The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

How to Understand Russia's Shadow War Against the West

By Ionuț-Vlad Şutea

July 24, 2024

Spanish police at the scene of the murder of pilot Maxim Kuzminov. **@EurekaNews10**

Recent reports highlighting an escalation in Russia's "shadow war" against the West, including the foiled hit on Rheinmetall CEO Armin Papperger, have reignited discussions on Below Threshold of War Operations (BTWO). Russian-linked sabotage and espionage activities in Europe have surged, reflecting a broader strategy targeting critical infrastructure and key individuals.

Russian-linked attacks in the West have included arsons at warehouses and defense industry sites in Britain and Germany, cyberattacks against private and public companies, and sabotage against a plethora of other objectives. Additionally, there has been a notable increase in recruitment and reconnaissance efforts by Russian intelligence services.

Russia has also targeted defectors, journalists, and European officials for years. Recent examples include the attack on the Estonian Interior Ministry and the assassination of a

Russian helicopter pilot who defected to the West in Spain, both of which occurred in February 2024. Now, the U.S. is strengthening security at its military bases in Germany due to heightened risk levels.

Russia's aim is clear: disrupt Western military aid to Ukraine, prevent Europe from permanently transitioning away from Russian energy, and intimidate Western governments from taking bold action against Moscow.

While Russian intelligence services are "doing their job," their campaign has been on an escalatory trajectory that the West cannot afford to ignore. In the era of Great Power Competition with near-peer adversaries like China and Russia, competing while remaining under the threshold of war – a critical boundary that, when crossed, leads to the start of formal warfare – is in the Kremlin's interests.

BTWO exists in the gray zone, a conflict spectrum between open warfare and peaceful competition. It encompasses actions such as cyberattacks, political warfare, economic pressure, fake news campaigns, sabotage, and assassinations, all intended to weaken, intimidate, or coerce an opponent while avoiding a full-scale war.

While hybrid warfare involves mixing conventional military tactics with unconventional ones, BTWO focuses on staying below the war threshold.

While Hybrid warfare describes an aggressor's methods, BTWO describes an adversary's attempts to avoid open conflict. While related, these concepts are not necessarily symbiotic.

Related article: Why Russian Propaganda Isn't as Sophisticated as You Think

Probably the most important aspect of BTWO is that it maintains plausible deniability for the aggressor. In this case, Russia strives to obscure its involvement and evade accountability. While Russian intelligence agencies have a long track record of sloppiness, they can still be devastatingly effective. Additionally, much like the military, these organizations have learned some lessons the hard way and are improving in areas such as dynamic targeting, coordination, and asset recruitment among its European diaspora. As one NATO European official told The Financial Times, "Russian mischief is coordinated and at scale."

Whether they leave traces behind to indicate Russian involvement or not, the Kremlin only has one card to play when accused: the deniable one.

Unsurprisingly, Russian officials deny any connection to the string of arsons, explosions, and other acts of sabotage reported in the West, rejecting all Western accusations as baseless and empty. Leading this effort is Russian Presidential Spokesperson Dmitry Peskov.

However, such denials are expected. Covert operations necessitate political disavowal to ensure the operations do not cross the threshold of war. An open admission could force NATO countries to retaliate, potentially locking the two parties into a cycle of escalation that can spiral out of control.

Nonetheless, Russian officials, including President Vladimir Putin, have not refrained from issuing not-so-veiled threats. In late May 2024, Putin ominously said, "NATO countries, particularly European ones, must remember that these are states with a small territory and a very dense population." This came weeks after the Financial Times reported Western intelligence warnings about Russia's capability and willingness to ramp up sabotage operations within NATO countries.

Putin's remarks are pushing the limits of gray zone warfare by almost openly threatening multiple states with what can easily be interpreted as kinetic warfare targeting urban centers to cause mass casualties. This rhetoric is noteworthy as it typically emanates from lesser officials or propagandists like Dmitry Medvedev, and TV personalities such as Vladimir Solovyov, whose threats against Western states have a "flavor of the week" fashion.

Related article: The World Missed the Warning of 2014 Ukraine Invasion

The covert and increasingly assertive nature of Russian BTWO in the gray zone makes it essential that the West adopts a robust defensive posture and adapts to any challenge Russia throws at it.

Improved intelligence and counter-intelligence measures are vital to identifying and stopping BTWO attacks. Enhanced intelligence capabilities will provide the necessary insight into who is behind these attacks and how they operate. Given that Russian intelligence is profiting from the free movement offered by Schengen, increased coordination and intelligence sharing among European allies will become key to foiling attacks. Within NATO or the European Union, a task force dedicated to protecting national critical infrastructure should be considered.

National governments and private enterprises must secure critical national infrastructure (CNI) and other sensitive sites, such as energy facilities, seabed cables, and defense industry plants. This involves not only increasing physical security but also investing in monitoring and intelligence measures to detect and analyze potential threats.

Furthermore, NATO and the EU should make sure the public are aware of Russia's efforts. Publicly revealing BTWO activities and those responsible can undermine their effectiveness and garner international support. This requires a strategic communications campaign capable of countering contingency narratives deployed by adversaries to obfuscate the truth.

However, exposing the truth is challenging and often impossible, as it can endanger or compromise classified intelligence assets or capabilities used to collect evidence of Russian involvement. Here is where Open-Source Intelligence (OSINT) plays a crucial role. Whenever possible, openly available information and unclassified methods should be utilized to provide evidence and raise public awareness. OSINT is also an effective tool for fact-checking and verifying information, ensuring that accurate and timely data is disseminated to the public, thus strengthening the credibility of counter-narratives.

Western armed forces and intelligence agencies must also develop tools and doctrines specifically designed to counter covert attacks. Proactive measures, rather than reactive responses, are essential to address crises, hostile provocations, and malign activities

effectively.

Russia's BTWO strategy represents a significant and evolving threat that Western nations cannot afford to ignore. By understanding BTWO and developing effective countermeasures, the West can navigate this complex and evolving landscape and enact retribution. Proactive measures such as the ones listed above are essential to mitigate the risks of inaction, as failing to respond will only create a false perception of attack tolerance, inviting even bolder assaults on Western interests.

It is time to recognize and address Russia's escalating shadow war with decisive action.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2024/07/24/how-to-understand-russias-shadow-war-against-the-west-a85814