

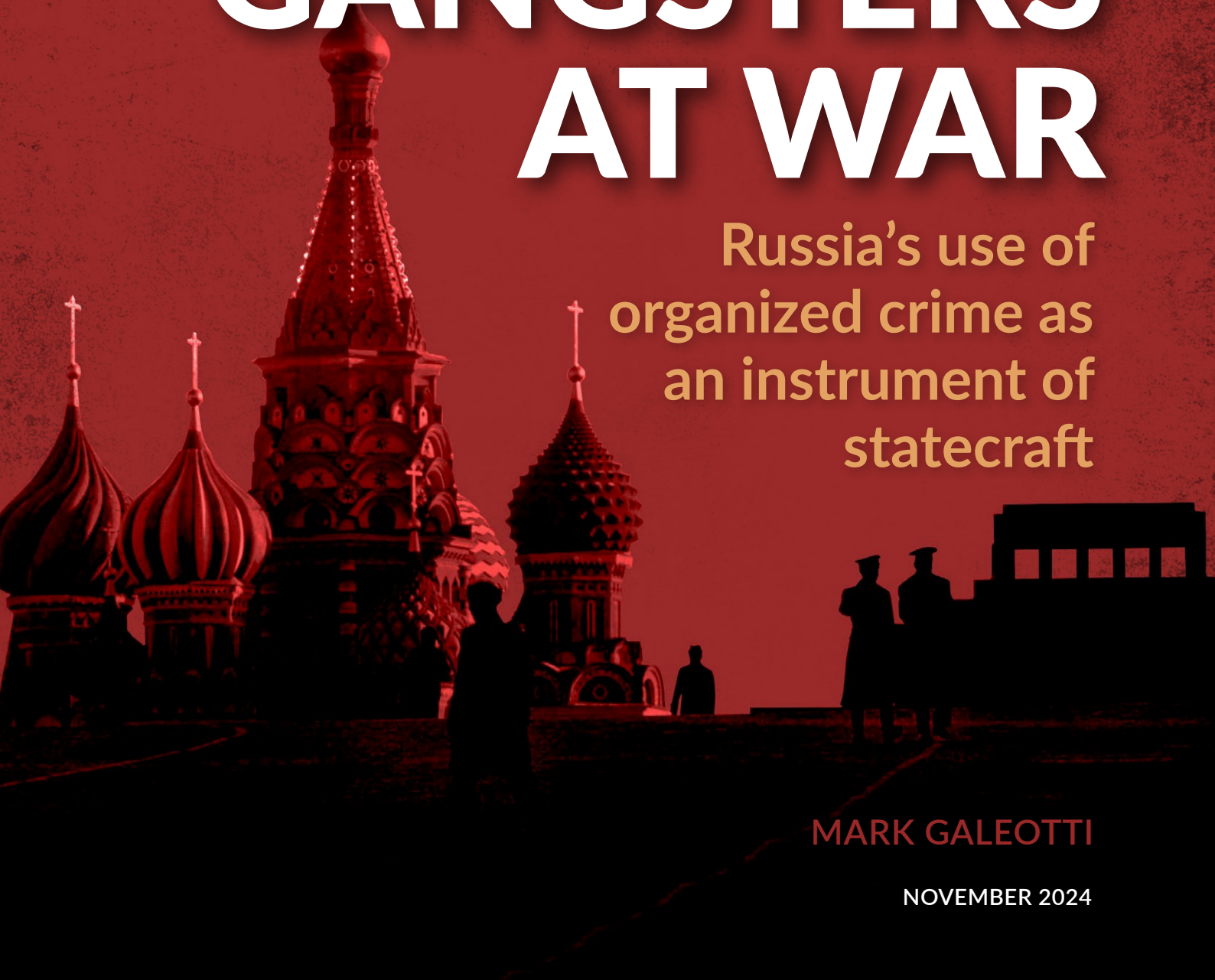


**GLOBAL
INITIATIVE**

AGAINST TRANSNATIONAL
ORGANIZED CRIME

GANGSTERS AT WAR

Russia's use of
organized crime as
an instrument of
statecraft



MARK GALEOTTI

NOVEMBER 2024



GANGSTERS AT WAR

*Russia's use of organized crime as
an instrument of statecraft*

MARK GALEOTTI

November 2024

ABOUT THE AUTHOR

Dr Mark Galeotti is the executive director of the Mayak Intelligence consultancy and a member of the Global Initiative Network of Experts. An expert on Russian crime, politics and security, he is an honorary professor at University College London, senior associate fellow with the Royal United Services Institute and the Council on Geostrategy and a senior non-resident fellow with the Institute of International Relations Prague. His recent books include *The Vory: Russia's Super Mafia* (2018), *We Need to Talk About Putin* (2019), *Putin's Wars: from Chechnya to Ukraine* (2022) and, co-authored with Anna Arutunyan, *Downfall: Putin, Prigozhin and the fight for a new Russia* (2024).

A NOTE FROM THE AUTHOR

Just as the Russian state's relationship with, and use of, organized crime has changed, so too has the study of this problem. I first seriously addressed this in the report *Crimintern: How the Kremlin uses Russia's criminal networks in Europe*, commissioned and published by the European Council on Foreign Relations in 2017. The problem has become much more serious since then, but I would like to thank them for the foresight in allowing me to explore its earlier stages then. I also return to this challenge in my book *The Vory: Russia's super mafia* (Yale University Press, 2018).

© 2024 Global Initiative Against Transnational Organized Crime.
All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Global Initiative.

Cover photo: © Grant Faint/Getty Images

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland

www.globalinitiative.net

CONTENTS

Glossary.....	2
Introduction: This means war	4
Active measures.....	6
The mobilization state	7
A history of connections.....	8
Russia's criminal diaspora.....	9
The early 'crimintern'	12
Criminal warfare: Transformation since 2022	14
The (criminal) revolution in Russian politics	16
Managing the proxies	17
Criminal tradecrafts	19
Sanctions-busting	20
Illegal financial flows.....	22
Cyber.....	25
Filling intelligence gaps.....	29
Weaponizing migration.....	30
Influence and information operations.....	33
Arson, assassination and intimidation.....	34
Dark futures	37
'Proxy proxies'	38
Going transatlantic.....	39
'Donbasization'.....	41
'Mafia state'	42
'Nationalization'.....	43
Beyond admiring the problem: Recommendations	45
Naming and knowing the beast.....	46
Security beyond tanks.....	47
Making friends.....	48
Punishment to fit (or deter) the crime.....	49
Notes	51

GLOSSARY

AP	Presidential Administration
Avtoritety	'Authorities', senior criminal-business figures
DNR	Donbas People's Republic
EU	European Union
FSB	Federal Security Service
GI-TOC	Global Initiative Against Transnational Organized Crime
GRU	Main Intelligence Directorate of the General Staff (now technically the GU, but still widely known as the GRU)
GU	Main Directorate of the General Staff (military intelligence)
HUMINT	Human intelligence
KGB	Committee of State Security (Soviet security and intelligence agency)
LNR	Lugansk People's Republic (in Ukrainian: Luhansk)
MVD	Ministry of Internal Affairs
SB	Security Council of the Russian Federation
SK	Investigatory Committee
SOIMS	Operational Information and International Relations Service (also known as the Fifth Service of the FSB)
SVO	Special Military Operation (official Russian term for its invasion of Ukraine)
SVR	Foreign Intelligence Service
TsIB	Information Security Centre (of the FSB's First Counterintelligence Service)
Vorovskoi mir	'Thieves' world', traditional Russian criminal subculture
Vory	'Thieves', members of the traditional Russian criminal fraternity
Vory v zakone	'Thieves within the code' (literally, 'thieves-in-law'), leaders within the 'thieves' world'





INTRODUCTION: THIS MEANS WAR

Putin addresses the Federation Council in February 2023 with anti-West rhetoric. © Kremlin Press Office/Handout/
Anadolu via Getty Images

As we can see now, the promises of Western leaders, their assurances that they were striving for peace in the Donbas turned out to be a sham and outright lies. ... In fact, the anti-Russia project is part of the revanchist policy towards our country to create flashpoints of instability and conflicts next to our borders. Back then, in the 1930s, and now, the plan remains the same and it is to direct aggression to the East, to spark a war in Europe, and to eliminate competitors by using a proxy force.

– VLADIMIR PUTIN'S PRESIDENTIAL ADDRESS TO THE FEDERATION COUNCIL, 2023¹

In May 2022, Lithuanian police raided two underground factories where counterfeit cigarettes worth some €73 million were being produced.² This happens all the time, and even the involvement of a Russian-linked organized crime group was hardly unusual. However, as the investigation extended to Belgium (where the goods would be transhipped to Britain), it became clear that behind the gangsters lay Russian intelligence officers, who were using the business – or at least part of its profits – to raise operational funds for their activities in Europe.

With Putin regarding himself as 'at war' with the West, at a time when Europol chief Catherine de Bolle is warning that organized crime is on the rise across Europe,³ and Thomas Haldenwang, head of Germany's counter-intelligence agency, is assessing 'the risk of [Russian] state-controlled acts of sabotage to be significantly increased',⁴ it is perhaps unsurprising that gangsters and spies would find themselves brought together in his campaign.

It has, after all, become commonplace since the full-scale invasion of Ukraine in February 2022 to characterize the relationship between Russia and the West as some shade of war: economic, political, but typically more than just cold. Indeed, even as he insists that his invasion is not a war, just a 'special military operation' (SVO) – actually calling it a 'war' can conceivably get Russians a 15-year prison sentence⁵ – Putin freely uses the term when describing his country's engagement with the West. However, it is less clearly understood just how significant and long held this view of his may be.

In this context, it does seem in hindsight that Putin has considered himself as de facto at war with the West – or, more precisely, that the West has been warring against him – since at least around 2012. After stepping back from the presidency to the position of prime minister in order to observe the letter, if not the spirit, of term limits, all the while clearly still running the country, when Putin announced he would be returning to the



A protest rally marks the fifth anniversary of the anti-Putin Bolotnaya Protests. © Kirill Kudryavtsev/AFP via Getty Images

Kremlin, this was for many the last straw. Demonstrations that became known as the Bolotnaya Protests were mastered and dispersed, but Putin seems to have been unable or unwilling to accept that they were a genuine, organic expression of dismay. Instead, he chose to see them as spurred by the US Department of State, after then-Secretary of State Hillary Clinton 'gave the signal' to opposition leaders.⁶

There had been a growing school of thought within Russian security circles that the West was using 'political technologies' to topple hostile governments, and support for civil society, democratization and the rule of law were seen as part of this campaign. As a former Kremlin insider put it, Putin was

scared, then angry. As far as he was concerned, this was it, this was a sign that the West – the Americans – were coming for him. So he was determined to fight back, and that didn't just mean defending himself, the repressions and arrests, it meant going on the attack. He was clear, he made it clear to us all: if the West was coming to mess with him, we would mess them up worse, by whatever means necessary.⁷

Active measures

Putin's apparent conviction that he was, in effect, at political war with the West led to a revival in the use of 'active measures' by the Russian state and, especially, its security apparatus.⁸ *Aktivnye meropriyatiya* was a term used by the Soviet Union from the 1950s for a whole range of covert and subversive operations, from disinformation to assassination.⁹ This wartime mentality receded during Mikhail Gorbachev's reform era in the later 1980s and then the chaotic 1990s. In the early 2000s, although Russia's intelligence services began to be restored to their previous prominence and budgets, active measures were still largely practiced only in the neighbouring post-Soviet states.

By the mid-2000s, as Putin became increasingly disenchanted with the West, active measures also became used more widely, but still with more restrictive rules of engagement. As a US intelligence officer saw it, 'They could lie, cheat and steal, but not kill – Westerners, anyway – and generally had to be *kulturny* [cultured] about it'.¹⁰ In effect,

Moscow embraced the notion that it was fighting what veteran American scholar-diplomat George Kennan had called 'political war' back in 1948.

the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP—the Marshall Plan), and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states.¹¹

Chief of the General Staff Gen. Valery Gerasimov would indirectly acknowledge this perspective when he warned that in the modern world, without any declaration of war, or even military deployment, 'a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war' through the application of 'political technologies'.¹² This was not so much an admission of some sinister new Russian doctrine as a reflection of how Moscow perceived Western capabilities and intent, and the threat to which it planned to respond in its own terms.

The mobilization state

The boundaries between public and private, lawful and illegal, have always been porous and protean in Putin's Russia, making it something of a 'hybrid state'. However, under pressure of the perceived need to fight a shadow war with a richer and more powerful West, it became even more hybrid, going through two distinct transitions, each of which would have significant implications for its use of organized crime as an instrument of statecraft.

From 2012 onwards, it became ever more clearly what could be described as a 'conscription state'. There was still a very wide space for civic activity and licit and illicit economic business, yet with the understanding that at any time, the state could demand covert service from any individual, company – or criminal gang.

This was typically for a single, specific service, usually when the regular intelligence services were overstretched or lacked some particular capability, and was also often transactional, carrying with it the promise of some benefit to be accrued in return. Sometimes, in fairness, the 'benefit' in question was simply the avoidance of prosecution, but either way it provided a modest, but useful supplement to the Kremlin's existing active measures assets, from the intelligence community (see the box below) to the diplomatic service and foreign media outlets, all of which had their roles to play.

Since the 2022 invasion of Ukraine and subsequent sharp deterioration in relations with the West, the conscription state has shifted into a full 'mobilization state', in which all elements of society – illegal as well as legal – are expected to play their full part in the war. From prison camp inmates drafted into military service to artists expected to exalt the SVO in their work, no element of Russian society is immune at a time when there is no more middle ground between the patriot and the traitor.¹³

The Russian intelligence community

Putin's intelligence agencies look very similar in roles and remit to their Western counterparts, but reflect a very different model of governance.¹⁴ Putin's 24-year-and-counting rule has depended heavily on the time-honoured tactics of divide and rule. To this end, the various intelligence agencies have deliberately overlapping functions to encourage empire-building at each other's expense.

The Foreign Intelligence Service (SVR) is the main civilian intelligence-gathering agency, traditionally focused on human intelligence operations run by officers embedded in foreign embassies under diplomatic cover. It is also increasingly involved in cyber operations.

The Main Directorate (GU) of the General Staff – formerly the Main Intelligence Directorate (GRU) – is the military intelligence agency. This large and powerful force, including the *Spetsnaz* special forces as well as a substantial foreign intelligence wing known as the *Agentura*, or Office, includes a cyber and information warfare capacity.

The Federal Security Service (FSB) is essentially a domestic security agency responsible for everything from counter-espionage to investigating serious crimes. It has also acquired a growing foreign dimension, first within countries of the former USSR, and then more widely. Whereas the other two agencies have long-established foreign missions, the FSB's external operations arm is relatively new. Thus it often operates in unconventional ways, eschewing embassy cover identities and relying more upon criminals and proxies.

A history of connections

All this has particular significance for the relationship between the state and the underworld. There have long been such connections: Bolshevik revolutionaries collaborating with bank robbers to raise operational funds; the early post-Revolutionary regime impressing rural bandits as local agents; or the Stalinist political police leaning on the professional criminals of the *vorovskoi mir* (thieves' world), the traditional underworld subculture, to keep the political prisoners in line.

A more complex relationship emerged from the 1970s, with the KGB – the Soviet combined foreign intelligence and domestic security agency – employing criminals as intelligence assets at home. Pimps, black marketeers and money changers engaging with tourists were often expected to report on the activities and attitudes of foreigners, as much to identify potential targets for recruitment as to spot enemy spies.

Until this time, the state – and corrupt Communist Party officials in particular – had been very much the dominant party in such arrangements. With the collapse of the USSR at the end of 1991 and the subsequent decade of political and economic chaos in Russia, the relationships were in many ways reversed: gangsters and black-market entrepreneurs became dominant, with security officers desperate for their pay and patronage.

Since Putin's first election to the presidency in 2000, however, the power of the state has been reaffirmed, and institutions such as the FSB have reacquired the whip-hand, even though corruption remains endemic. However, this does mean that there are strong connections between the police and security agencies and organized crime. Connections with hacking groups and smugglers can simply be activated and exploited

to suit the Kremlin's agenda. As a British security officer with direct responsibility for addressing Russian organized crime put it, 'Basically, the Russian intelligence community has a perverse advantage, precisely because it's so dirty. When they need to work out which criminal can carry out one op or another, they just have to ask around their mates.'¹⁵

It may not always be quite so straightforward, but this interpenetration of intelligence community and organized crime, and the long traditions of using criminals as agents, provides a strong basis for Russian active measures, which have become more of a feature since the start of the 2010s, and have increased dramatically since 2022.

Russia's criminal diaspora

The potential value of organized crime as an instrument of statecraft is compounded by its truly global reach. When former president Boris Yeltsin infamously warned that Russia was becoming a 'superpower of crime', this was in part a rhetorical admission and in part a bid for more Western assistance.¹⁶ Instead, it was more the case that Russia quickly became both integrated into world-spanning illicit networks and also experienced a rapid out-migration of criminals looking for new opportunities or simply more congenial climes.

In the 1990s, not only was the Russian economy in periodic crisis, but there was a continuing fear of a Communist revanche or even a nationalist coup. It was thus a sensible precaution to use new-found freedoms to trade abroad and move assets and even personnel outside the country. Early efforts to take over the underworld of former subjects of Moscow's, in the Baltic States and central Europe, foundered in the face of resistance by local police and criminals. During the 'bloody autumn' of 1994, for example, there were around a hundred murders in Estonia connected with a struggle for dominance between Russian and Chechen gangs.¹⁷ This was unsustainable and largely quelled.¹⁸

However, a criminal diaspora did emerge across Europe and beyond, especially once Russian-based networks shifted from would-be conquerors to deal-making merchant-adventurers. By the 2000s, they were returning to Europe, in particular. There were those, largely Russian-based gangs of Georgian and North Caucasus origin, that continued to try to operate at scale on the streets, most notably the Moscow-connected Georgian Kutaisi 'clan'. However, these inevitably attracted adverse attention from law enforcement. The Kutaisi clan, for example, was targeted in 2013 by coordinated arrests in Italy, the Czech Republic, France, Hungary, Lithuania and Portugal, followed in 2023 by further arrests in the US, where it had been forced to move as a result of the previous crackdown.¹⁹ The groups that survived and prospered tend to be the ones operating not on the street but further up the supply chain, offering the assets and capabilities at their disposal to existing gangs, working as facilitators and wholesale suppliers.

The case of the Kutaisi criminal grouping also illustrates a key issue relating to definitions. While predominantly Georgian, it also included a range of other ethnicities. Its Shulaya outfit active in the US also included Jews, Central Asians and an Armenian.²⁰ The Soviet Union was a multi-ethnic state and its underworld was similarly ethnically diverse. Much the same is true of post-Soviet Russia. It is not just that it, too, is diverse (ethnic Russians make up only around three-quarters of the total population), but its

criminal networks also include members from other, now-independent countries, from Armenia to Uzbekistan.

Various formulations have been applied to break away from the misleading implications of 'Russian organized crime', from 'Eurasian organized crime' to 'Russian-speaking organized crime'. None are wholly satisfactory: these gangs may well not speak Russian in their day-to-day activities and, besides, there is a huge difference between a St Petersburg smuggling ring and a Tajik drug warlord, for all their common 'Eurasianness'. For the purpose of this study, Russian-based organized crime is the best definition (see the box below). It is the presence of the grouping's centre of gravity or significant assets within Russia that makes it susceptible to being used by the state, whatever the nationality or ethnicity of its members.

Russian-based organized crime

It is easy to assume that organized crime based in Russia is also ethnically Russian, but that is a mistake. Many criminal groups hail from the Caucasus, for example.²¹ The most useful definition in this context is thus Russian-based organized crime for those groups, which, even while operating abroad, retain a strong stake in Russia. This applies whether their operations depend on access there or they simply have sufficiently valuable assets or family still left behind. This gives the state leverage. In the words of a Western counter-intelligence officer about one senior Russian-based organized crime figure believed to be involved in attempts to use heroin-trafficking operations through Ukraine also for intelligence gathering, 'So long as his balls were in Moscow, the Russians could always squeeze.'²²

These groups are often not predominantly ethnically Russian. The 2005 anti-mafia campaign in Georgia, for example, saw traditional underworld authority figures driven to Russia because, as 'thieves within the law' (*kanonieri qurdebi*), they faced prison time. Likewise, there are some Russian criminals who ought no longer to be considered part of Russian-based organized crime. Since 2022, for example, many of the Russian gangster-expats in Spain have essentially cut politically dangerous ties with networks back home. Likewise, a sizeable Georgian and Armenian organized burglary ring active across France and Belgium, which was broken up in 2012, was initially described as 'Russian organized crime' but its members and leaders had no real connection with Russia.²³

Beyond a need to diversify for their own security, the other key driver behind the internationalization of Russian-based crime has been a keen awareness of just how much profit there was to be made in such activity. As one Italian finance police analyst recalled:

[It] was Italians – Mafia, Camorra, 'Ndrangheta, all of them – who first saw the value of Russia's banking system [in the early 1990s]. It was corrupt, opaque, perfect for them at a time when we were getting better and better at tracking their money laundering operations. But they'd move money through Russia and, poof, it disappeared as far as we were concerned. It took years for us to build proper connections with the Russian police to share intel reliably, and even then, we never knew if we were getting the real story, so extensive was the level of corruption.²⁴

This was about more than exploiting the essentially uncontrolled nature of Russian banking in the 1990s. It was also about the insatiable demand for unaffordable Western goods (a steady flow of stolen cars headed into Russia, for example²⁵) and the permeability of the country's borders. A northern route for Afghan opiates headed to Europe through Russia soon emerged to challenge or supplement the traditional routes via Pakistan, Iran, Turkey and the Balkans. Counterfeit goods from China also destined for the West began moving along the Trans-Siberian Railway.²⁶

This reflected a transition in the Russian underworld, already underway in the later 1980s, whereby the old-school tattooed gangsters of the *vorovskoi mir* and their *vor v zakone* ('thief in law') leaders were succeeded by a new generation of criminal businessmen known as *avtoritety* ('authorities'). Whereas the *vory* tended towards traditionalism and classic gangster activities, the *avtoritety* were as happy to engage in legal and illegal activities, less interested in 'honour' and upholding the macho code of the *vory* than as making as much money as possible.²⁷

These criminal operations tend to be highly flexible, highly entrepreneurial and highly profitable. The Russian gang that was broken in the Portuguese Operation Matrioskas in 2016, for example, laundered the proceeds of its operations at home by investing it into struggling European football clubs. That money and those stakes were used to bankroll illegal betting operations in Portugal, Austria, Estonia, Germany, Latvia, Moldova and the UK.²⁸

Russian-based organized crime networks, while in the main not especially active in terms of street-level crime in Europe, North America and beyond, are nonetheless pervasive as strategic allies and suppliers. Although the war in Ukraine has, by various estimates, halved the flow of the northern drug route into Europe, for example, Russian-based organized crime networks still provide a substantial share of the heroin sold by the continent's gangs, as well as other narcotics, including cocaine swapped for heroin and precursor chemicals with Latin American gangs.

Kyiv shortly after the invasion. The war in Ukraine is regarded by the Kremlin as but one front in a wider struggle with the West. © SOPA Images/LightRocket via Getty Images



These relationships between Russian-based organized crime and local gangs are strictly transactional. As one Italian police officer put it, referring to the Calabrian 'Ndrangheta: 'They will deal with the Russians, but not do them any favours.'²⁹ Nonetheless, they offer not just drugs but also everything from guns and people to counterfeit goods and untaxed cigarettes, generally imported in large consignments and sold on to local gangs, as well as underworld services ranging from money laundering to hacking.

As a result, although they have particular concentrations, such as in Spain, Israel and Germany, these networks are present to some extent across the West and, more to the point, have a wide range of contacts with local, non-Russian criminals. As they are increasingly employed as a tool of the Kremlin, this also means that there is a risk that such operations may be subcontracted to local criminals (more of which later).

The early 'crimintern'

Soon after Putin's election in 2000, it was made clear that the state was back in control and would not accept the kind of overt lawlessness on the streets that had marked the 1990s. Anything that looked like a direct or implicit challenge to the state would be treated severely, especially any attempt by Chechen groups to support their brethren back home, given that at the time the Second Chechen War (1999–2009) was raging, as Moscow reimposed its will on this rebellious territory. In the main, these new rules of the game were accepted, being reinforced from time to time by high-profile and heavy-handed arrests of senior criminals perceived as failing to recognize their place.

Since around 2011, however, proscription of crime began increasingly to be supplemented by increased prescription.³⁰ The Kremlin still identified no-go areas, such as the 2014 Sochi Winter Olympics and the 2018 FIFA World Cup, both of which were considered national flagship soft power events, not to be marred by undue predation on foreign visitors. For example, a Moscow gang notorious for its organized pickpocketing ring targeting tourists was encouraged by the local police to take a 'holiday'.³¹

However, cases in which criminals at home and abroad were induced to perform tasks for the state began to be more widely evident. BIS, the Czech Security Information Service, noted in its 2011 annual report: 'Contacts of officers of Russian intelligence services with persons whose past is associated with Russian-language organized criminal structures and their activities in the Czech Republic are somewhat disturbing.'³² When later pressed as to what this meant, a BIS officer clarified that 'local Russian gangsters were being "invited" into the embassy, and when they came out, their activities would be different, or else they maybe were doing favours for the [intelligence officers] alongside their own businesses'.³³

This became more evident from 2014, following the annexation of Crimea (itself, as will be discussed later, facilitated through state-crime connections) and the subsequent imposition of sanctions. These created new markets, with stolen goods smuggled into Russia via Poland, Lithuania and Belarus.³⁴


This began to assume a more sinister dimension as evidence began to emerge that these routes were also being used as support networks for intelligence operations. As a report on Moscow's activities noted, 'For years prior to the full-scale invasion, the Ukrainian Border Guard Service noted close relationships between Russian officers and smuggler networks across all of Ukraine's borders.'³⁵ This was, however, essentially limited, transactional and characterized by mutual mistrust.

It was with the 2022 invasion that the co-option of Russian-based organized crime as an instrument of Russian tradecraft abroad – a 'crimintern' instead of the old, ideological Comintern, the Communist International, of Soviet times – would truly become a key element in Russia's political war campaign against the West.



CRIMINAL WARFARE: TRANSFORMATION SINCE 2022

Spanish officers investigate the scene where Maxim Kuzminov, a Russian pilot who defected to Ukraine, was assassinated by Russian agents in 2024 in Spain. Russian-based organized crime networks are active in Spain. © *Rafa Arjones/Informacion.es* via Reuters



When, in August 2023, Russian Captain Maxim Kuzminov flew his Mi-8 helicopter to a Ukrainian base near Kharkiv, in a defection that also doomed his two crew members to death at the Ukrainians' hands, he must have known that the Russian state was not going to rest until it had had its vengeance. As Sergei Naryshkin, director of the SVR, went on to say, 'This traitor and criminal became a moral corpse at the very moment when he planned his dirty and terrible crime.'³⁶ In any case, Kuzminov was rewarded by Kyiv for his part in Operation Synytsia with US\$500 000, and a new identity in Spain as a purported Ukrainian citizen, one Ihor Shevchenko.³⁷ However, he did not keep a low profile: he spent profligately, picked fights with equal abandon and, crucially, broke one of the fundamental rules of witness relocation and reached out to an ex-girlfriend in Russia.

Shortly thereafter, while walking to his car under a residential complex in Alicante, two as-yet-unknown assailants put six 9mm bullets into him and, for good measure, ran him over with their car. While there is no real question but that this was a Russian government hit – Spanish newspaper *El País* reported that 'the only doubt experts have is whether the operation was the work of the Foreign Intelligence Service ... the Federal Security Service ... or of the Military Intelligence Service' – nonetheless there is a strong suspicion that the actual killing was outsourced to or through the Russian-based organized crime community that is still so active in Spain – and especially in Alicante, the Spanish province with the largest Russian population.³⁸ A Spanish judicial police investigator noted that 'the methods, the overkill, that does not sound like some *Spetsnaz* hit squad, but a couple of gangsters'.³⁹ The investigator added that 'the killers may well not be Russians, but any thugs, perhaps from abroad'.

Russian-based organized crime in Spain

From the 1990s, Russian-based organized crime was drawn to Spain for its congenial climate, its membership of the EU and – at least in the early days – its relatively permissive law enforcement. Major networks established branches there and for a while, it seemed as if they were unassailable. However, especially thanks to the pioneering work of figures such as Judge Jose Grinda, in due course the state launched a series of comprehensive and high-profile criminal prosecutions.⁴⁰

The Guardia Civil's Operation Dirieba targeted the Moscow-based Taganskaya group in Mallorca in 2013 and Operation Troika against the Tambovskaya gang in 2008.⁴¹ Under this pressure, some groups left, some remained and others put down roots, moved their assets out of Russia and broke ties with their parent networks.⁴² There remains a significant Russian-based organized crime presence in Spain, but policing operations continue and their strength and freedom of manoeuvre has been substantially constrained.⁴³



A suspected member of the Tambovskaya-Malyshevskaya gang is arrested in Spain, 2008. © Jaime Rossello/AFP via Getty Images

The (criminal) revolution in Russian politics

The revolution in Kremlin thinking and policy since February 2022, and in particular the rapid transformation of the mobilization state into the conscription state, is only part of the reason why the Kremlin has turned increasingly to the use of Russian-based organized crime – as is likely to have happened in Kuzminov's case – as part of its statecraft.

Nonetheless, it is clear that the current war in Ukraine is regarded as only one front of a wider struggle with the West, and one that Putin considers existential. In his speech to mark the Victory Day celebrations in 2023, he warned that 'the Western globalist elites ... pit nations against each other and split societies, provoke bloody conflicts and coups, sow hatred, Russophobia, aggressive nationalism, destroy family and traditional values which make us human' and that 'a real war is being waged against our country again'.⁴⁴ Even setting aside the rhetorical overkill, it is clear that the Kremlin is operating on the basis that it is at war, and thus anything that furthers victory is acceptable.

A second reason for the increased use of criminals is a perverse outcome of the massive and coordinated campaign of expulsions from Western embassies of Russian diplomats known or believed to have been intelligence officers, totalling some 400 from Europe along within the first six months of the war.⁴⁵ This has made the Russian intelligence community look for new proxies of every kind, including petty criminals. Many of these are the rankest amateurs, attracted only by the promise of pay, and will quickly fail, be



exposed or arrested. Moscow in many cases will have recruited them online or through cut-outs (which may well be more senior underworld figures) such that they do not even know they are working for Russia, and are regarded as disposable. A senior Western military intelligence official told *The Wall Street Journal* that 'these cheap and seemingly bumbling efforts are nothing to be sneered at. They are part of a large toolbox of intelligence gathering that has helped Russia destroy key materiel with minimum investment.'⁴⁶

Likewise, active political efforts to isolate and condemn the Russian state have generated a backlash that almost embraces the sense of the country being a pariah, at least in the eyes of the West (as opposed to the Global South, which Russia increasingly calls the 'World Majority').

With Russia being variously damned as 'fascist' in *The New York Times* or 'imperialist and racist' in the European Parliament, there is a greater willingness on the part of the Kremlin to take risks and conduct operations that once would have been considered too potentially damaging to its reputation and its relations with other countries.⁴⁷

Managing the proxies

To the degree to which this campaign is coordinated, this is handled by the Presidential Administration (AP), and especially the Secretariat of the Security Council (SB), a largely autonomous part of the overall AP.⁴⁸ The SB Secretariat has developed something of an ad hoc role managing the interaction between elements of the intelligence community, in the absence of any structure like the US Director of National Intelligence or

In his 2023 speech to mark Victory Day, Putin's rhetoric railed against 'Western globalist elites' and 'Russophobia'. Any measures that further victory are deemed acceptable by the Kremlin. © VCG via Getty Images

the UK's Joint Intelligence Organisation. However, there does not appear to be much strategic-level direction specifically relating to the use of proxies such as organized crime. Instead, tasking is very much focused on outcomes, not means, and so each of the agencies has developed its own subtly different approach.

While the SVR has developed its own cyber-espionage capacity, and is 'widely acknowledged to be the most sophisticated of the special services in conducting technical surveillance and signals intelligence collection', it is still largely a traditional human intelligence (HUMINT) agency.⁴⁹ Although it has made considerable efforts to recover some of the capacity lost through the mass expulsions of its officers from Western embassies, this is still very much as work in progress. Meanwhile, military intelligence (GU, although still widely known as the GRU) has more of a focus not simply on gathering relevant information, but also conducting operations with a direct military-strategic advantage, such as sabotage and assassination.

It was the FSB that pioneered the use of criminal proxies and agents, first at home and in due course abroad, reflecting both its domestic security priorities and also the high levels of corruption within its ranks, which opened up further channels to the underworld.⁵⁰ Initially, it had minimal foreign activity, beyond running some informants inside criminal gangs and terrorist movements targeting Russia, and engaging some hackers for occasional operations. Anton Nosik, activist and journalist, one of the godfathers of the Russian internet, claimed in 2006 that 'each [Russian] hacker, who is not in prison, has a curator. Either in FSB, or in the Directorate K of the Ministry of Internal Affairs ... Our criminal hackers are connected with the MVD and FSB completely ... Because over them [all] a general is sitting, who gives them orders. A general of the FSB.'⁵¹ Unlike Directorate K, the MVD's cybercrimes unit, the FSB saw this as an opportunity also for sporadic activity abroad.⁵²

Over time, its Fifth Service, the Service for Operational Information and International Communications (SOIMS) also acquired an increasingly significant external role. Not only did it operate in countries of the former USSR (including Ukraine, where it would reportedly launch a series of assassination and subversion operations in the SVO⁵³), but it began using what was known as Line RT operations – *Razvedka na terriore*, or 'intelligence on the (home) territory' – to recruit foreigners as agents while they were in Russia. Then, as Moscow's relations with the West worsened, it extended this to wider operations abroad. Unlike the SVR and GRU, this was never really through officers embedded within embassies. It involved more untraditional means, including recruiting criminals, and a focus not so much on intelligence gathering as active measures, including subversion, disinformation, sabotage and assassination.



CRIMINAL TRADECRAFTS

The 2017 NotPetya cyberattack revealed Ukraine to be a testing ground for Russian cyber warfare capabilities, targeting, among other sites, the country's power infrastructure. © Viacheslav Ratynskiy/Reuters



Kristian Vanderwaeren, head of the Belgian General Administration of Customs and Excise, noted in late 2022 that by 'midyear, we had seen a massive increase in traditional illegal activity from Russian-linked groups that appear to have Russian government backing working to develop new revenue streams to replace damage from the sanctions'.⁵⁴ With a state budget of around half a trillion rubles, the Russian Federation is not turning to cigarette smuggling and the like to fund itself, though. Rather, such criminal operations allow it to raise operational funds for its covert operations abroad, destabilize the West and provide channels and contacts that can be developed illegally to import sanctioned or restricted goods into Russia. 'Crime,' observed one experienced British intelligence officer, 'is the magic answer to so many of Putin's problems.'⁵⁵

Sanctions-busting

In July 2024, Maxim Marchenko, a Russian businessman living and operating several companies in Hong Kong, was sentenced to three years in prison by a New York court on smuggling and money laundering charges. Primarily, he was responsible for smuggling military-grade electronics to Russia, which could be used in telescopic sight, night vision goggles and similar systems, using shell companies to claim that they were destined for end-users in China and elsewhere for medical research and hunting rifles.⁵⁶ His incautious visit to the US, which allowed the FBI to arrest him, ended that particular criminal venture, but as an FBI officer connected with that case confirmed, 'For every one network we break, one, two, three more pop up, run by everyone from dodgy businesspeople who spot an opportunity to out-and-out gangsters.'⁵⁷

There have been sanctions on Russian banking and business since 2014, but in 2022, a vastly more extensive range of measures intended in particular to starve its defence-industrial complex of imported components and spare parts has been imposed. Over time, sanctions and also the secondary effects of controls on payments, which have made it difficult for Russian companies to pay foreign suppliers, have also led to shortages in everything from aircraft spare parts to medicines.

Nature abhors a vacuum, and criminals will supply markets that cannot be satisfied through legal means. A massive array of smuggling operations has emerged to get round these controls, something visible in the increase in economic crime in Russian border regions best suited to such activity.⁵⁸ The bulk of sanctions-busting activity is managed by commercial facilitators, businesspeople arranging imports to third countries, whence they can quietly be reimported to Russia. This grey or parallel market in sanctioned consumer goods is essentially ignored by through-states such as Turkey, the UAE and the countries along Russia's southern periphery.

While imports of German cars and automotive spares quickly fell to near-zero, a spike in sales to Armenia and Kazakhstan shows such 'grey market' re-export was neither helped nor hindered by the Kremlin.⁵⁹

These methods also have direct military applications. Advanced modern 'smart products', from washing machines to gaming consoles, have microchips that can often be reprogrammed for use in precision-guided missiles. This helps explain why sales of refrigerators from the EU to Kazakhstan trebled in 2022.⁶⁰ Their microchips began to turn up in Russian missiles and drones, even though the overwhelming majority of these components were simply bought from suppliers through legitimate channels and then re-exported to Russia.⁶¹

More than US\$1.5 billion in 'grey market' electrical goods were reportedly routed through the UAE in the first year of the war alone.⁶² As a result, according to a joint study by the Yermak-McFaul International Working Group on Russian Sanctions and the Kyiv School of Economics, the sanctions against Russia, while by no means ineffective, are having a sharply limited impact, because:

In the first ten months of 2023, imports of what the USA, EU, UK, and other partners of Ukraine have identified as priority battlefield goods reached \$8.77 billion – only a 10 per cent decline compared to the pre-sanctions period. For all items that we consider to be critical for Russia's military industry, they were even higher – \$22.23 billion.⁶³

Overall, according to one estimate, more than 6 000 companies have supplied Russia with nearly US\$4 billion worth of sanctioned microchips.⁶⁴ Of course, Moscow has a history of turning to illegal means to bypass sanctions and export controls. The Soviet Union developed complex and cunning means of bypassing Western CoCom (the Coordinating Committee for Multilateral Export Controls) sanctions meant to prevent access to military technologies.⁶⁵ In the past, though, this was essentially the business of the KGB, the Soviet intelligence and security agency. While the intelligence community is still heavily involved in such activities today, where they cannot rely on purely commercial grey market facilitators, they are much more actively turning to organized crime groups to supplement their activities.

It is an open secret that gangs willing and able to smuggle materials that the state needs (the old Soviet term *defitsitny*, 'in deficit', once used in Soviet times simply for hard-to-find consumer goods, has been revived and repurposed for such strategic necessities) can expect not only generous payment but also often negotiated privileges, such as free passage to export illicit commodities.⁶⁶

If anything, 2024 has seen a decline in cases such as the theft of Rotax engines from microlights to drive drones, or roadside speed cameras for their advanced optics.⁶⁷ This is a result of Russian efforts to procure components becoming more organized. As a Swedish intelligence analyst observed, 'The criminals seem to have been more of a temporary response – the government wanted reliable, large-scale supplies, and now that it seems to be able to get them [through the grey-market traders], then there's less emphasis on the kind of piecemeal operations [the gangs could run].'⁶⁸

Illegal financial flows

More significantly, all sanctions-busting operations, whether handled by the intelligence community, grey-market facilitators or organized crime networks, depend on the capacity to transfer funds, almost invariably in defiance either of international controls on Russian finance or outright law-enforcement surveillance. The structures that have emerged often seamlessly blend money laundering, state influence operations and personal enrichment.

In Moldova, for example, Igor Chaika (son of former Prosecutor General Yuri Chaika) was the official envoy of the Russian business association Delovaya Rossiya ('Business Russia') to Moldova and also the breakaway, Russian-backed pseudo-state of Transnistria. In its announcement of sanctions against Chaika, the US Treasury alleged that he tried to set up a crypto-mining business in Transnistria, while in contact with the FSB's SOIMS and also allowed his companies to be used by the Kremlin 'to funnel money to the collaborating political parties in Moldova', some of which was 'earmarked for bribes and electoral fraud'.⁶⁹

Was this illicit financial activity an example of criminal enterprise, of covert state interference or financial self-interest? Probably all of these, and in many ways this is the point: existing financial conduits can quickly be adopted by the state for its own ends.⁷⁰



Putin visits Russia's financial oversight agency, Rosfinmonitoring. Cryptocurrencies provide a means for the Russian state and companies to operate in an environment of financial sanctions.
© Alexey Druzhininapf via Getty Images

Russian-based organized crime in Cyprus

In 2013, a report by Global Financial Integrity described Cyprus as a 'laundry machine for dirty Russian money', while a Czech observer called it a 'Russian bank with dirty money posing as an EU state'.⁷¹

Since then, Cyprus has – despite some genuine recent efforts to clear up its act⁷² – largely retained its role as a hub for Russian illicit financial activities. To a large degree, this has entailed tax evasion and not work on behalf of the Kremlin. Much of this was capital flight and laundering embezzled state assets, something even official sources accepted. However, flows often operate both ways, and especially since 2022, it has been used for a variety of transactions connected with the Russian state and its intelligence services, as well as criminals.⁷³

This has encouraged and been facilitated by a substantial and, until 2022, growing Russian-speaking population, especially in Limassol, which reportedly became home to some 50 000 Russian speakers, comprising around 20 per cent of its total population of almost 240 000.⁷⁴

Within this sector is a thriving Russian-based organized crime community, including Pontian Russians of Greek descent, who also act as a bridge between the Russian and Greek underworlds. Nonetheless, the primary role of Cyprus within the global Russian criminal economy remains as a node for the illegal flow of capital in and out of the country, and increasingly this means catering to the state, not simply the gangsters.

Organized crime structures established to move and launder money have therefore become increasingly pivotal. As a British National Crime Agency analyst bemoaned, 'The single greatest potential point of failure for Russian smuggling operations is the money flow – and arguably this is what we have had least success in cracking.'⁷⁵

Despite the extension of sanctions on its banking system and a growing array of individuals and companies believed to be facilitating Moscow's covert financial operations, which is increasingly looking like 'an effort to set up a global financial embargo on Russia', the Kremlin must find ways to buy necessary materials, support its treasury and pay for overt and covert operations abroad.⁷⁶

Although it has proven imaginative in its use of alternative structures, from Chinese banks to online payment systems, as more and more avenues are closed to Moscow, largely for fear of coming under secondary sanctions, it has had to turn to criminal money-movers. To a considerable extent, this means taking advantage of financial jurisdictions that have long been favoured by Russian criminal networks, such as Cyprus, Serbia, Turkey and the UAE.

Indeed, the challenges of international sanctions, greater scrutiny of any accounts even suspected of having some kind of Russian connection and the closure of many Russian government institutions in the West have all created an intelligence dilemma. Many activities require operational funds that can be disbursed, whether to pay for physical assets, buy transport tickets or pay off hirelings. A crucial need is that this be *chornaya kassa*, or 'black account' money, with no apparent connection to Russia. Some of these payments can be made through virtual cryptocurrencies, but others need to be in other forms.

A Central European counter-intelligence officer observed:

They need hard currency to operate in Western and Central Europe and while sanctions have not devastated Russia, we have clear indications that there's a cash crunch for off-the-books intelligence operations that were once funded by oligarchs at the request of Moscow ... And we have seen a shift to completely illegal activity from drugs, to bootleg products, to illegal sales of oil and gas, and even a shift by state-controlled industries, particularly Belarus, to producing illegal or counterfeit goods like pharmaceuticals.⁷⁷

Often, the intelligence community is not so much directly involved in crime as, in effect, 'taxing' Russian-based organized crime operating in the West. This involves demanding that they pay some of their (laundered) criminal profits there into accounts that can then be used for operational purposes. One officer of the BfV, Germany's security service, described how

a gang in a German port ... is made up of a mix of Russians, Lithuanians and Germans, but the Russians are in charge. They smuggle meth in from Russia, using fishing boats in the Baltic. One day, the FSB turns up at their suppliers in St Petersburg and lays out the way things are going to go. They can carry on their business with the gang in [Germany] ... but only so long as the Rostock guys pay a certain amount each month into a different European bank account each month. The FSB officer knows who lives where, how much everyone is making, but is cutting a reasonable deal, working out in this case as something like 5 per cent of the profit. That still leaves 95 per cent, and the alternative is to lose 100 per cent, so of course they do the deal.⁷⁸

It is impossible to know how much 'black cash' is generated this way, nor how many Russian-based organized crime groups have actually been tapped for it. One Europol analyst suggested in January 2024 that it was 'still pretty rare, but definitely a growing trend'.⁷⁹

However, the need to maintain illicit financial flows for state purposes – which can also be used by criminals for their own ends – has created a particular policy dilemma regarding cryptocurrencies. The Kremlin has long been suspicious of cryptocurrencies for the way they allow Russians to evade the attention of Rosfinmonitoring, its financial intelligence and oversight agency. As of 2021, crypto market activity in Russia was estimated at US\$500 billion, and with over 17 million cryptocurrency investors, it was third globally in terms of holders and second (after Ukraine) in terms of how widely used cryptocurrency is among the population.⁸⁰

There is also concern about the escalating energy demands of crypto-mining, which accounts for 16 billion kilowatt-hours per year, almost 1.5 per cent of Russia's total electricity consumption, such that Putin has warned that it would lead to local power shortages.⁸¹ Hence, there has been heightened pressure for deterrent sentencing, and the Supreme Court's overturning in 2023 of an acquittal represented the first conviction for money laundering through cryptocurrency.⁸² In 2022, the Bank of Russia even published a consultation paper warning that 'the growth of cryptocurrencies seriously jeopardizes Russians' well-being and the stability of the financial system, and causes threats associated with the use of cryptocurrencies for illicit settlements' and proposing draconian controls.⁸³



A US Department of Justice press conference following the arrest of the founder of Bitzlato, a virtual currency exchange. The US authorities found the exchange had links to illicit Russian finance. © US Government staff/Reuters

On the other hand, cryptocurrencies also provide a means for the Russian state and companies alike to operate in an environment of financial sanctions. For instance, in January 2023, FinCEN, the US Treasury's Financial Crimes Enforcement Network, identified the virtual currency exchange Bitzlato as a 'primary money laundering concern' in connection with Russian illicit finance, including criminals connected with the Russian government.⁸⁴

Likewise, cryptocurrency transactions have been identified as involved in a range of recent covert influence and subversion operations, such as under-the-counter payments made to politicians through the Voice of Europe propaganda outfit.⁸⁵ Thus, Rosfinmonitoring head Yuri Chekhanchin recognized the 'need for businesses, especially in cases involving sanction mechanisms, when they need to enter the international market, and it can't always be resolved through standard methods' when his agency supported a draft bill allowing the creation of infrastructure for international (not domestic) payments in cryptocurrencies in July 2024.⁸⁶

Over time, then, the likelihood is that while the Kremlin will seek to control the domestic use of cryptocurrency, Russia will become even more open to its use for external activities. In addition to supporting sanctions-busting activities, this would also facilitate criminal operations such as ransomware, and drug and people trafficking. This is especially the case for crypto-to-fiat services, allowing criminals to move money from anonymous crypto wallets into conventional currency in the name of a nominee from another country, who may be a proxy, a supplier or an associate.⁸⁷

Cryptocurrencies would also be of value to the Russian intelligence community as a means of anonymously – or less detectably, at least – providing operational funds and payments to their proxies and operations abroad.

Cyber

Cryptocurrency is one of many factors making it easier for Russian cybercriminals to operate – especially when they operate under the tacit protection of the state. In May 2024, Anne Keast-Butler, director of the UK's signals intelligence service GCHQ, warned that her agency was 'increasingly concerned about growing links between the

Russian intelligence services and proxy groups to conduct cyber-attacks – as well as suspected physical surveillance and sabotage operations'.⁸⁸ Likewise, US Assistant Attorney General for National Security John Demers claimed that 'no country has weaponized its cyber capabilities as maliciously or irresponsibly as Russia, wantonly causing unprecedented damage to pursue small tactical advantages and to satisfy fits of spite'.⁸⁹

There is, of course, evidence that Russia's own intelligence agencies have robust and aggressive cyber capabilities, which they use not merely for information gathering but also, in the new combative environment, for active sabotage, launching sophisticated and often long-term online operations.⁹⁰ For example, in 2023, Sandworm, a group the US and other governments believes operates within the GU's Military Unit 74455, reportedly spent more than six months inside the systems of Kyivstar, Ukraine's largest mobile phone operator, in order to gather intelligence before launching an attack that disrupted services for 24 million users.⁹¹ Even so, that was relatively benign compared with their former operations, such as unleashing the NotPetya malware on Ukraine's power systems in 2017.⁹²

There is also a long tradition of the use of criminal hacker communities, whether for targeted attacks or as 'surge capacity', in wider operations. The DDoS (distributed denial of service) attacks on Estonia in 2007, Georgia in 2008 and periodically Ukraine have sought to overwhelm and crash systems by flooding them with traffic. These especially benefit from mass participation, including from the amateur 'patriotic hackers' who are often provided with the tools to participate.⁹³ In the words of one assessment:

Ukraine's largest telecoms company was hacked in 2023 reportedly by a Russian group. The company denounced it as an 'act of war'. © Global Images Ukraine via Getty Images



Contrary to popular belief, the Kremlin does not control every single cyber operation run out of Russia. Instead, the regime of President Vladimir Putin has to some extent inherited, and now cultivates, a complex web of Russian cyber actors. This network includes: cybercriminals who operate without state backing and inject money into the Russian economy; patriotic hackers and criminal groups recruited by the state on an ad hoc basis; and proxy organizations and front companies created solely for the purpose of conducting government operations, providing the Kremlin a veil of deniability. This web of cyber actors is large, often opaque, and central to how the Russian government organizes and conducts cyber operations, as well as how it develops cyber capabilities and recruits cyber personnel.⁹⁴

Targeted operations that appear to have been, in effect, commissioned or encouraged by the state have increased since February 2022. These include attacks on Estonian public institutions and private companies, and the Latvian parliament in August 2022.⁹⁵ The group known in the West as ‘Smokey Spider’, for example, uploads malware against targets for financial gain, and in March 2022 distributed DanaBot payloads subsequently used in DDoS attacks against Ukrainian targets.⁹⁶ The Stanford Cyber Policy Center also found that Western companies that withdrew from the Russian market or suspended operations in Russia following the invasion were more likely to experience ransomware attacks in the following months, suggesting at least a degree of official encouragement, or an active ‘patriotic’ agenda.⁹⁷

Another example is the campaign being waged against the European railway system, intended both to cause generalized chaos and establish back-door access for more serious future disruption. Czech transport minister Martin Kupka has, for example, highlighted the ‘thousands’ of attacks made against national rail company České dráhy and other European lines since 2022, from ticketing to signalling systems. The European Union Agency for Cybersecurity (ENISA) has noted also attacks on the Latvian, Lithuanian, Romanian and Estonian rail systems, and placed the blame on ‘pro-Russian hacker groups’.⁹⁸ Likewise, ENISA has noted ‘a surge in DDoS attacks by pro-Russian hacktivist groups who aimed to disrupt healthcare providers and health authorities in the EU’.⁹⁹

While the Kremlin’s ‘official’ cyber operators focus on strategic targets, these disruptive attacks – many of which are also monetized in their own right, through the use of ransomware that locks up the target systems or threatens to leak sensitive data until a ransom is paid – are, in effect, ‘subcontracted to cybercriminal gangs already known to the Russian authorities’, according to one Europol analyst.¹⁰⁰

According to Juhan Lepassaar, head of ENISA, online attacks originating within Russia ‘doubled from the fourth quarter of 2023 to the first quarter of 2024’.¹⁰¹ Many of these are relatively trivial in their own terms. In May 2024, for example, dozens of schools in and around Athens received bomb threats, and many had to be evacuated.¹⁰² Ten days later, similar threats were sent to schools in Cyprus, all from a Russian server. Although the service provider claimed the emails had originated from the US, the Greek authorities continue to assume these were Russian-instigated attacks intended to ‘disrupt public order’.¹⁰³ A Greek official with knowledge of the investigation said that preliminary findings were that the emails were indeed sent from the US, but by a ‘small-scale cybercriminal working on Moscow’s behalf’.¹⁰⁴



The UK's Government Communications Headquarters has expressed growing concerns about the Russian intelligence service and its proxies' weaponization of its cyber capabilities.

© David Goddard/Getty Images

The haphazardness of these attacks may in part reflect opportunism, but also the degree to which a blind eye is turned to hackers who are left to carry out attacks with only minimal direct oversight, let alone specific targeting guidance. The so-called Cyber Army of Russia group (or sometimes Cyber Army of Russia Reborn), for example, seemed to take it upon itself to attack the water utility's control systems of the small Texas town of Muleshoe, leading to 'a leak of tens of thousands of gallons of water'.¹⁰⁵ Although the group appears to have some loose connections to the GU's Unit 74455 (Sandworm), it is hard to see Muleshoe's waterworks as high on any Kremlin list of targets.¹⁰⁶

While it will carry out very carefully targeted operations with its own cyber assets, the Kremlin also regards its broader goal of spreading disruption in the West and demonstrating that support for Ukraine comes at a cost as also met by encouraging attacks of almost every kind. Indeed, it is facilitating such attacks by Russian-based gangs simply by extending an implicit offer of impunity. Law enforcement cooperation has all but collapsed except in some areas such as terrorism and paedophilia. In that context, Russian online criminals know that so long as they confine their attacks to Western targets, they face no risk of investigation, let alone extradition.

When the notorious ransomware operator Mikhail Matveev was asked 'Between the FSB and the FBI, who scares you the most?', he candidly admitted, 'If these two structures start cooperating with each other — then I'll get fucked up.'¹⁰⁷ Such a prospect seems inconceivable at present.

This has led to the particular rash of ransomware attacks. Even before the war, Lindy Cameron, chief executive of the UK's National Cyber Security Centre, called ransomware 'the most immediate danger facing the country in the online realm', and noted that 'cybercriminals based in Russia and neighbouring countries are responsible for most of the devastating ransomware attacks against UK targets'.¹⁰⁸

Although 2022 saw an unexpected lull, likely in part because of disruption caused by the invasion, this proved a short-lived respite.¹⁰⁹ Through 2023, when operations at

the container terminal at Japan's port of Nagoya were significantly disrupted and the Qilin hacker group targeted the courts in the Australian state of Victoria, and through 2024, when healthcare providers, from American health insurance giant UnitedHealth Group to a laboratory providing blood tests to the British National Service, have been targeted, this has become a growing challenge.¹¹⁰

In 2022, it was estimated that 74 per cent of all ransomware earnings in 2021 went to Russia-linked hackers. This proportion has at the very least held stable and is more likely to have increased since then.¹¹¹ By offering enrichment with impunity, Moscow can enlist criminals into its campaign of disruption against the West at no real cost to itself.

Filling intelligence gaps

In April 2024, a Polish national known publicly only as Paweł K, was arrested on allegations that he was assisting a plot by the Russian intelligence services to assassinate Ukrainian president Volodymyr Zelensky. He was reportedly gathering security information for the GU about Rzeszów-Jasionka Airport in south-eastern Poland, near the Ukrainian border, a gateway for international military and humanitarian supplies for Kyiv.¹¹² Obviously the (as-yet uncorroborated) claims of an assassination plot monopolized the headlines, but every bit as striking was the extent to which the GU, an agency that once had an extensive network of agents and handlers in Poland, was having to rely on a local of unconfirmed loyalty and competence, communicating with him only over the internet.

While cyberattacks, sanctions-busting and associated illicit financial flows have been widespread since 2014, there has been a marked change in the degree to which the Russian intelligence community is having to use organized crime – and other, often unknowing proxies – to fill the gaps between their current aspirations and their capacities, especially in Europe.

With so many officers expelled from embassies across the West, and at a time when the Kremlin's demands for both information and active measures is only increasing, these 'Lubyanka street irregulars' have become vital in providing typically low-level support, freeing up the remaining professional intelligence officers for more vital and complex missions.¹¹³

Much of the tradecraft of intelligence activity depends on such basic activity as collections from 'dead-letter boxes' or other drops, simple surveillance and leaving encoded messages in plain sight (such as chalking a cross on a particular post box). '[This] is much the same as the day-to-day activity of, say, a drugs gang,' observed a German security officer.¹¹⁴

In some cases, local criminals, operating without the potential stigma of Russian citizens, have been engaged for such activities by the intelligence community working through their Russian-based organized crime suppliers. For example, in a substantial operation uncovered in Poland, a 23-year-old Ukrainian appears to have been the leader of the 16-man spying network working for the GU. Mainly impoverished young Ukrainians, Belarusians or Poles, they were largely tasked with simple activities, especially connected

with monitoring the flow of military aid to Ukraine, such as placing cameras along railway lines.¹¹⁵

There have been past examples of such activity. In 2014, Estonian Kapo (security police) officer Eston Kohver was seized by an FSB commando team that abducted him into Russia when he was expecting to meet an informant within a small-scale smuggling gang. The reason for this brazen operation, which led to Kohver being spuriously charged with 'espionage', turned out to be that the gang was engaging in low-level intelligence gathering in return for free passage with counterfeit cigarettes across the border.¹¹⁶ There are also more serious mercenary intelligence-gathering operations conducted by organized crime gangs on Moscow's behalf, for which sums as high as €400 000 have reportedly been paid.¹¹⁷

Just as with the hacking operations, these often reflect the criminals having specific skillsets or access to opportunities of value to the Russian intelligence community. Back in 2010, the Russian deep-cover agent known as Christopher Metsos, arguably the most effective and professional member of the so-called 'Illegals Ring' that had just been broken up by the FBI, managed to make it to Cyprus but was then arrested and, while bailed, could not find a legal way home. Although the US intelligence services were maintaining surveillance on him, he disappeared and the balance of probabilities is that he was smuggled into Greece by Russian-based organized people traffickers, from where his SVR handlers could exfiltrate him back to Russia.¹¹⁸

This was an early example of the use of criminals to fill gaps in intelligence community capacity, as although there were many intelligence officers embedded within Cyprus's large Russian community, they lacked the specific connections to get Metsos off the island, not least because they themselves were coming under increased scrutiny precisely to try and prevent that from happening. (Furthermore, it is possible that Metsos was allowed to flee by the Cypriot authorities to avoid a confrontation with Moscow, using criminals rather than intelligence officers to maintain deniability.¹¹⁹) In a similar vein, though, in 2023 it is believed that a team of Serbian people smugglers managed to spirit home Russian businessman Artem Uss, who was under house arrest in Italy awaiting extradition to the US on charges of smuggling military technology to Russia.¹²⁰

Weaponizing migration

In November 2022, as temperatures dropped to -22 degrees centigrade, hundreds of would-be migrants, mainly young men from Syria, Yemen, Iraq and Somalia, started crossing the Finnish–Russian border on bicycles and scooters.¹²¹ Foot travel between these border checkpoints was banned, making this an ingenious workaround. The bikes and scooters were being provided by the Russian authorities. However, unlike earlier attempts by the Belarusian authorities to swamp Polish border points in 2021, after President Alexander Lukashenko had threatened to 'flood' Europe with 'drugs and migrants', the Russians were not operating a vertically integrated venture whereby they recruited people, transported and directed them.¹²² Instead, theirs was a kind of public–private partnership in which they made it clear to existing people-smuggling operations that this opportunity would become available, and expedited the entry of would-be migrants into and across Russia before sending them across the border. This



avoided the need for the state itself to do the leg work, and provided Moscow with a certain (if threadbare) deniability.

A specific variety of organized criminality that has come to the fore in recent years is the weaponization of migrant smuggling as a means of political destabilization. The aim is to put the hostile neighbouring state in a lose-lose situation: either allow in virtually uncontrolled migration and exacerbate nativist and xenophobic forces at home, or (as Finland chose¹²³) close the border in a pragmatic move that nonetheless goes against Western values of allowing asylum for those with deserving cases. This not only generates political tensions in the target country, but it also provides material for Russian propaganda narratives in the Global South, where Moscow seeks to present the West as hypocritical and neo-colonial.¹²⁴

In the main, the people smugglers themselves are not ethnic Russians or even part of Russian-based organized crime, but are instead part of existing networks, often based in the Middle East or North Africa, with whom the Russian gangs have contacts (particularly as more and more Russians are being recruited by these networks, especially to captain boats carrying migrants across the Mediterranean¹²⁵) and who can simply be alerted to a new opportunity. In some cases, though, they are migrants who have settled in Russia and leveraged that position to establish new illegal businesses. For example, one report alleged that Abu Kamel, an Iraqi who had moved to Moscow with his family following the US-led invasion of his homeland, and who became a respected migrant smuggler.¹²⁶ One of Kamel's clients, a Tunisian, who had repeatedly failed to enter Europe via Turkey before engaging Kamel and successfully making it into Finland,

The Polish border with Russian enclave Kaliningrad. Russia has weaponized migration as a means of political destabilization. © Anadolu Agency via Getty Images



The Libyan Arab Armed Forces have reportedly received support from the Africa Corps, the successor to the Wagner mercenary group active in Libya. © Abdullah Doma/AFP via Getty Images

called him a ‘a trusted smuggler ... very well known for what he does’, especially because of his connections with travel agencies and the Russian border guards.¹²⁷ Men like him had previously been running operations moving a handful of potential migrants at a time, often only every few months, but their presence gave Moscow a ‘surge capacity’, such that they could be alerted and encouraged to step up their activities when the Kremlin wanted to put pressure on a neighbour.

However, the most serious potential escalatory option at Russia’s disposal comes from its operations in North Africa. A perennial concern is that Moscow’s interests in Libya, in particular – where the activities of the Wagner mercenary army have been rolled into the new Africa Corps, a structure under closer GU control¹²⁸ – is that if it acquired a degree of influence there it could, as an Italian intelligence officer put it, ‘turn the migration tap on or off’ at will.¹²⁹ It may be something of an exaggeration to claim, as one security source reportedly did, that ‘if you can control the migrant routes into Europe then you can effectively control elections, because you can restrict or flood a certain area with migrants in order to influence public opinion at a crucial time’.¹³⁰ Nonetheless, it is clear that this would provide Moscow with options for disruption – or political blackmail of southern European states. To this end, for example, in June 2022, Rome claimed that Wagner, an organization operating across the boundaries between legality and crime, was itself working with people smugglers and General Khalifa Haftar’s Libyan Arab Armed Forces to facilitate the flow of migrants by sea from the Cyrenaica to Sicily.¹³¹ Italian Defence Minister Guido Crosetto subsequently described this as ‘part of a clear strategy of hybrid warfare’, after a further upsurge that saw some 20 000 migrants reach Italy in the first quarter of 2023, compared with just 6 100 in the same period of 2022.¹³²

Since Wagner's mutiny in June 2023, the Africa Corps is still very active in Libya,¹³³ which a report from the Polish Institute of International Affairs (PISM) described as the Corps's 'emerging centre'.¹³⁴ With Libya's migrant smuggling business becoming increasingly extensive and well-organized – now also extending its services to customers from Egypt, Bangladesh, Syria and Pakistan¹³⁵ – the scope for subversion by people smuggling becomes all the greater.¹³⁶ With the GU also operating extensive and undamaged networks across Africa, which maintain links not just with corrupt government officials but also transnational criminal groups – 'these [GU officers] are the guys who don't wear suits, but are comfortable out in the deep bush with a pistol in their waistband swapping cases of Kalashnikovs for influence or access'¹³⁷ – this is something that could quickly and easily be ramped up into a major crisis.

Influence and information operations

In May 2024, blood-red hands were stamped onto the Wall of the Righteous outside the Shoah memorial in Paris, in an act of vandalism reminiscent of a similar campaign of anti-Semitic vandalism the year before, when the Star of David was spray-painted onto buildings in and around the capital.¹³⁸ Political and racist graffiti is hardly unusual in France, but the nature and timing of these incidents has led to serious speculation on the part of the French security apparatus that this was done at Moscow's behest. In the words of one commentator close to the DGSI, France's counter-intelligence and anti-terrorism agency, 'There's nothing definite – yet – but a strong sense that both attacks were ordered by someone abroad, carried out by French people, whether racist or just petty criminals, but paid for by foreigners. And yes, that means probably Russians.'¹³⁹ After all, the 2023 attacks were blamed on the FSB's 5th Service, after two Moldovans were arrested in connection with the case.¹⁴⁰

Since early 2023, the SOIMS had been embarked on a campaign to magnify existing social and political divisions within European countries. They began with using Moldovans in Poland to daub anti-NATO slogans ostensibly from disaffected Poles, and then generally encouraged disruptive attitudes and movements across the continent, from sparking demonstrations in Spain against 'Russophobia' to amplifying angers over Gaza (something also done in the US).¹⁴¹ The actual 'foot soldiers' of this campaign ranged from assets recruited from migrant communities from the post-Soviet states, such as the aforementioned Moldovans, through genuinely discontented locals who were usually 'radicalized' online and encouraged to take matters into their own hands, to petty criminals, typically paid a small sum for each action. To take another example, the GU recruited young Poles and Ukrainians over the online messaging service Telegram to spray-paint anti-war graffiti on specified locations for 30 złoty (€7) a time, not simply to spread their messages but also as a means of attracting individuals who could be cultivated for more serious operations.¹⁴²

This all represents something of a shift in Russian strategy and tactics. In the past, the goal was often to cultivate 'agents of influence' and through them to institute a degree of 'elite capture'. In Serbia, for example, there has long been a concern about the scale of Kremlin influence. Likewise, in Hungary through the early 2000s, there were recurring concerns about the influence of Semion Mogilevich, a powerful financier of Russian-based organized crime (arrested in Moscow in 2008 but controversially released the

following year¹⁴³). Mogilevich's business empire reached across Europe but he was alleged to have a network of clients and corrupted agents throughout the Hungarian state. A former associate of his claimed under oath that Viktor Orbàn received almost a million Deutschmarks (now worth around €500 000) from Mogilevich in cash in 1996 or 1997.¹⁴⁴

However, early fears (or, for Moscow, hopes) that corruption, blackmail and disinformation could swing elections and suborn national politicians have largely been exploded. The actual influence on polls such as the 2016 US presidential elections and Brexit vote in the UK, both of which had outcomes Moscow appreciated, proved not to have been significantly influenced by Russian information operations. Likewise, figures such as Serbia's Aleksandar Vučić and Hungary's Orbàn, whose policies often seem to favour Russia, have turned out to be simply working to their own advantage, happy to play Moscow against Brussels when it suits, no more.

Instead, then, the goal is paralysis through division, using whatever means at Russia's disposal to widen existing fault lines and amplify populist and disruptive voices. Moscow still supports the politicians and 'agents of influence' it thinks may be useful, often using *chornaya kassa* assets such as the cryptocurrency and physical cash that were distributed through the Voice of Europe propaganda front outlet in Prague until it was closed down in 2024.¹⁴⁵ However, the novelty is the degree to which these tactics are now supplemented by other activities meant to convey a sense of rising disaffection and chaos.

The newer methods employed by Russia offer much more scope to be outsourced to criminals, and have the virtue of being cheap and easy. Along with anti-war graffiti and petty vandalism, for example, criminals can be used to spread fear and dismay, as in the aforementioned Greek bomb hoaxes. In and of themselves, these incidents are largely trivial. However, when combined they magnify existing tensions and weaknesses evident in Western political systems and generally contribute to a climate of uncertainty that can be exploited by other disinformation and campaigns to corrode the legitimacy of Western political systems and, above all, the consensus for strong and sustained support for Ukraine in its war against Russia.

Arson, assassination and intimidation

Around midday on 23 August 2019, Zelimkhan Sultanovich Khangoshvili, an ethnic Chechen of Georgian origin who had fought against the Russians in both the Second Chechen War and the 2008 Russo-Georgian War, before becoming an organizer supporting Chechen independence, had left prayers and was walking through Berlin's Kleiner Tiergarten park. A man approached him and shot him three times with a suppressed Glock 26 pistol, killing him instantly. The assassin, who went by the name 'Vadim Sokolov', turned out to be Vadim Krasikov, a convicted Russian contract killer who had been engaged by the FSB, according first to investigations by the Bellingcat citizen journalism organization, then by the German authorities, and after he was released in a prisoner swap, by the Russians themselves.¹⁴⁶ The degree to which Krasikov's release seems to have been a deal-breaker for Moscow in the August 2024 exchange was already a sign that he was being considered as an agent rather than a convicted gangster.¹⁴⁷



A portrait of Chechen war veteran Zelimkhan Khangoshvili, who was reportedly murdered by a contract killer engaged by Russia's Federal Security Service. © Sean Gallup/Getty Images

This was not the first time Moscow had used gangsters rather than professional intelligence officers to carry out assassinations. In particular, organized crime proxies appear to have been used for killings in Istanbul and Vienna for over a decade.¹⁴⁸ For instance, the men alleged by Turkish police to be behind the murders of three suspected Chechen terrorists in Istanbul were members of a Moscow-based gang that had until then specialized in car theft (and, indeed, showed no appetite for foreign assassination later, suggesting that this was a one-off commission).¹⁴⁹ The prosecutor in the criminal case alleged that these men had also been engaged by Russian intelligence organizations.¹⁵⁰ Likewise, organized crime gangs had been used by the GU to provide additional muscle, and a degree of deniability, in some of their operations, including the seizure of Crimea in 2014 and the alleged failed coup in Montenegro in 2016.¹⁵¹ The latter, intended to forestall the country joining NATO, appears to have been coordinated by Viktor Boyarkin, a GU officer working with Unit 29155, its sabotage and assassination team, but also with Serbian organized crime groups.¹⁵²

Of course, one analytical challenge is that every fire, accident or accidental death can be spun as a potential Russian attack, especially as actually confirming foul play, let alone attributing it to Russia, can be difficult, time-consuming and inconclusive. A series of railway derailments in Sweden, for example, have been ascribed to Russian mischief in some quarters, even though at present, the authorities are unsure whether this is the case, with the Swedish Säpo security service simply stating: 'It cannot be ruled out that a foreign power is involved.'¹⁵³ However, it is hard to deny that, since mid-2023, there has been growing evidence of criminals – among other proxies, including 'patriotic' Russian dual-nationals living abroad – becoming involved in crimes that appear to be of political or strategic significance. This only escalated in the first half of 2024, with a number of incidents suspected to have been instigated by Moscow (see the box below).

Alleged sabotage plots in Europe, January–June 2024

January, Poland: A Ukrainian man, reportedly recruited by the Russian intelligence community, is arrested for planning an arson attack against unnamed facilities located ‘close to elements of strategically important infrastructure’ in Wrocław.¹⁵⁴

March, Lithuania: Leonid Volkov, former chief of staff to Russian opposition leader Alexei Navalny, is hospitalized after being attacked with a hammer in Vilnius.¹⁵⁵ Two Polish ‘radical hooligans’ are subsequently charged with the attack, which Polish Prime Minister Donald Tusk claimed was arranged through a Belarusian presumed to be working on Moscow’s orders,¹⁵⁶ although Volkov’s team later accused Leonid Nevzlin, an ally of rival opposition leader Mikhail Khodorkovsky of being behind it, something both men deny.¹⁵⁷

March, UK: An arson attack on two warehouses takes place in Leyton, east London, linked to a Ukrainian businessman involved in organizing aid for Ukraine. The following month, a British man is charged with orchestrating the attack, after allegedly being recruited by Russian intelligence.¹⁵⁸

April, Germany: Two German-Russian nationals are arrested in Bayreuth, southern Germany, on suspicion of plotting sabotage attacks, including on US military facilities, while working for a foreign secret service, presumed to be Russian.¹⁵⁹

May, Poland: Nine people of various nationalities (Poles, Ukrainians, a Belarusian) are arrested and charged with carrying out ‘beatings, arson and attempted arson’ in Poland, as well as in Lithuania, Latvia and possibly Sweden. Tusk claimed they were behind the attempted arson in Wrocław, as well as a fire in Poland’s largest shopping centre, Marywilka 44, and one at an Ikea in Vilnius, although questions have been raised about some of these claims.¹⁶⁰ Tusk said it was ‘likely’ that Russia was involved, but noted that the investigation was ongoing.

May, Germany: A fire at the Diehl metal factory in Berlin is officially ascribed to technical problems, but security services claim it was the result of sabotage.¹⁶¹

June, France: A 26-year-old Ukrainian with known pro-Russian views is taken to hospital, and later arrested, after the homemade bomb he was making in a hotel room near Paris Charles de Gaulle Airport exploded. On investigation, he turned out to have been intending to launch a series of sabotage attacks, starting with a bomb attack on an outlet of the home improvement chain Bricorama, that unnamed French intelligence sources suggested was on Moscow’s instructions, possibly to inflame the situation before parliamentary elections.¹⁶²



The scene in Vilnius where Leonid Volkov, a close political ally of opposition leader Alexei Navalny, was the victim of an attack arranged, some suggest, on Moscow’s orders. © Petras Malukas/AFP via Getty Images




а!

ЗАКВОБЕ

DARK FUTURES

'For Putin!' A rally in support of the president is held outside the US Embassy in Moscow, March 2023, protesting against the ICC's arrest warrant for Putin. © Getty Images



I honestly can't see things [with Russia] getting better – not for years. Actually, my most optimistic hope is that things don't get much worse. I could see things getting much, much more dangerous in Russia, and so for us all, whether Putin stays the course or gets swept away.

– RETIRED SENIOR NORWEGIAN INTELLIGENCE OFFICER, 2024¹⁶³

It is difficult to see Russia's current trajectory and the interaction between the Kremlin and criminals changing. It is more likely that the kinds of interactions currently happening between representatives of upperworld and underworld power will persist, driven by an asymmetrical balance of power:

The former do not care about or trust the latter; the latter will do the minimum necessary to placate the former, while seeing how they can turn the situation to their advantage. However, so long as criminals depend on the tolerance of the state, and so long as the state is desperate to maximise its capacity to conduct active measures, the conversations will presumably continue.¹⁶⁴

Even when the shooting war in Ukraine ends – which may well be not for years – then Putin will continue to regard himself as at political war with the West. Almost as important is that, as the security services and organized crime become ever closer, it will be another hard struggle to try and pry them apart: the criminals appreciate the security and opportunities provided by their new alliances, and the security officers consider the gangsters not just useful instruments but also partners in enrichment. After a time in which corruption at all but the highest levels seemed to be being contained, it is once again on the rise. This will have serious implications not just for Russia's neighbours and antagonists, but for the country itself, and what follows should not be considered specific predictions so much as potential scenarios for that potentially dark future.

'Proxy proxies'

The main job of HUMINT agencies is to recruit foreigners as agents, sometimes without even letting them know they are working for Moscow, whether Russian *avtoritety*, South Caucasus *vory*, or members of some other gangs now so strongly connected to its underworld that they can be considered part of Russian-based organized crime. For example,

a Ukrainian-led gang largely made up of Belarusians who were trafficking cocaine from the Dominican Republic to Russia via Belarus was broken up in 2019.¹⁶⁵ While they originally planned to service the domestic market in Belarus, they became dependent on the Russian market, and thus also on powerful wholesale underworld buyers there, bringing them into the orbit of Russian-based organized crime.

To date, the Russian intelligence community has largely concentrated on Russian-based organized crime when looking for proxies, except for the simplest and least mission-critical tasks, whether because of the existing connections in play or an assumption that they are more likely to be 'patriotic'. However, the way many Russian-based organized crime structures have established themselves as wholesaler providers, brokers and service providers to other domestic gangs across Europe and beyond means that they could also be used to widen the network of criminals potentially available to Moscow in its political warfare campaign. Bulgarians, for example – with certain historical and cultural ties to Russia – have begun to emerge as agents, recruits and proxies of choice, sometimes directly as intelligence assets (such as the six charged with membership of a suspected Russian spy ring operating in the UK¹⁶⁶).

However, the real nightmare for one Dutch intelligence analyst is 'Russian proxies who are not Russians – and don't even know they are working for Russia'.¹⁶⁷ The easy use of internet communications and payments has created an era of 'gig geopolitics' and 'pay-as-you-go sabotage', in which not just professional criminals but any down-on-their-luck individuals can be recruited for simple tasks and paid in cryptocurrency or through finance apps. They may well have no idea they are working for Moscow, and in some cases quite complex operations can be run through a series of basic acts. This already seems to sometimes have happened in the online realm, where anonymity or false identities are that much easier to maintain, and in any case often the 'recruits' live abroad. For example, Karim Baratov, is a Canadian of Kazakh extraction but was still willing to be recruited by the FSB for an operation against Yahoo.¹⁶⁸

However, the next step is engaging people without their being any the wiser – or deliberately encouraging them to believe they are working for someone other than the Russians. Indeed, one Ukrainian SBU (security service) officer claimed that some Ukrainian criminals have been approached by members of the Russian intelligence community claiming to be from the SBU.¹⁶⁹

Going transatlantic

As of writing, there seems to be a sharp differential in Russia's rules of engagement towards Europe and the US. America, the so-called 'Main Enemy', is not so much considered a harder operational target but rather a challenging political one. The nature of Putin's essentially 19th century geopolitics, wherein the world is divided into a handful of 'great powers' (including Russia) and vassal states, means that he is much more cautious about a direct challenge or provocation of the US.¹⁷⁰ As one Russian intelligence community veteran put it, 'As far as [Putin] is concerned, why should he care what Norway thinks, or Greece? France, Germany and Britain, to a degree, yes, but America? Absolutely.'¹⁷¹ Thus, while the US has been the target of cyber-attacks and disinformation and political subversion operations, it has avoided the more serious and direct incidents that appear to be now a recurring problem in Europe.

Russian-based organized crime in the United States

What has generally been described as 'Eurasian organized crime' by the US government has emerged in waves.¹⁷² First came criminal elements within the Jewish emigration of the 1970s from the USSR, which largely preyed upon their own, within such enclaves as New York's Brighton Beach. Then, with the collapse of the USSR, a wave of Russian emigrants saw the number of Russian-speakers in the US grow from under a quarter of a million in 1990 to over 700 000 in 2000. While most were wholly law-abiding, among them were criminals, including such powerful *vory v zakone* as Vyacheslav 'Yaponchik' Ivankov.

Ivankov tried to bring Russian and post-Soviet organized crime groups, which were and still are especially involved in large-scale frauds, into the orbit of the gangs back home.¹⁷³ This was largely a doomed venture, and while some links remain, including transactional business ties and familial ones, in the main such groups could not meaningfully be described as Russian-based organized crime, as they have cut themselves off from the Motherland and do not depend on connections back to Russia. (Indeed, given the prominence of Armenian gangsters within US 'Eurasian organized crime', one FBI analyst said that 'there was more of an Armenian-based organized crime problem' in the US than a Russian one.¹⁷⁴)



Russia's 'godfather' in the US, Vyacheslav 'Yaponchik' Ivankov, died in 2009. © Konstantin Zavrazhin/Getty Images

Nonetheless, this does not mean that Moscow could not step up its operations against the US, using criminals as proxies, should it want to do so. There are Russian-based organized crime networks active there, especially those heavily involved in large-scale frauds (which would lend themselves to extortion for *chornaya kassa* funds), although in practice their ties with the Motherland are becoming increasingly attenuated. It is likely that they would resist being used for Moscow's ends, and it would take positive inducements rather than pressure to recruit them.

Rather more plausible is that street gangs and similar criminals with less to lose could be used as knowing or unknowing proxies. Russian gangs do, for example, have significant connections with their counterparts in Latin America, which could potentially be leveraged to broker deals with street gangs inside America. After all, Russian gangs already swap Afghan heroin and domestic methamphetamines with Latin American



The Russian embassy, Washington DC. Putin regards himself as at political war with the West. © Shawn Thew/AFP via Getty Images

drug cartels for cocaine, and there is also a growing flow of Russians seeking to make an illegal entry into the US through Mexico, leading to further links to Russian-based organized crime.¹⁷⁵ Meanwhile, there is still a strong Russian intelligence presence in Central and South America,¹⁷⁶ especially in Mexico.¹⁷⁷

However, there is no doubt that this would be a politically high-risk strategy for Moscow and would probably only be adopted if the Kremlin either felt that the US leadership was so fragmented or distracted that it could or would not respond seriously or, more likely, if Putin felt desperate, in a corner with little to lose.

‘Donbasization’

Until their annexation by Moscow in 2022, the Donetsk and Lugansk People’s Republics (DNR and LNR, respectively) were essentially criminalized pseudo-states, controlled by Moscow but run by a motley array of gangsters, opportunists and warlords. Without international recognition, and engaged in a steady low-level conflict with Ukraine, they only survived through covert subsidies from Moscow and large-scale criminal operations such as coal smuggling.¹⁷⁸ The result was a top-to-bottom criminalization of these regions, in which the police were often little more than just another militia, and violent and organized crime proliferated (and spread to neighbouring regions of Russia).

Putin has repeatedly (and essentially empty) promised that the lives of the inhabitants of the former LNR and DNR would be brought up to the levels enjoyed in Russia. In practice, the demands of the present war and the lasting damage done to the economy



Pro-Ukrainian flags mark the entrance to the Russian-annexed Donetsk People's Republic. © Konstantin Zavrazhin/SOPA Images/LightRocket via Getty Images

and the state's legitimacy, as well as the return home of battle-scarred and disillusioned veterans, may instead lead to the 'Donbasization' of the Russian Federation. A return to the 'wild 90s' remains unlikely but is by no means either impossible or implausible. Levels of organized, violent and armed crime are all rising; the police are under-strength; and the risk of local alliances forming between organized crime and corrupt authorities on both a local and national level are increased by the state's desire to use the criminals for its own ends. As a retired Russian police officer acknowledged, 'These connections go both ways; the spooks may think they are using the criminals, but they themselves get corrupted in the process – or even more corrupted, to be accurate.'¹⁷⁹

'Mafia state'

The corollary of the above is in effect state capture by organized crime, as the political and security structures become comprehensively penetrated or suborned to criminal networks. Russia is often described even now as a mafia state, but this is misleading: it is undoubtedly ruled by a kleptocratic elite, but there is a distinction between

corruption and 'mafias', and more to the point, this formulation mistakenly implies that the Kremlin runs the underworld or vice versa. The real situation is much more complex and nuanced: there are undoubtedly connections between state structures and organized crime groups, but the relationship in the main is still one of 'understandings' – *ponyatiya* in Russian – and transactional deals between the two. The state is able to set the broad parameters of the relationship and the limits of 'acceptable criminality', beyond which it will crack down with performative severity, but it lacks the will and the resources to do more.

However, a continued and accelerated deterioration in the cohesion, authority and capacities of the state, combined with growing connections between its institutions and leaders and the underworld, could lead to a much greater level of state capture, whether on the local or national level. This could happen peaceably and under the radar, as essentially took place in much of the USSR in the 1970s. Hollowed out by comprehensive corruption, much of the country became to a degree dominated by local cabals of officials, including the KGB and police as well as Communist Party officials, who were able to co-opt organized crime and black marketeers.¹⁸⁰ This variety of state capture subverts and weakens central authority, and brings the risk of a nationalist and statist backlash, but a greater concern would be the criminal co-optation of the commanding heights of the state apparatus – possibly while the country is still committed to its campaign against Ukraine and the West.

'Nationalization'

The converse of the previous scenario is arguably more likely: that the Russian state, appreciating the value of organized crime as an instrument abroad, desperate for income and reconciled with the fact that, at least as far as the West is concerned, it is a pariah state, doubles down on this strategy. It is certainly turning to Iran for guidance on sanctions-busting and similar operations,¹⁸¹ and the degree to which the Iranian Revolutionary Guards Corps (IRGC) has moved into large-scale smuggling activities both to raise funds for its activities and to disrupt hostile states cannot have gone unnoticed.¹⁸²

However, an even more pertinent and dangerous example may come from North Korea. Moscow is strengthening its strategic relationship with Pyongyang on a variety of fronts, and the evidence suggests North Korea has sent extensive arms shipments to Russia.¹⁸³ Russia could also look to Bureau 39 of the Secretariat of the Korean Workers' Party as an example, in effect North Korea's 'ministry of organized crime'. It operates globe-spanning criminal enterprises, from amphetamine trafficking to insurance fraud, to bypass sanctions, support North Korea's faltering economy, and procure in-demand commodities for the ruling Kim family and their allies and cronies.¹⁸⁴ It (and the associated Bureau 38, which operates even more directly for the personal gain and security of the Kims), uses everything from diplomats to hackers in its work.¹⁸⁵

The intelligence community in general, and the FSB in particular, has taken the lead in using Russian-based organized crime as a tool. At the same time, the Russian state is still the 'biggest gang in town', able to arrest senior criminal figures and break up gangs without serious challenge or the need to make a convincing case in the courts. Given

these factors, it is possible that the Kremlin will seek to impose tighter control over those aspects of the underworld it finds useful. This could follow the Iranian model, in which the IRGC runs some operations itself but also works closely with criminal networks who understand that they are very much the junior partners, but could just as easily see some Russian counterpart to Bureau 39 established to bring this under more formal footing. The FSB, after all, established much of its early cyber operations elements, notably within its TsIB (Information Security Centre) by directly recruiting – dragooning, in some cases – criminal hackers. This programme had a distinctly rocky start, as too often the hackers simply continued their old activities, albeit now with the privileged access offered by their new stats, leading to, for example, the arrest and subsequent conviction in 2019 of Colonel Sergei Mikhailov, head of TsIB’s 2nd Directorate.¹⁸⁶ However, an official from the UK’s GCHQ noted in 2023 that ‘they seem to have got a lot better at controlling or socializing their hackers; [the FSB] still recruits from the wider hacker world from time to time, although they are also training up their own people now, but there’s much greater discipline than there was at first’.¹⁸⁷


It would be more complex to move beyond that to the wider criminal realm, but by no means impossible. Of course this would not mean a true ‘nationalization’, not least as so many Russian-based organized crime networks also depend heavily on assets, partners and groups outside Russia. Instead, it would largely take the form of a further renegotiation of the social contract between the Kremlin and the underworld, and a selective takeover of physical assets (such as methamphetamine labs or factories producing counterfeit goods) and tighter control of smuggling routes and money laundering facilities. Quite how successful this would be is open to question – in North Korea’s case, it was the state itself that set up many of these criminal enterprises rather than having to force them into its control – but even a partial ‘nationalization’ would give the Kremlin substantially greater options abroad, as well as representing a further degradation of Putin’s regime. As a NATO intelligence official put it:

It’s one thing to traffic and produce counterfeit pharmaceuticals or illegal drugs, that’s evergreen, but access to a national industrial base like Belarus and Russia means exponential changes in scale and we are already seeing major increases in production, as well as money that normally goes to the gangs used to fund Russian intelligence operations. And every indication is that this will get much worse.¹⁸⁸



BEYOND ADMIRING THE PROBLEM: RECOMMENDATIONS

Riot police are deployed in Moscow's Red Square during an anti-Ukraine invasion protest.
© Kirill Kudryavtsev/AFP via Getty Images



If we don't get a handle on how Moscow is weaponizing serious and organized crime, then it's not just that this will be a constant threat for as long as we're at loggerheads, we can also expect other antagonists to take note. It's bad enough facing the obvious Chinese threat of strategic corruption and technological penetration, for example: just think if they picked up Putin's playbook.

– SENIOR UK POLICE OFFICER, 2024¹⁸⁹

The use of Russian-based organized crime and other criminal elements as instruments of Russia's political war poses complex social and ethnical challenges, as well as practical ones. Most Russian emigrés and travellers are law-abiding, and many are horrified by their own government's conduct in Ukraine and would have nothing to do with subversion and sabotage abroad. To rely on blanket bans, intrusive surveillance and curtailment of human rights would not only be immoral but also a vindication of the Kremlin's toxic propaganda line to the effect that the current conflict is a result of Western 'Russophobia'. On the other hand, there is an undeclared and largely bloodless war taking place outside Ukraine, as Putin seeks to punish the West for its support for Kyiv and deter it from continuing and expanding this assistance.

To a degree, this hostile campaign can be addressed simply through the everyday activities of law enforcement. Western agencies are, after all, engaged in a constant struggle against the underworld, which includes those Russian-based organized crime networks most directly available to the Kremlin. However, this is not enough: the malign instrumentalization of organized crime by the Russian government for its political ends demands a more serious and focused response.

Naming and knowing the beast

In part, this is a challenge of recognizing and understanding the threat posed by the Russian intelligence community's exploitation of organized crime for its own purposes, and feeding that understanding into policy and practice. The following approaches should be considered.

- **Public recognition:** It is important to recognize that the state-criminal threat from Russia is not just a policing challenge but also a direct security concern. Understanding this will help unlock public policy discussion, but also inform police

priorities and tasking. Ironically, Russian-based organized crime is rarely considered to be a security threat as such, considering that it generally does not operate directly at street level but instead facilitates the gangs whose activities have the most direct impact on society. As a result, the temptation is for overworked and under-resourced police services to focus on crimes that have an immediate social impact (which is typically what the public and politicians are demanding), and leave the rather tougher target of Russian-based organized crime for another day. In the words of a British National Crime Agency officer, 'Going after a Russian network is often going to take up massive resources, especially forensic analysts, who are always totally overburdened, with no promises of any success, especially as Moscow's not even pretending to cooperate any more.'¹⁹⁰

- **Bridging the police-intelligence gap:** A logical consequence of the above is for governments to ensure better cooperation between law enforcement agencies and the intelligence community. Of course, they have different ways of working and primary responsibilities but despite some laudable information-sharing initiatives (especially where agencies such as the FBI straddle the divide between counter-intelligence and law-enforcement), it is generally accepted that this remains a problem. One FBI officer recounted the problems they had cooperating with a European police agency, 'not because they didn't share our objective of closing down a Russian smuggling ring, but ... because what we were looking at as essentially an [intelligence] operation, they considered just a criminal one, and a pretty minor one, at that'.¹⁹¹
- **Expanding the knowledge base:** Russian-based organized crime has its own particularities, personalia and ways of operating, with a particular emphasis placed on extensive and up-to-date expertise. To take one example, the criminal slang term *obshchak* originally meant a gang's common funds, used to support the dependents of members who were killed or imprisoned. In modern usage, it tends instead to mean the gang's operating funds, which can be used to provide start-up funding for new ventures and the like. Even now, though, some police agencies still presume that the earlier definition applies, meaning that they mistake the implications when an *obshchak* suddenly shrinks.¹⁹² Addressing errors such as this demands greater engagement with the outside expert community, but also the maintenance of adequate in-house expertise, and not letting law-enforcement capabilities simply to be cannibalized by the security services, as too often happens.

Security beyond tanks

Properly addressing the threat of Russian-based organized crime cannot be done simply by public statements and the reallocation of existing resources, as the author warned (largely in vain) back in 2017:

Specialised police intelligence units, proper visa screening, more financial intelligence analysis, tougher due diligence, and a less tolerant attitude towards shell companies, all have a direct cost on the public purse or an indirect one through adding costs to companies or forcing them to turn away business. This is, however, part of the cost not just of business, but of war.¹⁹³

To this end, it will have to be appreciated, especially in Europe, that countering the combined Russian intelligence-crime threat is in its own way every bit as important as addressing any potential military threat. Despite the increasingly urgent, and frankly questionable, claims about the imminence of a Russian military attack on NATO,¹⁹⁴ the political war threat is real and current. To this end, Western countries need, even in the current times of financial stringency, to be willing to spend on this threat as well as the military one.

- **More resources for policing Russian-based organized crime:** No police agency will ever say it has enough money and personnel, but there is a need for ring-fenced spending to address the particular threat of Russian-based organized crime. This is not simply for experts and operational resources, but also political capital. Operations against larger and more significant networks are often difficult and time-consuming, with unpredictable outcomes given that these networks can often afford the best lawyers and lobbyists. As a result, there is an inevitable temptation on the part of agencies and prosecutors, hard pressed by their political masters to deliver quick results and maintain high success rates, to stick to easier cases. They need to be granted the latitude to fail to catch the big fish, if the more dangerous Russian-based organized crime operations are to be tackled.
- **Increased spending on counter-intelligence:** There remains a huge disparity in the level of resources committed to allowing security and counter-intelligence services to combat the Russian intelligence community and their criminal allies.¹⁹⁵ At a time when there is a consensus that NATO members ought to be devoting at least 2 per cent of their GDP to defence (even if not all do), there is no similar common sense of an appropriate spend on national intelligence communities. As a result, the spending is often orders of magnitude different, with some countries moving to increase the appropriate budgets in line with the threat. In May 2024, Polish Prime Minister Donald Tusk announced an additional 100 million zloty (€23.4 million) for the Internal Security Agency and Foreign Intelligence Agency – almost a 9 per cent increase on their existing budgets¹⁹⁶ – while others are still lagging. Within alliances, though, whether NATO or the EU, weak links become problems for everyone, making this more than just a national issue.

Making friends

Demonizing the Russian diaspora is not just a boon for Putin's propagandists: it also denies Western law enforcement and security agencies opportunities to gather information and avert the recruitment of new criminal assets.

- **Developing positive relationships with the Russian diaspora:** The overwhelming majority are not gangsters (if anything, they, like so many diasporas, are actually disproportionately victimized by their criminal co-nationals) and most do not support Putin or the war: a large number of recent arrivals, after all, consider themselves not emigrés but temporary 'relocants' awaiting the chance to return.¹⁹⁷ A survey of emigrants to Germany, France, Cyprus and Poland, for example, found 71 per cent to be 'somewhat' or 'definitely' disapproving of current Russian policy.¹⁹⁸ Building closer and more positive relationships with them will, as with all diaspora crime, generate crucial sources of information. At the very least, efforts must be made

to ensure that diaspora communities are not driven into the arms of criminals or the Russian intelligence community by clumsy stereotyping and heavy-handed policing.¹⁹⁹

- **Recruit from Russian minorities:** Especially in countries with a large ethnic Russian community, or where they have been present for generations, there is arguably a case to be made for specific efforts to recruit police, analysts and intelligence officers from their number. In many cases, efforts were made during the 1990s but were then allowed to fade, especially after jihadist terrorism became the priority. Such a programme may require greater screening to weed out potential double-agents or security risks, but would bring with it officers better able to circulate – overtly or covertly – within Russian diasporic communities, a better awareness of the cultural complexities in play and a clear demonstration that Putin’s claims about Western Russophobia are unfounded. It was, after all, with the recruitment of Joseph Petrosino to the New York Police Department and later the ‘Italian Squad’ that allowed for much more effective policing of the Italian immigrant Black Hand and Cosa Nostra mafias in the early 20th century.

Punishment to fit (or deter) the crime

Greater scrutiny from law enforcement and security agencies alike would inevitably act as a deterrent to those Russian-based organized crime networks contemplating cooperation with the Kremlin. Indeed, it could help push some of their local ‘branches’ to emancipate themselves from their parent organizations, as seems to be happening in Spain, for instance. However, there are also specific measures that could be adopted to sharpen the Western response.

- **Disruption:** While the natural goal of police agencies is a successful prosecution, internal security agencies often must content themselves with disruption, whether of terrorist plots or foreign intelligence operations. To this end, they may well deploy a range of covert tactics of state-sanctioned malice and deception not typically used against organized crime. However, if Russian-based organized crime – especially those elements believed already or potentially to be cooperating with the Russian intelligence community – is accepted to be a security threat rather than just a crime problem, then measures intended to undermine handlers’ trust in the criminals and vice versa, and other aspects of their activities would appear to be entirely appropriate.
- **Virtual counterattacks:** Fighting fire with fire is largely impossible and inappropriate. Unlike Putin’s regime, Western nations are bound by national and international law. Furthermore, there are inevitable risks, from triggering Russian escalation to alienating portions of domestic public opinion. Although there are hints that the UK has already launched retaliatory cyberattacks against ransomware gangs,²⁰⁰ it would be possible to take a much more robust approach to striking back against officially non-state online groups, whether by doxing their members (publicizing their identities and personal information) or attacking their systems. Proxies at home or abroad do not, after all, have the same protected status as government agencies.

- **Go after the money:** Money is not just at the heart of why gangsters turn to crime, but also why the Russian intelligence community turns to Russian-based organized crime, and how it motivates organized crime to act on behalf of the state. Targeting the illegal financial flows relating to Russian-based organized criminal activity will thus be crucial both to prevent the Kremlin from exploiting these criminals and to deter criminals from such operations – while also denying the Russian intelligence community of the *chornaya kassa* funds needed for their own activities. To this end, a much more aggressive campaign ought to be launched, akin to the measures taken to seize or freeze terrorism funds after the 9/11 attacks. Countries failing to play their role in this (which at present would include Cyprus, Israel, Luxembourg, Lichtenstein and Latvia, according to a number of sources²⁰¹), must face greater pressure to address the problem.
- **'Prophylactic chats':** The Russian security apparatus learned from its KGB predecessor the art of the 'prophylactic chat', intended to intimidate potential dissidents.²⁰² Especially since Putin's accession to the presidency, the technique has been used to considerable effect in modifying organized crime behaviour, from deterring Chechen gangs from supporting their people in the Second Chechen War to limiting crime against foreigners during the 2014 Sochi Winter Olympics and 2018 FIFA World Cup.²⁰³ There is scope for similar tactics to be used against Russian-based organized crime, especially as it is something with which criminals are already familiar: not intimidation, but a polite and indirect warning that they are on the authorities' radar and ought to think twice before committing acts that could trigger serious police activity.

NOTES

- 1 Presidential Address to Federal Assembly, 21 February 2023, <http://en.kremlin.ru/events/president/news/70565>.
- 2 Russian spies have gone full mafia mode because of Ukraine, *Vice*, 27 October 2022, <https://www.vice.com/en/article/k7bx4v/russia-traffickers-spies>.
- 3 »Die Kartelle suchen sich eine kleine Stadt, bieten neue Drogen an, es ist wie Marktforschung«, *Der Spiegel*, 20 July 2024, <https://www.spiegel.de/panorama/justiz/europol-chefin-catherine-de-bolle-ob-jemand-stirbt-ist-egal-es-wird-ein-anderer-folgen-a-d0977dd3-0c2c-441c-9ccc-5fd815797249>.
- 4 Russia recruiting far-right extremists to launch attacks in the West, *The Telegraph*, 11 May 2024, <https://www.telegraph.co.uk/news/2024/05/11/russia-recruiting-far-right-extremists-attacks-west-putin/>.
- 5 Although, as of writing, the most severe penalty has been a nonetheless disproportionate seven years. See Russia: Municipal councillor sentenced to seven years in jail for opposing the Ukraine war, Amnesty International, 8 July 2022, <https://www.amnesty.org/en/latest/news/2022/07/russia-municipal-councillor-sentenced-to-seven-years-in-jail-for-opposing-the-ukraine-war/>.
- 6 Vladimir Putin accuses Hillary Clinton of encouraging Russian protests, *The Guardian*, 8 December 2011, <https://www.theguardian.com/world/2011/dec/08/vladimir-putin-hillary-clinton-russia>.
- 7 Conversation with former Kremlin official, Moscow, January 2014.
- 8 Mark Galeotti, Active measures: Russia's covert geopolitical operations, Marshall Center for Security Studies Security Insights No. 31, June 2019, <https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0>.
- 9 See, for example, Pavel Sudoplatov, *Special Tasks*, Little, Brown & co., 1994.
- 10 Conversation with a US intelligence officer, Washington DC, January 2023.
- 11 George Kennan, The inauguration of organized political warfare, 4 May 1948, State Department Office of History, <https://history.state.gov/historicaldocuments/frus1945-50Intel/d269>.
- 12 Valery Gerasimov, Ценность науки в предвидении, *Voenno-Promyshlennyyi Kur'er*, 27 February 2013, https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html.
- 13 Kremlin, in change of language, says Russia is 'at war' due to West's role in Ukraine, Reuters, 22 March 2024, <https://www.reuters.com/world/europe/kremlin-says-russia-is-war-due-western-intervention-ukrainian-side-2024-03-22>.
- 14 For a detailed analysis of these agencies and their aims and activities, see Mark Galeotti, Putin's hydra: inside Russia's intelligence services, European Council on Foreign Relations (ECFR) policy brief, 11 May 2016. [http://www.ecfr.eu/page/-/ECFR_169_-_INSIDE_RUSSIAS_INTELLIGENCE_SERVICES_\(WEB_AND_PRINT\)_2.pdf](http://www.ecfr.eu/page/-/ECFR_169_-_INSIDE_RUSSIAS_INTELLIGENCE_SERVICES_(WEB_AND_PRINT)_2.pdf).
- 15 Conversation with a British security officer, London, April 2022.
- 16 Yeltsin: Russia a 'superpower of crime', Associated Press, 7 June 1994.
- 17 Mark Galeotti, Crimintern: How the Kremlin uses Russia's criminal networks in Europe, ECFR policy brief, 18 April 2017, https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.
- 18 See Federico Varese, *Mafias on the Move: How Organized Crime Conquers New Territories* (Princeton University Press, 2011), chapter 4.
- 19 US Department of Justice, Leader of Georgian crime syndicate and associates charged with extortion offenses, 14 November 2023, <https://www.justice.gov/usao-sdny/pr/leader-georgian-crime-syndicate-and-associates-charged-extortion-offenses>.
- 20 US Department of Justice, Members and associates of Russian crime syndicate arrested for racketeering, extortion, robbery, murder-for-hire conspiracy, fraud, narcotics, and firearms offenses, 7 June 2017, <https://www.justice.gov/usao-sdny/pr/members-and-associates-russian-crime-syndicate-arrested-racketeering-extortion-robbery>.
- 21 Federico Varese, Jakub Lonský and Yuriy Podvysotskiy, The resilience of the Russian mafia: an empirical study, *British Journal of Criminology*, 61, 1 (2021).
- 22 Conversation with a Western counter-intelligence officer, London, 2015.
- 23 Vladimir Odintsov, The scope of activities of Georgian organized crime groups, *New Eastern Outlook*, 12 September 2013, <https://journal-neo.su/2013/09/12/rus-o-razmahe-deyatel-nosti-gruzinskih-opg>.

- 24 Conversation with an Italian finance police analyst, Rome, April 2018.
- 25 Russian mob will be at the heart of the EU, *The Guardian*, 10 December 2002, <https://www.theguardian.com/world/2002/dec/10/eu.russia>.
- 26 United Nations Office on Drugs and Crime, Afghan opiate trafficking along the northern route, June 2018, https://www.unodc.org/documents/publications/NR_Report_21.06.18_low.pdf.
- 27 This is explored more in the author's *The Vory: Russia's super mafia* (Yale, 2018).
- 28 Europol, Police dismantle Russian money laundering ring operating in the football sector, 4 May 2016, <https://www.europol.europa.eu/media-press/newsroom/news/police-dismantle-russian-money-laundering-ring-operating-in-football-sector>.
- 29 Email communication with former Italian police officer, 2015.
- 30 Mark Galeotti, Crimintern: How the Kremlin uses Russia's criminal networks in Europe, ECFR policy brief, 18 April 2017, https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.
- 31 Recounted to the author by a Russian police officer, Moscow, April 2019.
- 32 BIS, Annual Report of the Security Information Service of the Czech Republic for 2011, p 10, <https://www.bis.cz/vyrocni-zpravaENc2ed.html?ArticleID=26>.
- 33 Conversation with a BIS officer, Prague, 2016.
- 34 Mark Galeotti, Tough times for tough people: Crime and Russia's economic crisis, Radio Free Europe/Radio Liberty, June 2015, <http://henryjacksonsociety.org/wp-content/uploads/2015/06/Tough-Times-for-Tough-People.pdf>.
- 35 Jack Watling, Oleksandr V Danylyuk and Nick Reynolds, Preliminary lessons from Russia's unconventional operations during the Russo-Ukrainian war, February 2022–February 2023, Royal United Services Institute (RUSI), 2023, p 11, <https://static.rusi.org/202303-SR-Unconventional-Operations-Russo-Ukrainian-War-web-final.pdf>.
- 36 Нарышкин назвал «моральным трупом» угнавшего Ми-8 российского летчика, RBC, 20 February 2024, <https://www.rbc.ru/politics/20/02/2024/65d462b29a7947e18f6665e9>.
- 37 Russian links emerge in murder of helicopter pilot defector, *Kyiv Post*, 1 April 2024, <https://www.kyivpost.com/post/30410>.
- 38 Gunmen sent by Moscow killed defector sheltering in Alicante, Spanish intelligence services say, *El País*, 22 February 2024. <https://english.elpais.com/international/2024-02-22/gunmen-sent-by-moscow-killed-defector-sheltering-in-alicante-spanish-intelligence-services-say.html>.
- 39 Online conversation with a Spanish judicial police investigator, May 2024.
- 40 Mark Galeotti, Spain versus Russia's kleptocracy, ECFR, 4 May 2016, https://ecfr.eu/article/commentary_spain_versus_russias_kleptocracy_7017.
- 41 Lucía Bohórquez, *Taganskaya: Un empresario ruso entrega un hotel en Mallorca*, *El País*, 16 May 2016, https://elpais.com/politica/2016/05/16/actualidad/1463410627_385966.html; Major Russian mafia trial opens in Spain, BBC, 19 February 2018, <https://www.bbc.co.uk/news/world-europe-43112443>.
- 42 Sebastian Rotella, A gangster place in the Sun: How Spain's fight against the mob revealed Russian power networks, ProPublica, 10 November 2017, <https://www.propublica.org/article/fighting-russian-mafia-networks-in-spain>.
- 43 See, for example, Europol, Spain dismantles top Russian-speaking organised crime network that had infiltrated public institutions, 17 December 2020, <https://www.europol.europa.eu/media-press/newsroom/news/spain-dismantles-top-russian-speaking-organised-crime-network-had-infiltrated-public-institutions>.
- 44 President of Russia, Victory Parade on Red Square, 9 May 2023, <http://en.kremlin.ru/events/president/news/71104>.
- 45 Dan Sabbagh, Half of Russian spies in Europe expelled since Ukraine invasion, says MI6 chief, *The Guardian*, 21 July 2022, <https://www.theguardian.com/uk-news/2022/jul/21/half-of-russian-spies-in-europe-expelled-since-ukraine-invasion-says-mi6-chief>.
- 46 Karolina Jeznach, Thomas Grove and Bojan Pancevski, The misfits Russia is Recruiting to spy on the West, *The Wall Street Journal*, 15 May 2024, <https://www.wsj.com/world/europe/the-misfits-russia-is-recruiting-to-spy-on-the-west-7417b2b5>.
- 47 See Timothy Snyder, We should say it. Russia is fascist, *The New York Times*, 19 May 2022, <https://www.nytimes.com/2022/05/19/opinion/russia-fascism-ukraine-putin.html>; European Parliament, European Parliament resolution on the need for unwavering EU support for Ukraine, after two years of Russia's war of aggression against Ukraine (2024/2526(RSP)), 26 February 2024, https://www.europarl.europa.eu/doceo/document/B-9-2024-0157_EN.html.
- 48 For a wider analysis of this, see Mark Galeotti, Controlling chaos: How Russia manages its political war in Europe, ECFR policy brief, 1 September 2017, https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe.
- 49 Jack Watling, The Kaleidoscopic campaigning of Russia's Special Services, RUSI, 20 September 2022, <https://rusi.org/explore-our-research/publications/commentary/kaleidoscopic-campaigning-russias-special-services>.
- 50 Tim Maurer, Why the Russian government turns a blind eye to cybercriminals, *Slate* (accessed through the Carnegie Endowment), 2 February 2018, <https://carnegieendowment.org/posts/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals>.
- 51 Interviewed on *Ekho Moskvy*, quoted in Volodymyr Lysenko and Catherine Brooks, Russian information troops, disinformation and democracy, *First Monday*, 23, 5 (2018), <https://firstmonday.org/ojs/index.php/fm/article/view/8176/7201>.
- 52 See, for example, US Department of Justice, U.S. charges Russian FSB officers and their criminal conspirators for hacking yahoo and millions of email accounts, 15 March 2017, <https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions>.
- 53 «Натворил много зла». Буданов назвал «очень проблемного» для Украины российского генерала, *New Voice*, 12 October 2023, <https://nv.ua/world/countries/>

- sergey-beseda-problemnyy-dlya-ukrainy-rossiyskiy-general-budanov-50360007.html.
- 54 Mitchell Prothero, Russian spies have gone full mafia mode because of Ukraine, *Vice*, 27 October 2022, <https://www.vice.com/en/article/k7bx4v/russia-traffickers-spies>.
 - 55 Conversation with a British intelligence officer, London, October 2023.
 - 56 US Department of Justice, 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, 17 July 2024, <https://www.justice.gov/usao-sdny/pr/russian-international-money-launderer-sentenced-three-years-prison-illicitly-procuring>.
 - 57 Telephone conversation with an FBI officer, July 2024.
 - 58 Ростовская область вошла в рейтинг регионов с высокой экономической преступностью, *Gazeta-ru – Rostov*, 11 August 2022, <https://rostovgazeta.ru/news/2022-08-11/rostovskaya-oblast-voshla-v-reyting-regionov-s-vysokoy-ekonomicheskoy-prestupnostyu-1379873>.
 - 59 War in Ukraine: Sanctions busters—Germany’s exports to Russia, Hanse Analytics, 6 June 2023, <https://hanseanalytics.io/insights/blogs/germany-exports-to-russia>.
 - 60 Oliver Moody, Russia suspected of smuggling EU fridges to strip for weapon parts, *The Times*, 7 November 2022, <https://www.thetimes.co.uk/article/russia-suspected-of-buying-eu-fridges-to-strip-for-weapon-parts-p73sdtnhc>.
 - 61 James Byrne et al, *Silicon Lifeline: Western Electronics at the Heart of Russia’s War Machine*, RUSI, 2022.
 - 62 Russia-Ukraine war: How Putin’s oligarchs are supplied with luxury Western goods despite sanctions, *The i*, 26 May 2023, <https://inews.co.uk/news/russia-ukraine-war-putins-oligarchs-supplied-luxury-western-goods-despite-sanctions-2365727>
 - 63 Olena Bilousova et al, Challenges of export controls enforcement: How Russia continues to import components for its military production, Yermak-McFaul International Working Group on Russian Sanctions and the Kyiv School of Economics, 2024, p 4, <https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf>.
 - 64 Россия в обход санкций импортировала западных чипов на \$4 млрд через 6000 подставных компаний, *The Moscow Times*, 25 July 2024, <https://www.moscowtimes.ru/2024/07/25/s-nachala-voini-rossiya-v-obhod-sanktsii-importirovala-zapadnih-chipov-na-4-mlrd-cherez-6000-podstavnih-kompanii-a137776>.
 - 65 Aaron Arnold and Daniel Salisbury, The sanctions-busting architects: Moscow’s preparations for the West’s sanctions, *Lawfare*, 4 March 2024, <https://www.lawfaremedia.org/article/the-sanctions-busting-architects-moscow-s-preparations-for-the-west-s-sanctions>.
 - 66 In the words of one Europol analyst, ‘If you can smuggle microchips in, the FSB will probably turn a blind eye to your smuggling drugs, people or whatever out.’ Email conversation, January 2022.
 - 67 Howard Altman, Same type of Rotax engines used in Iranian drones targeted in bizarre theft wave, *The Drive*, 25 October 2022, <https://www.thedrive.com/the-war-zone/bizarre-theft-wave-targets-same-rotax-engines-used-in-iranian-drones>; Roadside cameras stolen in Sweden may end up in Russian drones – media, *The Press United*, 21 October 2022, <https://thepressunited.com/updates/roadside-cameras-stolen-in-sweden-may-end-up-in-russian-drones-media>.
 - 68 Telephone conversation with a Swedish intelligence analyst, June 2024.
 - 69 US Department of the Treasury, Treasury targets corruption and the Kremlin’s malign influence operations in Moldova, 26 October 2022, <https://home.treasury.gov/news/press-releases/jy1049>.
 - 70 David Lewis and Tena Prelec, New dynamics in illicit finance and Russian foreign policy, SOC ACE Research Paper No. 17 (2022), <https://www.socace-research.org.uk/s/SOCACE-RP17-NewDynamics-Aug23.pdf>.
 - 71 Russia hemorrhages at least US\$211.5 billion in illicit financial outflows from 1994-2011 – New GFI study, *Global Financial Integrity*, 13 February 2013, <https://gfiintegrity.org/press-release/russia-hemorrhages-least-us211-5-billion-illicit-financial-outflows-1994-2011-new-gfi-study>; Louis Ashworth, Why Cyprus is a ‘Russian bank with dirty money posing as an EU state’, *The Telegraph*, 2 March 2022, <https://www.telegraph.co.uk/business/2022/03/02/cyprus-russian-bank-dirty-money-posing-eu-state>.
 - 72 Menelaos Hadjicostis, Cyprus sees Russian bank deposits plunge as government seeks to clean up its financial image, AP, 24 January 2024, <https://apnews.com/article/cyprus-russia-sanctions-evasion-fd6ad076f6439d3be8c0252dcd7d7b8>.
 - 73 Abdelhak El Idrissi and Anne Michel, *A Chypre, argent sale et fortunes russes continuent de narguer l’Europe*, *Le Monde*, 14 November 2023, https://www.lemonde.fr/les-decodeurs/article/2023/11/14/a-chypre-argent-sale-et-fortunes-russes-continuent-de-narguer-l-europe_6200064_4355770.html.
 - 74 Nektaria Stamouli, In Cyprus, a faraway war forces a city to redefine its Russianness, *Politico*, 30 May 2022, <https://www.politico.eu/article/in-cyprus-a-faraway-war-forces-a-city-to-redefine-its-russianness>.
 - 75 Conversation with a British National Crime Agency analyst, London, June 2024.
 - 76 Tom Espiner, US widens Russia sanctions in banking crackdown, BBC, 13 June 2024, <https://www.bbc.co.uk/news/articles/ckvv1wydkwqo>.
 - 77 Mitchell Prothero, Russian spies have gone full mafia mode because of Ukraine, *Vice*, 27 October 2022, <https://www.vice.com/en/article/k7bx4v/russia-traffickers-spies>.
 - 78 Conversation with a German security service officer, Berlin, March 2024.
 - 79 Online conversation with a Europol analyst, January 2024.
 - 80 Eva Jovanova, A Russian crypto winter? Why banning crypto would be terrible news for Russia, University Consortium, 2022, <https://uc.web.ox.ac.uk/article/a-russian-crypto-winter-why-banning-crypto-would-be-terrible-news-for-russia>.
 - 81 President of Russia, Совещание по экономическим вопросам, 17 July 2024, <http://kremlin.ru/events/president/news/74566>.
 - 82 ВС впервые разрешил считать отмыванием конвертацию биткоинов в рубли, *Russian Legal*

- Information Agency, 28 June 2023, https://www.rapsinews.ru/judicial_analyst/20230628/309030466.html.
- 83 Bank of Russia, Криптовалюты: тренды, риски, меры, 2022, https://www.cbr.ru/content/document/file/132241/consultation_paper_20012022.pdf.
- 84 Financial Crimes Enforcement Network, FinCEN identifies virtual currency exchange Bitzlatto as a 'primary money laundering concern' in connection with Russian illicit finance, 18 January 2023, <https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlatto-primary-money-laundering>.
- 85 Europäische Politiker sollen Hunderttausende Euro aus Russland bekommen haben, *Der Spiegel*, 27 March 2024, <https://www.spiegel.de/politik/deutschland/verdaechtig-es-internetportal-voice-of-europe-westliche-geheimdienste-enttarnen-russische-desinformationskampagne-a-338f85ac-1714-4a05-b472-6e0ac3678675>.
- 86 Elena Fabrichnaya, Russia weighs risk of embracing crypto for international payments, Reuters, 17 July 2024, <https://www.reuters.com/markets/currencies/russia-weighs-risk-embracing-crypto-international-payments-2024-07-17>.
- 87 Transparency International, New investigation highlights major Russian dirty money risk at crypto payment providers, 31 October 2023, <https://www.transparency.org.uk/new-investigation-highlights-major-russian-dirty-money-risk-crypto-payment-providers>.
- 88 Matthew Field, Putin is plotting 'physical attacks' on the West, says GCHQ chief, *The Telegraph*, 14 May 2024, <https://www.telegraph.co.uk/business/2024/05/14/putin-plotting-physical-attacks-west-gchq-chief>.
- 89 US Department of Justice, Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace, 19 October 2020, <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>.
- 90 For a good summary of the various threat actors, see: US Cybersecurity and Infrastructure Security Agency (CISA), Russian state-sponsored and criminal cyber threats to critical infrastructure, 9 May 2022, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>.
- 91 Tom Parfitt, Russian hackers spent months inside Ukrainian telecoms giant, *The Times*, 4 January 2024, <https://www.thetimes.com/world/russia-ukraine-war/article/russian-hackers-spent-months-inside-ukrainian-telecoms-giant-cr0g83339>; US Department of Justice, Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace, 19 October 2020, <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>.
- 92 Andy Greenberg, The untold story of NotPetya, the most devastating cyberattack in history, *Wired*, 22 August 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world>.
- 93 Justin Sherman, Untangling the Russian web: Spies, proxies, and spectrums of Russian cyber behavior, Atlantic Council Issue Brief, 19 September 2022, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web>.
- 94 Justin Sherman, Untangling the Russian web: Spies, proxies, and spectrums of Russian cyber behavior, Atlantic Council Issue Brief, 19 September 2022, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web>.
- 95 Antoaneta Roussi, Estonia fends off 'extensive' cyberattack following Soviet monument removal, *Politico*, 18 August 2022, <https://www.politico.eu/article/estonia-extensive-cyber-attack-following-soviet-war-monument-removal>.
- 96 CISA, Russian state-sponsored and criminal cyber threats to critical infrastructure, 9 May 2022, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>.
- 97 Karen Nershi and Shelby Grossman, Assessing political motivations behind ransomware attacks, Stanford Cyber Policy Center, 13 July 2023, <https://cyber.fsi.stanford.edu/news/new-paper-assessing-political-motivations-behind-ransomware-attacks>.
- 98 Russia is trying to sabotage European railways, warns Prague, *Financial Times*, 4 April 2024, <https://www.ft.com/content/f8207823-f5e1-4caf-934d-67c648f807bf>.
- 99 ENISA warns of 'hacktivism' targeting healthcare and authorities, ICT & health, 2 July 2024, <https://ictandhealth.com/news/enisa-warns-of-hacktivism-targeting-health-care-and-authorities>.
- 100 Online conversation with a Europol analyst, January 2024.
- 101 Derek Gatopoulos, Europe's cybersecurity chief says disruptive attacks have doubled in 2024, sees Russia behind many, AP, 29 May 2024, <https://apnews.com/article/europe-election-cybersecurity-russia-ukraine-5b0cca725d17a028dd458df77a60440c>.
- 102 Bomb threats target dozens of Attica schools in suspected hoax, *Ekathimerini*, 29 May 2024, <https://www.ekathimerini.com/news/1239994/bomb-threats-target-dozens-of-attica-schools-in-suspected-hoax>.
- 103 Yiannis Souliotis, Hoax bomb threats sent to schools lead to US-based company, *Ekathimerini*, 6 June 2024, <https://www.ekathimerini.com/news/1240781/hoax-bomb-threats-to-greek-schools-lead-to-the-us-based-company>.
- 104 Online conversation with a Greek official, July 2024.
- 105 Andy Greenberg, A (strange) interview with the Russian-military-linked hackers targeting US water utilities, *Wired*, 8 May 2024, <https://www.wired.com/story/cyber-army-of-russia-interview>.
- 106 Ibid.
- 107 Dmitry Smilyanets, An interview with initial access broker Wazawaka: 'There is no such money anywhere as there is in ransomware', *The Record*, 26 August 2022, <https://therecord.media/an-interview-with-initial-access-broker-wazawaka-there-is-no-such-money-anywhere-as-there-is-in-ransomware>.
- 108 Dan Sabbagh, Russia and neighbours are source of most ransomware, says UK cyber chief, *The Guardian*, 11 October 2021, <https://www.theguardian.com/technology/2021/oct/11/russia-and-nearby-states-are-origin-of-most-ransomware-says-uk-cyber-chief>.
- 109 Ransomware payments exceed \$1 billion in 2023, hitting record high after 2022 decline, Chainalysis, 7 February 2024, <https://www.chainalysis.com/blog/ransomware-2024>.

- 110 Catherine Sbeglia Nin, Japanese port hit by Russian ransomware attack, RCR Wireless News, 5 July 2023, <https://www.rcrwireless.com/20230705/security/japanese-port-hit-by-russian-ransomware-attack>; Ben Knight and Harrison Tippet, Cyber attack on Victoria's court system may have exposed recordings of sensitive cases, ABC News, 1 January 2024, <https://www.abc.net.au/news/2024-01-02/victoria-court-system-targeted-in-cyber-attack-russian-hackers/103272118>; Zack Whittaker, UnitedHealth confirms ransomware gang behind Change Healthcare hack amid ongoing pharmacy outages, TechCrunch, 29 February 2024, <https://techcrunch.com/2024/02/29/unitedhealth-change-healthcare-ransomware-attack-blackcat-pharmacy-outages>; Britain's NHS reels from a ransomware attack, *The Economist*, 13 June 2024, <https://www.economist.com/britain/2024/06/13/britains-nhs-reels-from-a-ransomware-attack>.
- 111 Joe Tidy, 74% of ransomware revenue goes to Russia-linked hackers, BBC, 14 February 2022, <https://www.bbc.co.uk/news/technology-60378009>.
- 112 Polish Prosecutor's Office, *Prokuratura Krajowa przedstawiła zarzuty osobie podejrzanej o zgłoszenie gotowości do działania na rzecz wywiadu Federacji Rosyjskiej*, 18 April 2024, <https://www.gov.pl/web/prokuratura-krajowa/prokuratura-krajowa-przedstawiła-zarzuty-osobie-podejrzanej-o-zgłoszenie-gotowosci-do-działania-na-rzecz-wywiadu-federacji-rosyjskiej>.
- 113 The Lubyanka is the imposing building on Moscow's Dzerzhinsky Square that was formerly the headquarters of the KGB and is now occupied by the FSB.
- 114 Conversation with a German security officer, Berlin, March 2024.
- 115 Karolina Jeznach, Thomas Grove and Bojan Pancevski, The misfits Russia is recruiting to spy on the West, *The Wall Street Journal*, 15 May 2024, <https://www.wsj.com/world/europe/the-misfits-russia-is-recruiting-to-spy-on-the-west-7417b2b5>.
- 116 Spy who ensnared Kohver now in prison, *Postimees*, 14 September 2017, <https://news.postimees.ee/4243551/spy-who-ensnared-kohver-now-in-prison>.
- 117 Nick Paton Walsh, Sarah Dean and Karolina Jeznach, From \$7 graffiti to arson and a bomb plot: How Russia's 'shadow war' on NATO members has evolved, CNN, 10 July 2024, <https://edition.cnn.com/2024/07/10/europe/russia-shadow-war-nato-intl-latam/index.html>.
- 118 Alleged Russian spy fixer 'simply disappeared', *Newsweek*, 1 July 2010, <https://www.newsweek.com/alleged-russian-spy-fixer-simply-disappeared-217410>. The people trafficker dimension was raised by both US and Canadian security officials in multiple conversations on this case, between 2010 and 2012.
- 119 Alkman Granitsas, Cypriots speculate over spy's escape, *The Wall Street Journal*, 5 July, <https://www.wsj.com/articles/SB10001424052748704699604575342991962704142>.
- 120 Killings, coups and chaos: inside Putin's secret spy war on Europe, *The Times*, 28 June 2024, <https://www.thetimes.com/world/europe/article/killings-coups-and-chaos-inside-putins-secret-spy-war-on-europe-jlqmfqnb5>.
- 121 Why are asylum seekers pushing bicycles to the border?, *Yle*, 22 November 2023, <https://yle.fi/a/74-20061511>.
- 122 Lithuanian PM calls Lukashenko 'migrants and drugs' threats absurd, *LRT*, 27 May 2021, <https://www.lrt.lt/en/news-in-english/19/1418870/lithuanian-pm-calls-lukashenko-migrants-and-drugs-threats-absurd>.
- 123 Finnish Interior Ministry, *Suomi jatkaa rajoituksia itärajalla tilanteen hallitsemiseksi – hallituksella valmius uusiin tiukennuksiin*, 12 December 2023, https://valtioneuvosto.fi/en/-/1410869/finland-to-continue-restrictions-at-eastern-border-to-manage-the-situation-government-prepared-to-take-further-measures?language=fi_FI.
- 124 Kadri Liik, From Russia with love: How Moscow courts the global south, ECFR policy brief, 21 December 2023, <https://ecfr.eu/publication/from-russia-with-love-how-moscow-courts-the-global-south>.
- 125 Lorenzo Tondo, People-smugglers 'recruiting Russian captains for migrant boats to Italy', *The Guardian*, 22 January 2023, <https://www.theguardian.com/world/2023/jan/22/people-smugglers-recruiting-russian-captains-for-migrant-boats-to-italy>.
- 126 Siraaj Al Mughamir and Leon Spring, EU-migration by way of Russia: is Moscow or Brussels to blame?, openDemocracy, 3 April 2024, <https://www.opendemocracy.net/en/beyond-trafficking-and-slavery/eu-migration-by-way-of-russia-is-moscow-or-brussels-to-blame>.
- 127 Siraaj Al Mughamir and Leon Spring, EU-migration by way of Russia: is Moscow or Brussels to blame?, openDemocracy, 3 April 2024, <https://www.opendemocracy.net/en/beyond-trafficking-and-slavery/eu-migration-by-way-of-russia-is-moscow-or-brussels-to-blame>.
- 128 John A Lechner and Sergey Eledinov, Is Africa Corps a rebranded Wagner Group?, *Foreign Policy*, 7 February 2024, <https://foreignpolicy.com/2024/02/07/africa-corps-wagner-group-russia-africa-burkina-faso>.
- 129 Telephone conversation with an Italian intelligence officer, May 2024.
- 130 Hayley Dixon, Revealed: how Putin plans to flood West with migrants, *The Telegraph*, 29 February 2024, <https://www.telegraph.co.uk/news/2024/02/29/putin-russia-wagner-militia-africa-immigration-europe>.
- 131 Giuliano Foschini and Fabio Tonacci, *L'arma dei migranti sul voto: i barconi spinti in Italia dai mercenari della Wagner*, *La Repubblica*, 29 July 2022, https://www.repubblica.it/politica/2022/07/29/news/migranti_elezioni_politiche_barconi_wagner-359574463.
- 132 Manuela Perrone, *Migranti, cosa c'entra il boom di sbarchi con i mercenari della Wagner?*, *Il Sole 24 Ore*, 14 March 2023, <https://www.ilssole24ore.com/art/migranti-cosa-c-entra-boom-sbarchi-i-mercenari-wagner-AEaR13C>.
- 133 Year after failed mutiny, Russia tightens grip on Wagner units in Africa, *The New York Times*, 25 June 2024, <https://www.nytimes.com/2024/06/25/world/africa/russia-wagner-africa-corps.html>.
- 134 Filip Bryjka and Jędrzej Czerep, *Korpus Afrykański – Nowa odsłona starej wojskowej obecności Rosji w Afryce*, Polish Institute of International Affairs, May 2024, p 20, <https://pism.pl/publications/africa-corps-a-new-iteration-of-russias-old-military-presence-in-africa>.
- 135 Matt Herbert, Rupert Horsley and Emadeddin Badi, Illicit economies and peace and security in Libya, UN Security Council Illicit Economies Watch, GI-TOC, July 2023, <https://>

- globalinitiative.net/analysis/illicit-economies-and-peace-and-security-in-libya.
- 136 Federico Manfredi Firmian, *Libia: vecchie rivalità e rischio di nuova instabilità*, Italian Institute for International Political Studies, 18 September 2023, <https://www.ispionline.it/publicazione/libia-vecchie-rivalita-e-rischio-di-nuova-instabilita-143823>.
- 137 Conversation with a US intelligence officer, Washington DC, August 2022.
- 138 *A Paris, le Mur des Justes du Mémorial de la Shoah vandalisé, Emmanuel Macron dénonce un «odieux antisémitisme»*, *Libération*, 14 May 2024, https://www.liberation.fr/societe/religions/a-paris-le-mur-des-justes-du-memorial-de-la-shoah-vandalise-20240514_B5VDPYC6UZENTFUPID47BS2SGM.
- 139 Conversation with a commentator close to France's counter-intelligence and anti-terrorism agency, London, June 2024.
- 140 *Étoiles de David taguées à Paris : l'opération était pilotée par le FSB russe*, *Le Figaro*, 23 February 2024, <https://www.lefigaro.fr/international/etoiles-de-david-taguees-a-paris-l-operation-etait-pilotee-par-le-fsb-russe-20240223>.
- 141 Dan de Luce, Russia is trying to exploit America's divisions over the war in Gaza, NBC, 30 April 2024, <https://www.nbcnews.com/news/investigations/russia-trying-exploit-americas-divisions-war-gaza-rcna149759>.
- 142 Karolina Jeznach, Thomas Grove and Bojan Pancevski, The misfits Russia is recruiting to spy on the West, *The Wall Street Journal*, 15 May 2024, <https://www.wsj.com/world/europe/the-misfits-russia-is-recruiting-to-spy-on-the-west-7417b2b5>.
- 143 Семен Могилевич попросил зарегистрировать на него бренд «Арбат Престиж», *Vedomosti*, 19 April 2011, https://www.vedomosti.ru/opinion/articles/2011/04/19/ni_zh_achto_sidel; A cosmetic ruling: fortuitous failure to file key documents may mean wanted mobster Mogilevich walks, In *Moscow's Shadows*, 10 October 2010, <https://inmoscowsshadows.wordpress.com/2010/10/10/a-cosmetic-ruling-fortuitous-failure-to-file-key-documents-may-mean-wanted-mobster-mogilevich-walks>.
- 144 Anastasia Kirilenko, Чемодан от солнцевских. У Путина есть видеокompromat на лидера Венгрии?, *The Insider*, 2 February 2017, <https://theins.ru/korruptsiya/43801>.
- 145 Zdislava Pokorná, *Nová zjištění: Jak fungovala ruská vlivová operace a které evropské politiky si Putin platil*, *Deník N*, 5 June 2024, <https://denikn.cz/1443953/putinuv-europrojekt-jak-rusko-chtelo-ziskat-vliv-v-evrope-a-jake-dalsi-politiky-tajne-sluzby-podeziraji>.
- 146 'V' For 'Vympel': FSB's secretive department 'V' behind assassination of Georgian asylum seeker in Germany, *Bellingcat*, 17 February 2020, <https://www.bellingcat.com/news/uk-and-europe/2020/02/17/v-like-vympel-fsbs-secretive-department-v-behind-assassination-of-zelimkhan-khangoshvili>; *Mord im Kleinen Tiergarten: Bundesregierung droht Russland mit weiteren Strafmaßnahmen*, *Der Spiegel*, 18 June 2020, <https://www.spiegel.de/ausland/mord-im-kleinen-tiergarten-bundesregierung-droht-russland-mit-weiteren-strafmassnahmen-a-847c3a5d-975d-4938-9a25-957e84b41bc9>; Elena Chernenko, Что русскому хорошо, то немцу спод, *Kommersant*, 2 August 2024, <https://www.kommersant.ru/doc/6876517>.
- 147 Jake Lapham, Putin wants Berlin assassin Vadim Krasikov, but prisoner swap is murky, BBC, 31 March 2024, <https://www.bbc.co.uk/news/world-68555627>; Nikita Jolkver, Vadim Krasikov: Vladimir Putin's trump card in prisoner swap, DW, 3 August 2024, <https://www.dw.com/en/vadim-krasikov-vladimir-putins-trump-card-in-prisoner-swap/a-69844254>.
- 148 Have Russian hitmen been killing with impunity in Turkey?, BBC, 13 December 2016, <http://www.bbc.co.uk/news/magazine-38294204>; Stefan Berg, Murder in Vienna leads investigators to Chechen President, *Der Spiegel*, 23 June 2010, <http://www.spiegel.de/international/world/risk-factor-murder-in-vienna-leads-investigators-to-chechen-president-a-702146.html>.
- 149 Have Russian hitmen been killing with impunity in Turkey?, BBC, 13 December 2016, <http://www.bbc.com/news/magazine-38294204>.
- 150 Chechens killed in Istanbul in the name of Russian intel, prosecutor claims, *Hurriyet Daily News*, 19 February 2014, <http://www.hurriyetaidailynews.com/chechens-killed-in-istanbul-in-the-name-of-russian-intel-prosecutor-claims.aspx?PageID=238&NID=62656&NewsCatID=341>.
- 151 Intent on unsettling E.U., Russia taps foot soldiers from the fringe, *The New York Times*, 24 December 2016, <https://www.nytimes.com/2016/12/24/world/europe/intent-on-unsettling-eu-russia-taps-foot-soldiers-from-the-fringe.html>.
- 152 Jack Watling, Oleksandr V Danylyuk and Nick Reynolds, The threat from Russia's unconventional warfare beyond Ukraine, 2022–24, RUSI, 2024, p 31, <https://static.rusi.org/SR-Russian-Unconventional-Weapons-final-web.pdf>; US Department of the Treasury, Treasury targets Russian operatives over election interference, World Anti-Doping Agency hacking, and other malign activities, 19 December 2018, <https://home.treasury.gov/news/press-releases/sm577>.
- 153 *Uppgifter: Planerar attentat i Europa*, *Svenska Dagbladet*, 5 May 2024, <https://www.svd.se/a/jQPyke/underrattelsestjanster-ryssland-planerar-attentat-i-europa>.
- 154 Poland detains Ukrainian suspected of spying for Russia, *Polskie Radio*, 16 February 2024, <https://www.polskieradio.pl/395/9766/artykul/3335773.poland-detains-ukrainian%2%A0suspected-of-spying%2%A0for-russia>.
- 155 Navalny's former chief of staff Volkov attacked in Lithuania, *LRT*, 12 March 2024, <https://www.lrt.lt/en/news-in-english/19/2220647/navalny-s-former-chief-of-staff-volkov-attacked-in-lithuania>.
- 156 Suspects linked to Vilnius attack on Navalny ally Volkov arrested in Poland, *France 24*, 19 April 2024, <https://www.france24.com/en/europe/20240419-suspects-linked-to-vilnius-attack-on-navalny-ally-volkov-arrested-in-poland>.
- 157 Opposition financier accused of ordering attacks on Navalny allies, *The Bell*, 26 September 2024, <https://en.thebell.io/opposition-financier-accused-of-ordering-attacks-on-navalny-allies>.
- 158 Daniel Sandford, Two British men charged with helping Russian intelligence, BBC, 26 April 2024, <https://www.bbc.co.uk/news/uk-68899130>.

- 159 Paul Kirby, German spying: Two men held over suspected Russian sabotage plot, BBC, 18 April 2024, <https://www.bbc.co.uk/news/world-europe-68843541>.
- 160 Russia 'likely' behind fire that destroyed Warsaw shopping centre, says Tusk, Notes from Poland, 21 May 2024, <https://notesfrompoland.com/2024/05/21/russia-likely-behind-fire-that-destroyed-warsaw-shopping-centre-says-tusk>.
- 161 Bojan Pancevski, Russian saboteurs behind arson attack at German factory, *The Wall Street Journal*, 23 June 2024, <https://www.wsj.com/world/europe/russian-saboteurs-behind-arson-attack-at-german-factory-c13b4ece>; Scholz bekam Hinweis über Putin-Angriff in Berlin, *Bild*, 26 June 2024, <https://www.bild.de/politik/inland/brand-bei-waffenkonzern-hinweis-ueber-putin-angriff-in-berlin-6673fd-c5f1e88233b6dcdadb4>.
- 162 Jacques Follorou, *Derrière l'opération avortée d'un Russo-Ukrainien à Roissy-en-France, une vaste campagne de sabotage orchestrée depuis Moscou*, *Le Monde*, 26 June 2024, https://www.lemonde.fr/societe/article/2024/06/26/derriere-l-operation-avortee-d-un-russo-ukrainien-a-roissy-en-france-une-vaste-campagne-de-sabotage-orchestree-depuis-moscou_6244099_3224.html; Guillaume Biet, *Projet d'attentat dans un Bricorama: le suspect sous influence de la Russie selon les renseignements*, *BFM*, 28 June 2024, https://rmc.bfmtv.com/actualites/police-justice/projet-d-attentat-dans-un-bricorama-le-suspect-sous-influence-de-la-russie-selon-les-renseignements_AV-202406280410.html.
- 163 Conversation with a retired senior Norwegian intelligence officer, Oslo, April 2024.
- 164 Mark Galeotti, 'We have conversations': The gangster as actor and agent in Russian foreign policy, *Europe-Asia Studies*, 75, 6 (2023), <https://www.tandfonline.com/doi/full/10.1080/09668136.2022.2154316>.
- 165 В Гомеле завершено расследование дела о международном канале поставки кокаина из Доминиканы, *Belta*, 13 May 2019, <https://www.belta.by/incident/view/v-gomele-zaversheno-rassledovanie-dela-o-mezhdunarodnom-kanale-postavki-kokaina-iz-dominikany-347095-2019>.
- 166 Daniel de Simone, Sixth person charged with spying for Russia in UK, BBC, 27 February 2024, <https://www.bbc.co.uk/news/uk-68419311>.
- 167 Conversation with a Dutch intelligence analyst, Rotterdam, May 2024.
- 168 Why the Russian government turns a blind eye to cybercriminals, *Slate* (accessed through the Carnegie Endowment), 2 February 2018, <https://carnegieendowment.org/posts/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals>.
- 169 Conversation with a Ukrainian security service officer, London, March 2023.
- 170 Mark Galeotti in conversation with Andrew Keen, How Putin thinks like a warmongering 19th-century imperialist and why Ukraine will be his last colonial war, *LitHub*, 11 November 2022, <https://lithub.com/how-putin-thinks-like-a-warmongering-19th-century-imperialist-and-why-ukraine-will-be-his-last-colonial-war>.
- 171 Conversation with a Russian intelligence community veteran, Moscow, March 2014.
- 172 FBI, Grant D. Ashley, Assistant Director, Criminal Investigative Division, FBI, Before the Senate Subcommittee on European Affairs, Washington DC, 30 October 2003, <https://archives.fbi.gov/archives/news/testimony/eurasian-italian-and-balkan-organized-crime>.
- 173 Michael Schwartz, For a departed mobster, wreaths and roses but no tears, *The New York Times*, 13 October 2009, <https://www.nytimes.com/2009/10/14/world/europe/14mobster.html>.
- 174 Conversation with an FBI analyst, London, December 2023.
- 175 Yulia Vorobyeva, Entrepreneurial newcomers: Russian-speaking migrant smugglers on the US southern border, GI-TOC, 11 May 2023, <https://globalinitiative.net/analysis/russian-migrant-smugglers-us-southern-border>.
- 176 Latin America remains a playground for Russian intelligence, *The Economist*, 14 September 2023, <https://www.economist.com/the-americas/2023/09/14/latin-america-remains-a-playground-for-russian-intelligence>.
- 177 Yolande Monge and Elias Camhaji, US general: Russia has more spies deployed in Mexico than in any other country, *El País*, 26 March 2022, <https://english.elpais.com/international/2022-03-26/us-general-russia-has-more-spies-deployed-in-mexico-than-in-any-other-country.html>.
- 178 For a more comprehensive dissection of this process, see Mark Galeotti and Anna Arutunyan, Rebellion as racket: Crime and the Donbas conflict, 2014–2022, GI-TOC, July 2022, <https://globalinitiative.net/analysis/donbas-conflict-crime>.
- 179 Telephone conversation with a retired Russian police officer, June 2024.
- 180 See, for example, Владимир КАЛИНИЧЕНКО, бывший следователь по особо важным делам при Генеральном прокуроре СССР: 'Всесильный министр МВД СССР Щелоков принял решение о моем физическом устранении. В ответ на это Андропов приказал группе «Альфа» меня охранять', *Gordon*, 7 November 2004, <https://www.gordon.com.ua/tv/kalinichenko>.
- 181 Tom Keatinge, Developing bad habits. What Russia might learn from Iran's sanctions evasion, RUSI Occasional Paper, June 2023, <https://static.rusi.org/developing-bad-habits-what-russia-might-learn-from-irans-sanctions-evasion.pdf>; Matthew Karnitschnig, Iran teaches Russia its tricks on beating oil sanctions, *Politico*, 9 November 2022, <https://politico.eu/article/iran-russia-cooperation-dodging-oil-sanctions/>.
- 182 See, for example, Sarah Canna, IRGC's role in the black economy, Virtual Think Tank, May 2020, https://nsiteam.com/social/wp-content/uploads/2020/12/NSI-VITTa_IRGC-Black-Econ_CENTCOM-Q2_final-for-posting.pdf; and, for a specific example, David Rose, Revealed: How fake papers were used to smuggle a £20m oil shipment for Iran's IRGC, *The Jewish Chronicle*, 29 May 2024, <https://www.thejc.com/news/world/revealed-how-fake-papers-were-used-to-smuggle-a-20m-oil-shipment-for-irans-irgc-u22znwe1>.
- 183 International Institute for Strategic Studies, The surge of activity in relations between North Korea and Russia, November 2023, <https://www.iiss.org/publications/strategic-comments/2023/the-surge-of-activity-in-relations-between-north-korea-and-russia>; Josh Smith, North Korean weapons extending Russian stockpiles, German

- general says, Reuters, 9 September 2024, <https://www.reuters.com/world/north-korean-weapons-extending-russian-stockpiles-german-general-says-2024-09-09/>.
- 184 John Walcott, Cash, yachts, and cognac: Kim Yo-Jong's links to the secretive office keeping North Korea's elites in luxury, *Time*, 29 April 2020, <https://time.com/5829508/kim-yo-jong-money-office-39>.
- 185 See Julian Rademeyer, Diplomats and deceit: North Korea's criminal activities in Africa, GI-TOC, September 2017, <https://globalinitiative.net/analysis/diplomats-and-deceit-north-koreas-criminal-activities-in-africa>.
- 186 Как Америка узнала о «русских хакерах», *The Bell*, 6 December 2017, <https://thebell.io/kak-amerika-uznala-o-russkih-hakerah>
- 187 Conversation with an official from the UK's GCHQ, London, November 2023.
- 188 Mitchell Prothero, Russian spies have gone full mafia mode because of Ukraine, *Vice*, 27 October 2022, <https://www.vice.com/en/article/k7bx4v/russia-traffickers-spies>.
- 189 Conversation with a senior UK police officer, London, January 2024.
- 190 Conversation with a British National Crime Agency officer, London, June 2021.
- 191 Telephone conversation with an FBI officer, February 2024.
- 192 This is from the author's personal knowledge and regular frustration; one European service, for example, was very slow to realize in 2022 that the sudden diminution of *obshchak* funds did not mean payouts to imprisoned criminals but the kick-off of an expansion venture into a new criminal market.
- 193 Mark Galeotti, Crimintern: How the Kremlin uses Russia's criminal networks in Europe, ECFR policy brief, 18 April 2017, https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.
- 194 German defence minister Boris Pistorius, for example, suggested this could happen in 'five to eight years', while Jacek Siewiera, head of Poland's National Security Bureau talked of just three years. See *Verteidigungsminister im Interview: Könnten Sie Kanzler, Herr Pistorius?, Tagesspiegel*, 19 January 2024, <https://www.tagesspiegel.de/politik/boris-pistorius-uber-die-kriegsgefahr-ich-will-unsere-gesellschaft-wachrutteln-11070250.html>; *Liczna armia jest potrzebna, Nasz Dziennik*, 2 December 2023, <https://naszdziennik.pl/index.php/polska-kraj/288082,liczna-armia-jest-potrzebna.html>.
- 195 Mark Galeotti, Trump was right: NATO is obsolete, *Foreign Policy*, 20 July 2017, <https://foreignpolicy.com/2017/07/20/trump-nato-hybrid-warfare-hybrid-defense-russia-putin>.
- 196 Poland boosts security spending amid concern over Russian covert activities, Notes from Poland, 14 May 2024, <https://notesfrompoland.com/2024/05/14/poland-boosts-security-spending-amid-concern-over-russian-covert-activities>.
- 197 Dmitry Gudkov, Vladislav Inozemtsev and Dmitry Nekrasov, The new Russian diaspora: Europe's challenge and opportunity, French Institute of International Relations, 2024, https://www.ifri.org/sites/default/files/atoms/files/ifri_gudkov_inozemtsev_nekrasov_new_russian_diaspora_2024.pdf.
- 198 Center of Analysis and Strategies in Europe, Survey of Russian emigrants to Germany, France, Cyprus & Poland, 2024, p 9, https://case-center.org/wp-content/uploads/2024/06/DOCLAD_fin.pdf.
- 199 Kirill Shamiev and Ksenia Luchenko, Life in exile: A new approach to Russian democrats in Europe, ECFR policy brief, 14 March 2024, <https://ecfr.eu/publication/life-in-exile-a-new-approach-to-russian-democrats-in-europe>.
- 200 GCHQ, Director GCHQ discusses how 'whole of cyber' approach is disrupting criminals, 10 May 2022, <https://www.gchq.gov.uk/news/director-cyberuk2022>.
- 201 Six different European law enforcement/security officers with a direct or limited role in financial investigations were asked which countries posed particular problems in this respect: all six mentioned Cyprus, Israel, Luxembourg and Lichtenstein; five Latvia; and three each the US and Greece.
- 202 Edward Cohn, A Soviet theory of broken windows: Prophylactic policing and the KGB's struggle with political unrest in the Baltic Republics, *Kritika*, 19, 4 (2018).
- 203 The 'prophylactic conversation' and the management of Russian organised crime: the Ekaterinburg example, In Moscow's Shadows, 30 August 2017, <https://inmoscowsshadows.wordpress.com/2017/08/30/the-prophylactic-conversation-and-the-management-of-russian-organised-crime-the-ekaterinburg-example/>; Alec Luhn, Russia clamps down on football hooligans before World Cup, *The Telegraph*, 9 June 2018, <https://www.telegraph.co.uk/news/2018/06/09/russia-clamps-football-hooligans-world-cup/>; «Вору в законе» сделали последнее предупреждение, *Rosbalt*, 24 May 2018, <https://www.rosbalt.ru/moscow/2018/05/24/1705519.html>.



GLOBAL INITIATIVE

AGAINST TRANSNATIONAL
ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 700 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net