Russian-Eurasian organised crime, muddled with their ex-KGB and corrupt-official partners, had founded legal commercial banks in their adopted countries, and invested in strategic sectors in target states’ economies.^{63,64} ‘Trade mafias’ had also proved incredibly useful to the new regime, able to smuggle goods in that were otherwise unavailable in Russia.⁶⁵ In addition, the new ‘authorities’ established a system of protection for their legitimate rivals in the banking and market services. In their organisations, representatives of these new networks, either former corrupt bureaucrats, ex-KGB agents or the gangster-businessmen, sat on the boards of a private enterprise of banks.

The ‘**merchant-adventurer**’ model provides one lens to understand this process. Russian crime groups, operating as rational economic actors and professional service providers, partner indiscriminately with other organisations and leverage political connections to evade law enforcement. With deep ties to corrupt bureaucrats and business elites, these groups effectively straddle both the criminal underworld and the legitimate financial system, returning to what had worked in Russia: filling gaps in “markets and meeting real or perceived needs,” acting as a complex shadow service economy with great scale, sophistication and stability. This new model, what Mark Galeotti refers to as ‘the merchant-adventurer,’ has four main characteristics.

⁵⁹ Abbink, J., and Salverda, T., *The anthropology of Elites: Power, culture, and the complexities of distinction*, Springer, 2012.

⁶⁰ Petrunov, G., “Organised Crime and Social Transformation in Bulgaria”, *European Journal of Sociology*, 47(2), 2006, pp. 297–325.

⁶¹ Canada: Immigration and Refugee Board of Canada, *Poland: Extent of organised crime and activities of organised crime groups; extent of Russian organised crime in Poland; measures taken by the state to combat organised crime; state protection available to those victimized by members of organised crime groups (January 2001 - September 2003)*, UNHCR, POL41923.E, September 5, 2003.

⁶² Hanley-Giersch, J., “The Baltic States and the North Eastern European Criminal Hub”, *Global Risk Affairs*, 2010.

⁶³ Conley, et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*. Washington, D.C.: CSIS, 2016.

⁶⁴ Stefanov and Vladimirov, *The Kremlin Playbook in Southeast Europe*, Sofia: CSD, 2020.

⁶⁵ Dawisha, *Putin’s Kleptocracy: Who Owns Russia?* 2014, pp. 30-31.

1. **Commodity & Service Providers** – Russian-based organised crime (RBOC) groups partner with local criminals to supply illicit goods (e.g., drugs, smuggled goods) and services (e.g., money laundering, fraud training).
2. **“Honest” Criminal Facilitators** – RBOCs position themselves as reliable underworld service providers, leveraging global Russian diaspora networks for money laundering, often routing funds through ex-Soviet states, as well as others like Israel and Cyprus, before final cleansing in London.
3. **Opportunistic Collaboration** – Unlike insular groups (e.g., Cosa Nostra), RBOCs work with any criminal entity for profit, regardless of ethnicity or structure.
4. **Elite Corruption & State Ties** – RBOCs thrive by blending into legal and illegal worlds, using political connections, shell companies, and expat networks. The Russian state often aids them with intelligence or resources, viewing them as strategic assets.

The notion of ‘**transplantation**’ examines how these mafia groups and criminal networks developed new franchises abroad. Together, these two theories provide insights into the transnational evolution of organised criminal networks, specifically those originating from Russia.^{66, 67} The former theory emphasises fluid, entrepreneurial individuals who exploit global opportunities with minimal attachment to structure or territory,⁶⁸ whilst the transplantation model focuses on the relocation and reproduction of entire criminal organisations in new environments, contingent on favourable local conditions. The former highlights innovation and adaptability in a globalised criminal economy, whereas the latter underscores the sociological and institutional factors that enable the successful embedding of criminal groups. Together, these perspectives illuminate the diverse strategies through which organised crime navigates and capitalises on shifting geopolitical and regulatory landscapes.

Domestically, the *avtoritety* became respected businessmen and politicians, bringing their criminal clans to the halls of government, including the FSB, the Ministry of the Interior, the customs, the courts, and regional/municipal administrations. Indeed, “the legal and illegal structures in Russia are closely interconnected” – if not inseparable.

Though officers in the security services may seek the pay and patronage of organised criminals in Russia, and certain ministers owe their rise to criminal networks, it is a stretch to suggest that organised crime controls the Kremlin. In Putin's Russia, there is little doubt amongst everyone who is in charge. Putin oversees the entire networked landscape of actors –from organised crime groups, the security services, to the oligarchs– in a **shadow convergence that benefits Russia's foreign policy**. Indeed, the extent organised crime can be controlled by his administration was most evident with Russia's hosting of

⁶⁶ Varese, F., *Mafias on the Move*, Princeton, NJ, USA: Princeton University Press, 2011.

⁶⁷ Varese, F. *The Cost of Non-Europe in the area of Organised Crime and Corruption in Europe*, [Briefing Paper]. European Parliamentary Research Service, PE 579.320, 2016.

⁶⁸ Galeotti, M., *Beware the Underworld Merchant-Adventurer*, Commentary in *International Centre for Defence and Security, Diplomaatia*, May 15, 2019.

the 2014 Winter Olympics and the 2018 FIFA World Cup. Both were pet passion projects of Putin and presented significant opportunities to increase Russia's global soft power. Eager to impress global onlookers, these organised criminals by and large suspended operations during these events.

Yet, in exchange for such cooperation, these organised crime groups receive preferential market access with the support of the state, state 'contracts' and of course, permission to operate. These connections between the state and the underworld are particularly useful during periods of economic contraction in Russia, and the level of corrupt cooperation tends to increase during major financial shocks to the Russian economy. This increase in incestuous links was particularly notable following the 2008 financial crash and the sanctions imposed on Russia after the annexation of Crimea. This was especially true at a local level, where local law enforcement, local street muscle and local criminal representatives are increasingly hard to distinguish between. Today, international law enforcement agencies are wrestling with the same difficulties in distinguishing where the state and criminal differ.

THE KREMLIN'S CRIMINALS

Since 2014, it has become increasingly evident that the line between Russian organised crime and the state is indistinct. This status quo has had serious implications for the Russian State. Sanctions have had serious impact on the Russian economy, significant portions of the Kremlin's vast 'diplomatic' spy networks have been expelled from their zones of operation, and the execution of Putin's war has strained the State's manpower reserves. Facing such consequences, Putin has, like many Russian leaders before him, turned to criminal networks to enact the affairs of the State.

The blurring of lines between state and non-state actors has greatly complicated the threat landscape, which continues to evolve. This symbiotic relationship between 'hybrid threat actors,' such as Russia and its allies, and organised criminal networks allows both parties to increase their malign capabilities and extend their global reach, as they "leverage each other's resources, expertise, and protection to achieve their objectives."⁶⁹

Organised criminal networks may be attracted by financial gain, state protection and the provision of havens or access to capacity-enhancing resources, for instance, though the motivations for these working relationships are likely nuanced. For Russia and her allies, the benefits of these shadow alliances are vast. The beginning of the war triggered new dynamics **where political and war objectives substitute profit-making as a primary objective** of this shadow fusion. The contributions of each different set of criminal actors and networks playing in this shadow partnership are examined in this section.

Mercenaries, Bikers and Little Green Men

The invasion of Crimea was mostly executed by Russia's 'little green men' – the now-infamous special forces operating without insignia, whom Putin refused to claim as his troops. Instead, he claimed these troops were local 'self-defence units' - despite several of these troops being recorded on camera providing statements to the contrary. Further evidence pointing to the Russian origin of these troops' uniforms and weaponry was similarly disregarded.⁷⁰ Yet, not all were highly trained special forces. These *vezhlivyye lyudi* (polite people),⁷¹ the little green men, had their numbers reinforced by significant numbers of Crimea-originating gangsters and thugs, particularly from Bashmaki and Salem, the two main ethnic Russian organised crime groups in Crimea.⁷²

⁶⁹ Europol, *European Union Serious and Organised Crime Threat Assessment - The Changing DNA of Serious and Organised Crime*, 2025, p. 14.

⁷⁰ Schreck, C., "From 'Not Us' To 'Why Hide It?': How Russia Denied Its Crimea Invasion, Then Admitted It", *Radio Free Europe/Radio Liberty*, February 26, 2019.

⁷¹ A known Kremlin euphemism for Putin's 'little green men,' often repeated by Editor in Chief of RT, Margarita Simonyan; Barros, G., *Warning: Russia May Send 'Little Green Men' to Belarus*, Institute for the Study of War, 2020.

⁷² Galeotti, M., and Arutunyan, A., *Rebellion as Racket: Crime and the Donbas conflict, 2014–2022*, Geneva: Global Initiative Against Transnational Organised Crime, 2022, p. 4.

Shortly after the Kremlin's troops without insignia took control of the Crimean Peninsula, Russia began amassing tens of thousands of troops along its Western border with Ukraine. Taking advantage of anti-government, pro-Russian protests in several of Ukraine's eastern and southern cities, Putin initiated a coordinated military and political campaign to claim the region. Once again, armed units of men outfitted by the Russian military began seizing control of local government buildings, police stations, town halls and other state institutions throughout Eastern Ukraine. Once these buildings were seized, they were then generally handed over to local pro-Russian separatists.⁷³ This would assist Moscow in its ability to deny that these soldiers were theirs, as they did in Crimea just weeks before. Indeed, Putin once again claimed these little green men and paramilitary combatants were local "self-defence" forces. However, though they were largely equipped with modern Russian arms, a more conscious effort was made to appear less connected: "In eastern Ukraine, the gunmen's kit, equipment and tactics are more varied... trying hard to look a lot less well-trained and well-organised."⁷⁴ Yet, despite such efforts, evidence once again pointed to the Russian origin of these combatants, particularly their Russian boots, brand-new Kalashnikov rifles, and advanced anti-tank weapons. Ukraine's SBU security service also claimed to have intercepted communications from Russian special forces directing these troops.

By May 2014, the separatists held a referendum on the status of the Donbas, which intended to legitimise the independence of the Donetsk and Luhansk oblasts as republics. The 2014 referendums in the Donetsk People's Republic (DPR) and Luhansk People's Republic (LPR), whose legality and legitimacy are widely questioned, led to their self-proclaimed independence, though they lack international recognition. The advantage of using forces like the 'little green men' or arming local separatists is undeniable: the use of these combatants provided the Kremlin with **plausible deniability** on the international stage, which temporarily delayed international condemnation and response. This modus operandi has since been adopted in Putin's political war on Europe, using various organised criminal networks and illegal private security organisations as a tool in his hybrid war.

Biker Gangs and PMCS

Chief among these groups are the **Night Wolves** and the infamous **Wagner Group**. These organisations operate as extensions of Kremlin influence, acting as 'Silent Partners' who employ a combination of soft, hard, and sharp power to project Russian interests domestically and internationally.⁷⁵ Their paramilitary activities, particularly in Crimea and the Donbas, reveal their utility in Russia's hybrid warfare strategy, blurring the line between civilian groups and state-sponsored militias, enabling plausible deniability while fostering instability in targeted regions. The Night Wolves, originating as a motorcycle club, has emerged as a sharp power tool to project force and influence domestic politics in former Warsaw-pact countries. The Wagner Group (or

⁷³ Buckley, N. et al., "Ukraine's 'little green men' carefully mask their identity", *Financial Times*, April 16, 2014.

⁷⁴ Buckley, et al., "Ukraine's 'little green men' carefully mask their identity", *Financial Times*, April 16, 2014.

⁷⁵ Keene, S.D., *Silent Partners: Organised Crime, Irregular Groups and Nation-States*, Monographs, Books, and Publications, 389, US Army War College Press, 2018.

Network) – often described as a private military company – is a more overtly militarised tool. Unlike traditional Western PMCs, Wagner operates in a legal grey area, blending mercenary activities and organised crime with state-sponsored missions. It serves as a versatile instrument for training, recruiting, and deploying combatants while executing tasks that conventional Russian forces cannot undertake openly. Wagner’s activities include direct combat, intelligence operations, and securing natural resources in conflict zones. Relying on criminal networks and convict recruits, they reflect a deliberate strategy to exploit extra-legal means for state purposes.

Box 1: The Night Wolves

The Night Wolves is a Russian motorcycle club that started life in 1989 as an association for hard rock music and motorbikes. It has since morphed into a club-turn-gang with paramilitary tendencies with between 5,000-7,000 members across the world and chapters throughout the former Soviet Union and beyond.^I The Night Wolves gained notoriety in large part due to their close connections to Putin and steadfast allegiance to the Kremlin. This cosy relationship has earned the group the epithet ‘Putin’s angels.’ Members of the group are typically involved in criminal activities (such as tax evasion, armed robbery and illegal production of fuel),^{II} many are convicted felons, and the gang has contributed to the annexation of Crimea and the Donbas. Despite this, the law enforcement agencies of Western states generally do not acknowledge the Night Wolves’ criminal links or the security threat they pose.^{III} This appears to be the exact aim of the Night Wolves. By moving under the radar of these Western law enforcement agencies and avoiding police scrutiny, they have rapidly expanded into almost 50 countries. By obfuscating any criminal links or military involvement, they maintain credibility with the local populations and try to present themselves as legitimate challengers to what they frame as Western moral decline. In countries where they lack broad support, they tend to stay within legal boundaries and align with local groups that share pro-Russian, anti-Western, or extremist political views.^{IV}

- I. Snyder, T., *The Road to Unfreedom: Russia, Europe, America*. London, U.K.: The Bodley Head, 2018, p. 140.
- II. *Tsekhovik/ tsekhoviki*: to own an underground black-market factory.
- III. Atlantic Council, “Direct Translation: Meet the Ex-Convicts, Bullies, and Armed Bikers Who Helped Seize Crimea”, *New Atlanticist*, June 19, 2014.
- IV. Harris, K., “A Hybrid Threat: The Night Wolves Motorcycle Club”, In - *Studies in Conflict & Terrorism*, 46(9), pp. 1784–1816, 2021.

During the annexation of Crimea, the Night Wolves rose to international prominence by fighting alongside the little green men, joining the separatist insurgency.⁷⁶ According to Denis Kuznetsov, deputy commander of the Luhansk

⁷⁶ Kleiner, J., Gregor, M., and Mlejnková, P., “The Night Wolves: Evidence of Russian Sharp Power and Propaganda from the Victory Roads’ Itinerary”, - In: *Problems of Post-Communism*, 71(2), 2023, pp. 145–155.

Night Wolves, they established the first checkpoints in Crimea, patrolling Sevastopol whilst armed with Russian weaponry.⁷⁷ In addition to fighting in Crimea, the Night Wolves also contributed to the capture of the Donbas. They were “among the pro-Russian fighters deployed to carve out breakaway ‘people’s republics,’” with the US government believing they shared close links with the Russian special forces.⁷⁸ They had also aligned themselves with the Interior Ministries of the unrecognised separatist republics, maintaining their paramilitary function. For their actions in the Crimean Peninsula, the Night Wolves were sanctioned by the US.⁷⁹

Since 2015, the Night Wolves have continued to spread their influence, acting as a form of **soft - sharp power** for Russia. This has been most notable throughout the former Soviet Union in Europe, though they are also active in Germany, Romania, Republika Srpska in Bosnia, Bulgaria, Montenegro, North Macedonia, Serbia and as far as the Philippines and Australia.⁸⁰ In these countries, they have endeavoured to promote Russian propaganda, provide security at pro-Kremlin events whilst supporting pro-Russian politicians; patrolling streets in Russian-captured areas and, in October 2022, established a volunteer unit to fight in Putin’s war in Ukraine.⁸¹ They have received vast support from the Kremlin to perform this sharp power role. Between 2013 and 2015, the Kremlin provided the gang with grants worth approximately 21.5 million rubles, ostensibly to stage anti-Western shows for children and to build a ‘patriot’ youth centre in Sevastopol. In Slovakia, the Night Wolves have established their ‘European headquarters’ just 70km from the capital Bratislava. The base, apparently a Second World War Museum, is shared with a Slovak nationalist group called NV Europa, and houses numerous old military vehicles, including tanks and armoured cars.⁸²

Figure 2: The ‘European Headquarters’ of the Night Wolves, located in Dolna Krupa, Slovakia.



Source: Radio Free Europe | Radio Liberty.⁸³

⁷⁷ Losh, J., “Putin’s Angels: the bikers battling for Russia in Ukraine”, *The Guardian*, January 29, 2016.

⁷⁸ Losh, “Putin’s Angels: the bikers battling for Russia in Ukraine”, *The Guardian*, January 29, 2016.

⁷⁹ Office of Foreign Assets Control, *Specially Designated Nationals and Blocked Persons list: Night Wolves*, US Department of the Treasury; Government of the United States, updated January 13, 2025.

⁸⁰ Sabev, Georgiev and McLaren, *Safeguarding the Foundations*, Sofia: CSD, 2024.

⁸¹ Ночные Волки, [Night Wolves], “Бригаде “Пятнашка” - 10 лет”, [Brigade “Pyatnashka” - 10 years], *Nightwolves.ru*, July 4, 2024.

⁸² Peter, L., “Slovakia alarmed by pro-Putin Night Wolves bikers’ base”, *BBC News*, July 31, 2018.

⁸³ Radio Free Europe | Radio Liberty, “Russia’s Night Wolves Mark Territory In Slovakia”, *Radio Free Europe*, July 26, 2018.

The Slovakian response to the Night Wolves' threat illustrates the benefits of such an organisation to the Kremlin. Despite the Slovak President Andrej Kiska recognising the base as a serious security risk for the country and identifying the gang as a **"a tool of the regime that has been involved in the occupation of a neighbouring country,"** the state was limited in what it could do. As foreign ministry spokesman Peter Susko stated, "they claim to be a club... they are not a government organisation, so it's difficult to intervene through the [Russian] embassy."⁸⁴ Realizing the threat, the EU included the Night Wolves in their seventh wave of economic sanctions following the Russian invasion of Ukraine.

A similar logic of plausible deniability has ensured the continued use of the 'private military company' (PMC) Wagner Group by the Russian State. Like the Night Wolves, **Wagner Group** rose to international prominence for their involvement in the war in Donbas, where it fought alongside Russian separatists. Originally, the Group acted as a vehicle for the Kremlin to train, recruit and deploy armed forces (mercenaries) with plausible deniability, providing security for friendly regimes or training their armed forces.⁸⁵ Over time, though, their *modus operandi* changed drastically, and with it, the need for shadow operations. Yevgeny Prigozhin, known as 'Putin's chef' and Wagner's founder and public face, oversaw the group's rise from consisting of approximately 250 members in 2014 to 85,000 by 2023.⁸⁶ It is believed that Wagner emerged, at Prigozhin's suggestion, as a private company under his ownership backing separatist rebels in Ukraine – though it would receive payment from the Russian state. It was also an effort to please Putin and increase his own power in the President's court.

Since its infamy increased in the mid-2010s, Western media outlets have generally referred to the organisation as a PMC – much like Erik Prince's Blackwater, for lack of a suitable alternative.⁸⁷ However, Wagner falls outside widely used definitions, despite performing some similar functions. It is not a legally registered company in Russia, and PMCs are illegal in the country.⁸⁸ It nonetheless fulfils covert military functions that lie both within and outside the Russian Armed Forces. Originating as a clandestine creation of the Russian military, it relies on state-supplied equipment but ultimately operates in service of Putin's personal agenda. Owing to the distinctions between traditional (Western) PMCs and the Wagner Group, it may be more appropriate to label Wagner as one of several "armed groups operating more along the lines of 'war by proxy' instigated by Moscow," as a mercenary group,⁸⁹ or simply, **a hybrid warfare tool** in the Kremlin's toolkit (and a hybrid between mercenaries and PMCs).

⁸⁴ Peter, "Slovakia alarmed by pro-Putin Night Wolves bikers' base", *BBC News*, July 31, 2018.

⁸⁵ Reynolds, N., *Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group*, Washington, D.C: Carnegie Endowment for Peace; *The Return of Global Russia*, 2019, p. 1.

⁸⁶ Euromaidan Press, "Frontline report: Prigozhin's video exposes high losses and failure of Wagner Group in battle for Bakhmut", May 27, 2023.

⁸⁷ Lechner, J., *Death Is Our Business: Russian Mercenaries and the New Era of Private Warfare*, Bloomsbury USA, 2025.

⁸⁸ Reynolds, *Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group*, Washington, D.C: Carnegie Endowment for Peace, 2019, p. 1.

⁸⁹ IRSEM: Institut de Recherche Stratégique de l'École Militaire [Strategic Research Institute of the Military School], *Private Military Companies in Russia: Not so Quiet on the Eastern Front*, October 12, 2018.

From the concept of *mercenary group*, Wagner takes its 'essence', particularly its methods, adopted from mercenaries in the post-Soviet era. From the latter, PMCs, Wagner take its 'form' – relating to Western-style PMCs that operated in Afghanistan and Iraq in the early 21st century.⁹⁰ Beyond these two concepts, Wagner has been infused with something almost uniquely Russian: **crime as a central form of statecraft.**

From its formation, Wagner has operated outside the law and embraced those who similarly live beyond it. At the most basic level, the Wagner Group is an illegal organisation in Russia: Russia has no legislative framework for PMCs and its criminal code outlaws the participation of mercenaries in armed conflicts.⁹¹ Wagner Group has also committed crimes in most of their operations and actively seeks to utilise convicted criminals for the state's foreign policy aims.⁹² In the words of Prigozhin himself, "We need your criminal talents," speaking to inmates at a Russian prison.⁹³ These talents have contributed to Wagner being officially designated as a transnational criminal organisation (TCO) by the United States Treasury Department, and being sanctioned by the EU, UK, Australia, Canada, and Japan.⁹⁴ The most serious crimes Wagner is accused of committing pertain to its activities in Africa, particularly in Mali, the Central African Republic and Sudan.

The Wagner Group has also been accused of having broken international law by laying landmines and booby traps in civilian areas around the Libyan capital, Tripoli. They are believed to be responsible for several massacres in Mali,⁹⁵ are accused of committing various atrocities in Syria,^{96,97} and committing sex-ual crimes in most areas of their deployment. Beyond its violations of interna-tional humanitarian law and possible war crimes, the expertise of its criminal combatants (that Prigozhin was seeking) has been highly visible in Wagner's criminal enterprises.

Since its involvement in the war in Syria, Wagner Group has been involved in natural resource extraction in its field of operation. Between 2017-19, the Assad regime sweetened its deal with Wagner for its military services by offering the group a quarter of the profits stemming from the oil and gas fields that it seized for the Syrian government. Following its deployment to Africa, similar deals would be reached with the governments of the Central African Republic and Sudan, though these would involve gold and diamonds instead

⁹⁰ IRSEM, *Private Military Companies in Russia: Not so Quiet on the Eastern Front*, 2018.

⁹¹ Reynolds, *Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group*. Washington, D.C, 2019, p. 1.

⁹² Giustozzi, A., and Lewis, D., *Did Wagner Group prove an effective tool for Russian foreign policy?*, Washington, D.C: The Russia Program; George Washington University and Institute for European, Russian, and Eurasian Studies (IERES), Academic Policy Paper Series (4), 2024.

⁹³ Sokolov, A., Whewell, T., and Nazarova, N., "Russian convicts released to fight with Wagner accused of new crimes", *BBC News*, August 10, 2023.

⁹⁴ U.S. Department of the Treasury, *Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization* [Press Release], Government of the United States, January 26, 2023.

⁹⁵ Burke, J., "Russian mercenaries accused over use of mines and booby traps in Libya", *The Guardian*, May 26, 2022.

⁹⁶ Bouzo, E., *The Wagner Group in Syria: Profiting Off Failed States*, Washington, D.C: Fikra Forum, The Washington Institute for Near East Policy, 2023.

⁹⁷ Ljubas, Z., "Paramilitary Group Wagner Sued in Russia for War Crimes in Syria," *OCCRP: Organised Crime and Corruption Reporting Project*, March 16, 2021.

of oil and gas. Wagner was also believed to be involved in diamond and gold extraction in Mali and Burkina Faso. Due to its criminal connections, some countries have begun referring not to the Wagner Group, but to **the Wagner Network**.⁹⁸

Whilst some of these deals have no doubt been reached with the governments of these countries, and some of its mineral extraction and transportation was in accordance with the law, most of its activity related to natural resource extraction mostly in African countries is specifically designed to assist Russia in evading Western sanctions – an illegal act in itself.⁹⁹ But Wagner and Prigozhin-linked companies, such as *M Invest* and *Meroe Gold*, have long been involved in the exploitation and smuggling of natural resources, which forms the group's most direct **connection to environmental and transnational organised crime**.¹⁰⁰ The Wagner Group has been accused of preying on and exploiting artisanal and small-scale gold mining in Sudan, which is then smuggled out of the country. The preferred smuggling routes often see the cargo routed and laundered through the UAE, flown directly to Russia, or transported overland to the CAR (due to the intimate relationship the Russians have developed with the CAR government). As stated by Gartenstein-Ross and colleagues, Wagner almost certainly plays a role in **facilitating these smuggling operations**¹⁰¹ and uses the proceeds to spread its malign influence around the globe.¹⁰²

In order to facilitate its illegal mining activities, Wagner relies on a vast network of shadowy international finance channels.¹⁰³ This network utilises major financial actors and shell firms across the globe in a sophisticated manner. Western banks such as JP Morgan, Chase Bank, and the HSBC Group have unwillingly acted as intermediary banks, contributing to Wagner's growing influence (just as they did with Hezbollah- particularly Western Union).¹⁰⁴ Firms like the UAE-based Kratol Aviation have provided support to Wagner's operations also, moving personnel, equipment and possibly finances on behalf of the group.¹⁰⁵ The convergence between licit and illicit systems enables the group to procure essential supplies like mining equipment as well as to **transfer funds for its commercial and military activities**. Chinese and African banks have also facilitated these ventures.¹⁰⁶ The complex, global financial arrangements have allowed Wagner to maintain its operations regardless of being sanctioned.

⁹⁸ UK Government, *Guns for gold: the Wagner Network exposed*, House of Commons Foreign Affairs Committee, HC 167 incorporating HC 1248, 2023.

⁹⁹ Gartenstein-Ross, D., Chace-Donahue, E., and Clarke, C.P., *Understanding the US Designation of the Wagner Group as a Transnational Criminal Organisation*, The Hague: International Centre for Counter-Terrorism, 2023.

¹⁰⁰ Gartenstein-Ross et al., *Understanding the US Designation of the Wagner Group as a Transnational Criminal Organisation*, 2023.

¹⁰¹ Gartenstein-Ross et al., *Understanding the US Designation of the Wagner Group as a Transnational Criminal Organisation*, 2023.

¹⁰² U.S. Department of the Treasury, *Treasury Targets Financier's Illicit Sanctions Evasion Activity*, [Press Release], Government of the United States, July 15, 2020.

¹⁰³ UK Parliament, *Guns for Gold: the Wagner Network Exposed*, 2023.

¹⁰⁴ Johnson, M., Aliaj, O. and Franklin, J., "Yevgeny Prigozhin secretly used JPMorgan and HSBC for Wagner payments", *Financial Times*, September 24, 2024.

¹⁰⁵ U.S. Department of the Treasury, *Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization*, 2023.

¹⁰⁶ Al-Monitor, "US sanctions UAE-based aviation firm with ties to Russia's Wagner", January 26, 2023.

The Wagner Group's use of financial crimes plays an important role in supporting the Russian state's geopolitical goals, particularly in the realm of sanctions evasion. The group's activities ensure the continued flow of revenue from smuggling operations and natural resource exploitation to the Russian state. For the official state, Wagner's involvement in financial crimes provides **a low-cost, low-risk method of furthering both political and economic objectives**. The group's operations fall outside the ordinary state mechanisms, maintaining the Kremlin's plausible deniability, while funding its own influence operations and active measures. Simultaneously, the Kremlin benefits from Wagner's smuggling and resource deals, particularly in the post-2022 world. By leveraging Wagner's illicit networks, the Russian state also gains access to valuable resources such as gold and diamonds.¹⁰⁷

Smugglers and Sanctions Evaders

As mentioned, the imposition of sanctions following the launching of Russia's war of aggression on Ukraine has had a varying effect on both Russia's economy and its ability to wage war. In a similar vein to the use of criminal networks during the Soviet Union, the Russian Federation today has also turned to **criminal actors to supply goods otherwise unavailable to the Kremlin in wartime**, thus alleviating the possible impact of sanctions and export controls. The Russian state is also supported by the criminal actions that reduce the effectiveness of Western sanctions on Russian energy exports. Owing to the Russian economy's dependence on energy exports, this criminal activity is of particular importance, and Kremlin-linked Russian criminal networks and third countries prove essential in this endeavour.^{108,109}

Unlike the *kontrabandisty* of old who would once smuggle goods to stock Soviet shelves, or the low-level disposable criminals spreading disorder on the Kremlin's behalf, these actors primarily represent the newly updated class of the *avtoritet*. They are oligarchs or oligarch-affiliated businessmen who utilise their skills and connections, and have now been enlisted to aid Russia in its struggle against the West. The expertise of these smuggling networks is a highly valued asset to Putin's war effort, especially if such expertise leads to the provision of **microchips**. Of course, these criminal assets are highly rewarded by Putin's regime, representing once again the symbiotic nature of the regime and organised crime. That being said, other actors, including lower-level drug smugglers, members of the Wagner group and even local businessmen with no links to Russia have supported the Kremlin's war efforts through such criminal activity.

Despite the international and EU series of sanctions targeting key sectors of the Russian economy and military-industrial complex, Kremlin-affiliated entities, like the Wagner Group, and their networks have demonstrated a remarkable ability to circumvent these restrictions. This shall be explored further below vis-à-vis Russia's *Donbasization* strategy. By exploiting legal and regulatory

¹⁰⁷ Moeder, R., and Malobisky, J., *Legal Mechanisms to Combat the Wagner Group: Opportunities and Challenges With the RICO Statute*. Washington, D.C: New Lines Institute, 2024.

¹⁰⁸ Felbab-Brown, V., and Paz García, D., *Russia, Ukraine, and organised crime and illicit economies in 2024*, Washington, D.C: Brookings Commentary, February 6, 2024.

¹⁰⁹ Vladimirov, M., et al., *The Kremlin Playbook in Türkiye: Geoeconomics Unfolded*, Sofia: Center for the Study of Democracy, 2025.

gaps, they have developed sophisticated methods to continue their operations, including smuggling dual-use goods, backdating financial documents, and employing intricate corporate structures, using company incorporation, shell companies and transferring assets to family members or associates to obscure the origins of their funds.¹¹⁰

Previously, the Russian-based organised crime groups were expected by the intelligence community to pay in order to be allowed to operate unbothered. These funds from criminal profits were paid into FSB accounts, which can then be used for operational purposes – ‘**black cash.**’ A German security service officer observed such a *modus operandi* with a criminal network smuggling meth into a German port. This group, consisting mainly of Russian nationals, would use fishing boats to smuggle meth from Russia through the Baltic Sea. They were allowed to carry on their business as long as they paid a certain amount to the FSB into a different European bank account each month.¹¹¹ Again, though, such organised crime groups may be exempt from these payments should they prove useful enough to the State.

Following the annexation of Crimea and the resulting imposition of sanctions, sanctioned goods otherwise unavailable to Russia were provided through smuggling routes through Poland, Lithuania and Belarus.¹¹² As highlighted by the Ukrainian Border Guard Service at the time, Moscow’s officers often helped and cooperated with these smuggler networks to this end.¹¹³ Perhaps the most important good on the Kremlin’s (inbound) smuggling wish list is microchips. Chips are essential for modern warfare systems for the Russian military. Certain specialist chips, like the gallium nitride and gallium arsenide-integrated circuit boards, are particularly essential to drones and other surveillance equipment. The Kremlin has long been aware of its inability to compete with Western and Asian chip manufacturing, arriving late to the party and never catching up technologically.¹¹⁴ For decades it has instead focused on acquiring foreign components, which could only be achieved illegally:

“The Russian government made a decision several decades ago that it was going to rely on smuggled technology for some of its most sensitive defence applications because it would be simply too expensive to produce it domestically and it would be militarily inconceivable to go without it... And so the choice was made just to rely on the cutting edge of commercial capabilities smuggled into Russia.”¹¹⁵

This reliance on smuggling as a means of sourcing these chips significantly increased in importance following the onset of Putin’s ‘special military oper-

¹¹⁰ Vladimirov, et al., *The Kremlin Playbook in Türkiye*, Sofia: CSD, 2025.

¹¹¹ Testimony of a German security service officer, Berlin, March 2024; cited in Galeotti, *Gangsters at War: Russia’s use of organised crime as an instrument of statecraft*, 2024.

¹¹² Galeotti, M., “Tough Times for Tough People: Crime and Russia’s Economic Crisis”, *Radio Free Europe/Radio Liberty*, Russia Studies Centre, 2015.

¹¹³ Watling, J., Danylyuk, O.V., and Reynolds, N., *Preliminary Lessons from Russia’s Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023*, London: Royal United Services Institute (RUSI), 2023, p. 11.

¹¹⁴ Cook, C., and Seddon, M., “The shadowy network smuggling European microchips into Russia”, *Financial Times*, 12 November, 2023.

¹¹⁵ Professor Chris Miller, cited in Cook and Seddon, “The shadowy network smuggling European microchips into Russia”, 2023.

ation.' Not only would chips be harder to obtain as a result of sanctions, but they were needed now more so than ever. Thus, as ever, the Russian state would readily embrace the skills of criminal networks.

But Putin can also rely on the skills of Russian oligarchs and their vast international networks to provide materials such as microchips. As with Putin's grand deal with organised crime, Putin's arrangement with oligarchs also ensures their cooperation when it comes to engaging in criminal acts in the service of the Kremlin. Take Maxim Ermakov, for instance, a sanctioned Russian businessman used by the Kremlin's intelligence services to procure sanctioned dual-use goods and bypass European export controls. Ermakov's plot involved *Ommic*, a French semiconductor company with a 150mm gallium nitride chip production line in Limeil-Brevannes (Val-de-Marne) – the first of its kind in Europe.¹¹⁶ Despite its rare abilities, *Ommic* became somewhat cash-strapped, which allowed Ermakov to convince its Director-General, Marc Rocchi, to become complicit in a Russian state smuggling operation and ultimately support the Kremlin's war effort.

Maxim Ermakov established a network of front companies ('*panamas*') and international partners to supply materials for Istok, a Russian defense manufacturer. Since 2004, Istok had sourced French-made chips, but following the 2014 annexation of Crimea and subsequent US-EU sanctions, procurement became more difficult. From 2014 to 2021, Ermakov's network adapted by using a front company, Fly Bridge, to purchase the chips in Paris. These were then sold to an Irish intermediary, which shipped them to Russia via China, the UAE, or India. In some cases, Istok received the chips directly from Marc Rocchi, the Director-General, who is now charged with supplying sensitive technologies to Russia, violating export laws, and falsifying documents.¹¹⁷ The French police believe that in 2021 alone, 13,500 chips were shipped to Russia using falsified documents.

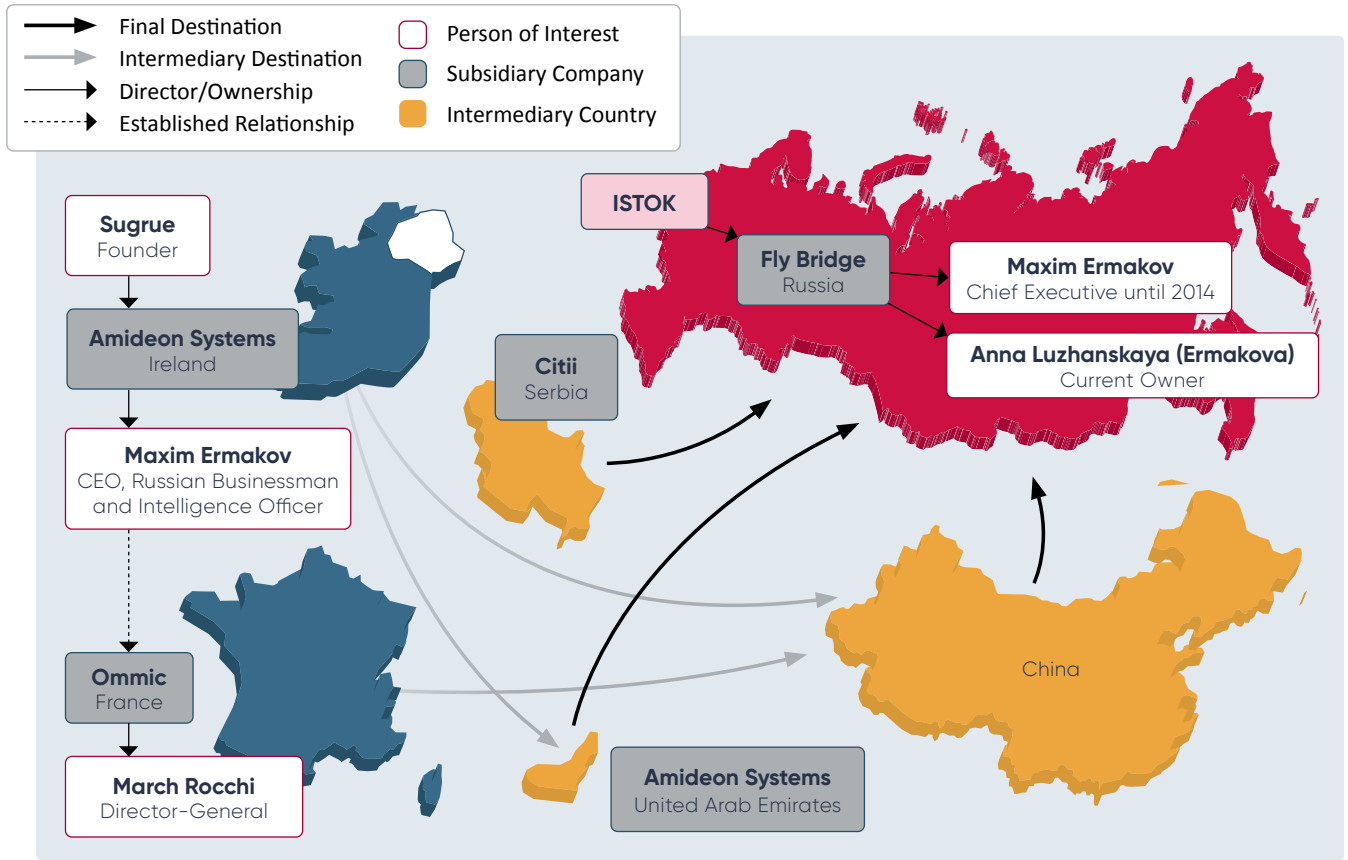
Though the French Connection is no longer active, Ermakov's networks are very much operational. A Serbian subsidiary of Fly Bridge known as *Citi* has facilitated Istok's importing of \$8.5 million worth of materials since February 2022. These are sometimes listed as being made in Serbia, though may be operating like Ermakov's earlier Irish importers. Some of these goods are listed as German products which are then shipped to Russia. Other countries involved include China and the UAE.¹¹⁸

¹¹⁶ Loukil, R., *Le français Ommic ouvre la seule usine de puces en nitrure de gallium sur plaquettes de 150 mm en Europe*. [French company Ommic opens Europe's only 150mm gallium nitride chip factory], *L'usine Nouvelle [The New Factory]*, September 26, 2017.

¹¹⁷ Cook and Seddon, "The shadowy network smuggling European microchips into Russia", *Financial Times*, 2023.

¹¹⁸ Cook and Seddon, "The shadowy network smuggling European microchips into Russia", 2023.

Figure 3: The Ermakov Smuggling Network



Source: CSD, adapted from Cook & Seddon, 2023.

Ermakov is just one of many Russian businessmen engaging in criminal acts for Putin’s war machine. Maxim Marchenko is another Russian businessman suspected of smuggling for the Kremlin. Marchenko and two Russian confederates are accused of using his several Hong-Kong-based businesses, such as *Alice Components*, *Neway Technologies Limited*, and *RG Solutions Limited*, as *panamas* to smuggle large quantities of dual-use, military-grade microelectronics, specifically OLED micro-displays, on behalf of Russia-based end users. These goods would ostensibly be used for manufacturing electron microscopes for hunting rifles or medical research purposes for users in China, Hong Kong or third countries. In reality, these would be shipped to their ultimate destination in Russia, in aid of Putin’s war.^{119, 120}

As with the Ermakov and Marchenko cases, such smuggling operations are further complicated by the **involvement of multiple countries and parties**. For instance, several Russian nationals with ties to the Wagner Group were revealed to be facilitating arms transfers from North Korea to Russia through a representative of the Korea Mining Development Trading Corporation in Syria.¹²¹ Iranian criminal networks have been active along established smug-

¹¹⁹ U.S. Attorney’s Office, *Russian International Money Launderer Sentenced To Three Years In Prison For Illicitly Procuring Large Quantities Of U.S.-Manufactured Dual-Use, Military Grade Microelectronics For Russian Entities* [Press Release], Southern District of New York, July 17, 2024.

¹²⁰ Center for the Study of Democracy, *Illicit Financial Flows and Strategic Corruption*, Policy Brief No. 157, April 2025.

¹²¹ United Nations Security Council (UNSC), *Final report of the Panel of Experts submitted pursuant to resolution 1874 (2009), S/2024/215*. UNSC Panel of Experts, 2024.

gling routes in the Caspian Sea region,¹²² which is used to smuggle arms such as anti-tank missiles, RPGs, drones and artillery shells for Putin's invasion force.¹²³ Indian smuggling networks active in Dubai assisted in the cleaning and laundering of assets bound for Russia, like cash and gold, whilst other countries turned a blind eye (or actively supported) to the use of their country to help Russia evade sanctions.^{124, 125} Countries like Turkey, Kazakhstan, Georgia, Serbia and the UAE have seen a significant increase in the registration of newly incorporated foreign-owned companies, behind many of which are Russian or affiliated individual(s) associated with Russia's Federal Security Service.^{126,127}

Indeed, a wide range of countries and their nationals are engaged in criminal activities in support of the Kremlin's war aims. This is especially true of states allied to the Kremlin in its conflict against the West, particularly North Korea, Iran, and China.

Box 2. North Korea's Criminal Statecraft

North Korea has a long tradition of conducting illicit activities as a means of survival, owing to its historic reputation as a pariah state (with corresponding sanctions). Following the onset of sanctions against the Russian Federation, the Kremlin has turned to Pyongyang to help bypass sanctions. Put simply, in return for supplying Putin with his war-making materials, namely weaponry, artillery shells and missiles,ⁱ North Korea receives Russia's military technology blueprints, food and, notoriously, oil.ⁱⁱ These transactions are generally conducted through the port of Rason and via rail links, which often involve criminal actors. Yet, it is not just fellow pariah states or their criminal citizens that assist the Kremlin in this regard.ⁱⁱⁱ

- I. Jang, S., "North Korea Ramps Up Arms Sales to Russia, Iran, Syria, and Others", *The Diplomat*, 5 September, 2023.
- II. MacKenzie, J., "Satellite images show Russia giving N Korea oil, breaking sanctions", *BBC News*, 22 November, 2024.
- III. Bermudez, J.S.Jr., Cha, V., and Jun, J., *Dramatic Increase in DPRK-Russia Border Rail Traffic After Kim-Putin Summit*, Washington, D.C: Beyond Parallel; Center for Strategic and International Studies (CSIS), 6 October, 2023.

¹²² McKernan, B., and Mironova, V., "Russia 'using weapons smuggled by Iran from Iraq against Ukraine'", *The Guardian*, April 12, 2022.

¹²³ Nissenbaum, D., and Faucon, B., "Iran Ships Ammunition to Russia by Caspian Sea to Aid Invasion of Ukraine", *The Wall Street Journal*, April 24, 2024.

¹²⁴ Nechepurenko, I., "How Western Goods Reach Russia: A Long Line of Trucks Through Georgia", *The New York Times*, January 13, 2023 .

¹²⁵ Felbab-Brown and Paz García, *Russia, Ukraine, and organised crime and illicit economies in 2024*, Washington, D.C: Brookings, February 6, 2024.

¹²⁶ O'Shea, L. et al., *Illuminating the Role of Third-Country Jurisdictions in Sanctions Evasion and Avoidance*, SOC ACE Research Paper 21 Birmingham: University of Birmingham, 2023, pp. 18-20.

¹²⁷ U.S. Attorney's Office, *Five Russian Nationals, Including Suspected FSB Officer, and Two U.S. Nationals Charged with Helping the Russian Military and Intelligence Agencies Evade Sanctions*, [Press Release], Eastern District of New York, December 13, 2022.

The connections of individual businessmen and the assistance of organised crime groups from other states contribute greatly to the Kremlin's ability to source sanctioned goods otherwise unavailable to Putin's war efforts. Again, of particular value are advanced microchips. However, the use of criminal acts and networks helps the Kremlin's goals in many more ways beyond just smuggling goods into Russia. **The importance of evading sanctions on Russian fuel exports** is of critical importance to an economy so dependent on the industry. In this regard, the Kremlin has been assisted once again by its businessmen-oligarch class and **willing confederates in third countries – including in sanctioning states**.¹²⁸ Smugglers employ tactics such as disabling vessel tracking systems, altering vessel identification, and falsifying documents to obscure the origin of Russian oil and enable it to reach markets despite sanctions – all illegal acts.¹²⁹ The maritime industry plays a significant role in facilitating this illicit trade, with ships from both non-sanctioning third countries and those politically aligned with sanctions providing logistical support.

In 2024, the European Union enacted a **directive criminalizing the violation and circumvention of EU sanctions**, in response to Russia's aggression against Ukraine.¹³⁰ This directive mandates that member states define specific actions as criminal offences, including aiding sanctioned individuals or entities, trading restricted goods, and providing prohibited financial services. Yet, despite these measures, criminal networks within the EU have been instrumental in assisting Russia to evade sanctions.¹³¹ Investigations have uncovered operations involving shell companies and clandestine shipping practices that obscure the origin of Russian oil, allowing it to enter international markets despite sanctions. Additionally, coordinated law enforcement actions have dismantled extensive money laundering networks linked to Russian oligarchs and organised crime, which facilitated the movement of illicit funds and supported sanctioned entities.

But, despite formal commitments to uphold EU sanctions, several European actors, particularly banks, 'big oil' corporations and trading companies, have been complicit, knowingly or otherwise, in helping Russia circumvent restrictions imposed after it invaded Ukraine. One example of such a network has Coral Energy at its heart: a trading firm with strong ties to Russian oil giant Rosneft and operations linked to Switzerland and Dubai. Although Coral Energy officially claimed to cut Russian ties in 2022, an investigation by *Le Monde* revealed that Coral had continued to trade in Russian hydrocarbons through a hidden network of 'red' (covert) and 'blue' (public-facing) entities.¹³² The primary hydrocarbon in question was naphtha, "a common product that can be reprocessed into gasoline or used in the petrochemical industry."¹³³

¹²⁸ Vladimirov, et al., *The Kremlin Playbook in Türkiye*, Sofia: CSD, 2025.

¹²⁹ O'Shea, et al., *Illuminating the Role of Third-Country Jurisdictions in Sanctions Evasion and Avoidance*, SOC ACE Research Paper 21 Birmingham: University of Birmingham, 2023.

¹³⁰ European Union, *Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures and amending Directive (EU) 2018/1673*, Official Journal of the European Union, April 29, 2024.

¹³¹ Felbab-Brown, and Paz García, *Russia, Ukraine, and organised crime and illicit economies in 2024*, Washington, D.C: Brookings, 2024.

¹³² Bouissou, J., Michel, A., and Tchoubar, P., "Shell Companies, Ghost Ships and Secret Traders: How Russia Circumvents Western Oil Sanctions", *Le Monde*, October 30, 2024.

¹³³ Jérôme Sabathie; cited in Bouissou, Michel and Tchoubar, "Shell Companies, Ghost Ships and Secret Traders: How Russia Circumvents Western Oil Sanctions", *Le Monde*, October 30, 2024.

This shadow structure enabled Coral to launder refined Russian oil products by disguising their origin through offshore transshipments, blended cargo, and shell companies, whilst European financial and corporate support played a significant role in keeping this system afloat. For instance, French bank *Société Générale* reportedly financed Coral's trading activity with at least €51.9 million, and Austria's *Raiffeisen Bank* had an outstanding credit of €2.2 million as of May 2024. UBS in Switzerland also had financial links, though on a smaller scale. These banks provided essential low-interest funding, giving the 'blue' side of the network access to capital much cheaper than what would be available within Russia.

Moreover, major European insurers, such as Britain's *West of England* and Norway's *Gard*, provided maritime insurance for shipments that likely violated the EU's price cap on Russian oil products. Meanwhile, oil giants such as **TotalEnergies**, **Shell**, and **BP** continued trading with Coral, despite the introduction of sanctions. Though these companies claimed compliance and due diligence through origin certificates, such documentation has been shown to be easily falsified. This Coral Energy case illustrates how **European financial institutions, insurers, and corporations have indirectly supported the Kremlin's war effort** by enabling continued exports of Russian oil in violation of sanctions. Despite legal frameworks and regulatory warnings, economic incentives and loopholes continue to undermine Europe's sanctions regime.

Greece, an EU member state party to sanctions on Russia has also emerged as one of the most significant hubs for providing such logistical support to the Kremlin. The Greek connection in the Coral case, for example, is subtle but highly significant, particularly in this context of maritime logistics, which are critical to sanctions evasion schemes involving Russian oil. One of the key methods used by Coral Energy and its affiliated shell companies to evade sanctions is **transshipment at sea**, a process where oil is transferred between ships away from port scrutiny. A notable example took place in Greece's Laconian Gulf, off the coast of the Peloponnese, which has become a hotspot for these covert maritime operations.

Box 3. Greek Ship-to-Ship Transfers

On December 29, 2023, a vessel named *Osaka* – which had loaded naphtha from the Russian Black Sea port of Novorossiysk – transferred its cargo at sea to another vessel, the *Marlin-Lome*. This Greek coastal location was deliberately chosen to avoid detection by port authorities and customs. Satellite imagery confirmed the transshipment, which was part of a broader strategy to disguise the Russian origin of oil products and move them on to international buyers such as Switzerland's *Trafigura*. Despite Greece having enacted restrictions on ship-to-ship transfers after the Russia-Ukraine war, the use of Greek waters and Greek-owned, or-flagged vessels reflects the broader challenge of maritime enforcement—and EU member states complacency regarding sanctions enforcement. Greece is home to one of the largest merchant fleets in the world, and many shipping companies operate with layers of opacity, using foreign flags and shell ownership structures.¹

I. Reuters, "Greece extends naval advisory to deter Russian oil ship-to-ship transfers", *Reuters World*, 8 May, 2024.

A number of Greek individuals and their business dealings have also come under scrutiny for their involvement in violations of the embargo on seaborne imports of Russian crude oil, first by transporting the oil themselves and later by selling ships to obscure buyers with ties to Russia.^{134,135} Following the imposition of the \$60-per-barrel price cap on Russian crude oil in December 2022, Greek ships played a major role in keeping Russia's oil trade alive.¹³⁶ Almost 50% of tanker capacity departing Russian ports is currently provided by Greek vessels, a substantial increase from 33% before the war.¹³⁷ In February 2024 alone, on the second anniversary of the war, around 841,132 tons of Russian crude oil were delivered to the EU in violation of the embargo, and four crude oil tankers that made voyages facilitating these deliveries were owned by Greek companies: the *Nissos Delos*, *Seavigour*, *Minerva Olympia* and the *Ephesos*.¹³⁸

The Greek role doesn't stop at transporting sanctioned fuel. Greek companies found a more profitable strategy – selling their tankers, particularly older ones, to mysterious buyers in countries not bound by Western sanctions. Following the imposition of sanctions, the Kremlin rushed to develop a network of aged (15-20+ years old), clandestine oil tankers to evade international monitors and restrictions. The Kremlin has invested approximately \$10 billion since early 2022, which has resulted in a **shadow fleet numbering somewhere between 400-1,200 ships**.¹³⁹ This fleet is another one of the Kremlin's highly intricate criminal operations at sea. It operates by signalling incorrect geolocations, hiding its true location and hence being able to operate without being seen. In addition, the use of conveniently flagged ships helps oil to reach Turkey, China, and India with less suspicion. The flags under which they operate are mainly the Cook Islands, Gabon, Liberia, Marshall Islands, and Panama, among others. By operating under these jurisdictions' flags international sanctions can be easily bypassed since the ships can circumvent seizures or interdictions. These flags are explicitly chosen because they do not enforce EU/G7+ sanctions, allowing them to continue exporting Russian oil with minimal restrictions.

Since the war began, Greek firms have sold nearly 300 ships, worth billions of dollars, far surpassing any other nation. These vessels largely end up in the UAE, China, Turkey, and India, nations that have either increased imports of Russian oil or served as hubs for its redistribution. Many of the new owners are shadowy entities with little to no public profile whose ships lack proper insurance or clear ownership, complicating accountability and oversight.

¹³⁴ Levi, I., *Russian oil on EU soil: Bulgarian refinery skirts sanctions and buys Russian crude worth an estimated EUR 1.1 billion in tax to the Kremlin*, Helsinki: Centre for Research on Energy and Clean Air, Center for the Study of Democracy, 2024.

¹³⁵ Jack, V., "Putin rakes in extra €1B for his war chest via Bulgaria sanctions loophole", *Politico*, November 9, 2023.

¹³⁶ Center for the Study of Democracy, *Sanctions Evasion and Derogation on Russian Oil*, Policy Brief No. 140, November 2023.

¹³⁷ Braw, E., "Greece Is Making a Killing Selling Ships to Russia", *Foreign Policy*, September 11, 2023.

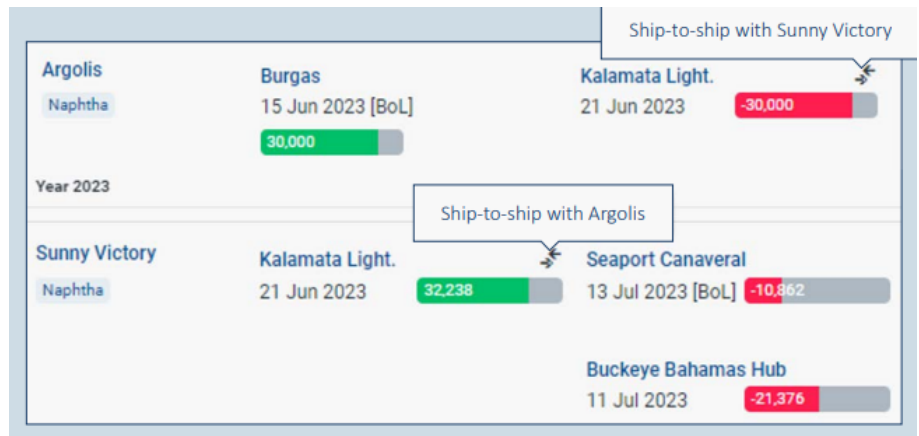
¹³⁸ Black Sea Institute of Strategic Studies, "Violations of the embargo on the imports of crude oil from Russia into the EU in February 2024", *Black Sea News*, March 15, 2024.

¹³⁹ Hilgenstock, B., Hrybanovskii, O., and Kravtsev, A., *Assessing Russia's Shadow Fleet: Initial Build-Up, Links to the Global Shadow Fleet, and Future Prospects*, Kyiv School of Economics (KSE) Institute, June 2024.

The export of Russian oil, an internationally sanctioned good, violates said sanctions; however, the very structure of the shadow fleet itself involves additional violations. First of all, focusing on the oil itself, there are several techniques to hide its origins. Ship-to-ship transfers are one of the most common methods. This method consists of transferring liquid cargo between two, or more, ships in open water. This is usually done multiple times to blur the origins of the oil. This is done in several areas, the Mediterranean and the Black Sea being two of the most prominent ones. Following the imposition of Greek restrictions on ship-to-ship transfers after the Russia-Ukraine war, STS activity experienced a sharp initial decline, with cargo volumes dropping significantly before stabilizing – yet still 40% below pre-restriction levels, indicating a lasting operational impact. Between May and August 2024, a total of 122 STS transfers took place in alternative locations, with the Malta lightering area alone accounting for 44% of these activities, followed by Augusta (9%) and Lome (7%). This shift, involving 236 vessels in 2024 alone and the relocation of 85% of previously active ships from Greek waters, underscores the maritime sector’s adaptability in response to changing regulatory pressures.¹⁴⁰

In essence, Greek shipowners have profited immensely from both the continued transportation and the strategic sale of tankers, enabling Russia to sidestep sanctions and keep its oil economy afloat. While technically legal, their actions have undercut international efforts to pressure Russia economically and have introduced significant safety and environmental hazards to the global maritime industry.

Figure 4. A Ship-to-Ship Transfer of Russia-made Oil Products to the US



Note: The vessels Argolis and Sunny Victory undertook a ship-to-ship transfer at Kalamata Lighthouse (Greece), transferring the 30,000 MMbbl of naphtha.

Source: KPLER based on assessment by CREA; CSD.

¹⁴⁰ Bogdanos, K., “Greece ‘behind Russia’s ability to evade EU sanctions’”, *Brussels Signal*, January 12, 2024.

The evasion of sanctions on Russian oil reveals not only the adaptability of global maritime logistics but also the strategic entwinement of criminal activity with statecraft in the Kremlin's toolkit. Far from being isolated acts of smuggling, these activities – ranging from the use of shadow fleets and STS transfers to the exploitation of legal grey zones via non-sanctioning states – form a deliberate and sophisticated campaign to undermine Western sanctions. The use of criminal tactics, opaque corporate structures, and permissive jurisdictions allows Russia to maintain vital energy revenues, which in 2023 alone generated €5.4 billion in tax income via Turkish oil re-exports. This blurring of lines between criminal enterprise and state strategy reflects a broader pattern of how the Russian state leverages transnational illicit networks not only for economic survival under sanctions but also as a means of asserting geopolitical resilience and influence in the face of Western pressure.¹⁴¹

The Cybercriminals

Russia has widely adopted the use of Crime-as-a-Service (CaaS) in its political war on Europe and the West, particularly in employing cybercriminals. Though the country's information technology (IT) sector constituted not even 6% of its GDP before it invaded Ukraine in February 2022, Russia is commonly recognised as a major cyber power.^{142,143} Of course, as with all other aspects of Russian power, Putin has co-opted all cyber abilities of the Russian state for his war on the West, and, like his grand bargain with the oligarchs and criminal network, the cyber-criminal class is not immune from being drafted into the service of the Kremlin.¹⁴⁴

Indeed, wherein the collapse of the Soviet Union facilitated Russia's rise as a 'Superpower of Crime,' a Mafia State and all other such labels, the collapse also allowed the Russian Federation to become an elite cyber force. Pervasive networks of corruption join IT professionals, the state and those involved with organised crime together, which allows for their use as a tool for Putin's geopolitical goals.¹⁴⁵ However, the Russian Federal Security Service's Centre for Information Security had originally suffered from a limited number of technical staff, with the more talented of Russia's IT professionals tending to be attracted by the higher salaries of the private IT industry, both domestically and in the West. With the more talented IT-savvy workers in legitimate businesses, cybercriminals would be recruited, sometimes straight from technical colleges, to work for the FSB – or the Directorate K of the Ministry of Internal Affairs. In other cases, cybercriminals would be recruited once they proved their hacking abilities. When a foreign government, generally Western, raised concerns about online crime and sought assistance from the Russian state in disrupting this criminal activity, the perpetrators would instead often end up

¹⁴¹ Raghunandan, V., Vladimirov, M., and Levi, I., *A Kremlin Pit Stop: The EU imported EUR 3 bn of oil products from Turkish ports handling Russian oil*, Sofia: Center for the Study of Democracy; Helsinki: Centre for Research on Energy and Clean Air, 2024.

¹⁴² Voo, J., Hemani, I., and Cassidy, D., *National Cyber Power Index 2022*, Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2022, p. 7.

¹⁴³ Jackson, A., *How the Collapse of the Soviet Union Made Russia a Great Cyber Power*, Cyber Defense Review, 2024.

¹⁴⁴ Insikt Group, *Dark Covenant 2.0: Cybercrime, the Russian State, and War in Ukraine*, Boston: Recorded Future, 2023.

¹⁴⁵ Jackson, *How the Collapse of the Soviet Union Made Russia a Great Cyber Power*, Cyber Defense Review, 2024.

working for the Russian government.¹⁴⁶ During the annexation of Crimea, the extent of the Russian security services' pioneering use of cybercrime as a tool of statecraft was revealed.

Since Putin expanded his war to the wider West following February 2022, the Russian state has been forced to rely on more ad-hoc working relationships with cybercriminals, primarily driven by profit or protection, to complement the work of its intelligence agencies. Criminals, who are primarily motivated by financial gain, continue to sell their cybercriminal services to the Russian state, often in exchange for cryptocurrency and state protection. This assists the Kremlin's ability to maintain a veneer of **plausible deniability** and to **conduct its hybrid-cyber warfare on the West at a smaller expense than expanding its in-house capabilities**.¹⁴⁷

Most notable cases of CaaS have been cyber-attacks, 'the apex of Crime-as-a-Service.'¹⁴⁸ Of these, a significant amount have been Distributed Denial of Service (DDoS) attacks on European countries' public institutions, whereby the Kremlin's cybercriminals seek to spread chaos amongst these state's publics.

This new type of criminal business model, CaaS, refers to the provision of cybercriminal tools and software to other actors who wish to commit cyber-crimes. Those who provide this business offer their services to anyone who will pay them, operating like legitimate businesses, ensuring that anyone who lacks the expertise to commit cybercrimes on their own can do so. The dynamic, complex and fragmented nature of the digital underground drives this economy, as cybercriminals diversify their skill set and areas of expertise to develop a market niche. This has contributed to the booming hidden 'service industry,' allowing for mass access to cyber-crime services that would previously have been hard to come by (or develop themselves). These services were mostly advertised on underground online forums – criminal marketplaces where resources are pooled, experience and expertise shared, and of course, where wares are bought and sold. These forums have generally been located on the Deep Web or the Darknet, providing anonymity and preventing tracking of the buyers and sellers.¹⁴⁹ CaaS providers operate akin to any other tech/IT development company, with the entity (cybercriminal) developing a product that can be sold or rented to consumers who lack the means to commit cybercrimes on their own – and do so very cost-effectively. Europol has identified some of the most common services that these 'tech businesses' provide:

Infrastructure as a Service: Would-be cyber criminals require infrastructure with which they can commit their crimes. Such infrastructure includes VPNs and proxy services that safeguard anonymity, hosting providers perform a critical role in offering secure storage for attack tools like malware and exploit kits, and 'bullet-proof hosts' offer customers needed resilience to evade law enforcement intervention.

¹⁴⁶ Former Chief Technology Officer Milan Patel, of the FBI's Cyber Division; cited in Insikt Group, *Dark Covenant 2.0: Cybercrime, the Russian State, and War in Ukraine*, 2023.

¹⁴⁷ Google Threat Intelligence Group, *Cybercrime: A Multifaceted National Security Threat*, Google Threat Intelligence, February 12, 2025.

¹⁴⁸ Europol, *Cyber-attacks: the apex of crime-as-a-service – Spotlight Report*, Internet Organised Crime Threat Assessment (IOCTA) 2023, 2023.

¹⁴⁹ Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2014*, 2014.

Distributed Denial of Service (DDoS) attacks are malicious, coordinated attempts to flood target machines with traffic to prevent normal functioning. The metaphor of a shop door being inundated with fake customers, preventing legitimate customers from entering and doing business, has often been evoked. They are generally used for hacktivism, extortion, retaliation or rivalry aims.

There has been a significant increase in the amount of DDoS attacks since Russia's invasion of Ukraine. In its political war on Europe, the Kremlin has coordinated attacks by pro-Russian hacker groups on the critical infrastructure and public institutions of EU member states and their Western allies, particularly those who demonstrate support for Ukraine in the conflict. A notable example of this comes in the form of **Killnet**, a pro-Russian hacktivist group. They claimed responsibility for attacks on the European Parliament, the Ministry of the Interior of Latvia and Connecticut's Bradley International Airport, amongst others.¹⁵⁰ These DDoS attacks have long formed a component of Russia's use of cybercrime as a tool for statecraft. Notable other incidents took place in Estonia in 2007, Georgia in 2008 and Ukraine between 2014 and the invasion.

Data-as-a-Service: Data has long been a central commodity of cybercrime. Credit cards, addresses, names and dates of birth, credit card and bank account details and other information have been highly sought after for those seeking to commit 'identity fraud' on unrealising victims. More recently, data such as social media account information, e-wallets and web logins (such as into an individual's work accounts) are increasingly sold on online underground markets. This also assists criminals to commit online and offline fraud.

Pay-per-Install Services: This refers to a type of business model whereby service providers receive remuneration depending on the number of downloads or installations their software gets. It is a popular way of receiving payment from selling malware.

Malware-based cyber-attacks "remain the most prominent threat and consist of multiple types of malware and intrusion techniques being deployed in conjunction in different attack stages."¹⁵¹ These attacks are usually defined by their end impact. For example, when malware is used to extract ransom from the victims, it is termed ransomware (which is the top threat). One recent example comes in the form of *RacoonStealer*, the product of a 'prolific Ukrainian cybercriminal' who fled the war in Ukraine. This was a data theft malware that had operated since 2019 and was sold to other criminals – with some paying \$200 per month in cryptocurrencies to use it.¹⁵²

Like DDoS attacks, malware has also been utilised as a tool for Russian statecraft abroad, and, as with the DDoS attacks on Estonia, Georgia and

¹⁵⁰ Avertium, *An in-depth look at Russian threat actor, Killnet*, 2022; cited in Europol, 2023.

¹⁵¹ Europol, *Cyber-attacks: the apex of crime-as-a-service – Spotlight Report*, Internet Organised Crime Threat Assessment (IOCTA) 2023, 2023, p. 7.

¹⁵² Europol, *Cyber-attacks: the apex of crime-as-a-service – Spotlight Report*, IOCTA, 2023, p. 7.

Ukraine, most come from one source: **Sandworm**. Sandworm is a cyberwarfare unit within the GRU¹⁵³ and is operated by Military Unit 74455. Sandworm has been accused of notable incidents including attempted blackouts in Ukraine using Industroyer malware (April, 2022), attacks on Denmark's power grid,¹⁵⁴ the Olympic Destroyer attack on the 2018 Winter Olympics, and spear-phishing campaigns targeting France's 2017 presidential election (which resulted in the indictment of six Russian nationals by the US government).¹⁵⁵

Hacking-as-a-service (HaaS) is similar to data-as-a-service in that it seeks to obtain similar data, like credit card information or the social media account information of a victim. Where it differs, though, is how it uses the information when stolen. HaaS instead seeks to 'stay in' the accounts it has penetrated, for whatever motivation the criminal has. Hackers may take advantage of an individual's social media accounts for their aims, hijack telephone numbers, use hacked accounts to take down communication infrastructure or command and control an army of bots, with which they can launch DDoS attacks. Hackers offer their services for a wide variety of goals: tracking, website defacement, intelligence gathering, malware distribution or DDoS.¹⁵⁶ A notable example of HaaS took place following Russia's invasion of Ukraine, which again, involved Sandworm. Throughout 2023, Sandworm allegedly spent several months inside *Kyivstar*, the largest mobile phone operator in Ukraine. This allowed the GRU to collect intelligence before launching an attack that would disrupt the network's services for 24 million users.¹⁵⁷

Translation Services: Many campaigns target victims in specific countries, for which the attacker may not be a native speaker of the target language. The use of translators to provide grammatically correct scripts maximises the impact of a campaign as poor language is often a giveaway that a particular message is part of a scam.

Disinformation Storms: The Kremlin's cyber-criminal networks have also been weaponised as a component of its foreign information manipulation and interference, disinformation and propaganda campaigns against the West.¹⁵⁸ By employing vast swaths of Russia's abundance of tech-savvy youth¹⁵⁹ alongside its other CaaS networks, the Kremlin affords itself an army of potential trolls to conduct influence operations on Europe. This could involve coordinated trolling campaigns, the manipulation of 'news,' the poisoning of elections (such as in Romania), the creation of fake social media accounts and the spreading of extremist/hate content which seeks to polarise communities from within.¹⁶⁰

¹⁵³ The Main Directorate of the General Staff of the Armed Forces of the Russian Federation.

¹⁵⁴ Prince, B., *Sandworm Team Targeted SCADA Systems: Trend Micro*, Security Week, 2014.

¹⁵⁵ Cerulus, L., "US calls out Russia for Macron campaign hack, even as France stays silent", *Politico*, October 20, 2020.

¹⁵⁶ Schram, G., *Hacking As A Service*, Cybrary, 2021.

¹⁵⁷ Galeotti, *Gangsters at War: Russia's use of organised crime as an instrument of statecraft*, GI-TOC, 2024.

¹⁵⁸ Novossiolova, T. and Georgiev, G., *Countering Hybrid Warfare in Bulgaria: A Strategic Assessment of National Capabilities and Infrastructure*, Sofia: Center for the Study of Democracy, 2023.

¹⁵⁹ Jackson, *How the Collapse of the Soviet Union Made Russia a Great Cyber Power*, Cyber Defense Review, 2024.

¹⁶⁰ Europol, *European Union Serious and Organised Crime Threat Assessment - The Changing DNA of Serious and Organised Crime*, 2025.

Disposable Hoodlums: Espionage, Assassinations and Active Measures

The mobilisation of almost every aspect of Russian society for Putin's 'special military operation' in Ukraine has left several other industries in Russia seriously short of manpower. As with other occasions in Russian history, particularly when its economy constricts or undergoes turmoil, the Russian state has turned to criminal networks to plug this hole. This has led to the employment of criminal networks that contribute to intelligence gathering, conducting sabotage and arson campaigns, and attempting assassinations throughout the European continent, all in support of Putin's foreign policy aims.¹⁶¹ The Kremlin has been forced to rely on 'operatives' with questionable abilities for such 'dumpster operations.'¹⁶² These low-level hoodlums are now forming the Kremlin's 'disposable' **sharp power force**, attempting to influence the internal political and social environments of the Kremlin's adversaries.¹⁶³

Not only were widespread sanctions imposed following the onset of the war in Ukraine, but scores of Russian diplomats and embassy officials were declared *persona non grata* by Europe and the US, and were expelled. By May 2022, approximately 425 staff from Russian embassies, consulates and trade missions were expelled from (mainly) Europe's NATO member states, the US and Japan. By the following year, this number would rise to around 600 – and is now believed to be over 750 from Europe alone.¹⁶⁴ The government of the Netherlands, who expelled 17 diplomats, explained the reasoning behind their actions: that these individuals were not diplomats – but instead were intelligence officers masquerading as diplomats.¹⁶⁵

That Russian diplomatic officials in their missions in Western states had been instead intelligence officers did not strike many as breaking news. In 2018, for instance, over 150 Russian diplomatic officials were expelled from Western states, in response to Russia's increased aggression. This was primarily in response to "Russia's use of a military-grade chemical weapon on the soil of the United Kingdom, the latest in its ongoing pattern of destabilizing activities around the world."¹⁶⁶ As Russia's destabilising activities, or '*shalit*,'¹⁶⁷ have only increased in intensity since 2018, such mass expulsions represent a natural response to Putin's war of aggression.

The loss of over 600 diplomats, all of whom were potential agents for the Kremlin's espionage activities, has had a serious impact on the effectiveness of Russia's intelligence community. Compounding their problems is the increased resources now devoted to Putin's war on Ukraine. The Russian state has thus turned to criminal networks and other low-level assets to plug this hole in their intelligence-gathering capabilities.

¹⁶¹ Walker, S., "'These people are disposable': how Russia is using online recruits for a campaign of sabotage in Europe", *The Guardian*, May 4, 2025.

¹⁶² Huppertz, C., et al., 'Make a Molotov Cocktail': How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder, *Organised Crime and Corruption Reporting Project (OCCRP)*, September 26, 2024.

¹⁶³ The Times, "Killings, coups and chaos: inside Putin's secret spy war on Europe", June 28, 2024.

¹⁶⁴ McCallum, K., "Director General Ken McCallum gives latest threat update" [Speech], MI5 Security Service, *Counter Terrorism Operations Center*, October 8, 2024.

¹⁶⁵ Al Jazeera, "European countries expel dozens of Russian envoys", March 29, 2022.

¹⁶⁶ The White House, *Statement from the Press Secretary on the Expulsion of Russian Intelligence Officers* [Press Release], March 26, 2018.

¹⁶⁷ To make mischief or chaos.

The use of **local criminal actors** throughout Europe has several obvious benefits to Russia's intelligence community and the GRU. By **recruiting 'disposable agents' for low-level operations**, more skilled agents may be made available for more complex operations, and the use of disposables allows for degrees of deniability should an operation go awry. Indeed, there is effectively no downside.¹⁶⁸ These low-level, day-to-day intelligence operations also tend to correlate with the day-to-day activities of local criminal networks, such as drug smugglers. These activities include jobs like 'dead-letter boxes,' exchanging encrypted messages and conducting and reporting on simple surveillance.¹⁶⁹ Some tasks involve monitoring military drills or the flows of military aid, though some more complex operations involve utilising people smuggling gangs to try and discretely move high-value Russians from the watch of Western intelligence services. This was the case with Russian businessman Artem Uss, who was sprung from house arrest in Italy by Serbian people smugglers.¹⁷⁰

These disposal agents are often local recruits, who operate without the suspicions associated with Russian nationals. These disposables may sympathise with the Kremlin, be motivated by financial gain or possibly not even be aware that they have become a tool in the Kremlin's sharp power playbook. For example, Dylan Earl (20) and Jake Reeves (22) were charged with helping Russian intelligence services following a suspected arson attack on a warehouse in London in March 2024. Two other British nationals were charged for contributing to the attack, whilst Reeves was also accused of knowingly accepting money from a foreign intelligence service.¹⁷¹ Such low-level disposable agents can be recruited through platforms like Telegram, chat functions of online games, or other online platforms.¹⁷²

Box 4. Telegram Recruitment

An example of a Telegram recruitment platform comes in the form of the 'Grey Zone,' a 550,000 subscriber-strong, pro-Russian channel associated with the Wagner Group. It regularly posts the Kremlin's propaganda narratives, shares sabotage footage and encourages individuals to stand up against the corrupt (Western) politicians manipulating the public. It also regularly suggests subscribers interact with a recruiter account – 'Privet Bot.'

This Privet Bot (*Privet* means hello/hi in Russian) account gathers initial information and 'work experience' from prospective operatives, such as their name, date of birth, current location, proof of identity and possi-

¹⁶⁸ Cited in The Times, "Killings, coups and chaos: inside Putin's secret spy war on Europe", June 28, 2024.

¹⁶⁹ Galeotti, *Gangsters at War: Russia's use of organised crime as an instrument of statecraft*, GI-TOC, 2024, p. 29.

¹⁷⁰ Giles, K., "Killings, coups and chaos: inside Putin's secret spy war on Europe," *The Times*, June 28, 2024.

¹⁷¹ Fatima, Z., "Two Men Charged over Alleged Russia-Linked Arson Plot", *BBC News*, August 3, 2024.

¹⁷² Jones, *Russia's Shadow War Against the West*, Washington, D.C: CSIS Briefs, 2025.

ble military experience. The account states that successful recruits may receive around \$10,000 per mission, and details the most sought-after types of operations: burning a Ukrainian military vehicle or a truck carrying military equipment; killing ‘fascists’ in their local environment; or conducting acts of sabotage on fuel depots. However, self-motivation and ingenuity is greatly encouraged.¹

I. Huppertz, C., et al., “‘Make a Molotov Cocktail’: How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder”, *Organised Crime and Corruption Reporting Project (OCCRP)*, 26 September, 2024.

In addition, criminal money laundering networks are also used to pay other criminals in the Kremlin’s employ. For instance, the vast money-laundering empire of two linked criminal networks, Smart and TGR, was recently uncovered by the UK’s National Crime Agency. Smart and TGR were revealed to have, in essence, acted as a bank to numerous criminal organisations and sanctioned individuals. These empires are described as ‘**multinational, poly-criminal enterprises**’ that defy easy categorisation, combining traditional cleaning techniques such as ‘front’ businesses and cash couriers “hiding bundles of notes in boxes of washing powder” with emerging techniques like the use of US dollar-backed stablecoins, like Tether (USDT).¹⁷³ These techniques have been used by individuals acting on behalf of Russia, like Dylan Earl and Jake Reeves, and are used to fund the Kremlin’s other malign activities in Europe, such as cyber-criminals, saboteurs and actors spreading Russian mis- and disinformation.

As the arson attack on the London warehouse attests to, the Kremlin has also used disposables, including local criminal actors, to carry out its active measures campaign across Europe. In this regard, Russia found its most willing conspirators in **Serbia** and **Bulgaria**, owing to the significant cultural capital and high levels of political support Russia enjoys in the two countries, coupled with the significant presence of criminal networks in these Balkan states.^{174, 175}

Other campaigns are more sinister. As the Kremlin turned to utilising criminal networks to fill manpower gaps, it had also re-discovered the old Soviet tradition of using **active measures** as a hybrid war tool. By committing acts of arson and other acts of sabotage, cyber-attacks (such as those listed in the section above), assassination attempts, kidnappings and attacks on critical infrastructure (and using disposables to do so), Russia has been able to continue its political war on the West without triggering a NATO response. Though too numerous to comprehensively list, not to mention the varying degrees of evidence linking acts to the Kremlin, notable examples of such attacks can be found in Germany, Poland, the Baltic States and the Balkan countries in particular. Russia is believed to have masterminded arson attacks on: a mall

¹⁷³ MacColl, J. and Westmore, K., *Operation Destabilise: Russia, Organised Crime and Illicit Finance*, London: Royal United Services Institute (RUSI), 2024.

¹⁷⁴ Andrei Soldatov, cited in “Killings, coups and chaos: inside Putin’s secret spy war on Europe”, *The Times*, June 28, 2024.

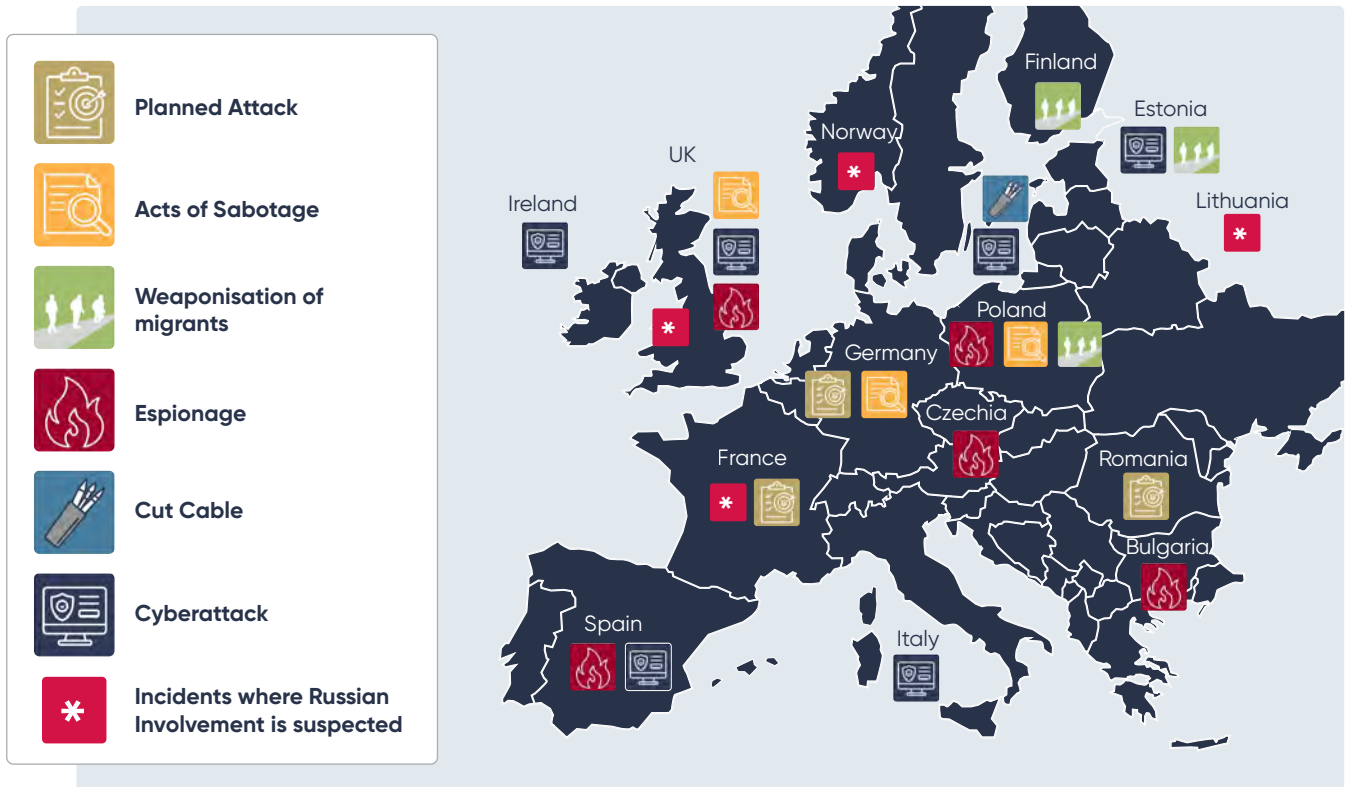
¹⁷⁵ Sabev, Georgiev and McLaren, *Safeguarding the Foundations*, Sofia: CSD, 2024.

in Warsaw (May 2024), an Ikea store in Vilnius (May 2024), a warehouse in London (March 2024), a Ukrainian logistics company in Madrid (March 2024), and a bus depot in Prague, which failed (June 2024).

The Kremlin is also specifically targeting Western **arms manufacturers and military facilities**, and is believed to be behind: a series of suspicious fires and explosions targeting Bulgarian arms company Emco, attempts to assassinate the CEO of German defence manufacturer Rheinmetall Armin Papperger (July 2024), foiled attempts to attack a military base in Bavaria (April 2024), an explosion and resulting fire at a BAE Systems manufacturing plant in Wales (March 2024), the severing of a communications cable at Evenes Air Base in Norway (April 2024), a fire in a Pennsylvania artillery shell manufacturer (March, 2024) and an explosion in a munitions manufacturing plant in Arkansas (July, 2024).

More complex operations targeting Europe include several attempts to **sabotage submarine telecommunications and gas infrastructure in the Baltic Sea**, fibre optic lines in Marseille (October 2022) and possibly the cyber-attacks at the Paris Olympic games in July 2024. Whilst some of these examples may be too sophisticated for the Kremlin's disposable assets, local criminals or cash-strapped locals working on behalf of the Kremlin are believed to be behind several of the above-listed examples. For instance, the Kremlin's weaponisation of migrant flows, particularly at the Poland-Belarus border, almost certainly involves the use of criminal gangs who specialise in migrant smuggling working for Russia (discussed below).

Figure 5. The Kremlin's Shadow War on Europe



Source: CSD.

Though many of these may seem random or unrelated, especially if conducted by criminal networks operating on opposite sides of the continent with no relation to each other, these criminal actors are nonetheless contributing to the Kremlin's foreign policy goals. This approach has been labelled as the '**woodpecker modus operandi**,' whereby incidents may originally be assessed as single events, but rather are:

"part of a larger strategic objective of destabilisation, involving persistent, targeted and cumulative disruptions rather than a single, overwhelming attack. Much like a woodpecker weakens a tree over time through repeated strikes, hybrid threat actors engage in ongoing, seemingly minor actions that collectively erode stability, security, and trust in institutions."¹⁷⁶

The People Smugglers

The Russian State is sponsoring any type of activity that may spread '*shal-it'* and destabilise Europe. The ultimate goal of spreading chaos throughout Europe is to make its populations feel vulnerable and unsafe, to undermine citizens' faith in their government's ability to protect them, demonstrate the power and reach of the Kremlin, and to spread the perception that the cost of further support to Ukraine would be too high.¹⁷⁷ Once again, this aligns with the Kremlin's sharp power aims of **influencing the domestic environments of Russia's adversaries**. Another technique the Kremlin has exploited to do this is sending vast numbers of migrants to the EU, to manufacture a perception that, if the EU cannot defend and control its own borders from migrants, how can it do so against the might of the Russian Federation? This does not only undermine public faith in mainstream political parties but also pushes concerned members of the public into the arms of (generally) extremist, far-right parties who often sympathise with the Kremlin, such as the *AfD* in Germany or Bulgaria's *Vazrazhdane*. This weaponisation of migration therefore forces the hand of European states: do they close borders, alienating the EU's neighbours and contradicting their obligations regarding migration, such as the principle of non-refoulement; or do they continue business as normal whilst attempting to fight off far-right nativist parties domestically, for all the danger that brings?

Concerns regarding the use of migration as a hybrid weapon have been growing for several years. In 2021, for instance, the European Commission proposed a regulation addressing situations of instrumentalisation of migration, and in 2024, passed a regulation amending it, to address situations of crisis and *force majeure* in the field of migration and asylum. The former was seen largely in response to the "state-sponsored instrumentalization of people at the EU's external border with Belarus" enacted by the regime of Aleksandr Lukashenko.¹⁷⁸ Lukashenko, in response to sanctions enacted by the EU (im-

¹⁷⁶ Europol, *European Union Serious and Organised Crime Threat Assessment - The Changing DNA of Serious and Organised Crime*, 2025, p. 15.

¹⁷⁷ Apps, P., "Russia's suspected sabotage campaign steps up in Europe", *Reuters*, October 21, 2024.

¹⁷⁸ Mentzelopoulou, M. M., *Instrumentalisation in the field of migration and asylum* [Briefing Paper], European Parliamentary Research Service, PE 739.204, 2022.

posed following the fraudulent presidential election in 2020 and suppression of civil society), began supporting migrants' attempts to enter the EU *en masse*. Belarusian authorities targeted Lithuania, Poland and Latvia in particular, generally with large numbers of refugees from Iraq, Afghanistan, Syria, Lebanon and Jordan.¹⁷⁹ By October 2021, Poland alone had registered approximately 23,000 irregular attempts to enter its territory.

Like all other criminal actions mentioned throughout, this too witnessed a dramatic upsurge following Putin's invasion of Ukraine. For instance, in 2024, **irregular migration arrivals** were up 66% compared to the previous year – solely at the Poland-Belarus border.¹⁸⁰ The Kremlin has sought to entice migrants from regions like the Middle East and North Africa (MENA) to migrate to the EU, generally via Belarus, and through the borders with Poland, the Baltic states, and Finland, and is doing so through a variety of means and many actors.

Box 5. Belarus' Role in Weaponising Migration

Belarus has been known to utilise its tourist agencies to offer trips to the country to citizens of Middle Eastern countries. These tours would be sold as opportunities for these citizens to enter the EU, which is 'easy to do' from Belarus.ⁱ The Russian and Belarusian states also provides administrative assistance to these migrants enticed into entering the EU, such as tourist or student visas. Indeed, 90% of migrants who illegally crossed the Polish-Belarusian border in 2024 had either a Russian tourist or student visa.ⁱⁱ Russian diplomatic missions in these migrants' home countries are believed to help these individuals receive these flimsy visas, who receive further logistical support from the Russian intelligence and security services. They often fly to Moscow or St. Petersburg and then travel to Belarus to attempt the crossing.ⁱⁱⁱ

- I. Mentzelopoulou, *Instrumentalisation in the field of migration and asylum*, European Parliamentary Research Service, 2022.
- II. Polish President Donald Tusk, cited in MacGregor, M., "Russia alleged to be smuggling migrants to Europe in 'hybrid attack'", *InfoMigrants*, May 22, 2024.
- III. MacGregor, "Russia alleged to be smuggling migrants to Europe in 'hybrid attack'", *InfoMigrants*, May 22, 2024.

But, with the functions of the Russian state so occupied with Putin's war, and the vast other borders Russia has with the EU that it could potentially weaponise, Belarus' usefulness to the Kremlin in this regard has its limitations. Russia shares a 1,340-kilometre-long border with Finland, whilst it also borders the three Baltic states and Poland (through Kaliningrad). Thus, as with all other aspects of its hybrid war on Europe, the Kremlin has turned to organised criminal networks. As mentioned, Russia has long been a hub for people smuggling and the trafficking of human beings, and, as such, has a significant presence of people smuggling rings in the country. It has sought to partner

¹⁷⁹ Mentzelopoulou, *Instrumentalisation in the field of migration and asylum*, European Parliamentary Research Service, PE 739.204, 2022.

¹⁸⁰ European Commission, *Commission steps up support for Member States to strengthen EU security and counter the weaponisation of migration* [Press Release], December 11, 2024.

with these Russian-based organised criminals and other foreign criminal networks in a form of malign ‘public-private partnership’ towards its hybrid war aims.¹⁸¹

Attempting to maintain a thin veneer of deniability, the Kremlin employs existing migrant smugglers and their networks based in or dominated by individuals from MENA. Often, these migrant smugglers have been approached through a Russian interlocutor, who may do business with this MENA gang. Militias, such as the Wagner Group, also have cooperated with local warloads in the region to help migrants find their way to fortress Europe. One notable instance comes from Khalifa Haftar, the warlord and commander of the Libyan National Army militia, who has worked closely with Kremlin-lined militias to ensure this.^{182,183} A recent Times investigation highlighted the case of a Yemini smuggler, ‘Abu Radad,’ whose expertise includes smuggling migrants from Russia to the UK, with the help of his Russian business partner. As with the Kremlin’s new ‘disposable’ agents, Abu Radad ‘recruited’ (manipulated) his clients through online platforms such as Telegram and WhatsApp, who may unwittingly be contributing to the Kremlin’s hybrid war.^{184, 185, 186} This reputation was in part built by Kamal’s connections with corrupt officials who can help migrants enter the EU, particularly on the border with Finland.¹⁸⁷ The nexus between individuals such as Kamel and Abu Radad and state officials provides Russia with a ‘surge capacity’ that could be mobilised when the Kremlin wishes to pressure a neighbour with weaponised irregular migration.

Donbasionisation: Annexation and Buffer-Zones

In addition to contributing to the capture of the Donbas for the Russian state in 2014, criminal gangs and other illicit networks have also assisted the Kremlin in managing the region, too. Owing to the lack of international recognition the captured territory received, the controversies surrounding effective taxation from either Kyiv or Moscow and the lack of policing, the Luhansk and Donetsk ‘People’s Republics’ (LDPR) found themselves prime targets for organised crime groups.¹⁸⁸ International sanctions grossly reduced the availability of a significant amount of goods, and, as in the case of the former Soviet Union, criminal networks would play an important role in providing necessary products for these unrecognised states. Even though the Donbas has long

¹⁸¹ Galeotti, *Gangsters at War: Russia’s use of organised crime as an instrument of statecraft*, GI-TOC, 2024.

¹⁸² Knipp, K., “Russia’s role in trafficking, smuggling from Libya to EU”, *Deutsche Welle*, April 22, 2025.

¹⁸³ Megerisi, T., “The Bear Who Came to Tea: Russia, Libya and the Kremlin’s Playbook for Fragile States”, *European Council of Foreign Relations*, March 28, 2025.

¹⁸⁴ Bakht, S., “How Russia uses migrants as weapons — and why some blame Britain”, *The Times*, March 14, 2025.

¹⁸⁵ Al Mughamir, S. and Spring, L., “EU-migration by way of Russia: is Moscow or Brussels to blame?”, *Open Democracy*, April 3, 2024.

¹⁸⁶ Galeotti, *Gangsters at War: Russia’s use of organised crime as an instrument of statecraft*, GI-TOC, 2024.

¹⁸⁷ Al Mughamir and Spring, “EU-migration by way of Russia: is Moscow or Brussels to blame?”, *Open Democracy*, April 3, 2024.

¹⁸⁸ GI-TOC. *New Frontlines: Organised criminal economies in Ukraine in 2022*, Geneva: Global Initiative Against Transnational Organised Crime, 2023.

existed as an established smuggling route, smuggling and illicit economies would grow still further to become so important that the survival of the region depended on it. The LDPR depends so much on organised crime that it may be more fitting to describe them as 'criminalized pseudo-states'¹⁸⁹ or 'mafia states',¹⁹⁰ in a similar vein to the drug empire status that Syria descended into under Assad.

These criminalised pseudo-states that were nominally independent were of course controlled by Moscow. However, its day-to-day management would be overseen by the criminal networks that had assisted Moscow in the rebellion in the first place. For years prior to 2014, the Donbas was plagued by organised crime. This was driven, amongst other factors, by a decaying industrial economy (particularly coal mining), a significant population of ethnic Russians, an unusually large number of prisons in the area,¹⁹¹ proximity to Russia and a lack of security-efficient institutions. Corruption, drug trafficking, gambling, human trafficking, and Russian-sponsored state capture were rife, whilst pro-Russian gangsters would exchange their muscle for money through protection rackets or other paid services. This might include offering to harass political rivals or interfering with political rallies.¹⁹² As the International Crisis Group states:

"The war in Ukraine's Donbas plunged an economically troubled region into ruin. A 427 km front line cuts through what used to be the most densely populated and industrially productive part of the country. Supply and market links have been shattered. Giant enterprises have shed jobs or collapsed. Entire communities have fallen into poverty, now exacerbated by the COVID-19 crisis."¹⁹³

Initially, those gangsters involved in protection rackets and other organised crime became involved in the pro-Russian protests against the government that replaced the Yanukovich administration in Kyiv. However, when Russian-sponsored actors began seizing key buildings and administration centres, as mentioned above, the 'muscle' of these gangs (often military veterans, athletes or martial artists) became important sources of gunmen. Seeing the potential of these local musclemen, the Kremlin would sponsor their transformation into, essentially, a state-sponsored militia – which it would then use in its hybrid war on Ukraine. As with the Wagner Group, support for such a group enables the Kremlin to destabilise its targeted territory cheaply, with plausible deniability and without the political costs that may potentially be accumulated by using the State's armed forces.

¹⁸⁹ Hedlund, S., *Nonrecognition and Trouble in International Relations*, Geopolitical Intelligence Services, 2019.

¹⁹⁰ Kosicki, P., and Nesterenko, O., "Eastern Ukraine has been a mafia state for years. Can Kiev break the cycle of violence?", *The New Republic*, June 5, 2014.

¹⁹¹ As of 2013, there were 20 prisons in Donetsk and 16 in Luhansk; and many ex-convicts chose to remain in the area following their incarceration (Kosicki & Nesterenko, 2014).

¹⁹² Idris, I., *Corruption, crime and conflict in eastern Ukraine*, SOC ACE: Serious Organised Crime & Anti-Corruption Evidence, University of Birmingham, 2022, p. 12.

¹⁹³ International Crisis Group, *Peace in Ukraine (III): The Costs of War in Donbas*, Europe Report No. 261. Kyiv; Brussels: International Crisis Group, September 3, 2020.

Once the republics were declared, these gangsters would become high-ranking authorities in these self-proclaimed new regimes, where their expertise would prove important for the survival of these states. Realising that the survival of these regimes would depend on criminal networks' ability to smuggle goods into them, the new authorities drafted as many criminals as possible to come to the new states. Beyond smuggling, crimes like extortion and car theft would be necessary for simply paying, or feeding, the insurrectionists – though self-enrichment was no doubt another motivating factor.¹⁹⁴

'Smuggling for survival' grew even more necessary after February 2017, following Kyiv's economic blockade of the LDPR, and, while Russia did provide aid for the region, its assistance extended to just essential state and war-related expenses, leaving a significant gap filled by illicit economies. This 'smuggling for survival' mode of existence offers an interesting comparison to the last major conflict on the European continent.

Following the collapse of Yugoslavia in the early 1990s and the resulting **international arms embargo** imposed on the region,¹⁹⁵ wartime smuggling and arms trafficking, often conducted with the tacit approval or direct involvement of state actors, became vital components of the war economy. As post-socialist states struggled with economic instability amid the broader collapse of state institutions following the dissolution of these regimes, criminal groups expanded their influence, blurring the lines between political elites, security services, and organised crime.¹⁹⁶

The legacy of wartime smuggling and arms trafficking continues to shape the political and economic landscape of the Balkans, underscoring the deep and enduring connections between organised crime and state structures in the post-Yugoslav space. The historical experience of arms smuggling and organised crime during the Yugoslav wars holds critical lessons for Europe as it navigates the ongoing war in Ukraine and its aftermath. It demonstrates how **embargoes, sanctions** and external economic pressures, rather than curtailing conflicts, can **fuel illicit networks** that sustain warfare and shape post-war political economies. The militarisation of post-Yugoslav states, facilitated by underground arms smuggling, underscores how war economies become deeply entrenched, influencing the political trajectories of nations long after hostilities end. This precedent is particularly relevant for Ukraine, where wartime smuggling networks are already emerging amid the ongoing Russian invasion.

As in the Balkans, Ukraine's conflict has led to the proliferation of weapons, paramilitary groups, and illicit trade routes, potentially setting the stage for similar long-term entanglements between political elites and organised crime. The conflict also illustrated that **once criminal networks become integrated into state structures**, they are exceedingly difficult to dismantle, leading to prolonged instability, corruption, and challenges to democratic consolidation – a legacy the Balkan peninsula still wrestles with today.

¹⁹⁴ GI-TOC, *New Frontlines: Organised criminal economies in Ukraine in 2022*, Geneva: Global Initiative Against Transnational Organised Crime, 2023, p. 1.

¹⁹⁵ Hajdinjak, M., *Smuggling in Southeast Europe*, Sofia: CSD, 2002.

¹⁹⁶ Hajdinjak, M., *Smuggling in Southeast Europe*, Sofia: CSD, 2002.

The most significant illicit economies keeping the Donbas pseudo-states alive relate to coal smuggling, the production of counterfeit cigarettes and alcohol, and financial crimes.

Coal mined in the Donbas was generally rerouted through Russia and sold in Europe, circumventing Kyiv's blockade. The Kremlin would utilise intermediaries, such as in South Ossetia, which acted as a conduit to bypass sanctions: LDNR coal is usually mixed with Russian coal and re-exported to the West, often through Belarus. The profits of this illicit trade assisted the LDNR while enriching individuals linked to the trade.¹⁹⁷

Cigarettes and Alcohol products became another prominent illicit trade. LDNR factories have produced, en masse, counterfeit and untaxed cigarettes through companies like Khamadey and Donetsk Tobacco Factory, who operated openly, supplying local and international markets. Corruption and smuggling networks enabled this trade, which peaked in 2016. Similarly, the region produced large quantities of illegal alcohol, which was then trafficked across borders and sold.

Financial Crimes and Cyber Operations also proved vital to the endurance of the criminal empire of the LDNR, with the region being effectively isolated from global financial systems. This, naturally, led to widespread financial crimes. As with coal smuggling operations, banks in South Ossetia would act as intermediaries, enabling transactions between the LDNR and Russia. Cryptocurrency mining would also be exploited as a means to bypass financial controls and market services for international money laundering.¹⁹⁸

Of course, the importance of smuggling operations to the livelihood of the pseudo-states-criminal-kingdoms would ensure that these illicit activities would seep into Ukrainian-controlled territory. The Russian-speaking (or native Russians) from the LDNR sought and developed alliances with their Ukrainian counterparts, together forming "a lucrative transnational smuggling highway between Russia and Western Europe that carried gold, timber, tobacco, coal, counterfeit/untaxed goods, humans and drugs."¹⁹⁹ This organised criminal alliance would develop into the strongest criminal ecosystem in Europe by the beginning of 2022.

Putin's attempted *coup de main* in Ukraine disrupted this flourishing ecosystem. Not only would the new battle lines interrupt the established smuggling routes, but those within the transnational criminal alliance would also break ties. Despite the dubious loyalty organised criminals had held towards the government of Ukraine, working with the Russians was deemed beyond the pale for most. The imposing of martial law would contribute to constricting criminal activity as well.²⁰⁰ The onset of full-scale war would present new opportunities and risks for organised crime in Ukraine and the unrecognised

¹⁹⁷ Idris, I., *Corruption, crime and conflict in eastern Ukraine*, 2022, p. 12.

¹⁹⁸ Galeotti and Arutunyan, *Rebellion as racket: Crime and the Donbas Conflict, 2014-2022*, GI-TOC, 2022.

¹⁹⁹ GI-TOC, *New Frontlines: Organised criminal economies in Ukraine in 2022, 2023*, p. 1.

²⁰⁰ GI-TOC, *New Frontlines: Organised criminal economies in Ukraine in 2022, 2023*, p. 1.

LDPR. Equally, members of organised crime groups would represent both opportunities and risks for the Ukrainian armed forces resisting the might of Putin's army.

Many Ukrainian criminals were swayed by their patriotic instincts into fighting for their country – even if their bosses fled abroad to Romania, Bulgaria, Italy, France or elsewhere.²⁰¹ Yet, these instincts may co-exist with other, more selfish, motivations. Criminals who answered the call may have sought to have their criminal slate wiped clean, or saw an opportunity for furthering their wealth, possibly through arms or conscript smuggling or through the trafficking of war-related refugees.

An Army of Criminals

Regarding Putin's army of criminals during the war, the Wagner Network's infamy increased even further. It famously sustained extraordinary numbers of casualties in its attempt at taking Bakhmut – the vast majority of which were recruited convicts. Growing tensions between Yevgeny Prigozhin and the Russian military leadership, particularly Defence Minister Sergei Shoigu and Chief of the General Staff Valery Gerasimov saw the Wagner Group chief accuse the latter two of using his forces as cannon fodder, as well as intentionally withholding resources from the Group. These tensions led to Wagner's march on Moscow, ostensibly to address grievances against the military leadership of the Russian armed forces. Though seemingly resolved through negotiation, the attempted coup would eventually end with the dramatic death of Prigozhin and other top leaders of Wagner in August 2023.

Before these tensions emerged, Putin utilised Wagner for a wide variety of roles during his war. The Wagner Network continued to train and support pro-Russian gangster militias in the LDPR, just as they had done in 2014. As well as their direct combat operations in Bakhmut-Soledar, Wagner are believed to have fought alongside, or at least provided logistical and tactical support, in Kharkiv and Zaporizhzhia Regions and around Kherson. Before their deployment in military operations bands of mercenaries, or transnational organised crime networks, performed various unconventional direct-action roles that the traditional armed forces could not. These included executing sabotage operations, intelligence gathering and reconnaissance, the recruitment of collaborators, management of proxies and the provision of protection, escort and evacuation services for military goods and personnel.²⁰² The Network is also believed to have orchestrated several assassination attempts on President Zelensky, travelling from the CAR to perform this mission.^{203,204}

'Silent Partners' like the Night Wolves and Wagner Group exemplify Russia's strategic use of non-state actors and criminal organisations to

²⁰¹ GI-TOC, *New Frontlines: Organised criminal economies in Ukraine in 2022, 2023*, p. 16.

²⁰² Sierra, F.D., et al., *Wagner Group Unchained in Ukraine: Military, political and human rights impact of the Wagner Group since the large-scale invasion in 2022*, Barcelona: Novact Institute for Nonviolence, 2023.

²⁰³ Rana, M., "Volodymyr Zelensky: Russian mercenaries ordered to kill Ukraine's president", *The Times*, February 28, 2022.

²⁰⁴ Rana, M., "Volodymyr Zelensky survives three assassination attempts in days", *The Times*, March 3, 2022.

advance its geopolitical and military goals.²⁰⁵ The Night Wolves, a motorcycle club turned paramilitary entity, have acted as cultural ambassadors and enforcers of Russian ideology. Closely aligned with Vladimir Putin, they propagate nationalist propaganda, establish youth programs, and secure pro-Russian events worldwide.

Both groups epitomise a hybrid approach to **power projection, merging military, cultural, and economic tools** to achieve Russia's objectives. Their operations rely heavily on exploiting local conflicts, fostering separatist movements, and leveraging organised crime networks. This model of statecraft minimises political risk for Moscow, as these entities operate with plausible deniability while engaging in activities ranging from smuggling to resource extraction and cyber operations. The symbiotic relationship between these groups and the Kremlin illustrates how Russia integrates non-state and criminal actors into its foreign policy apparatus. By leveraging such networks, Moscow effectively destabilises adversaries, extends its influence, and counters Western sanctions, all while avoiding direct accountability.

In essence, the Kremlin's criminal army represent Russia's innovative yet controversial methods of **asserting power in the modern geopolitical landscape**. Their activities highlight a broader strategy of using unconventional means to achieve strategic goals, blending soft and sharp power, paramilitary force, and criminal enterprise into a cohesive mechanism for statecraft. Meanwhile, in the Donbas, organised crime and state-sponsored militias like Wagner have perpetuated smuggling and other illicit activities to sustain the region under Russian control. These criminal economies include coal smuggling, counterfeit goods production, and financial crimes, which have been instrumental in supporting the unrecognised separatist states. Indeed, "(o)rganized crime was therefore baked into the political economies of both regions (LDPR & Crimea from the beginning." The fusion of criminal networks with political and military operations has turned the region into a "mafia state," reliant on illegal activities for survival.

²⁰⁵ Keene, *Silent Partners: Organised Crime, Irregular Groups and Nation-States*, Monographs, Books, and Publications. 389, US Army War College Press, 2018.

THE AUTHORITARIAN AXIS AND CRIMINAL NETWORKS

The Kremlin's war on the West has led to the emergence of an international arena that increasingly resembles the competing alliances of the Cold War: with those who support Ukraine's struggle against Russian aggression on one hand, a small 'non-aligned' movement, and Putin's rival coalition to the West - an 'Authoritarian Axis' - on the other. Mostly compiled of pariah states like North Korea and Iran, other contributors, notably China, see the alliance as an opportunity to challenge Western hegemony. All states in this informal alliance are united behind this overarching principle, but there are other factors uniting them as well: Iran, North Korea, China, Belarus, and Syria **all utilise the strategic incorporation of organised crime into their statecraft toolkit as a deliberate tactic** to augment their geopolitical influence while evading international constraints.²⁰⁶

North Korea has long exemplified the fusion of state functions with organised crime, employing illicit activities as essential components of its statecraft. In its quest for *Juche*, to be militarily, politically and economically self-reliant,²⁰⁷ as well as its long-established status as the world's foremost pariah state, the regime has in many cases been left with little option but to turn to criminal enterprise.

The North Korean state has orchestrated a series of sophisticated cyber heists, targeting financial institutions and cryptocurrency exchanges worldwide. These cyber operations have reportedly generated substantial revenue, which is then funnelled into North Korea's nuclear and ballistic missile programs, thereby sustaining its military ambitions despite stringent international sanctions. A prime example is the 2016 Bangladesh Bank heist, in which North Korean hackers attempted to steal nearly \$1 billion via the SWIFT banking system, ultimately making off with \$81 million.²⁰⁸ Another significant cyber-crime operation was the 2017 WannaCry ransomware attack, which infected hundreds of thousands of computers worldwide, disrupting hospitals, businesses, and government institutions.²⁰⁹ More recently, North Korean hackers have been involved in cryptocurrency theft, with estimates indicating that they have stolen over \$1.3 billion from digital exchanges between 2019 and 2023 to fund weapons development programs.

²⁰⁶ European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Protecting EU: a European Internal Security Strategy*, April 1, 2025.

²⁰⁷ Lee, G., *The Political Philosophy of Juche*, *Stanford Journal of East Asian Affairs* 3(1): 105-111, 2003.

²⁰⁸ White, G., and Lee, J.H., "The Lazarus heist: How North Korea almost pulled off a billion-dollar hack", *BBC News*, June 21, 2021.

²⁰⁹ NHS England, "NHS England business continuity management toolkit case study: WannaCry attack", 2023.

Additionally, North Korea has infiltrated Western companies by embedding operatives within IT departments, exploiting vulnerabilities in remote hiring practices. These operatives, masquerading as legitimate employees, aim to deploy malware and exfiltrate sensitive information, thereby advancing Pyongyang's espionage objectives. The regime has also been known to operate overseas businesses, particularly restaurants, which serve as fronts for money laundering and intelligence gathering, thereby circumventing international financial restrictions.

China's approach to integrating organised crime into its statecraft is multifaceted, involving both cyber and traditional criminal activities. And, as in Russia, Chinese cybercriminals have been co-opted by state intelligence agencies to conduct cyber espionage against foreign governments and corporations.²¹⁰ This collaboration enables China to acquire sensitive information and intellectual property, bolstering its economic and strategic positioning on the global stage.

China's criminal influence extends both domestically and abroad. Domestically, the government has employed criminal organisations such as the *triads* to suppress dissent and control political activism.²¹¹ Abroad, China has used illicit networks to extend its reach, particularly in Southeast Asia, Africa, and Latin America. In regions such as the South China Sea, Chinese criminal syndicates engage in illegal fishing and smuggling operations under the tacit approval of the state.

Box 6. The Hongmen Network

One such illicit network is **the Hongmen Network**, led by notorious crime boss Wan Kuok Koi ("Broken Tooth"). This network functions as a hybrid of criminal syndicate and political asset, serving the strategic objectives of the Chinese Communist Party (CCP) abroad. Although officially described as a cultural organisation, the *World Hongmen History and Culture Association* operates as a front for the 14K triad, engaging in crimes such as fraud, money laundering, human trafficking, and online scamming. U.S. sanctions and law enforcement investigations in multiple countries have not curbed its expansion. Instead, the network has demonstrated a deep entwinement with CCP interests, particularly across the Global South. Hongmen supports Beijing's geopolitical aims through influence operations that promote Chinese propaganda, support for the unification with Taiwan, and facilitation of the Belt and Road Initiative (BRI). This function is not dissimilar to the **sharp power role** that the Night Wolves plays for the Kremlin. It has provided logistical and security support for Chinese diplomats, set up Chinese overseas police centers (such as in Uganda), and advanced yuan regionalisation projects, **all under the banner of promoting Chinese**

²¹⁰ Luo, Q., "Cybercrime as an Industry: Examining the Organisational Structure of Chinese Cybercrime", *Humanities & Social Science Communications* 11, Art. No. 1554, 2024.

²¹¹ Lo, T. W., Kwok, S.I., and Garrett, D., "Securitizing the Colour Revolution: Assessing the Political Role of Triads in Hong Kong's Umbrella Movement", *British Journal of Criminology* 61(6), 2021, pp. 1521–1539.

national rejuvenation. Members have forged alliances with political elites in Southeast Asia and Africa, advancing China's strategic foothold in these regions.

Beijing tacitly tolerate Hongmen's illicit activities as long as they remain offshore and do not target Chinese citizens. This implicit arrangement allows the CCP to exploit Hongmen's criminal infrastructure for soft and sharp power projection and intelligence operations. For example, Wan's close interactions with Chinese officials—despite official denials—indicate state-level endorsement, including awards from entities tied to the CCP and the People's Liberation Army. Hongmen exemplifies the CCP's broader "United Front" strategy: the State co-opting overseas non-state actors, including criminal organisations, to advance state objectives while maintaining plausible deniability. **This fusion of organised crime and statecraft enables China to extend its influence through opaque, deniable, and often illicit means.¹**

I. Tan, R., and Wu, P.L., "Chinese association accused of mixing crime and patriotism as it serves Beijing", *The Washington Post*, June 24, 2025.

In regions that are targets for geopolitical influence, such as Africa and Latin America, the Chinese government has been identified as enabling organised crime, both directly and indirectly. The state is believed to have helped drug traffickers, such as by sourcing drug precursors and equipment for their activities,²¹² and possibly providing tacit approval to Chinese organised crime syndicates who offer human smuggling services into the United States from its southwest border.²¹³ Chinese nationals have also been involved in widespread illegal mining operations, particularly in sub-Saharan Africa.²¹⁴

Domestically, the Chinese state sector is significantly exposed to criminal activities. Corruption amongst local state officials is a significant issue, and many are believed to be involved in local criminal markets and activities. Naturally, these officials thus tend to be involved with organised criminal networks – the triads. The Chinese government has been known to use these triads to suppress dissent and exert control over certain communities, reportedly being involved in intimidating political activists and influencing foreign political landscapes in favour of Beijing's interests.²¹⁵ Once dominant in the coastal regions and in Taiwan and Hong Kong, these groups have now built vast grey empires in the industries of mainland China, where they operate both legitimate businesses whilst engaging in racketeering and other illicit activities in secret.²¹⁶

²¹² Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, United States of America, 2025, p. 4.

²¹³ US Department of State, *2024 Trafficking in Persons Report: China*, Office to Monitor and Combat Trafficking in Persons, 2024.

²¹⁴ Tom, A.M., *China's Illegal Mining Operations in the Democratic Republic of Congo*, Carr Center for Human Rights Policy; Harvard Kennedy School, n.d.

²¹⁵ GI-TOC, *Global Organised Crime Index: China*, Geneva: Global Initiative Against Transnational Organised Crime, 2023.

²¹⁶ Weinrich, B., *The Triad Trials: Consequences of Cooperation Between Chinese Organized Criminal Groups and Political Society*, *St Antony's International Review* 15(1), 2019, pp. 165–82.

Belarus, under President Alexander Lukashenko, has increasingly aligned with Russian strategies. Like other states in Putin's authoritarian 'coalition of the willing,' Belarus too has incorporated criminal elements into its statecraft. The regime has most notably been implicated in facilitating smuggling operations, including the trafficking of sanctioned goods and weapons to evade international restrictions. They are heavily involved in the Kremlin's weaponisation of migration. These illicit activities not only provide economic benefits to Belarus, but also dramatically assist the Kremlin's efforts in circumventing Western sanctions.

Goods smuggled by Belarus include oil products, military-grade equipment, and Western-manufactured technology banned under international sanctions. Belarus has also played a key role in the black-market trade of cigarettes and narcotics, helping Russia access restricted goods while generating revenue for both regimes. Furthermore, Belarus has been accused of employing criminal groups to suppress opposition and conduct covert operations against dissidents. The Belarusian regime has worked with organisations like the Night Wolves, helping their smuggling operations and intimidation campaigns against opposition figures. The regime has also collaborated with Russian paramilitary groups to train and deploy operatives for intelligence gathering and repression of dissidents.

Aware of Syria's pariah status, former Syrian President Bashar al-Assad turned **Syria** into a global hub for illicit drug production and trafficking, particularly through the trade of **Captagon**, an amphetamine-like stimulant. Assad's regime, in coordination with high-ranking military officials and members of his inner circle, had facilitated the mass production and export of Captagon to various countries, particularly in the Middle East and Europe, before his overthrow. This drug trade became a crucial economic lifeline for the Syrian government, generating billions of dollars annually.^{217,218}

The Assad regime's reliance on drug trafficking served multiple purposes. Economically, it provides a vital source of revenue amid crippling international sanctions and economic collapse. This also served to strengthen the regime politically, consolidating ties with loyalist military factions and ensuring their continued support. Additionally, by flooding neighbouring countries with Captagon, the regime exerts influence and destabilises rival governments, particularly in Gulf nations that have sought to oppose Assad's rule. The strategic use of the drug trade exemplifies how authoritarian regimes leverage criminal enterprises to sustain power and manipulate regional dynamics.

Similarly, **Iran** has also systematically woven criminal networks into its foreign policy framework, leveraging criminal networks to circumvent international sanctions and project influence across the Middle East. Central to this approach is the Islamic Revolutionary Guard Corps (IRGC). Ostensibly a branch of the Iranian Armed Forces, the IRGC is tasked with protecting the state from foreign interference, protecting the regime from internal threats

²¹⁷ Croft, A., "Inside Assad's Captagon drug-smuggling empire and how it funded brutal Syrian regime", *The Independent*, December 13, 2024.

²¹⁸ Arbid, J., *Captured by Captagon? Lebanon's Evolving Illicit Drug Economy*, Geneva: Global Initiative Against Transnational Organised Crime, 2017.

(such as coups) and crushing internal opposition movements that challenge the ideological legacy of the Islamic revolution. It also orchestrates a nexus of illicit activities, including drug trafficking, arms smuggling, money laundering, and oil smuggling. These operations not only fund Iran's regional proxies, most notably Hezbollah, but also enable the regime to sustain its geopolitical endeavours despite economic constraints. For instance, the IRGC has been linked to smuggling networks that traffic weapons to Yemen's Houthis and Shia militias in Iraq, further destabilising the region.

Moreover, Iran's cyber capabilities have evolved to incorporate criminal elements, blurring the lines between state and non-state actors. Cybercriminals with affiliations to the Iranian state have engaged in cyber espionage and financially motivated attacks, targeting entities in the United States and allied nations. Notable cases include the 2012 attack on Saudi Aramco, which crippled thousands of computers with the Shamoon virus, and the 2020 hacking campaign against U.S. presidential campaigns, which attempted to interfere with electoral processes. Iranian hackers have also targeted critical infrastructure, including water treatment facilities in Israel, exemplifying its willingness to engage in cyber warfare as a tool of statecraft.

COMINTERN TO CRIMINTERN

The systemic fusion of organised crime and the Russian state is not a domestic peculiarity, but a deliberate instrument of geopolitical strategy – one that poses an escalating threat to European security. What emerged, in its most recent guise, as opportunistic alliances between criminals and corrupt officials during the Soviet collapse has evolved, under Vladimir Putin, into a deliberate model of governance. Today, criminal networks are not merely tolerated in Russia – they are cultivated, weaponised, and exported. Russian-linked criminal networks operate across Europe with increasing sophistication, facilitating money laundering, sanctions evasion, arms trafficking, and destabilisation efforts, to name just a few. These groups often work in tandem with state actors, ‘private military companies’ like the Wagner Group, and proxies in vulnerable regions such as the Balkans. The effect is a double-layered threat: undermining the rule of law from within EU states while projecting Russian influence beyond traditional military or diplomatic channels.²¹⁹

This convergence of hybrid threat actors – where state-backed criminality becomes a tool of asymmetric-hybrid warfare – has resulted in what some have called a new Crimintern: **a shadow network where the boundaries between state power and illicit enterprise are deliberately blurred.**²²⁰ For Europe, this represents not just a law enforcement challenge, but a European and national security emergency. As authoritarian regimes begin to emulate this model, the strategic entanglement of crime and statecraft pioneered by Russia threatens to erode European stability, resilience, and sovereignty from within.²²¹

The severity of this threat to Europe was fully realised after the 2022 invasion of Ukraine and the consequent sanctions against Russia. With the Kremlin’s resources and capabilities eroded Russia has turned *en masse* to its criminal underworld to fill in the gaps. As Russia faces economic challenges, the ties between organised crime groups and the state have strengthened, a pattern consistent throughout Russian history. Indeed, by looking at the historical integration of organised crime into Russia’s statecraft (or that of the Soviet Union, or the Russian Empire), one can see a pattern emerging. The increasing links between the state and OCGs in the territory can be observed in the early Bolshevik state, to the prisoner amnesty during the de-Stalinisation period, to the Era of Stagnation and the Collapse of the USSR, when the new Federation quickly became a ‘Superpower of Crime’.

This pattern can assist one’s understanding of the description of Russia as either a terror state or a state sponsor of terrorism by international commentators. Activities such as drug smuggling, human trafficking and financial

²¹⁹ Europol, *European Union Serious and Organised Crime Threat Assessment - The Changing DNA of Serious and Organised Crime*, 2025.

²²⁰ European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Protect-EU: a European Internal Security Strategy*, COM(2025) 148 Final, 1, Strasbourg, April 1, 2025.

²²¹ Galeotti, M., *Crimintern: How the Kremlin Uses Russia’s Criminal Networks in Europe*, London: European Council on Foreign Relations, 2017.

crimes are regular methods to fund its covert or destabilising operations. Yet, terror groups often resort to drug dealing as a last resort for gathering finances, as it could lower support for groups in their own societies.²²² Such terror groups try to provide public goods for this very reason: to be seen to be providing benefits for the entire community. The strategy of Crimintern is part of a broader effort to secure strategic resources, expand Russia's sphere of influence, and disrupt global stability without the traditional price associated with such efforts.²²³ As the West grapples with Russia's revanchist aggression, it must also recognise that the lines between statecraft and organised crime have once more blurred in Russia.

Roads to a Response

The multi-layered, complex and evolving **shadow alliance** between the Russian state and criminal networks requires an equally multi-layered response from Europe. Russia is engaging in a full-scale hybrid war on Europe and is utilising both its own, and Europe's native criminal networks, to fight in this conflict. Europe has been slow to wake up to this reality and is hesitant to even acknowledge Russia as the source of violence and sabotage on European streets.²²⁴ By first acknowledging and understanding the threat posed by the Kremlin's utilisation of organised crime for the goals of the State, a cohesive response to the issue may begin to be crafted. Russia and her allies, such as Iran and China, must be clearly identified as the source. This should feed into Europe's ongoing efforts to rearm and take threats to its security more seriously and will help inspire public policy discussion. Doing so will also spur the allocation of increased resources to law enforcement agencies and assist with their prioritisation.

Europe's law enforcement agencies must also increase cooperation both with each other, between Member States, and internally, between security forces. Europe's approach to organised crime is not adequately set up to approach this 'changing DNA of serious and organised crime,' vis-à-vis the fusion between criminal networks and state actors. Counter-intelligence officers and counter-organised crime services largely 'stay in their own lanes,' rarely cooperating on joint threats. This approach is limiting the ability of Europe to respond to the threats posed by Russia's criminal actors. A more appropriate example may be found in the US, whose FBI houses **counterintelligence and counter-organised crime agents under the same roof**, increasing their cooperation.²²⁵

One answer to this may lay in one suggestion from the Niinistö report on *Strengthening Europe's Civilian and Military Preparedness and Readiness*. The EU's approach to open, borderless trade within the bloc stands in contradiction to member states' approach to national security issues, with the strict imposition

²²² Dishman, C., *Terrorism, Crime, and Transformation*, *Studies in Conflict and Terrorism* 24(1), 2001, pp. 43–58.

²²³ Europol, *European Union Serious and Organised Crime Threat Assessment - The Changing DNA of Serious and Organised Crime*, 2025.

²²⁴ Europol, *European Union Serious and Organised Crime Threat Assessment - The Changing DNA of Serious and Organised Crime*, 2025.

²²⁵ MacColl, J., and Westmore, K., *Operation Destabilise: Russia, Organised Crime and Illicit Finance*, London: Royal United Services Institute (RUSI), 2024.

of national jurisdictions, piecemeal intelligence-sharing capabilities and slow response time. Facing Europe's ongoing security challenges requires a deeper, more structured cooperation among member states. In the long term, the EU should develop a:

“fully-fledged intelligence cooperation service at the EU level that can serve both the strategic and operational needs of policy planning decision-making without emulating the tasks of Member States' national intelligence organisations, including in respect of their role in intelligence gathering.”²²⁶

In the immediate term, the capabilities of the Single Intelligence Assessment Capacity (SIAC) must be reinforced and improved – particularly the Hybrid Fusion Cell. SIAC, which consists of the EU Intelligence Centre and EU Military Staff Intelligence, along with other relevant security departments and other EU institutions should cooperate more with member states to develop joint, specific counter-espionage measures. Furthermore, data-sharing agreements between SIAC and other EU actors, such as Europol, should be strengthened and formalised.²²⁷ This may come in the form of an 'EU Foreign Influence Task Force.'²²⁸ Furthermore, this cooperation and data sharing should be increased among Europe's NATO allies, whose current stated priorities include countering hybrid warfare.²²⁹

In the spirit of increased cooperation, Member States' counter-intelligence practices, legislation and intelligence-sharing abilities should be harmonised as much as is feasible. This will reduce obstacles leveraging the full abilities of all member states armed services whilst reducing the ability of hostile actors to operate freely in the EU.²³⁰ As with incidents of cyber-attacks, immediate and full transparency by victims of attack should be encouraged. Member states should proactively share details of incidents and vulnerabilities that left them exposed. This will assist the EU's efforts to develop a joint threat response.

As mentioned, criminal networks are leveraging the licit economy as a means of increasing the potency of their coercive strategies and maximising their financial gain. Indeed, malign actors, most notably the Kremlin, utilised its economic footprint in critical sectors in target states to influence strategic foreign policy decisions and fuel instability, such as through weaponising criminal actors.²³¹ There must be an increased focus on the nexus between countering hybrid threats and guaranteeing economic security:

²²⁶ Niinistö, *Safer Together*, 2024, p. 23.

²²⁷ Niinistö, *Safer Together*, 2024, p. 23.

²²⁸ Vladimirov, M., Köppen, M., and Osiposa, D., *Networks of Power: Russia's Shadow Influence in Germany*, Potsdam-Babelsberg: Center for the Study of Democracy and Friedrich-Naumann-Stiftung für die Freiheit, 2024.

²²⁹ Vohra, A., “NATO to revise strategy on how to tackle hybrid warfare”, *Deutsche Welle*, May 12, 2024.

²³⁰ European Commission, *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, 2024, p.23.

²³¹ See CSD's Kremlin Playbook series, e.g. Shentov, Stefanov and Vladimirov, *The Kremlin Playbook in Europe*, Sofia: CSD, 2020.

- **Follow the Money.** As with its diplomatic officials, the Russian state provides cover for the leaders of its organised crime network, helping them 'double' as businessmen. Their presence in the economy is significant, and they are integrated into common practices and non-criminal activities. However, their presence in illegal activities is undeniable.^{232,233} Western sanctions should be targeted at RBOC leaders, facilitators, and their business fronts who help the Kremlin evade sanctions and who generate revenue for Putin's war chest. Furthermore, ownership structures of companies should be investigated to identify the largest stakeholders, as well as counter smuggling and illicit flows. Thus, strengthening financial intelligence-sharing between EU Member States to track and freeze assets linked to these groups would represent a serious challenge to their malign shadow alliance.²³⁴
- Related to this, **Financial Investigations Taskforces in high-risk regions could be launched.** Regional EU taskforces – in border regions like the Baltic and the Balkans – should unite financial intelligence, prosecutors, asset-recovery teams, banking regulators, and customs officials. Operated under Europol coordination, these taskforces should focus on identifying and prosecuting Russian-linked organised crime using methods like shell-company trading, trade mis-invoicing, and shadow-asset transfers. Annual public reports tracking seizures and prosecutions can demonstrate impact and incentivise further support. This model can replicate successes from London's Regional Asset Recovery Network, scaled to EU needs.
- **Enforce Sanctions and Tracking Illicit Financial Flows.** To further strengthen the EU's resilience against the illicit financing of Russian influence operations, a European effort to enhance the Anti-Money Laundering Authority (AMLA), sanctions enforcement, and investment screening should be established. EU member states and international partners should collaborate closely to ensure that sanctions against Russia are robustly enforced, effectively cutting financial flows to the Kremlin and its war apparatus.²³⁵ This enhanced resilience could be provided by equipping AMLA and the European Public Prosecutor's Office (EPPO) with **enhanced mandates, resources, and cross-border cooperation tools** to investigate and prosecute these crimes. In this case, this is most relevant for criminal networks facilitating Russian sanction evasions. Strategic emphasis should be placed on high-risk jurisdictions where foreign authoritarian regimes exploit illicit finance to capture national elites, public institutions, and key economic sectors. AMLA and EPPO should prioritise cases where **money laundering intersects with foreign interference and sanctions evasion.**
- **Mapping and Intelligence Sharing.** To track the activities of these groups, it is essential to map out their presence. Therefore, intelligence sharing among law-enforcement agencies would be essential, from national

²³² GI-TOC, *Global Organised Crime Index: Russia*, 2023, p. 7.

²³³ Stefanov, R., et al., *The Kremlin Playbook 2: The Enablers*, Washington, D.C: Center for Strategic and International Studies (CSIS); Sofia: Center for the Study of Democracy; Rowman and Littlefield, 2019.

²³⁴ Jones, *Russia's Shadow War Against the West*, Washington, D.C: CSIS Briefs, 2025.

²³⁵ Vladimirov, Köppen and Osiposa, *Networks of Power*, Potsdam-Babelsberg: CSD and FNE, 2024.

agencies to Europol and the European Multidisciplinary Platform Against Criminal Threats (EMPACT) network. These initiatives enhance the alignment of objectives and the exchange of information, strengthening efforts to combat organised crime networks, which are often widespread, and not considered a security threat by themselves unless specific gangs are operating at street-level.²³⁶ These gangs are the manifestation of the networks themselves, hence identifying and addressing them is of utmost importance.

- Furthermore, **national and regional asset registers to track cross-border holdings should be supported.** The EU, via the forthcoming EU Anti-Money Laundering Authority (AMLA), should create an integrated register linking key asset types—real estate, vehicles, bank accounts, luxury goods, artwork, and virtual assets—by harmonising data exchange standards across national registries. This would enable efficient tracing and freezing of illicit assets through shared intelligence. National authorities must connect domestic registries (e.g., land, corporate, crypto accounts) conforming to common data exchange standards. This facilitates tracing illicit Russian-state-affiliated networks' illicit wealth across borders and enables rapid freezing based on shared intelligence.
- **Integrate FDI screening with AML controls.** EU Member States should enhance national Foreign Direct Investment (FDI) screening frameworks, ensuring they include anti-money laundering (AML) indicators. Under the 2019 EU 'FDI Regulation', screening must account for non-EU investors' links to organised crime and illicit networks. Screening mechanisms should require applicants to submit beneficial ownership documentation, AML risk assessments, and source-of-funds evidence before project approval, particularly in strategic sectors like **energy, critical infrastructure, and the media and telecommunications**. A particular emphasis should be placed on exposing hidden beneficial ownership linked to foreign actors.
- **Enhance EU Asset Recovery Offices (AROs) and seizure framework.** EU AROs, mandated since 2007, facilitate tracing and confiscating proceeds of crime, ensuring crime does not pay. To combat Russian-state backed crime, AROs must receive more resources, coordinate seamlessly under CARIN/EUROPOL, rapidly freeze assets suspected of state or criminal linkages, and ensure that obstacles to the social reuse of seized assets are removed. Annual asset-tracing reports should aim to prioritise laundering routes tied to foreign influence operations. Incorporating AMLA data analytics could help AROs pre-empt cross-border financial flows before they occur.
- **Empower Europol's Organised Crime Centre with hybrid threat mandates:** Europol's Organised Crime Centre (OCC) should assume a formal mandate to address hybrid threats involving synchronised criminal, financial, and cyber activity. A dedicated unit would compile threat analyses focused on Russian-state tactics—such as money laundering, disinformation, procurement fraud, and crypto-enabled trafficking. Member States should fund seconded liaison officers and deploy Europol's iOCTA resources to detect and share real-time intelligence on Russian-organised crime networks.

²³⁶ Galeotti, *Gangsters at War: Russia's use of organised crime as an instrument of statecraft*, 2024.

For Europe, the post-war future of Ukraine must be carefully managed to prevent a scenario where criminal syndicates and war profiteers dominate reconstruction efforts, as was the case in the post-Yugoslav space. The European Union and NATO, both deeply involved in supporting Ukraine's defence and eventual recovery, must proactively address the risks posed by entrenched smuggling networks and illicit economies. A failure to do so could result in a weakened Ukrainian state, beholden to oligarchic interests and criminal enterprises, mirroring the persistent governance challenges seen in parts of the Balkans today. Moreover, the historical case of the Balkans illustrates how war-induced smuggling and sanctions evasion transcends borders, influencing neighbouring states and facilitating broader transnational crime. Given Ukraine's geographical position, the influx of arms and illicit trade could exacerbate criminal activities across Eastern and Central Europe, posing security risks for the entire continent.

As the EU contemplates Ukraine's long-term integration into its economic and political structures, it should learn the lessons and avoid the catalyst effect the Yugoslav wars had on organised crime networks in the continent. Strengthening border controls, enforcing robust anti-corruption measures, and ensuring accountability in post-war reconstruction will be essential to prevent the solidification of a war economy that could undermine Ukraine's democratic future. Equally important, European policymakers must recognise that smuggling and organised crime are not just by-products of war but key instruments of power that can entrench authoritarian tendencies and hinder state-building efforts. The legacy of the Balkan wars serves as a stark warning: without strategic planning and oversight, the post-war trajectory of Ukraine could mirror the persistent instability that has plagued parts of Southeast Europe for decades.

Putin's Russia has fully integrated criminal networks into its foreign policy arsenal, weaponizing them as a key component of the Kremlin's hybrid war against the West. This strategy draws on a deep historical tradition of Russian and Soviet leaders exploiting illicit networks. The Putin regime has perfected this model into a sustainable system for projecting influence, circumventing sanctions, and undermining adversaries—all while preserving plausible deniability.

Looking ahead, Putin is likely to expand these efforts by deepening alliances with transnational criminal organisations to evade tightening sanctions regimes, deploying cyber-criminal proxies for disruptive attacks on critical Western infrastructure, and using illicit finance networks to corrupt foreign political systems. The Kremlin may increasingly rely on these methods as conventional avenues of power projection become constrained by international countermeasures.

This evolution suggests organised crime is transitioning from being merely an instrumental tool to becoming an institutionalised feature of Russian state power. These criminal networks will likely assume an even greater role in compensating for Russia's diminishing conventional

leverage while providing Moscow with asymmetric advantages against its adversaries. The long-term implication is a dangerous blurring of lines between governments and criminal entities in international relations.

