NATO
ENERGY SECURITY
CENTRE OF EXCELLENCE

The Hidden Threat to Baltic Undersea Power Cables

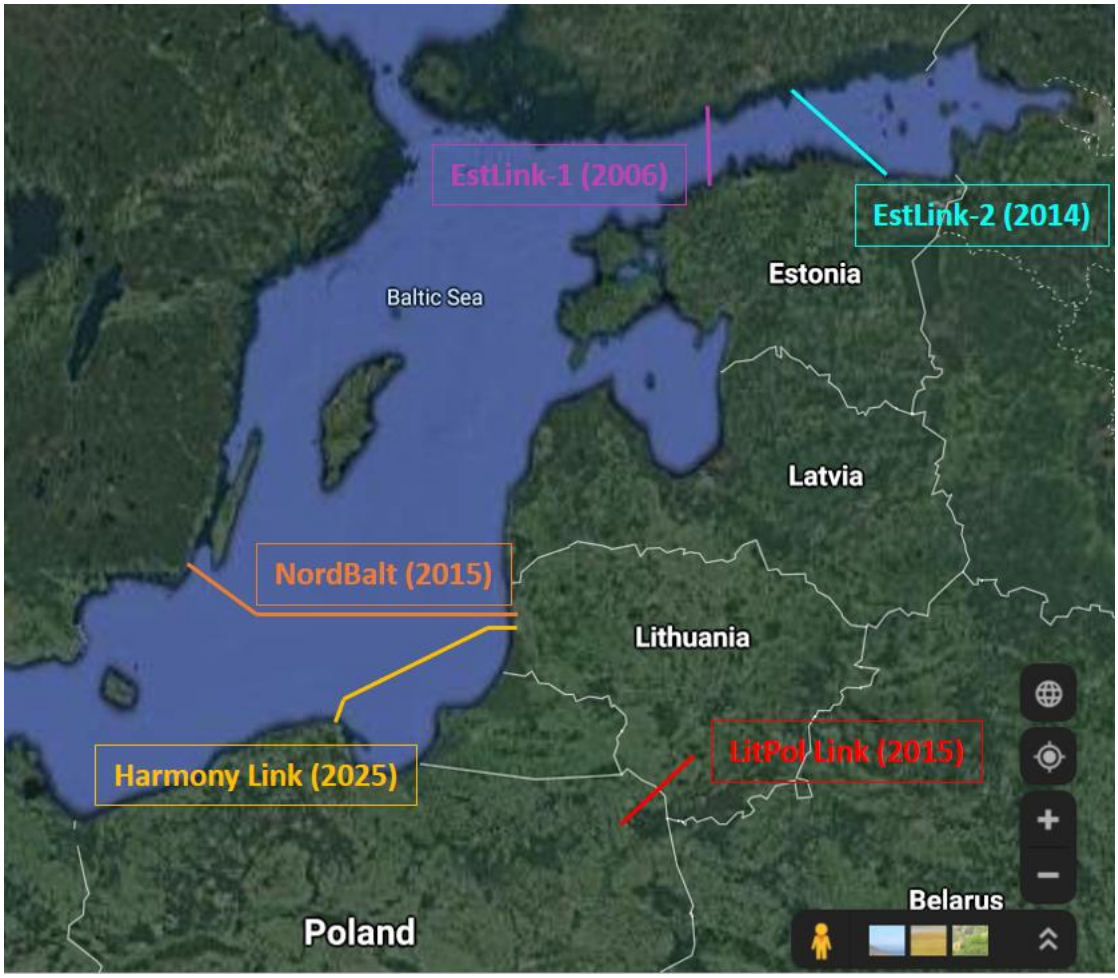
By Lukas Trakimavičius

Introduction

In recent years much ink has been spilled discussing the vulnerabilities of transatlantic internet cables, amid growing concerns that countries like Russia could disrupt them in times of conflict.[1] However, internet cables are not the only underwater objects that may be at risk. The same forces that could disrupt transatlantic internet cables might also threaten electric power transmission cables on the bottom of the Baltic Sea. If submarines or other naval vessels would target multiple power cables simultaneously, this might spell trouble for the three Baltic States.

To address the lack of domestic electricity production capacity, to diversify electricity import routes away from Russia and Belarus, and to facilitate the integration with the European Union energy markets, Estonia, Latvia and Lithuania have over the past decades made significant investments in new power interconnectors. Between 2006 and 2015, they have built four power links with Central and Northern Europe: one overhead transmission line with Poland (the 500 megawatt (MW) "LitPol Link"), one submarine power cable with Sweden (the 700 MW "NordBalt") and two submarine power cables with Finland (the 350 MW "EstLink-1" and the 650 MW "EstLink-2").

Lukas Trakimavičius works at the Research and Lessons Learned Division of the NATO Energy Security Centre of Excellence. Previously, he worked at the Economic Security Policy Division of the Lithuanian Ministry of Foreign Affairs. He also held several positions at NATO, where he focused on energy security, arms control, disarmament and non-proliferation



Main Baltic power interconnectors (Credit: Google Earth/L. Trakimavičius)

As things stand right now, all three Baltic States are net electricity importers. In 2020, they consumed a total of 28.3 terawatt-hours (TWh), produced 15.2 TWh, and ran a combined electricity deficit of 13.1 TWh.[2] Out of the three countries, Lithuania (7.9 TWh) was by far the most dependent on electricity imports, followed by Estonia (3.6 TWh) and Latvia (1.6 TWh). Most of their electricity imports came from Russia, Finland and Sweden.

Going forward, to enable the intended Baltic desynchronization from the Russian-led BRELL (Belarus, Russia, Estonia, Latvia and Lithuania) ring and the subsequent synchronization with the continental European network, the Baltics have decided to commission an additional submarine power cable – called "Harmony Link" – between Poland and Lithuania.[3] Once this new 700 MW power cable is up and running in 2025, the Baltics will decommission old Soviet-era land power cables, halt electricity trade with neighbouring Russia and Belarus, and rely for the bulk of their electricity imports on submarine power cables.[4]

While from an energy security point of view these steps will make the Baltics more independent from Russia than ever before, their growing reliance on submarine power cables might also expose them to new security risks.

Submarine power cables may be at risk from a wide array of threats, including anchoring, trawling or even terrorist attacks. However, there is also concern is that in the event of a political crisis, countries like Russia could use their naval forces to target multiple Baltic submarine power cables simultaneously, potentially causing supply disruptions or even grid failures.

Russia's naval capabilities

Despite Russia's best efforts of keeping it under wraps, there is ample evidence of the presence of a formidable military fleet of special purpose vessels located in Olenya Guba, on the coast of the Barents Sea.[5] Operating under Russia's Main Directorate for Deep Sea Research (known as GUGI in Russian), these vessels include traditional submarines, intelligence ships and auxiliary submarines, some of which are capable of disrupting undersea cable infrastructure.[6]

Olenya Guba naval base (Credit: Google Earth/ L. Trakimavičius)

Most importantly, Olenya Guba houses "special mission ships" or "oceanographic vessels" (both euphemisms for a reconnaissance vessel) like the project 22010-class ship "Yantar". These high-tech ships are capable of carrying manned deep-diving submersibles or drones for undersea engineering missions. Such missions, it is thought, may include cable cutting, laying of taps on undersea cables and other special tasks.[7]

In fact, few Russian ships have gained as much notoriety as "Yantar". Over the years, it was spotted off the east coast of the United States and Canada, near Portugal and in the Mediterranean, among other places.[8] It reportedly spent a lot of time hanging out around underwater internet cables, thereby raising concerns among Western officials about the nature of these missions and Russia's broader objectives.[9]

Granted, in the public domain there is no proof to suggest that Russia's special purpose vessels would have carried out any illegal operations against Western countries or their underwater internet cables. Yet, it is a fact that Moscow has actively been investing in advanced underwater military capabilities, which, in the event of a crisis, might pose a threat to the security interests of NATO member states and their partners.

Impact on Baltic energy security

There are no doubts that the same Russian forces that could disrupt transatlantic internet cables might also pose a challenge to Baltic submarine power lines. After all, in terms of depth and size, the Baltic Sea is but a pond compared to the Atlantic Ocean. And underwater attacks against power lines could prove to be effective, low-cost and low-intensity tools of power, where attribution is difficult, if not impossible.

But the important question is: how exactly might these disruptions affect Baltic energy security?

While it is difficult to provide a clear-cut answer to this question (an event like this has never happened before), it is possible to come up with at least three entirely hypothetical scenarios, which could be broken down based on the severity of their potential impact.

First, if one or two submarine cables would be cut between now and 2025, the overall impact on Baltic energy security would likely be quite negligible. The immediate power shortage could be covered by a combination of increased electricity imports from Poland and Russia (if Moscow would deny its responsibility and would be willing to cooperate), and a surge in domestic power generation. Depending on the weather conditions and availability of repair equipment, the submarine power cables could likely be fixed within weeks or a couple of months at most, and any lasting damage would be avoided.

Second, if the submarine power cables would be disrupted after the Baltics have left the BRELL ring, the situation might be more difficult, but not overwhelmingly so. Though currently it seems that in the Baltics more aging power plants are scheduled to be closed than new ones built, there is good reason to believe that by 2025, Estonia, Latvia and Lithuania would have enough reserve power generation capacity to withstand most supply shocks.[10] Lithuania, for instance, is planning to build one of the largest battery storage systems in the world by the end of 2021, and, in the coming years, it also intends to significantly increase its renewable energy generation capacity.[11] Such and other initiatives, coupled with the soon-to-be expanded "LitPol Link", would likely ensure an adequate supply of electricity even in a time of crisis.[12]

Third, if the submarine power cables were cut as part of a broader hybrid warfare campaign, it could have more serious consequences for the energy security of the Baltics, regardless whether it's pre- or post-2025. If, for example, the physical attacks against power lines would be accompanied by a series of coordinated cyber-attacks against the critical energy infrastructure of the Baltic States, it could cause large-scale grid disruptions. In such an event, it might become difficult for the transmission system operators to balance the load of the power grids or to keep

them running properly. Needless to say, all of this could result in supply shortages, cascading failures or even power blackouts.

Granted, the third and most risky scenario is also by far the least likely one. Not only because it would require a serious escalation in East-West tensions, but also because a cyber-attack campaign of such magnitude would have to be the result of years of painstaking planning on the behalf of the aggressor. Besides, grid operators usually run robust cyber-security protocols and often have sufficient redundancy to withstand component failure. This means that the hackers would have to get lucky a rather improbable number of times to achieve their intended outcome of simultaneously disrupting all three Baltic States.

As the Baltic energy landscape evolves, old security challenges will be overcome and new ones will inevitably arise. In the coming years submarine power cables will play an even greater role in ensuring Baltic energy security, but they might also expose them to new vulnerabilities. Though the Russian naval threat against Baltic power lines is arguably not as great as it is against transatlantic internet cables, underwater attacks could still prove to be a challenge, especially if accompanied by other hybrid threats.

---

[1] Brzozowski, Alexandra, "NATO seeks ways of protecting undersea cables from Russian attacks", *EurActiv*, 23 October 2020, https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/

[2] "2020 metais Baltijos šalims stigo 46 proc. Elektros", *DELFI*, 18 January 2020, https://www.delfi.lt/verslas/energetika/2020-metais-baltijos-salims-stigo-46-proc-elektros.d?id=86259763

[3] "Brussels approves 'unprecedented' funding for Baltic energy security", *LRT English*, 2 October 2020, https://www.lrt.lt/en/news-in-english/19/1244658/brussels-approves-unprecedented-funding-for-baltic-energy-security

[4] "Synchronization with continental Europe", *Elering*, https://elering.ee/en/synchronization-continental-europe

[5] Nilsen, Thomas, "From this secret base, Russian spy ships increase activity around global data cables", *The Barents Observer*, 12 January 2018, https://thebarentsobserver.com/en/node/3381

[6] Sunak, Rishi, "Undersea Cables: Indispensable, Insecure", *Policy Exchange*, 1 December 2017, https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf

[7] H I Sutton, "Russian ship loitering near undersea cables", *Covert Shores*, 13 September 2017, http://www.hisutton.com/Yantar.html

[8] Mizokami, Kyle, "What Is a Russian Spy Ship Doing in the Eastern Mediterranean?", *Popular Mechanics*, 19 September 2017, https://www.popularmechanics.com/military/navy-ships/a28276/yantar-spy-ship-eastern-mediterranean/

[9] "Concern over Russian ships lurking around vital undersea cables", *CBS News*, 30 March 2018, https://www.cbsnews.com/news/russian-ships-undersea-cables-concern-vladimir-putin-yantar-ship/

[10] "The Baltic region needs new power plants for after 2025", *Central Europe Energy Partners*, 16 June 2017, https://www.ceep.be/baltic-region-needs-new-power-plants-2025/

[11] Sytas, Andrius, "Lithuania to build one of the largest battery parks in the world", *Reuters*, 8 October 2020, https://www.reuters.com/article/lithuania-battery-idUSL8N2GZ280 ; "Government reaches a decision on the Baltic Sea territory where wind turbines will be constructed", *Lithuanian Ministry of Energy*, 23 June 2020, https://enmin.lrv.lt/en/news/government-reaches-a-decision-on-the-baltic-sea-territory-where-wind-turbines-will-be-constructed

[12] Navakas, Naglis, "Sinchroninis darbas su Lenkija – iš bėdos ir nuo 2021 m.", *VZ*, 12 March 2019, https://www.vz.lt/energetika/2019/03/12/sinchroninis-darbas-su-lenkija--is-bedos-ir-nuo-2021-m