Russian intelligence officers caught scouting undersea cables

Threat Memo - Date: 26/02/2020 - Version: 1.0

TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cyberwarfare Cyberespionage	Internet isolation SIGINT	EU	Digital infrastructure	A1

Key Points

- Russian agents were seen scouting undersea fibre-optic internet cables arriving at the Irish shore.
- Irish police sources link the agents to Russian military intelligence service GRU.
- It is currently unclear what their exact goal was.

Summary

Two press articles on February 16 announced[1,2] that Russian intelligence agents[3] were sent to Ireland to map the location of undersea internet cables connecting Europe and North America. Sources in An Garda Síochána (commonly known as Garda), Ireland's police service, reported to TheTimes that the Russians were also seen "monitoring Dublin port", which prompted a rise in security at a number of landing sites along the Irish coast. According to TheTimes, Garda believes the agents to be sent by GRU, Russia's military intelligence service, to check the fibre-optic cables for weak points. Undersea cables transport the vast majority of global internet traffic and are mostly owned and operated by private companies.

The articles cite three possible motives: espionage, sabotage and power projection. As regards espionage, the presence of tech firms in Dublin could be a reason for tapping Irish undersea cables. Since these cables are so crucial to the functioning of the internet, they are prime targets for sabotage as well, as cutting or otherwise damaging such cables will likely have a severe impact. The Business Insider article also mentions power projection as another possible motive, quoting a retired CIA officer.

Comments

Some two hundred cable-related outages take place[4] every year, most of them caused by dragging ship anchors. US military drone operations in Iraq were disturbed by such an incident in 2008. In 2018, the US Treasury Department issued sanctions[5] against a Russian firm for "providing support for underwater capabilities", which would have consisted of diving systems and a submersible craft for the FSB, Russia's domestic intelligence service, threatening underwater fibre-optic cables.

According to the Wall Street Journal[6], about 380 active submarine cables—bundles of fiber-optic lines that travel oceans on the seabed—carry about 95% of intercontinental voice and data traffic, making them critical for the economies and national security of most countries.

Another recent story illustrates the strategic competition to control submarine cables. In 2018, Australia announced it would help fund and build an undersea communications cable to the Solomon Islands, after the Pacific nation was convinced to drop a contract with Chinese company Huawei. However, Solomon Islands Prime Minister Rick Houenipwela said that the decision was taken because of "some concerns raised with us by Australia".

In 2017, the head of the UK Armed Forces warned that Russia could sever the UK's internet connectivity by cutting the undersea cables. His comments were likely caused by the Russian spy ship Yantar moving near such cables in 2017. This craft is known to host 2 deep-sea vessels, plausibly to be used in relation to the undersea cables. See CERT-EU's Threat Landscape Report of 2017Q4.

There is an extensive history[7] of Russia showing interest in the undersea internet cables. There is currently no reporting of their active sabotage or espionage via these cables. Nonetheless, these installations are vital to the functioning of the internet, making them a prime target in case of rising tensions.

Russian military intelligence agency GRU is not the first state actor to display an interest in these fibre-optic cables. Documents leaked by Edward Snowden have shown[8] in 2013 that UK's signalling intelligence agency GCHQ tapped this

[1] https://www.thetimes.co.uk/article/russian-agents-plunge-to-new-ocean-depths-in-ireland-to-crack-transatlantic-cables-fnqsmgncz
[2] https://www.businessinsider.com/russian-agents-went-to-ireland-to-inspect-undersea-cables-report-2020-2?r=US&IR=T
[3] It is unclear what definition of "agent" is being used in the article. Seen the context, it is likely that the operatives were "officers" rather than "agents". For disambiguation, see https://www.mi5.gov.uk/how-spies-operate
[4] https://www.businessinsider.com/ap-could-enemies-sabotage-undersea-cables-linking-the-world-2018-3?r=US&IR=T
[5] https://thehill.com/policy/cybersecurity/392577-spotlight-falls-on-russian-threat-to-undersea-cables
[6] https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466
[7] https://thehill.com/policy/cybersecurity/392577-spotlight-falls-on-russian-threat-to-undersea-cables
[8] https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

network in a large-scale interception effort. That same year, the Washington Post reported[9] having obtained a classified NSA slide showing the US National Security Agency (NSA)'s undersea cable interception activities.

The boldness displayed in the recent incident in Ireland bears some similarity with the Organisation for the Prohibition of Chemical Weapons (OPCW) Wi-Fi hacking attempt in 2018. In this event, four GRU operatives were caught[10] in the act of installing and activating Wi-Fi hacking equipment on a parking lot near OPCW premises in The Hague (Kingdom of the Netherlands), reportedly with the goal of hacking its networks. The operatives were detained and subsequently removed from Dutch territory[11] by security services. Their equipment, confiscated by Dutch military intelligence (MIVD), contained indications to previous operations as well as malware related to cyber threat actor Fancy Bear (AKA APT28), linked[12] to GRU.

Although current reporting does not indicate attempts to interception or sabotage in the Irish case, both cases indicate a willingness by GRU to perform impertinent reconnaissance missions outside of Russia, at least one of which (OPCW) contained cyber attack capabilities.

[9] https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html

[10] https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw

[11] https://www.nrc.nl/nieuws/2018/10/04/de-kofferbak-zit-vol-met-hackgereedschap-a2207759

[12] https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed