



September 9, 2026

## Russia's Shadow War

By Shelby Gingras

### Abstract

The Russo-Ukraine war has constrained Russia's ability to project power through conventional military means. Economic pressures, resource depletion, and the loss of military assets continue to stretch Russia thin as the conflict extends into its fourth year. This article examines the Baltics as a case study demonstrating how Putin has embraced hybrid warfare to exert international influence by disrupting NATO states' operations/governance, but below the threshold that would trigger armed conflict, providing suggestions of how NATO can increase their resilience against this pressure.

### Introduction

Russia has always conducted some level of grey zone activity to push boundaries and advance its foreign policy agenda, however the Ukraine war has accelerated and increased Russia's implementation and usage of these types of operations, shifting from on-and-off cases to becoming a key pillar in Russia's broader strategic approach and a way of combating NATO. These hybrid activities range from cyberattacks and the dissemination of disinformation to the targeting of critical infrastructure and drone incursions.



## Malign Activity in the Baltic's

The Baltic states are a good case study to look at to see the various types of hybrid warfare Russia has carried out and the differences in frequency during and pre-Ukraine conflict. The Baltics are especially interesting to examine, as Russia has long expressed its discontent with Estonia, Latvia, and Lithuania becoming independent states after the fall of the Soviet Union, which has only been exemplified as these states have moved away from Russian influence through joining the European Union, NATO, forming their own independent governments, and, more recently, condemning Russia's actions in Ukraine.

Previously, and at the start of the war, Russia focused more on cyber operations. During the peak of Russia's invasion of Ukraine, Latvia reported an increase in Russian cyberattacks, with 733 total attacks in August 2022, compared to the mean of 257.6 attacks per month from January 2021 to September 2022, before the full invasion. Since then, this higher trend of cyberattacks has continued, with 631 reported attacks in January 2025.<sup>1</sup> These cyberattacks range from the attacking of government websites to the targeting of civilian infrastructure, including the power grid, banking system, and other cyber-controlled infrastructure.<sup>2</sup> Latvia's military officials attribute these attacks to Russian and Belarusian officials, politicians, military leaders, and state-controlled media.

Lithuania has also seen an over 50% increase in offenses relating to electronic data and information systems compared to past years.<sup>3</sup> The National Cyber Security Centre (NKSC) registered 3,874 cyber incidents in 2024 alone.<sup>4</sup> This is directly impacting civilians, with twice as much money being lost to financial scams totaling over €10 million, compared to 2020.<sup>5</sup> The Lithuanian Armed Forces'

<sup>1</sup> CERT.LV, Q1 2025 In Latvian Cyberspace, CERTattributedatthe including,yberattacksLV, May 10, 2025, [https://cert.lv/uploads/eng/CERTLV\\_Q1\\_2025.pdf?utm\\_source=cyberattacks](https://cert.lv/uploads/eng/CERTLV_Q1_2025.pdf?utm_source=cyberattacks).

<sup>2</sup> "Valsts iestāžu mājaslapas piedzīvo intensīvus kiberuzbrukumus," *LSM.lv*, August 20, 2024, last modified 19:17, <https://www.lsm.lv/raksts/zinas/latvija/20.08.2024-valsts-iestazu-majaslapas-piedzivo-intensivus-kiberuzbrukumus.a565738/>; Murray Brewster, "Inside the Digital Cold War: How Canada Helps Defend Latvia from Russian Cyber-Attacks," *CBC News*, March 4, 2025, <https://www.cbc.ca/news/politics/nato-baltic-allies-cyberhunting-1.7473251>.

<sup>3</sup> "Cyberattacks in Lithuania Surge When War in Ukraine Began," Euractiv, [https://www.euractiv.com/short\\_news/cyberattacks-in-lithuania-surged-when-war-in-ukraine-began](https://www.euractiv.com/short_news/cyberattacks-in-lithuania-surged-when-war-in-ukraine-began).

<sup>4</sup> Ibid.

<sup>5</sup> Ibid.



Strategic Communication Department attributed this to Russia's ongoing war against Ukraine, which had the greatest impact on "hostile information activities" targeting Lithuania in 2024.<sup>6</sup>

With Lithuania, Russia also specifically increased its hybrid warfare in 2022 due to the blocking of sanctioned goods being transported into Kaliningrad.<sup>7</sup> This was carried out by the Russian-affiliated hacker group Killnet and resulted in a denial-of-service cyberattack against numerous government platforms.<sup>8</sup> Russian officials praised this attack, stating, "If in the near future cargo transit between the Kaliningrad region and the rest of the territory of the Russian Federation through Lithuania is not restored in full, then Russia reserves the right to take actions to protect its national interests."<sup>9</sup>

Beyond cyber, drone incursions have served as a way for Russia to violate the Baltic states' airspace, test their response rates, and cause regional disruptions. With Russia's proximity to the Baltic, and given the congested airspace around and bordering the Baltics, where there is an abundance of Ukrainian and Russian drones, it is plausible that drones could be accidentally downed in Baltic airspace, which Russia takes advantage of and uses as deniability for any malign intention. There have been at least 24 drone incidents these states have reported since 2025.<sup>10</sup> Resulting in flights being grounded, trains suspended, and in one case a NATO fighter jet being deployed to shoot down a drone.<sup>11</sup>

### Takeaways

These instances demonstrate the disruptions that these cyberattacks can cause, especially for neighboring states. The Ukraine war underscored how quickly technology can develop, making it easier for Russia to make its attacks more sophisticated and immune to existing deterrence efforts, through both conventional and nonconventional means, which can now be carried out cheaply and

---

<sup>6</sup> Venckūnas, Vilmantas. "Lithuania's Defence, Ukraine Aid in Focus of Russian Propaganda in 2024." LRT English, February 27, 2025. <https://www.lrt.lt/en/news-in-english/19/2499437/lithuania-s-defence-ukraine-aid-in-focus-of-russian-propaganda-in-2024-military>.

<sup>7</sup> "Russian Hackers Claim Responsibility for Cyberattack on Lithuania," *Al Jazeera*, June 27, 2022, <https://www.aljazeera.com/news/2022/6/27/russia-hackers-claim-responsibility-for-cyber-attack-on-lithuania>.

<sup>8</sup> Ibid.

<sup>9</sup> Ibid.

<sup>10</sup> Novaya Gazeta Europe. 2026. "At Least 24 Drone Incidents Recorded in Baltic States Since Start of 2025." Novaya Gazeta Europe. May 21, 2026. <https://novayagazeta.eu/en/articles/2026/05/21/at-least-24-drone-incidents-recorded-in-the-baltic-states-since-start-of-2025-en-news>.

<sup>11</sup> Ibid.



Citation: Gingras, Russia's Shadow War

NSM Blog September 2026, <https://new-school-of-multilateralism.uni-graz.at/en/the-nsm-blog>

in mass quantities. This makes collaboration and innovation key to combat Russia's shadow warfare for both the Baltic states and all NATO allies. Reflecting these priorities, the 2026 Ankara NATO summit introduced initiatives to further encourage collaboration and information sharing across the Alliance. One such program, Drone Edge, would strengthen initiatives to not only increase the production of drones but also increase counter-drone capabilities, implementing lessons learned from Ukraine, demonstrating one way NATO allies are adapting their defense posture to address a key pillar of Russia's hybrid warfare.<sup>12</sup> However, as Russia continues to adapt its hybrid tactics and implement emerging technologies, NATO must remain equally adaptable, ensuring that innovation and collective defense evolve just as rapidly.



**Shelby Gingras** is an M.A. student at the George Washington University studying Security Policy Studies concentrating in transnational security, graduating in December 2026. She holds a B.A. in International Relations and has experience interning in government at the state, federal, and international levels, as well as with an NGO. She has also published multiple pieces on Arctic security.



Dive into the blog:

<https://new-school-of-multilateralism.uni-graz.at/en/the-nsm-blog/>

---

<sup>12</sup> North Atlantic Treaty Organization (NATO), *NATO's Drone Edge*, July 7, 2026, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/07/natos-drone-edg>.