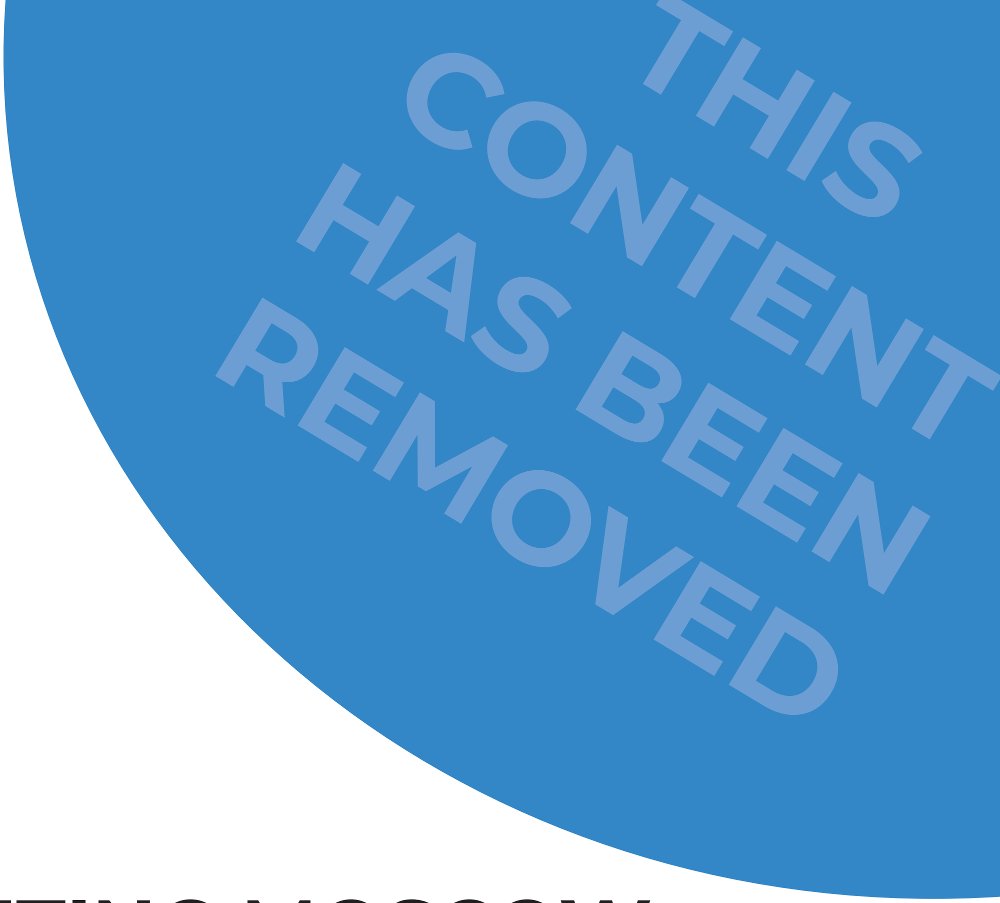
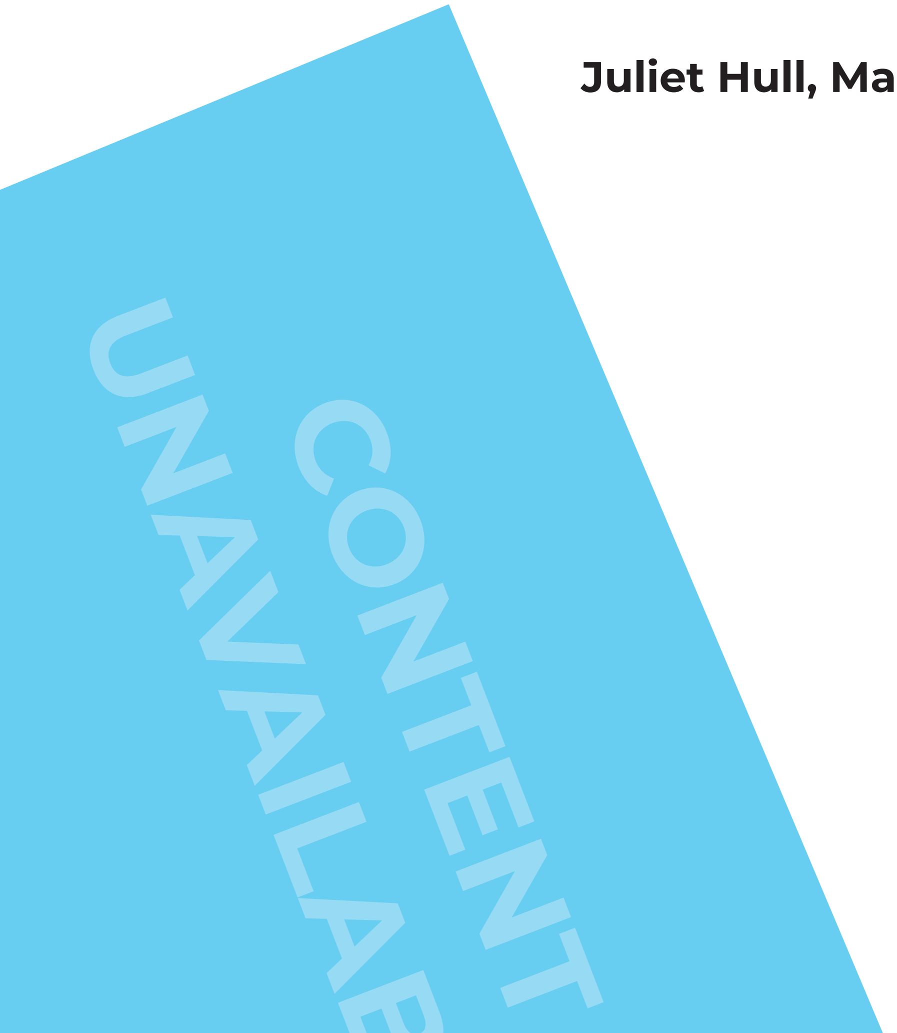


MUTING MOSCOW: EU Regulation No 2022/350 in Estonia

Juliet Hull, March 2025



2

Geopolitical Background

Russian relations with post-Soviet states have been tense since the dissolution of the USSR in 1991. The most distinct manifestation of growing Russian aggression is now of course the war in Ukraine; the violent conflict marks a historic turning point for the conflict and European security as a whole following Russia's annexation of Crimea. Scholars of international relations typically name one of three main motivations as the reason behind Russia's invasion: Putin's desire to 1) regain territory and influence in the face of eastward NATO expansion,[1] 2) subjugate Ukraine for defying Moscow and recover the nation as a bastion of Soviet strength[2] and 3) grow the Russian sphere of influence and realize the image of a "Russkiy Mir" by regaining control over all ethnic Russian majority territory.[3]

While Ukraine's vulnerability to Russian aggression is striking, it is not exceptional. Other Baltic nations – Estonia, Latvia, Lithuania – are also threatened by the Russian fist. This aggression, particularly towards Estonia, has largely been enacted digitally rather than physically, manifesting as cyber attacks and the sabotage of critical civic information and communication technology (ICT) infrastructure. In fact, Estonia is considered one of the first targets of state-on-state cyber attacks – victimized by, unsurprisingly, Russia, in 2007.[4] This attack is considered the "wake-up call" that spurred Baltic nations to become trail blazers in digital security.[8] Following Russia's full scale invasion of Ukraine, such attacks have only intensified across the region. Recently, Google's intelligence experts have warned that Moscow has deployed one of its most elite hacking groups, known as Sandworm, to probe Baltic energy grids for weaknesses.[5] Sandworm is the same strike team that has repeatedly turned off the lights in Ukraine.[6]

Russian attacks on Estonian ICT systems do not only take the form of "hacking," or brute-force digital techniques such as DDoS attacks, botnets, and phishing. Russia's cyber sabotage also includes the physical destruction of essential points of e-capacity and connectivity. This past Christmas, the eleven-ton anchor of a rickety oil tanker the size of two football fields gouged a 60 mile scar along the sea bed floor of the Gulf of Finland, severing the Estonia to Finland Estlink 2 subsea power cable in the process. That ship is believed to be a part of Russia's "shadow fleet" of aging vessels used to evade European sanctions.[7] The Estonia–Finland cross-border electricity was reduced to a third of its normal capacity, causing surges in Estonian electricity prices and tens of millions of euros in repair costs.[8]

The takeaway from this is that the menacing force of Russia is not only felt strongly by Ukraine, but nearby Baltic states as well, particularly through the lens of cybersecurity. It's no surprise then that Baltic states spend more on cybersecurity as a proportion of their GDP than most other NATO member nations. Estonia's cybersecurity funding quadrupled from €3.9 million in 2020 to €16.1 million in 2024.[9] Baltic officials fear they could be the next target of Putin's territorial ambitions if they extend beyond Ukraine.

In Decemember off Porkkalanniemi, Kirkkonummi, in the Gulf of Finland, oil tanker Eagle S (L), which flies under the flag of the Cook Islands, next to tugboat Ukko (R). Retrieved from NPR.[20]

Photo: Jussi Nukari/Lehtikuva/AFP via Getty Images.

EU Regulation No 2022/350

On March 1st 2022, the European Union passed EU Regulation No 2022/350.[10] The goal of this regulation is to restrict Russian disinformation, propaganda, and social engineering campaigns over network broadcast. Russian disinformation and influence operations continues to be a cybersecurity threat for a number of countries – most particularly Baltic States with proximity to Russia and large numbers of ethnic Russian inhabitants – because they have a striking capacity to mislead public opinion, damage political stability, erode societal trust, and destabilize both national governments and greater alliances like NATO and the EU. No 2022/350 is a binding legislative act, and must be applied entirety across the EU. It is in effect, in varying ways and degrees, throughout all EU member states (EUMS). EU regulations are one of the highest-ranking international laws available, and take precedence over individual EUMS national laws.

No 2022/350 amends a previous regulation passed by the EU in 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. No 2022/350 broadens the relatively narrow scope of former provisions, imposing new restrictive measures against Russian media outlets engaged in propaganda actions and stating that all restrictive measures are to be maintained until Russian aggression ceases. The regulation states that Russian-owned media outlets have channelled disinformation campaigns to destabilize neighbouring Baltic Countries, influence European political parties and Russian ethnic minorities throughout Europe, and justify its aggression against Ukraine, constituting a "significant and direct threat to the Union's public order and security."[10]

With respect to the Charter of Fundamental Rights, the EU's guiding constitution (which outlines inalienable rights such as the freedom of expression, information, and to conduct a business), the regulation introduces an urgent suspension of the broadcasting activities of such media outlets in the Union (ie by EUMS) or directed at the Union (ie by Russia).The regulation notes that there are no additional restrictions on other activities other than broadcasting, such as research and interviews.[10]

No 2022/350 in Action: Estonia

Protecting against Russian disinformation in Estonia requires securing networks and ensuring the integrity of online content to prevent malicious state actors from exploiting information to achieve harmful objectives. One of the key factors that contributes to Estonia's resilience is the country's view that disinformation is a security threat and should be treated as such. Estonia's 2017 National Security Concept identifies the tactics of strategic communication (defined as communication meant to improve the cohesion of society) and psychological defense (efforts to inform Estonians about harmful information-related activities) as important strategies in countering false narratives.[11]

While the vast majority of political, social, and cultural content is freely available to users, Estonia employed No 2022/350 to block hundreds of websites. According to information provided by the Estonian Consumer Protection and Technical Regulatory Authority (TTJA), 307 websites and 53 television channels remained blocked in Estonia as of May 2024.12 Affected Russian state-controlled networks and websites include Russia Today (including its subsidiary networks such as RT France and RT Germany) and the Sputnik News Agency.[10] Prolonged sanctions spanning across the EU include disinformation outlets regularly disseminating propaganda in support of Russia's aggression against Ukraine, including RTR-Planeta, Russia 24, and TV Centre International.[13] Between July and December 2023, Facebook restricted access in Estonia to 82 items for alleged violations of local laws and 100 items that violated EU sanctions on Russian state-controlled media.[14] Google received five requests from the Estonian government to remove a total of nine pieces of content during that same period, and removed eight of the requested items.[15]

While removing many Russian-owned networks from the airwaves and internet, Estonia has adapted its media sector to present alternatives for ethnic Russian residents by creating Estonian-made news content in the Russian language, such as the Estonian Public Broadcasting (ERR) Russian-language radio and TV channel. The aim of these platforms is to bring Russian-speakers into the broader Estonian media sphere while countering the risk of Russian-state propaganda.[16] Estonia has also developed a reputation on the international stage for its heavy focus on media literacy education in an effort to combat disinformation. At all levels of education, Estonian classrooms incorporate media literacy into their lessons. These efforts have resulted in Estonia having some of the highest media literacy levels in Europe.[17]

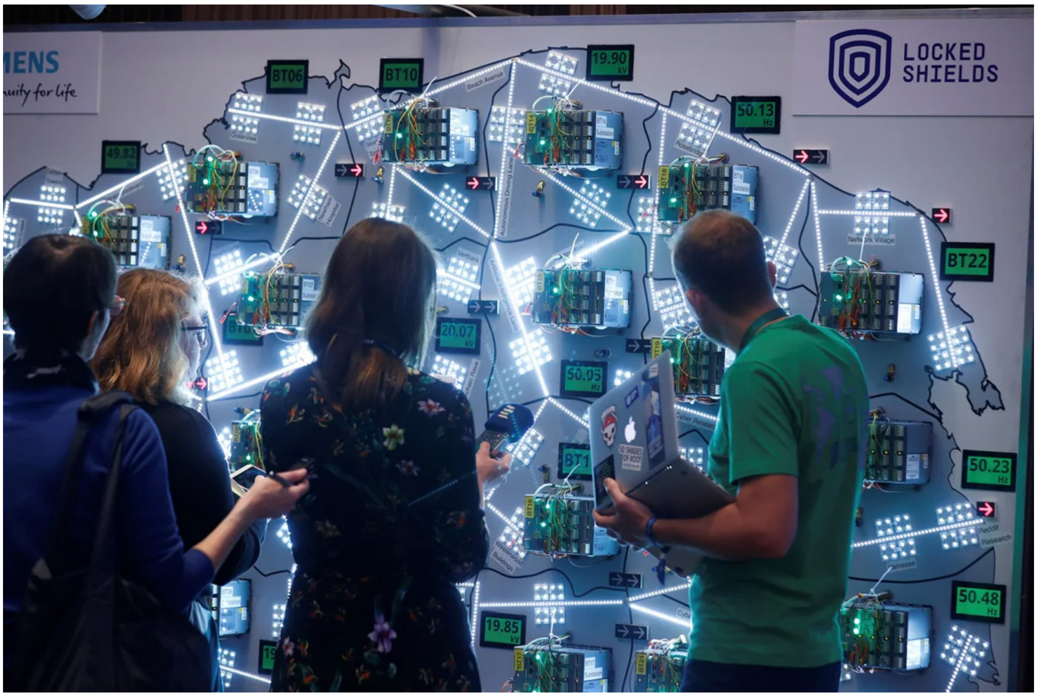
Efficacy of No 2022/350

No 2022/350 is a necessary and largely beneficial law, given the heightened threat of Russian disinformation since the full-scale invasion of Ukraine. The law equips the Estonian government with a greater arsenal of content moderation powers. For example, a post spread on social media in March 2024 used statistics published on the Russian Ministry of Defence's Telegram channel to falsely claim that Estonia had sent 190 "mercenaries" to fight in Ukraine. Though the post had limited reach, fact-checkers labelled it as "Russian propaganda."[21]

Equipping the Estonian government with stronger content moderation powers is essential in countering false narratives that could destabilize public trust or incite hostility toward vulnerable groups, such as Ukrainian refugees. This is particularly salient considering Estonia's information society and the degree of digital interconnectedness between the government, private sector, and individual citizens. While free speech concerns are always worth considering, the strategic use of this law to debunk and limit the spread of harmful misinformation seems justified in Estonia's current security landscape – it's not just a question of security, but sovereignty.

That said, the law has not been entirely effective in eliminating disinformation, nor was that ever the realistic expectation. Soon after the invasion, false information about Ukrainians attacking Russians in Estonia was shared across Facebook and Instagram.[18] In August 2022, Estonian authorities acknowledged that the spread of disinformation, which often sought to stigmatize Ukrainian refugees living in the country, had increased significantly since the invasion, particularly on Telegram.[19] Generally, disinformation is evident in Estonian online channels. In September 2020, the Global Disinformation Index (GDI) found that one quarter of Estonian media sites presented a high risk of spreading disinformation to their online readers. Some of these sites were based in Russia, and they were not part of Estonia's mainstream media market.[20]

Promulgating up-to-date, effective laws that are capable of combating Russian threats will be a prevailing challenge. As always, laws are iterative and never absolutely capable of eradicating the behavior they intend to discourage. Yet Estonia's cybersecurity and media literacy landscape is a testament to resilience in the face of aggression – despite its small size, Estonia is weathering Russian threats through its innovative policy and legal landscape, accepting calculated risks with the support of international organizations and allies.



People look at the visualisation during the Locked Shields, cyber defence exercise organized by the NATO Cooperative Cyber Defence Centre of Exellence in Tallinn. Via CNN. [21]

Photo: Inta Kalnins/Reuters.

Works Cited

1. “Why NATO and Ukraine are a flash point with Russia 30 years after the end of the Cold War,” PBS, February 2022, https://www.pbs.org/newshour/world/why-nato-and-ukraine-are-a-flash-point-with-russia-30-after-the-end-of-the-cold-war.

2. Reynolds, Maura. “‘Yes, He Would’: Fiona Hill on Putin and Nukes,” Politico, February 28 2022, https://www.politico.com/news/magazine/2022/02/28/world-war-iii-already-there-00012340.

3. Young, Benjamin R. “Putin Has a Grimly Absolute Vision of the ‘Russian World’,” Foreign Policy, March 6 2022, https://foreignpolicy.com/2022/03/06/russia-putin-civilization/.

4. Traynor, Ian. “Russia accused of unleashing cyberwar to disable Estonia,” The Guardian, May 16 2007. https://www.theguardian.com/world/2007/may/17/topstories3.russia.

5. Clark, Sam and Victor Jack. “Baltics brace for cyberattacks as they depart Russian electricity grid,” Politico, February 5 2025, https://www.politico.eu/article/baltics-brace-cyberattacks-depart-russian-electricity-grid-brell/.

6. Ken Proska, et al. “Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology,” Google, November 9 2023, https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/.

7. Schuler, Mike. “Baltic Sea Cable Probe: Finnish Investigators Suspect Shadow Tanker ‘Eagle S’ Dragged Anchor for Over 60 Miles,” G Captain, January 9, 2025, https://gcaptain.com/baltic-sea-cable-probe-finnish-investigators-suspect-shadow-tanker-eagle-s-dragged-anchor-for-60-miles/.

8. GZero Media. “Russia’s next target? Why the Baltics are wary of Putin | Ian Bremmer Explains.” YouTube, February 28 2025, https://www.youtube.com/watch?v=bAFP2a9gPKU.

9. “Cybersecurity Strategy 2024–2030: Cyber-Conscious Estonia,” DigWatch, February 2024, https://dig.watch/resource/cybersecurity-strategy-2024-2030-cyber-conscious-estonia#:~:text=Estonia’s%20cybersecurity%20funding%20increased%20from,financial%20incentives%20and%20regulatory%20measures.

10. “Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia’s actions destabilising the situation in Ukraine,” Official Journal of the European Union, Vol 65, No 2, March 2 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:065:FULL&from=EN.

11. Walsh, Sophia. “Combatting Russian Disinformation: Estonia’s Response to the War in Ukraine,” Democratic Erosion Consortium, August 13, 2023, https://www.democratic-erosion.com/2023/08/13/combatting-russian-disinformation-estonias-response-to-the-war-in-ukraine/.

12. Official website of the Consumer Protection and Technical Regulatory Authority, https://ttja.ee/ariklient.

13. “Content restrictions based on local law: Estonia,” Facebook, https://transparency.facebook.com/content-restrictions/country/EE.

14. “Government requests to remove content: Estonia,” Google, https://transparencyreport.google.com/government-removals/government-requests/EE

15. Walsh, Sophia. “Combatting Russian Disinformation.” https://www.democratic-erosion.com/2023/08/13/combatting-russian-disinformation-estonias-response-to-the-war-in-ukraine/

16. “Estonia ranks 4th in Media Literacy Index 2022.” Education Estonia. https://www.educationestonia.org/media-literacy-index-2022/

17. Iver Tambur and Sten Hankewitz, “Fake news about Ukrainians attacking Russians in Estonia circulate in social media, while Russia warns the Baltics,” Estonian World, March 5, 2022, https://estonianworld.com/security/fake-news-about-ukrainians-attacking-russians-in-estonia-circulate-in-social-media-while-russia-warns-the-baltics/.

18. “The Online News Market in Estonia ,” Global Disinformation Index, September 30, 2020, https://www.disinformationindex.org/country-studies/2020-9-30-the-online-news-market-in-estonia/

19. Malts, Kaili, “FAKTIKONTROLL | Eesti ei ole sõdureid Ukrainasse saatnud - tegemist on Vene propagandaga [FACT CHECK | Estonia has not sent soldiers to Ukraine - this is Russian propaganda],” Delfi, March 25, 2024,https://epl.delfi.ee/artikkel/120280462/faktikontroll-eesti-ei-ole-sodureid-ukrainasse-saatnud-tegemist-on-vene-propagandaga.

20. Rosman, Rebecca. “What to know about Finland, Russia’s ‘shadow fleet’ and a severed undersea cable,” NPR, December 31, 2024, https://www.npr.org/2024/12/31/nx-s1-5243302/finland-russia-severed-undersea-cable-shadow-fleet

21. Ivana Kottasová. “How Russian threats in the 2000s turned this country into the go-to expert on cyber defense,” CNN, June 18, 2021, https://www.cnn.com/2021/06/18/tech/estonia-cyber-security-lessons-intl-cmd/index.html