rusi.org

How Might the Kremlin Test NATO’s Collective Defence?

16–20 Minuten

Preparing the defences: UK forces in Poland as part of Exercise Steadfast Defender 2024, which saw troops deploy across the entirety of NATO's eastern flank. Image: MOD Crown Copyright News/ Editorial Licence

With irregular warfare escalating across land, air, sea, cyber and space, Russia's sub-threshold operations may challenge NATO's collective defence doctrine sooner than expected.

The Kremlin is growing in confidence. Although sustaining immense costs, it has regained the initiative on the Ukrainian front. Simultaneously, its ‘active measures’ campaigns to influence and disrupt the West have increased in intensity, including arson, bombings and attempted assassinations. Ken McCallum, Director General of MI5, gave a press conference in which he announced the Kremlin’s security services had ‘gone feral’ and were seeking ‘sustained mayhem’ on the streets of the UK and other European countries. Closer to the Kremlin’s borders, investigative journalists have noted increased reconnaissance activity around Kaliningrad (a Russian enclave between Poland and the Baltic states) and the wider region. Concurrently, the election of Donald Trump is likely to be accompanied by a strategic desire by the US to have European partners share more of the security burden. This is likely to be further fuelled by his reported perception (which is not unjust) that

European allies have been taking advantage of the US and have grown too relaxed about their own security. This has raised concerns that the Kremlin will attempt to take advantage. Against this backdrop, Denmark's defence minister has remarked that the Kremlin may 'test' a NATO country within 3–5 years.

According to NATO's Article V, 'an attack on one is an attack on all', and therefore a test against any member is a test of NATO's core concept of collective defence. This raises the crucial question: how might the Kremlin test NATO's collective defence? This article, complemented by brief interviews with Lt Gen (retired) Sir Rob Fry and Professor Mark Galeotti, will seek to answer this question through the use of the 5WH format:

1. What form would this test take?
2. Where would it occur?
3. Why would the Kremlin pursue this action or target?
4. Who would conduct it?
5. When would the test(s) take place?
6. How will these operations be conducted?

The first is the easiest to answer. Even before it had been heavily degraded by the invasion of Ukraine, the Kremlin could not match the combined forces of NATO; it must therefore avoid a direct confrontation. Therefore, any initial actions prior to a direct offensive are likely to be irregular. As Sir Rob Fry surmises:

> 'If there was an overt action, the response would have to be decisive as it would be the first test. The boundaries will be tested from below. So long as they are insidious, the risk is lower.'

The second easiest to break down is 'where'. This article will break down the warfighting domains of Land, Air, Sea, Space and Cyber and outline possible locations, then answer why, who and how across each domain according to Kremlin irregular doctrine and observed methods.

Land

The oldest domain of warfare has seen significant developments over the past decade. Today, less manpower, time and money are needed to have a great effect, offering significant sub-threshold opportunities.

Where: It is said that in warfare, 'amateurs talk tactics, experts talk logistics' – making military bases and logistical points (such as transport links and arms depots) the best strategic targets.

Why: Ukraine's war effort has demonstrated the primacy of logistics in operational effectiveness. By targeting military bases and logistical hubs, the Kremlin could disrupt supply chains, weaken operational capabilities and diminish troop readiness. This would undermine enemy resilience, forcing delays and reducing the effectiveness of military campaigns, thus further diminishing the risk appetite among NATO members in the long term.

> By targeting military bases and logistical hubs, the Kremlin could disrupt supply chains, weaken operational capabilities and diminish troop readiness

Who: Kremlin special services would have greater influence and reach in eastern Europe. In Western Europe, however, where the Kremlin's security services have been diminished, there is evidence of a rise in single-use proxies and outsourcing to criminal organisations, with Professor Galeotti noting that their use in modern Kremlin statecraft has become more common. Most of these seem to have been financially motivated. However, Sir Rob Fry points to increasing polarisation in the West as an added potential motivator for recruitment:

> 'There is a new radicalism in Europe and the West on both the left and the right due to Gaza and the disintegration of society that can be recruited. An agent of conviction is worth half a dozen paid agents.'

Localised recruitment, although less reliable than professionally trained teams, has the benefit of ambiguity that the Kremlin can exploit in order to profess denial. Locals are also more likely to be familiar with the operational environment and thus to go unnoticed until the late stages of planning or after the operation.

How: Kremlin sabotage doctrine and recent operations suggest that arson and bombings, potentially complemented by insider threats, are the preferred methods. The 2014 sabotage of a Czech Arms Depot containing weaponry intended for Ukraine, killing two people and causing evacuations, serves as a case study. More recently, there have been arson attacks in Western Europe. These operations have the potential to cause further disruption and degradation over time via the diversion of resources towards enhanced security measures. This in effect creates 'weaponised inconvenience', according to Professor Galeotti.

Air

The Air domain has evolved from the rudimentary reconnaissance planes of the First World War to modern technology like jets, stealth aircraft, and drones, bringing precision and strategic dominance to the air – especially when paired with electronic warfare (EW).

Where: Aircraft seem an obvious target, and there are concerns around the attempted sabotage of cargo airliners by the Kremlin as a 'dry run'. However, radar installations would be a target of more significant impact.

Why: Radar instillations have proven critical in past conflicts. They provide real-time detection and tracking of airborne threats to ensure early warning and swift responses, allowing for coordination of defence and protection of valuable assets. Damaging them, and NATO's subsequent inability to defend the Air domain, would likely shape policymakers' response to Kremlin aggression in other domains.

Who: Sir Rob Fry argues that due to the competencies required to operate in the Air and Sea domains, attacks in these domains would be easier to attribute, potentially altering the Kremlin's risk calculus – why risk discovery of EW capabilties for limited payoff? However, while EW cannot be easily outsourced, the conflict in Ukraine has demonstrated the use of small drones as a potential solution to this problem of attribution, as they are easily used by proxies with a low skill threshold.

How: An effective strategy would likely utilise specialised services for EW while outsourcing the use of small drones to local proxies. There have already been instances of drones flying over US bases in the UK and significant disruption to airports from drone incursions, alongside the jamming of aircraft. If intensified with jamming followed by explosive drones and guided to strategic targets like radar, this could result in long-term degradation.

Sea

The maritime domain is vital for security and prosperity – ensuring trade, dominating critical shore territory, and defending chokepoints. It continues to expand, however, especially due to the increased capability for deepwater operations.

Where: Despite many strategic targets sitting above the waterline, those on which a strike would cause maximum effect without war sit on the sea floor – specifically, communication cables and energy pipelines. Concerns about these potential targets have risen significantly since the destruction of the Nord Stream 2 pipeline, demonstrating the relative ease with which cables and pipelines can be targeted, especially in the Baltic Sea with its shallower waters. To be considered a significant test, multiple cables and pipelines would need to be destroyed at once.

Why: Undersea cables are critical to data traffic, with an estimated 95% of the world's data going through them. Damage would disrupt and degrade communications, financial transactions, and other critical services in addition to energy, creating shortages and price rises that would result in societal instability.

Who: Activities such as these require professional training. Consequently, it is likely that the Kremlin would rely on organisations such as GUGI – the Main Directorate of Deep-Sea Research – with its divers and specialist deep-sea submarines. While this reduces deniability, the purpose of sub-threshold operations creates the necessary ambiguity to frustrate policymaking; would NATO risk war over energy and data infrastructure?

How: Recent activities have provided an indication of how these actions can be carried out with remotely operated drones, mines or divers with specialist tools – likely launched from Kaliningrad, the home of Russia's Baltic Fleet.

Space

Space, originally used for surveillance, communication and targeting, has evolved, with states now equipped with anti-satellite weapons and defensive capabilities to secure strategic assets.

Where: Based on the weapons available to the Kremlin and space-related critical infrastructure, any operations would be undertaken in geosynchronous orbit, where there are satellites for telecommunications and observation.

Why: Recent Russian military doctrine has emphasised the importance of information dominance in warfare, including information infrastructure. This makes space assets – with their capacity for storing and transmitting data – valuable targets, as their destruction could disrupt communications and intelligence-gathering capabilities.

Who: Unsurprisingly, this would require not just professional experience but significant resources, meaning any operation in Space would almost certainly be conducted by the Aerospace Forces of Russia.

How: One option would be direct-ascent anti-satellite missiles, designed to destroy satellites and create substantial 'space junk' that could cause further surrounding damage. Another would be a weapon that releases radiation, frying satellite signals. However, the damage such operations would cause cannot be regarded as limited and could not be deniable; it would cause vast disruption and degradation of NATO states' capabilities (as well as those of other non-aligned states), including a breakdown of comms and online services that could only serve to benefit an irreversible state of hostility. Consequently, Sir Rob Fry surmises that 'this would not be a test. It would be the first act in a large-scale conflict'.

Cyber

In kinetic warfare, cyber continues to be seen as a force-multiplier rather than a standalone force. It was only officially recognised as a fifth domain by NATO in 2016. But as a facet of sub-threshold operations, it has become one of the most ubiquitous tools.

> Geopolitical competition increasingly takes place in the information domain. The Kremlin recognises this and will almost certainly utilise subversion as its primary weapon

Where: The connectivity of the modern world provides multiple targets. Professor Galeotti goes as far as to argue that 'we may need to lose the idea of cyber as a separate domain, because everything is cyber'. Transportation, finance, energy, and government and military communications are just a few facets of society that are at risk, but a large-scale attack on healthcare would be considered a test.

Why: The immediate effects of disrupting healthcare would be panic, with repeated and prolonged outages leading to loss of life. Second-order effects would include weakening trust in institutions, causing further long-term degradation to resilience. Both would benefit the Kremlin by forcing states to focus on internal damage control rather than Kremlin aggression.

Who: In Putin's Russia, the lines between criminal hackers and government cyber actors are heavily blurred. The regime tolerates criminal groups provided that they target outside of Russia, while also maintaining significant cyber capabilities of its own. Therefore, the choice of actor would depend less on capability and more on the target and desired level of ambiguity. A mass attack on healthcare would almost certainly be carried out by criminal proxies.

How: The most dangerous form of attack would be a 'zero-day exploit' – targeting a vulnerability in a system that is unknown. However, this can only be done once, and would likely be saved for war. A Distributed Denial of Service attack is more likely, overwhelming multiple target servers or networks with massive traffic and causing a crash. Another option is ransomware, which encrypts a target's data and demands payment for decryption. These are typically conducted via phishing links clicked on by unsuspecting members of the target organisation – demonstrating that in the cyber domain, it is people who are the biggest vulnerabilities.

Cognitive: The Sixth Domain?

Evgeny Messner, a former Tsarist officer considered a 'godfather of subversion warfare' whose work is experiencing a revival in Russia, remarked that 'the ultimate benefit of any military action is its psychological impact on the enemy'. The scenarios suggested would have a similar impact on policymakers and populations, conveying an image of an all-powerful and insidious Kremlin. Professor Galeotti notes that 'the outcome is political, not operational' and that 'the irony is that the psychological impact is greater than the physical'.

Geopolitical competition increasingly takes place in the information domain. The Kremlin recognises this and will almost certainly utilise subversion as its primary weapon, using disinformation to turn societal divides into fissures, undermine trust in the government and institutions, enforce the concept that truth is unknowable, create panic with false alarms, and cultivate a perception that supporting NATO's Article V would be risking a Third World War. Artificial intelligence and recruitment of local actors further lower the threshold for these operations and increase their authenticity, reach and potential impact on behaviours.

When could these activities take place? While the Kremlin currenly conducts many sub-threshold operations, according to Sir Rob Fry, we can expect an operational pause before a significant test. Likewise, Professor Galeotti suggests that 'the smart money is on eight years for reconstitution' (i.e. when the Kremlin would be prepared for a significant kinetic struggle). However, we will almost certainly see other 'dry runs' to maintain the initiative and potentially prepare for more significant operations.

> 'The Kremlin will need a period to restock and reconsolidate, easing stresses on the economy and implementing doctrinal lessons from Ukraine. But you need to keep the pot boiling, and ambiguous warfare can fill the gap.' – Sir Rob Fry
>
> 'From Putin's point of view, Ukraine is not just about Ukraine. He will continue to see the West as hostile and the response is not just about disruption, but to demonstrate to it that its support for Ukraine [in effect responding to Kremlin aggression] has consequences.' – Professor Galeotti

None of these scenarios are guaranteed, nor are they exhaustive; this would require study by a range of subject-matter experts across all the domains cited. However, one of the underlying issues contributing to the greatest defence failures of the modern age – 9/11, the full-scale Invasion of Ukraine, 7 October – was 'a failure of imagination'. It's time to start thinking and forming responses now, before a Kremlin-sponsored situation in a NATO member state is added to this list.

The views expressed in this Commentary are the author's, and do not represent those of RUSI or any other institution.

For terms of use, see Website Ts&Cs of Use.

Have an idea for a Commentary you'd like to write for us? Send a short pitch to commentaries@rusi.org and we'll get back to you if it fits into our research interests. Full guidelines for contributors can be found here.

keywords

WRITTEN BY

Joe Morley-Davies

External Expert

View profile