Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Sean Wiswesser

How Russia's intelligence services will respond to the war's changing tides

Russia's intelligence services are entering a more uncomfortable phase of the war.

For years, success within the Kremlin's security apparatus was measured less by objective reality than by political usefulness.

The priority was never to produce accurate intelligence or effective operations; it was to produce assessments that pleased the "Boss," as the services call Vladimir Putin.

The goal of their sycophantic obsequiousness was to reinforce the Boss's assumptions. That formula led them into this war and worked while Russia appeared to be advancing.

It becomes far more dangerous when the headlines no longer flatter the Kremlin.

As military setbacks accumulate, sanctions continue to hit in uneven but still impactful ways. Ukraine demonstrates remarkable resilience.

The three principal Russian intelligence services (collectively the RIS) – the FSB, SVR, and GRU – are almost certainly engaged in the oldest bureaucratic exercise in authoritarian regimes: protecting themselves while finding someone else to blame.

Understanding that instinct matters because it will shape not only internal Kremlin politics but also the risks Europe, NATO, and the United States are likely to face over the coming months.

Accountability for a downturn in the war

Three general themes are likely to develop, or are underway right now, within and among these services.

The first theme for the RIS is accountability for a downturn in the war, one felt by the population and, in particular, in the energy sector. But accountability will be directed everywhere except inward.

Corruption has long been the operating system of the Russian state, rewarding loyalty over competence and patronage over performance.

> RIS services will undoubtedly be constructing narratives explaining why disappointing outcomes were somebody else's responsibility

In the RIS, as in much of the vast Russian kleptocracy, advancement depends on connections and on satisfying political expectations rather than on delivering uncomfortable truths.

In such an environment, intelligence becomes a commodity traded for influence rather than a public good.

Each of the RIS services will undoubtedly – based on past precedent – be constructing narratives explaining why disappointing outcomes were somebody else's responsibility.

The FSB will undoubtedly be eager to identify failures among military commanders, regional officials, industrial managers, or even other RIS services, whom they call their "cousins" (for the GRU, they are called the "distant cousins" in RIS parlance to the FSB; the SVR are the "near cousins" since they are, together with the FSB, both remnants of the old KGB). But the familial ties end with nicknames.

Backstabbing and shifting blame

The Russian services have deep-seated animosities toward one another. Backstabbing and shifting blame are the norm.

A downturn in the war, as is being experienced now, all over the headlines, even in Russia, is sure to draw the RIS leaders into a game of "there is hell to pay, and the Boss wants to know WHO is to blame…"

The SVR will likely excuse its failures, attributing them to Western resolve proving stronger than anticipated and to diplomatic failures beyond its control.

They have responsibility for information warfare in their Directorate MS, which is responsible for "active measures."

But of course, Russia has not done a good job of convincing any countries – via covert action or otherwise – to align with them.

And, over the past year, Russian allies have been dropping like flies – some from elections like in Hungary, others from regime change like in Venezuela, but none of these are good report cards for the RIS.

> The Kremlin has always rewarded those who tell leadership what it wants to hear

The GRU has much to answer for, too. As the military intelligence service, they don't have any dramatic successes to turn to like Ukraine's "Operation Spiderweb": drones popping out of containers across Russia and attacking strategic air bases. But the GRU will no doubt blame and cite battlefield constraints imposed by politics rather than by military planning.

What none of them can afford to admit is that systemic flaws – distorted reporting, inflated confidence, endemic corruption, and wishful thinking on all their parts – helped lead to the current predicament.

The FSB is the largest of the services by far, but is to blame more than most because it was their Fifth Service that took the lead in planning and whose operational analysis convinced the Boss they would win, and win quickly.

The Kremlin has always rewarded those who tell leadership what it wants to hear. That creates an intelligence culture in which institutional survival often takes precedence over strategic honesty.

The FSB also should answer for the wave of assassinations of generals and other leadership figures across Moscow in the past year, but again, they will find others to blame, probably the police.

Hybrid warfare and gray-zone operations

The second theme of the blame game above, and turning the tide of war for these services, is perhaps more concerning for Western democracies.

As visible progress in conventional military efforts becomes increasingly difficult to showcase, there will likely be a continued rise in reckless hybrid warfare and gray-zone operations.

Every Russian intelligence agency will actively seek opportunities to demonstrate its relevance and ensure Putin perceives its effectiveness, potentially leading to more aggressive and destabilizing actions.

That creates incentives for escalation in areas below the threshold of open conflict, the definition of gray-zone escalation we see playing out across Europe: cyber operations, sabotage, disinformation, influence campaigns, covert financing, infrastructure disruption, and "wet work" or assassinations.

The RIS has doubled down in recent years on the recruitment of criminal proxies and what academics call "non-state actors," but for the RIS, these are just old-school proxy-agent operations.

They are using them for arson, sabotage, and attacks on logistics networks.

Democracies should anticipate more hybrid war - FSB Chief Alexander Bortnikov (left)

These actions, which the RIS calls "direct measures," become attractive because they are comparatively inexpensive, politically deniable, and capable of generating headlines. Competition between services may make this trend even more dangerous.

Rather than acting with careful strategic discipline, individual services or units within them (such as the allegedly newly formed GRU Unit 795, meant to replace Unit 29155, which garnered too many headlines for failed ops in recent years) may increasingly pursue high-profile operations that demonstrate initiative and earn favor at the Kremlin.

The goal is to have quick wins to impress the Boss, gain favor, and earn promotion. The result, however, is not necessarily better-coordinated campaigns but more numerous and more reckless ones.

Democracies should therefore anticipate more hybrid war, much of it opportunistic, experimental, and deliberately calibrated to remain below the threshold that would provoke a conventional military response.

But the RIS pushes the limits, and absent a credible deterrent, that is, absent any pushback from the West, they will keep pressing.

The danger is not simply the scale of these operations but the growing willingness to accept risk in pursuit of political and coercive effects. The want Europe to be afraid to support Ukraine.

Exploiting democratic weakness

The third and most consequential question concerns how Russia's intelligence services intend to sustain the war as Ukraine evolves new weapons and potential Western support grows.

If battlefield victories remain elusive, sustaining access to technology, finance, industrial components, and sanctions evasion becomes a critical mission in its own right.

Recent reporting highlighting the exploitation of weaknesses in Japanese sanctions enforcement by a Russian intelligence-linked unit (reported by the New York Times) serves as a timely reminder that sanctions regimes are only as effective as their implementation.

It is tempting to criticize Tokyo for shortcomings in counterintelligence capacity or enforcement. But that temptation should quickly give way to a more uncomfortable question: are Europe and the United States truly any more prepared?

Russian intelligence has spent decades building sophisticated networks spanning procurement, front companies, illicit finance, technology acquisition, and covert logistics, from the KGB Line X of old to the new GRU 20th Directorate now apparently operating in Japan. They are masters at innovating to exploit democratic weaknesses.

Every inconsistency and weak link among allied sanctions regimes, every regulatory loophole, every under-resourced customs agency, and every jurisdiction with limited counterintelligence capability represents an opportunity for the RIS.

The Russian services are unlikely to regard sanctions as immovable barriers. Instead, they will continue to view them as potential operational opportunities that require creativity, persistence, and patient exploitation of bureaucratic weaknesses.

> Technology is driving this war, not assassinations or other "wet work"

This is where competition among Russia's intelligence agencies becomes damaging to the West.

The agency shows it can secure essential components, help evade sanctions, weaken export controls, or support defense industry gains, thereby increasing its influence within the Kremlin by directly aiding the war effort.

These actions usually do not garner the dramatic attention that covert operations or cyberattacks do.

However, they could have even greater long-term impacts, especially as Russia concentrates on ballistic missile strikes and Ukraine's air defenses become increasingly strained.

Technology is driving this war, not assassinations or other "wet work." It is increasingly a contest of industrial endurance, technological adaptation, and accelerated acquisition timelines. It is also a test of economic resilience.

Russian and Ukrainian Intelligence services are central participants in that competition, not merely collectors of information but active facilitators of national power.

This is not unique to the Russians. The Chinese certainly see the value in hybrid war and technology theft, and they are willing, in some cases, to share their expertise, particularly regarding their main adversaries – the United States, NATO, and Europe.

Formidable adversaries

Western policymakers should resist the temptation to view the Russian intelligence services as either omnipotent or incompetent.

They are neither. They are capable organizations operating inside a profoundly dysfunctional political and bureaucratic system. Corruption weakens them, yet it also makes them adaptive.

Bureaucratic rivalries undermine coordination, yet competition can generate innovation. And finally, the RIS has no accountability in Putin's system since he excuses their failures.

Underestimating Russian intelligence would be as dangerous as exaggerating its capabilities. They remain formidable adversaries.

Continued support for Ukraine remains not simply an act of solidarity but a strategic investment in European and transatlantic security

From Russia's main spy services, we can expect more efforts to weaken public support for Ukraine, more attempts to intimidate European societies, more targeting of defense industries and supply chains, and more sophisticated efforts to circumvent economic restrictions.

None of these activities individually changes the course of the war. Collectively, however, they seek to erode Western cohesion – the very foundation upon which Ukraine's resilience depends.

That is why continued support for Ukraine remains not simply an act of solidarity but a strategic investment in European and transatlantic security.

Continued and successful Ukrainian defense complicates the calculations of Russia's intelligence services.

Every demonstration of allied unity undermines the bureaucratic narratives these services hope to present to the Kremlin.

The intelligence battle surrounding this war is far from over. Indeed, it may become even more important as the conflict enters its next phase.

If Russia's security services are now searching for someone to blame, looking for new ways to strike democracies, and identifying fresh methods to sustain the war, then Western governments should respond with equal clarity of purpose.

The most effective answer is not complacency or fatigue but sustained support for Ukraine, stronger counterintelligence, tighter enforcement of sanctions, and continued allied resolve. Those are precisely the outcomes the Kremlin's intelligence services least want to see – and exactly why they remain indispensable.

Sean Wiswesser is a former CIA Senior Operations Officer and expert on Russian Intelligence, Espionage, and Defence Issues.