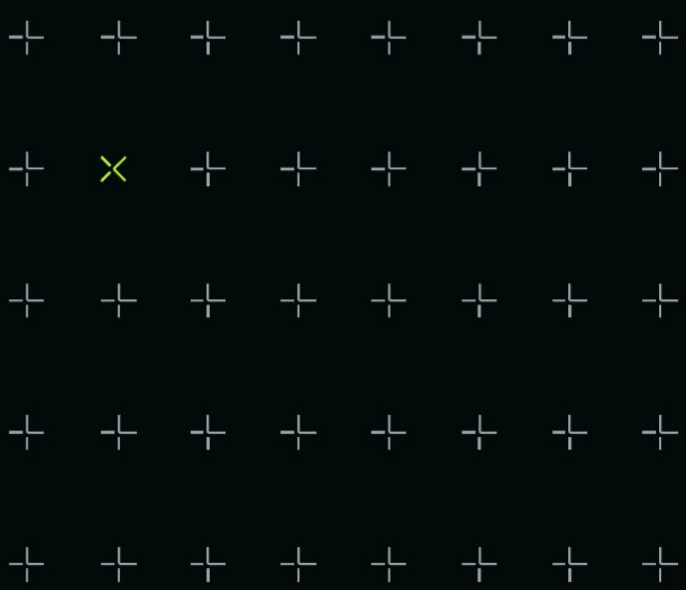
Cyber Cert Labs

Threat Intelligence Report:

The Russian Threat to Undersea Infrastructure



05.09.2023 TLP: AMBER

cybercertlabs.com

Strategic Overview

The following is a quote taken form the Forward of the National Risk Assessment[1] 2023:

"*Despite the risk of a pandemic and a breakdown in international peace having been included in previous iterations of the National Risk Assessment, the occurance of such risks remained almost inconceivable in our minds as they were something many of us had not experienced in our lifetimes. However, life has taught us the lesson of not underestimating the likelihood or the impact of risks, no matter how implausible they may initally seem.*"

Since the Russian invasion of Ukraine in February 2022, NATO and the European Union have continued to support Ukraine with humanitarian and military assistance in its resistance to the invasion. As a result European countries including Ireland are viewed as legitimate targets by Russia for offensive cyber security operations.

Since the start of the war cyber threat intelligence has pointed to a new hybrid warfare strategy by Russia where cyber and kinetic attacks are combined[2] to maximise the impact of the attack. Recent intelligence from NATO and other sources has confirmed that the Russian navy and auxiliary Russian maritime resources have been engaged in exercises to map undersea infrastructure such as subsea Internet fibre and electricity connectors in the North Sea, Baltic Sea and the Atlantic Ocean west of Ireland. The purpose of these exercises is interpreted by the intelligence as prelude to potential sabotage operations in the future, similar to the attacks in the NordStream[3] subsea gas pipelines in 2022.

The threat to the island of Ireland in relation to any potential sabotage of subsea Internet fibre infrastructure is elevated as several mapping exercises have already been conducted by the Russian navy and auxiliary Russian maritime resources as confirmed in the NATO – EU assessment. There have been a number of instances[4] where vessels with both undersea mapping capabilities as well as submersible capabilities have been tracked by the Irish navy and airforce.

Threat Landscape

In April 2023 the UK National Cyber Security Centre (NCSC) issued an updated bulletin on the Russian cyber threat citing new intelligence related to potential attacks against Critical National Infrastructure (CNI)[5]. While the report does not give specific details it does point to a broadening escalation of the offensive cyber security operations by the GRU (Russian Military Intelligence) and the SVR (foreign Intelligence) against European targets.

---

1 https://www.gov.ie/en/press-release/311d3-government-publishes-national-risk-assessment-2023-outlining-top-strategic-risks-facing-ireland/#

2 https://www.bbc.com/news/technology-61396331

3 https://www.irishtimes.com/life-style/2022/10/01/give-me-a-crash-course-in-the-nord-stream-leaks/

4 https://www.irishtimes.com/ireland/2023/03/31/russian-ships-return-to-west-coast-despite-appearing-to-depart-for-africa/

5 https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups

Given Ireland's lack of a dedicated domestic intelligence agency to monitor and gather intelligence on Russian operations, coupled with a lack of sufficient maritime (naval and airforce) capability to appropriately monitor our maritime space make Ireland a potential target for a hybrid cyber attack.

Remarks[6] by the Russian ambassador to Ireland Yuriy Filatov, regarding the death of an Irish citizen who had travelled to Ukraine to fight may be laying a justification pretext to any future activity. These remarks[7] are similar to previous remarks made when the Irish Taoiseach travelled to Ukraine in July 2022.

On the 3rd of May The Times in the UK published an article[8] that adds additional intelligence to the Russian threat to undersea cables in the North and Baltic Sea. Four Nordic public broadcasters led by DR, Denmark's state-owned radio and TV company, published details on analysis of Russian navy movements prior to the destruction of the Nord1 and Nord2 gas pipelines in September of 2022. This intelligence indicates that the Russian Navy mined both pipelines prior to destroying them. The intelligence also indicates that the Russian navy may have already mapped and targeted other undersea infrastructure. If this is the case then the potential impact of future attacks particularly on undersea power and Internet infrastructure could be more impactful than cutting these cables as multiple installations could be targeted in a single attack.

On 11th January 2023 the President of the European Commission and the Secretary General of NATO announced the establishment of a dedicated NATO-EU Task Force on the resilience of critical infrastructure. Ireland is now an active participant in the new taskforce[9].

On the 4th of May the Nato Secretary General Jens Stoltenberg met[10] with industry leaders in energy and communications infrastructure discussed NATO's role in contributing to the security of critical undersea infrastructure and cooperation with industry. NATO has also recently created an undersea infrastructure coordination cell to map vulnerabilities, and coordinate efforts between NATO Allies, partners, and the private sector.

On June 23rd 2023 the Taskforce published its Final Assessment Report[11] on the resilliance of Critical Infrastructure. The following is an exerp from this report "*Russia has already demonstrated that it sees critical infrastructure as a target through its actions in Ukraine. It is also mapping critical infrastructure in the Euro-Atlantic area, which it could target. Russia and groups associated with it have used cyber attacks as a means to disrupt essential services in the Euro-Atlantic area*"

---

6 https://www.irishexaminer.com/news/arid-41127799.html

7 https://www.irishexaminer.com/news/arid-40915835.html

8 https://www.thetimes.co.uk/article/nord-stream-pipeline-report-russia-putin-ships-site-explosion-3xx50vgbh

9 https://www.irishtimes.com/ireland/2023/05/04/nato-warns-ireland-over-russian-maritime-surveillance-activity/

10 https://www.nato.int/cps/en/natohq/news_214322.htm?selectedLocale=en

11 https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

TheTaskforce outlined 14 recommendations in their final assessment, number 8 is "*Exploring possibilities for exchanges on how to improve the monitoring and protection of critical infrastructure in the maritime domain by relevant authorities, and discussing ways to enhance maritime situational awareness;*"

The National Risk Assessment was published in July 2023 outlining the overview of strategic risks for Ireland. It reminds us that Ireland has positioned itself as a digital leader and an attractive target for attackers due to the presence of significant data infrastructure. The national reputation and reputations of the organisations based here that depend on this maritime infrastrature are at increased risk of failures that could lead to major societal disruption. This risk is particularly important for Ireland given our role as a host to data centres and other data infrastructure which plays a critical role in international digital services.The national risk assessment calls out maritime infrastructure specifically as a technology risk.

A recent newspapaer article[12] in the Financial Times on 3rd August 2023 quotes the Taoiseach Leo Varadkar admitting Ireland must do more to defend its waters from Russian sabotage. Conversely an Irish Times newspaper report on 23rd August 2023 discussed the mass exodus of naval personnel to the private sector due to pay and conditions. Two ships have been withdrawn from services due to personnel shortages and in the past 4 years the navy has gone from 9 ships with the current ships out of commission a total of 2 ships to patrol the Irish waters. This lack of monitoring and patrol increases the threat level.

Another article[13] published by ForeignPolicy.com is more daming of the Irish Naval capability and the inability for Ireland to protect its own sovernity and the 75 percent of trans-Atlantic undersea cables passing through or near Irish waters. It refereces the Commission on Defense Forces reports[14] in which there are two significant recomendations made speacifically on Maritime defence. To engage more deeply on the implemntation of the EUs Maritime Security Strategy and powers required by the Naval Service for effective enforcement, in support of national security, in the maritime domain should be addressed.

Threat Overview

The Russian invasion of Ukraine in 2022 and the subsequent war have created conditions where the Russian Navy (both military and civilian) in conjunction with the GRU and SVR may be exploring opportunities to conduct offensive cyber security attacks on European nations in response to their support to Ukraine in defence of their nation. Recent activity in March and early April off the west coast of Ireland indicates that the Russian navy may be exploring the option to sabotage undersea internet cables that connect the island of Ireland to the public Internet.[15] This activity is potentially part of a broader campaign to

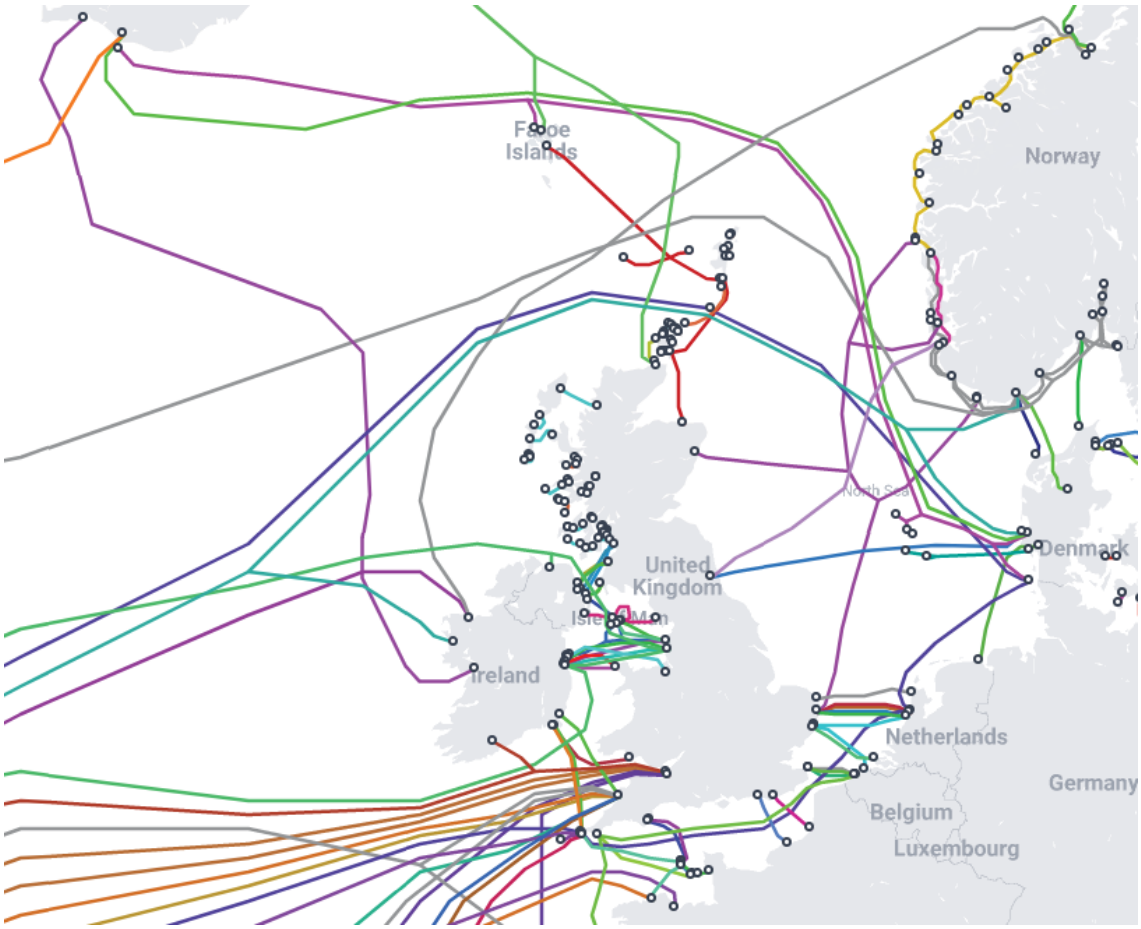
[12] https://www.ft.com/content/bfb26fd9-c1f5-49af-af97-f70351b20451

[13] https://foreignpolicy.com/2022/11/08/ireland-military-neutrality-russia-ocean-communication-energy-infrastructure-sabotage/

[14] https://www.military.ie/en/public-information/publications/report-of-the-commission-on-defence-forces/report-of-the-commission-on-defence-forces.pdf

[15] https://www.rte.ie/news/2023/0401/1367621-russia-ships-ireland/

target European undersea internet cables in the North Sea and the Baltic Sea[16] targeting the UK, Denmark, Sweden and Finland.[17] If the threat is realised and a number of undersea internet cables were to be cut then connectivity to the public Internet from the island of Ireland would be impacted. Based on the connectivity to mainland Great Britain and onwards from Great Britain to continental Europe means that the island may not be completely cut off from the public Internet. However any reduction in the overall capacity of public Internet connectivity could result in the remaining connectivity being overwhelmed with traffic. It is not clear exactly what the extent of the impact would be but it may include partial or complete connectivity loss to the public Internet for the whole of the island. An overview of the connectivity from the island of Ireland to the public Internet is shown in the image below:



The connectivity on the west and southwest coast of the island are the main connections both transatlantic and to continental Europe. The connectivity to the east of the island is mainly to mainland Great Britain.

There is no specific intelligence that the threat to undersea cables could be escalated by also coordinating a wider attack on critical services or infrastructure but this could be a possibility. A wider more focused campaign could include prepared malware or wiper

16 https://www.bbc.com/news/world-europe-65309687

17 https://www.rte.ie/news/uk/2023/0420/1378007-uk-russia-ship/

campaigns that may not need command and control connectivity to be launched.

Shetland Island Incident

On the 22nd of October 2022 the Shetland Islands in the United Kingdom suffered a major internet outage when the SHEFA-2 undersea cable connecting the island to both the Faroe islands and mainland Scotlans was cut[20]. The cable was cut in two places[21] severing both the connection to the Faroe islands which provides transatlantic connectivity and to the Scottish mainland which provides European connectivity. This effectively cut the island off from the public Internet. While previous incidents have been attributed to legitimate maritime activity such as trawling, this incident is highly unusual as the cable was cut in two places that are geographically relatively far apart. This incident provides an insight into the likely effect if the threat to undersea cables off the west coast of Ireland were to materialise.

Russian Presence in Ireland

The Russian embassy located on Orwell Road covers a site of approximately 5.5 acres and has an approximate staff of 30 registered diplomatic personnel. Given the relatively low volume of trade between Ireland and Russia and the relatively low numbers of Russian nationals in Ireland this is a significant site and staffing levels.

In 2015 Dún Laoghaire-Rathdown County Council granted planning permission for a significant redevelopment of the site which included additional buildings and a large underground complex. Also included in the permission were an underground car park, large water storage tanks and a dedicated ESB substation, indicating that the embassy would be able to continue to function even if water and power were cut off.

In March 2020 before substantial work could commence the Minister for Housing Eoghan Murphy signed an order to revoke parts of the permission on national security grounds.[22] The size and scale of the underground complex indicated that the complex would be used for purposes other than diplomatic relations and consular services.

The three buildings that can be seen in the google satellite image to the rear of the site are new buildings that were contained in the original permission. As you can see from the image the site remains under active development at the time of this satellite image.

[20] https://techblog.comsoc.org/2022/11/05/was-russia-or-a-fishing-trawler-responsible-for-shetland-island-cable-cut/

[21] https://www.bbc.com/news/uk-scotland-north-east-orkney-shetland-63326102

[22] https://www.rte.ie/news/primetime/2022/0310/1285699-russian-embassy-orwell-road-irish-government

As Ireland has no dedicated national intelligence agency it is possible that Russia views Ireland as a safe place to recruit, train and deploy agents both domestically and across the EU. With a porous border to the United Kingdom through Northern Ireland, Ireland also provides a more clandestine way to operate in the United Kingdom[23]. It has been speculated that the GRU operates a forward operating base (FOB) from the embassy and that the planning permission to expand the embassy facilities including the underground complex were to expand and enhance the capabilities of the FOB.

Technical Threat Analysis

Ireland as an island nation relies almost exclusively on subsea Internet cables for connectivity to the public Internet beyond networks directly connected on the island. In terms of national connectivity between the main Internet Service Providers (ISPs) and other operators of Autonomous Systems (AS) the INEX (Irish Neutral Exchange) provides a neutral exchange for these operators to provide network peering arrangements. Also a number of operators also have direct peering arrangements. In theory these peering arrangements would not be affected in the event of subsea Internet cables being cut and traffic should flow normally between these ASs. However it should be noted that Border Gateway Protocol (BGP) tables may readjust in the event of subsea Internet cables being cut as BGP announcements from peers that normally transit these cables will cease. It is not certain that this would not have an effect on peering arrangements on the island.

Potential Impacts

Overall the potential impact to the island of Ireland is difficult to predict but if enough subsea cables are cut then it is probable that there will be widespread outages of public Internet connectivity across the island. As seen with the incident on the Shetland Islands the duration of the outage could be significant taking days or even weeks to restore full connectivity. If the attack targets more than just the island of Ireland and also seeks to cut undersea cables in the North and Baltic Seas then the impact and duration could be even more significant.

---

[23] https://www.thetimes.co.uk/article/ireland-vulnerable-to-russian-espionage-with-many-spy-agents-likely-to-be-across-the-country-already-l8ps2wv7r

Recommendations

1. Impact Assessment

We recommend that each entity assess the impact of this threat on their organisation to discover what the specific risks to their operations may be and if any mitigation against this threat is already in place.

2. Critical or Important Business Services

We advise that the organisation investigate if there are any network connectivity elements related to the critical or important business services that involve extra-territorial connectivity. Map what the potential impact may be and investigate if any alternative connectivity can be implemented to limit the scope of the impact. Consider an incident response scenario for each critical or important business service.

Through our work with clients we have identified that access to critical applications should not depend on all DNS lookups for the URLs requiring transatlantic communications as their only method. Similarly corporate domains used for corporate communications configured in this way would leave an organisation exposed to the threat if disruption to transatlantic communications were to materialise then the resolution of Mail Exchanger (MX) records may be impacted and therefore corporate email may also be impacted.

3. Incident Response Simulation

It is advisable to ensure that the incident response plan is updated and considers an incident of this type. A robust plan would include a table top exercise run by an experienced third party as part of a simulation of how the organisation is prepared to respond should an incident of this nature arise. This would allow the relevant stakeholders practice their response in a safe environment and understand what improvements need to be made to limit the impact of the threat if realised.