SINOPSIS

CHINA IN CONTEXT AND PERSPECTIVE

Handing over infrastructure for China's strategic objectives

'Arctic Connect' and the Digital Silk Road in the Arctic

Frank Jüris*

7th March 2020†

Executive summary

With the constant increase of data flows there is a demand for better infrastructure to facilitate the growth of the digital sector. **Arctic Connect**, a Finnish plan to link Europe and Asia through a submarine communication cable along the Northern Sea Route (NSR), promises to deliver faster and more reliable internet connections between Europe, Russia and Asia due to shorter distances and fewer disruptions caused by human activity along the Northern Sea Route.

Finland is interested in this project, because it wants to attract investment into data centres by developing the necessary infrastructure. For its part, China is interested within the framework of the **Digital Silk Road** in building transcontinental and cross-border data cables, as well as finding markets for its data cable service providers, such as **Huawei Marine**, whose platform **has already been chosen** for the construction of Arctic Connect.

With the construction of Arctic Connect, China would increase its defensive **intelligence gathering capabilities**, because its data transfer with Europe would no longer go through foreign data cables and as such would be better shielded from outside actors. Chinese offensive intelligence gathering capabilities would also increase; the Chinese companies contracted to build the project are obliged by PRC law to collaborate with intelligence services.

In addition, the construction of Arctic Connect would enable China to implement **underwater surveillance capabilities** it has been developing through **military-civilian fusion in the South and East China Seas**. A 10,000 km data cable can itself be used for underwater acoustic sensing; together with sensors and underwater drones it would enable China to **extend its Underwater Great Wall** to the strategically important **Arctic region**. "Eyes and ears" under the Arctic Sea would significantly improve China's nuclear deterrence by increasing the visibility of an adversary's submarines in the strategically important area.

*Estonian Foreign Policy Institute.

†Policy brief presented at the conference "Beyond Huawei: Europe's adoption of PRC technology and its implications", Prague, 27 November 2019.

Recommendations:

- A **new political perception survey** and **feasibility study** of Arctic Connect project should be conducted with a focus on the aforementioned **security threats**.
- **Procurement procedures** for the best service provider for the Arctic Connect project should take into consideration potential security threats: a service provider's **relations with a foreign government** and its security apparatus, as well as its **previous behaviour**.
- An **EU policy framework and initiatives** should be developed in order to guarantee the **strategic autonomy** of communications infrastructure.
- **EU member states** should develop a **legal framework** for licensing telecommunications service providers on the basis of a **security assessment**.
- The EU and member states should work together to improve their **encryption capabilities**, in order to guarantee **data privacy**.

0 Introduction

This paper aims to research one aspect of the Belt and Road Initiative (BRI), namely the Digital Silk Road (DSR, 数字丝绸之路), first introduced as the "Information Silk Road" (信息丝绸之路) in 2015, with a special focus on one infrastructural project, the Arctic Connect.

The white paper "Vision and Actions on Jointly Building the Silk Road Economic Belt and 21st-Century Maritime Silk Road" foresaw the creation of the "Information Silk Road", calling for building cross-border and transcontinental optical cables and improving spatial information corridors along the BRI.[1] Today DSR can be divided into four fields: digital infrastructure; next-generation technologies; e-commerce and digital free trade zones; digital diplomacy and internet governance.[2]

The Finnish project called Arctic Connect plans to link Europe and Asia through a submarine communication cable on the seabed along the Northern Sea Route (NSR).[3] In March 2016, the Finnish state-owned company Cinia Oy announced on its website that they had chosen the Chinese ICT company Huawei Marine's (华为海洋网络有限公) platform for building the Arctic Connect undersea data cable connecting Europe with Asia.[4]

The building contractor is the Finnish company Cinia Oy, whose majority stakeholder is the Finnish Ministry of Transport and Communication.[5] Cinia has already built the C-Lion1 submarine cable that connects Helsinki and Rostock.[6] By adding the submarine communication cable on the Arctic seabed, Cinia will be able to connect Europe with Russia and Asia, and provide a better internet connection with lower latency, thanks to the shorter distance. Additionally, the lower shipping traffic along the NSR will make Arctic Connect cable less prone to disruptions caused by human activities.[7]

A preliminary study for Arctic Connect was launched in 2015, followed by a political feasibility study conducted the next year.[8] In June 2019, one of the biggest obstacles, that of finding a Russian partner, was overcome and a memorandum of understanding (MoU) was signed between Cinia and the Russian company Megafon.[9] In December 2019, Megafon agreed to create the split-ownership joint venture Arctic Link Development Oy with Cinia for the construction of the Artic Connect submarine cable.

[1] "推动共建丝绸之路经济带和 21 世纪海上丝绸之路的愿景与行动", Xinhua via 中国经济网, 28 March 2015; English version: Vision and Actions on Jointly Building the Silk Road Economic Belt and 21st-Century Maritime Silk Road, National Development and Reform Commission, Mar 2015.

[2] Clayton Cheney, "China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism", *Issues & Insights* (Pacific Forum) 19:8, 2019.

[3] The Northern Sea Route (NSR) is a shipping lane between the Atlantic Ocean and the Pacific Ocean along the Russian coast of Siberia and the Far East.

[4] "Cinia is building Direct Digital Silk Road between Asia and Europe by selecting Huawei transport platform", Cinia, 16 March 2016; "Cinia selects Huawei to Build Direct Digital Silk Road between Asia and Europe", Huawei, 16 March 2016.

[5] "Owners and responsibility", Cinia.

[6] "Cinia C-Lion1 Submarine Cable", Cinia.

[7] Jukka-Pekka Joensuu, "Project Arctic Connect", Cinia, 20 September 2018.

[8] Petri Hyyppä (Proceed Consulting Ltd) and Stan Kramer (The David Ross Group), "Teknistaloudellinen selvitys Koillisväylän merikaapelin toteutumisedellytyksistä" [A feasibility study on the implementation of the Northeast Passage submarine cable], Ministry of Transport and Communications, 15/2015; Paavo Lipponen and Reijo Svento, "Report on the Northeast Passage telecommunications cable project Summary", Ministry of Transport and Communications, 3/2016.

[9] Thomas Nilsen, "Major step towards a Europe-Asia Arctic cable link", *The Barents Observer*, 6 June 2020.

The total length of the cable will be 13,800 km. The project is expected to be finished between 2022-2023 with an estimated cost of 0.8 to 1.2 billion USD. The Artic Connect submarine cable will be owned by an international consortium, also including Russian companies.[10] According to a report by the Finnish Ministry of Transport and Communication, Norway, Russia, Japan and China have all shown interest in the Arctic Connect project.[11] Although no other MoUs have been signed yet, Chinese Telecom has shown interest in the project.[12]

The first section of this paper will give an overview of the development and current situation of the undersea cable network market. The second section analyses how Arctic Connect fits into the Digital Silk Road and the third section looks into Finnish interests in the project. The fourth section analyses the security threats related to dependence on foreign strategic telecommunications infrastructure, wiretapping and underwater surveillance. The final section of the paper gives and overview of Chinese strategic interests in the Arctic and the underwater surveillance capabilities China has been developing through military-civilian fusion that could be potentially used in the implementation of Arctic Connect project.

[10] "Мегафон получит до 50% в СП с финской Cinia Oy для прокладки оптоволокна в Арктике" [Megafon will receive up to 50% in a joint venture with Finnish Cinia Oy for laying optical fibre in the Arctic], TASS, 4 December 2019.

[11] Paavo Lipponen, Reijo Svento, "Selvitys Koillisväylän tietoliikennekaapelihankkeesta. Tiivistelmä" [Report on the Northeast Passage telecommunications cable project. Summary], Ministry of Transport and Communications, 2/2016.

[12] Ting Shi, "10,000 Kilometers of Fiber-Optic Cable Show China's Interest in Warming Arctic", Bloomberg, 13 December 2017.

1 Undersea cable networks

Nearly all transoceanic data comprising internet, phone calls and TV broadcasts travels through undersea fibre optic cables.[13] According to the specialist magazine *TeleGeography*, there are 378 submarine cables around the world, with a combined length of 1.2 million kilometres. Cables were traditionally owned by telecom companies, but in the late 1990s private companies specialised in undersea cable networks began building cables and selling off traffic capacity.[14] Currently we are witnessing a trend where internet content providers such as Google and Facebook are building their own undersea cable networks.[15]

In the 2015-2019 period, Chinese company Huawei Marine shared the third place with the Japanese NEC Corporation (formerly known as Nippon Electric Company) by being the supplier of 8 subsea systems, just behind Alcatel Submarine Networks (ASN) owned by Finnish company Nokia and American company SubCom, which both provided 11 subsea systems. SubCom, as the market leader, produced over 100,000 km of cable followed by NEC (68,000 km) and ASN (49,000 km), while Huawei produced less than 20,000 km of cables. In the category of systems installed during the same time period Huawei was just behind ASN (31%) and SubCom (18%) with a 13% market share.[16]

In total, Huawei Marine is involved in 98 projects around the globe, with a combined cable length of 59,500 km. The biggest completed project is the West Africa Cable System (WACS), over 14,000 km long, which runs across 14 countries and connects South Africa with the UK. The longest ongoing project is 6,000 km long and is planned to connect Brazil with Cameroon.[17]

In 2017, Huawei Marine faced a setback when Australia voiced security concerns over a 4,000 km internet cable project connecting Sydney with the Solomon Islands. According to Australia's Telecommunications Act, the Attorney-General can direct the Australian Communications and Media Authority to refuse a licence on security grounds.[18] In December 2019, Australian company Vocus completed the 4,700 km Coral Sea Cable System for the Australian Government. Besides the Coral Sea Cable System connecting Sydney with Honiara and Port Moresby, the project also included the 730 km Solomon Islands Domestic Network.[19]

The construction of new undersea cable networks is meeting the digital economy's growing need for greater data flows. In 1992 global total data flow was 100 GB per day and in 2017 it was already 45 TB per second. It is expected that by 2022 data flow will have reached 150.7 TB per second. Currently the digital economy is estimated to make up 4.5 to 15.5% of the world's GDP, depending on the definition.[20]

[13] Nicole Starosielski, "In our Wi-Fi world, the internet still depends on undersea cables", The Conversation Global, 25 January 2019.

[14] "Submarine Cable Frequently Asked Questions", *TeleGeography*.

[15] Chris Strohm, Todd Shields, "Justice Department Opposes Google's Undersea Cable From China", Bloomberg, 28 August 2019.

[16] Stephen Nielsen, "Submarine Telecoms Industry Report", Submarine Telecoms Forum 8, 2018/2019.

[17] "Experience", Huawei Marine.

[18] David Wroe, "Australia refuses to connect to undersea cable built by Chinese company", *The Sydney Morning Herald*, 26 July 2017.

[19] "Vocus Completes Coral Sea Cable System for the Australian Government", Vocus, 12 December 2019.S

[20] "Digital Economy Report 2019", The United Nations Conference on Trade and Development, 2019.

A great amount of data travels through data cables that are, for the most part, not thicker than a garden hose, which makes them vulnerable to natural disasters like earthquakes and landslides. Nevertheless, most disruptions in data flows are still caused by accidental human activities, where damage to the cables is caused by fishing nets, trawlers and anchors. Cables break down nearly 200 times each year and, in order to avoid interruptions in the data flows, data is rerouted to other cables.[21]

2 The Digital Silk Road

In 2014, the Central Leading Small Group for Cybersecurity and Informatisation (中央网络安全和信息化领导小组)[22] headed by Xi Jinping was convened for the first time. At the meeting, Xi emphasised the need to turn China into a cyber power (网络强国) to meet the country's security and development goals. The leading group's stated aim was to coordinate ICT-related work between different sectors and draft national strategies in order to build China into a cyber power with emphasis on indigenous technology, diverse services, sound infrastructure, a skilled workforce and international cooperation.[23]

In March 2015 the term "Information Silk Road" was first introduced in a BRI white paper. The white paper foresaw the creation of the "Information Silk Road", calling for building cross-border and transcontinental optical cables and improving spatial information corridors along the BRI.[24] The joint communiqué of the first BRI forum in 2017 introduced new areas of development and collaboration to the previously mentioned fibre optic cables and included e-commerce, digital economy, ICT technology.[25] The joint communiqué of the second BRI forum in 2019 presented the "Digital Silk Road" as a multilateral cooperation initiative and platform. The communiqué stressed the need to narrow the digital divide by encouraging the construction of fibre-optic highways and smart-cities and promoting e-commerce.[26]

At large, DSR can be divided into four fields: digital infrastructure; next generation technologies; e-commerce and digital free-trade zones; digital diplomacy and internet governance.

In digital infrastructure, China wants to become a cyber power in 5G technology, fibre optic cables and data centres. China is interested in improving its capabilities in

[21] James Griffiths, "The global internet is powered by vast undersea cables. But they're vulnerable.", CNN, 26 July 2019.

[22] In 2018, the Leading Small Group became the Central Cyberspace Affairs Commission under the Central Committee of the Communist Party of China (中央网络安全和信息化委员会). "中共中央印发《深化党和国家机构改革方案》" [Central Committee of the Communist Party of China publishes "The plan for deepening the structural reform of the party and state], Xinhua, 21 March 2018.

[23] "中央网络安全和信息化领导小组第一次会议召开" [Central Leading Small Group for Internet Security and Informatisation convened for the first time], Central People's Government, 27 February 2014; "Xi Vows to Build China into a Cyber Power", Xinhua via CRI, 27 February 2014.

[24] "推动共建丝绸之路经济带和 21 世纪海上丝绸之路的愿景与行动", op. cit.

[25] "'一带一路'国际合作高峰论坛圆桌峰会联合公报（全文）", Ministry of Foreign Affairs of the PRC (MFA), 15 May 2017; English version: "Full text: Joint communique of leaders roundtable of Belt and Road forum", Xinhua, 15 May 2017.

[26] "共建'一带一路'　开创美好未来第二届'一带一路'国际合作高峰论坛圆桌峰会联合公报", Xinhua, 27 April 2019; English version: "Belt and Road Cooperation: Shaping a Brighter Shared Future — Joint Communique of the Leaders' Roundtable of the 2nd Belt and Road Forum for International Cooperation", MFA, 27 April 2019.

satellite navigation, AI and quantum computing. In digital commerce, China wants to establish e-commerce free-trade zones, provide financial services through its mobile payment platforms and internationalise its currency. With DSR China is also exporting its centralised internet governance practices, which, contrary to the Western model, value sovereignty over openness.[27]

3 Arctic Connect

In 2015, the Finnish Ministry of Transport and Communications commissioned a study to evaluate the requirements and impact of building the Arctic Connect undersea cable. According to the study, the Arctic Connect cable would be shorter in distance and less prone to damages than the cables currently in use, which travel under the Red Sea, where they can be damaged by heavy fishing. A shorter distance also means an increase in connection speed.[28]

With Arctic Connect, Finland wants to improve regional connectivity and provide the necessary infrastructure for attracting data centres. The study points out that Finland is an attractive destination for data centres due to its reliable energy and internet infrastructure, access to green energy and cold climate-related reduction of cooling cost, reduced energy tax for data centres, transparent legislation and skilled workforce. In addition, its favourable geographic location between East and West and history of neutrality are believed to make Finland the "Switzerland of data". In total, Arctic Connect is believed to benefit the Finnish economy with €1.38 billion and over the period of a decade generate over a thousand jobs annually.[29]

Finland has already been successful in attracting investments into building data centres. In September 2019, Google's CEO Sundar Pichai announced an additional investment of €600 million to its already existing Hamina data centre, which raises the total investment by Google in Hamina to almost €2 billion.[30]

In 2016, the Finnish Ministry of Transport and Communications conducted a survey and published a report that analysed the international perception of the Arctic Connect project. According to the report, there are no political obstacles from the capitals of the participating countries, nor from Paris, Berlin, Brussels or Washington. A problem raised in the report is connected with the short ice-free period, which means that the cable should be laid from both sides at the same time and to great depth in order to shorten the construction period and avoid damage from drifting icebergs. Additionally, the report mentioned concerns related to data security and privacy, the environment, funding and ownership, but it was not within the scope of the preliminary study to address all these issues.[31]

[27] Cheney, op. cit.
[28] Hyyppä and Kramer, op. cit., p. 8.
[29] Ibid., pp. 11-14.
[30] "Google investment in Hamina data centre rises to €2bn", Yle, 20 September 2019.
[31] Lipponen and Svento, op. cit.

4 Security implications

Besides the enormous cost that potential disruptions in undersea cable networks might impose on the service providers of the digital economy, today's societies are increasingly dependent of the functioning of the internet in their daily activities, which makes a deliberate attack on an internet grid a serious security concern.

The first potential security threat is related to overreliance on one service provider in the strategic telecommunications infrastructure. Before World War I, Britain dominated the telegraph cables market by owning the majority of the transoceanic cables and cable-lying ships. A monopoly on critical communication infrastructure enabled Britain to cut Germany off from direct connections everywhere besides continental Europe and reroute all the remaining communication with its colonies through London, where British intelligence could intercept all the messages.[32] If Chinese companies in the future dominate the undersea data cable market, then China would enjoy a similar strategic advantage to the UK during World War I. Retired US Navy admiral and former supreme allied commander of NATO James Stavridis suggests that the US should develop less costly alternatives to Huawei Marine provided undersea cable networks in cooperation with the private sector in order to better compete with Chinese technology.[33]

A second potential security threat is related to the wire-tapping of the undersea data cables. In the 1970s, during the Cold War, the US navy successfully carried out Operation Ivy Bells in the depths of the Sea of Okhotsk, where navy divers placed surveillance equipment on communication cables connecting Soviet military bases. US intelligence was surprised that they were able to intercept military communication that was not even encrypted. Operation Ivy Bells lasted until the Soviets found out about it in 1981.[34] The US Navy submarine *Jimmy Carter* is believed to be capable of conducting underwater wiretapping operations and so is the Russian submarine *Podmoskovye*.[35]

With the construction of the Arctic Connect undersea cable network China could increase its offensive and defensive intelligence capabilities.[36] Offensive capabilities would increase without the need for conducting specific military undersea surveillance operations, because the technology for the construction of the undersea cable is provided by the Chinese company Huawei Marine. According to the Chinese National Intelligence Law (中华人民共和国国家情报法) introduced in 2017, Chinese organisations and individuals are obliged to cooperate with intelligence services upon request.[37] One way to counter these threats is to improve the end-to-end encryption capabilities or innovate on the means to test and protect the data that travels through the cables.[38]

[32] Jonathan E. Hillman, "Influence and Infrastructure: The Strategic Stakes of Foreign Projects", CSIS, 22 January 2019, pp. 21-22.

[33] James Stavridis, "China's Next Naval Target Is the Internet's Underwater Cables", Bloomberg, 9 April 2019.

[34] Matthew Carle, "Operation Ivy Bells", Military.com.

[35] James Griffiths, "How vulnerable are the undersea cables that power the global internet?", CNN, 26 July 2019; Thomas Nilsen, "Shipyard reveals unique video of spy submarine", *The Barents Observer*, 12 November 2016; Oleg Ivanov, "Военная тайна" [A military secret], Lenta.ru, 5 July 2019.

[36] Cheney, op. cit.

[37] "中华人民共和国国家情报法" [National Intelligence Law of the PRC], Ministry of Justice; English translation.

[38] Stavridis, op. cit.

According to a University of Jyväskylä report published in 2019, intelligence collection from Arctic Connect can take place by tapping, exploiting optical overflow or hacking into the control systems. For Russia the best potential place for tapping is when the cables enter its territorial waters either in the West or East just before being linked to the national grid or after the signal is enforced in the first amplifier in Russian waters.[39]

In addition, Chinese defensive intelligence capabilities will improve with the construction of Arctic Connect, because sensitive data will no longer travel through foreign cables and as such decrease the risk of being gathered by foreign intelligence services.[40] After Snowden's revelation of NSA and GCHQ's massive intelligence-gathering practices, both China and Russia are likely to be interested in shielding their data flows from outside interference, which Arctic Connect promises to deliver.[41]

A third potential security threat is related to undersea fibre-optic cables' dual-use capabilities, which means that data cables can also be used for gathering scientific and military surveillance information without disturbing the main function of transferring data. Fibre-optic cables equipped with sensors can collect information about the currents, seismic activities, temperature and composition of water and even transmit video from the seafloor. Even more, by using Distributed Acoustic Sensing (DAS) techniques, fibre-optic cables can be turned into acoustic sensors that can detect seismic waves, vibration and acoustic noise.[42]

DAS technology is based on a phenomenon called Rayleigh scattering, in which molecules in the atmosphere scatter sunlight at shorter wavelengths that match the size of the molecules and makes the human eye perceive the sky as blue. Similar scattering takes place in fibre-optic cables, where precise pulses of laser light are sent down the cable and the slightest fluctuations in the molecular structure are matched with the help of algorithms to the acoustic "fingerprints" of, for example, footsteps just ten metres from the cable, low-flying drones or damages in railway lines or oil pipelines. The British company QinetiQ has developed DAS solutions for countering hostile submarines by processing the acoustic data they created. Currently DAS technology is widely used for civilian purposes and QinetiQ's OptaSense provides fibre-optic cable solutions for the national railways of Germany, Switzerland and Japan, which enables them to monitor the condition of train wheels and tracks.[43]

The Russian Navy has, in addition to *Podmoskovye*, another special-purpose submarine, *Losharik*, which caught fire in the Kara sea in July 2019. *Losharik* was believed to be capable of conducting undersea surveillance operations. Contrary to the official scenario of *Losharik*'s last mission of hydrographic work, it is possible that it was working on methods for transporting and placing surveillance / anti-surveillance equipment on the Arctic seabed for the development of the Russian positioning system of underwater surveillance (*позиционная система подводного наблюдения*) by

[39] Martti Lehto et al., "Arctic Connect Project and cyber security control, ARCY", University of Jyväskylä, 2019, p. 20.

[40] Cheney, op. cit.

[41] Craig Timberg, "NSA slide shows surveillance of undersea cables", *The Washington Post*, 10 July 2013; Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian*, 6 June 2013; Olga Khazan, "The Creepy, Long-Standing Practice of Undersea Cable Tapping", *The Atlantic*, 16 July 2013.

[42] Lehto, op. cit., pp. 20-21; "The ear underground", *The Economist*, 4 January 2014.

[43] Philip Dunne, "Growing the Contribution of Defence to UK Prosperity", July 2018, p. 39.

the name of Harmony (Гармония).[44] The main component of the Harmony system are autonomous seabed stations (*автономные донные станции*), which are equipped with acoustic sensors and can detect the sound footprint of vessels from a distance of several hundred kilometres.[45] The *Losharik* accident occurred not far from the Russian military base 77360-H in Okolnoye, Belgorod Oblast, believed to be responsible for the maintenance and development of autonomous seabed stations.[46]

The Undersea Great Wall

The fact that the cables themselves, with or without additional sensing equipment, can be used for underwater monitoring raises another potential risk regarding the Arctic Connect project. This means that the planned 10,000 km undersea cable network could be turned into an undersea surveillance system along the Northeast Passage, detecting from the seabed acoustic abnormalities caused by submarines in the strategically important Arctic region. Having "ears and eyes" below the Arctic Ocean is a strategic advantage that great powers would like to possess. China has been developing undersea surveillance capabilities in the South and East China Seas for years, as shown below. It is not hard to imagine that the capabilities they have developed over the years in this field could be also put into use along the NSR.

According to an article in the WeChat group's Defence_SJY article by Shi Jiangyue 石江月, a veteran commentator on Chinese military affairs who has published several hundred articles on China's military build-up in media including the *Global Times*, the construction of the Undersea Great Wall (水下长城) is not only necessary for scientific reasons, but also serves national security interests. The Undersea Great Wall will increase China's anti-surveillance and area denial capabilities in the South China Sea, which, due to its great depth, is used for surveillance operations by US, Russian, Japanese and Australian submarines.[47]

China's 2015 white paper on military strategy states the importance of safeguarding China's development interests by protecting strategic SLOCs. Anne-Marie Brady, a professor at the University of Canterbury, New Zealand and an expert on China's polar policy, highlights the strategic importance of the Arctic and the Northern Sea Route as an alternative route to Western Europe that avoids the potential chokepoints of the Malacca strait and the Suez Canal, which China does not control.[48] Furthermore, Brady points out that Chinese scholars stress the NSR's importance to the military. China's vulnerable northern flank is situated in the Arctic, because the intercontinental ballistic missiles targeting China will transit through the Arctic and key US missile defence systems are located there. This is why, as early as 1959, China set the

[44] Ivanov, op. cit.

[45] Aleksey Ramm, "Россия разворачивает глобальную систему морского слежения" [Russia is deploying a global maritime tracking system], Izvestiya, 25 November 2016.

[46] Ivanov, op. cit.

[47] Shi Jiangyue, "中国建" 水下长城"，才是真正踩了美日 '尾巴'！" [Only if China builds an Undersea Great Wall will it genuinely step on US-Japan's tail], WeChat group Defence_SJY, 19 June 2017; "中国建 '水下长城' 这一举动真正踩到了美日尾巴" [China's move to build Underwater Great Wall truly is a step closer to US-Japan's tail], JSTV.com, 20 June 2017; "中国建" 水下长城" 这一举动真正踩到了美日尾巴" [China's move to build Underwater Great Wall truly is a step closer to US-Japan's tail], Sina, 20 June 2017. On the author, Shi Jiangyue 石江月: "萨德的故事，这些可能你并不知道！" [THAAD's story, something you might not know!], WeChat, 23 March 2017.

[48] Anne-Marie Brady, *China as a Polar Great Power*, Cambridge University Press, August 2017, pp. 60-62.

goal of developing submarines capable of operating in the Artic in order to have a second-strike capability for nuclear deterrence.[49]

Even though most recent Chinese military white papers have not yet directly mentioned the goal of establishing a PLAN presence in the Arctic, it is just a matter of time, according to an analysis by Ryan D. Martinson, a researcher at the US Naval War College's China Maritime Studies Institute. Martinson's argument is based on the gradual development of the Chinese Navy from a near to far-sea and in the future polar-sea force. His analysis cites a number of Chinese military experts and officers who have stated that the next frontiers for the PLA Navy are the polar regions. In order to successfully run nuclear deterrence patrols in the Arctic, the PLA Navy needs to improve its underwater acoustic capabilities, because the acoustic environment depends from multitude of factors: from temperature to depth and salinity, not to mention background noise created by drifting ice. As Martinson points out, Chinese scientists from the CAS Institute of Acoustics and Harbin Engineering University, which has close links with the PLA, have been conducting acoustic research in the Arctic since 2014.[50]

In December 2015, *China Ocean News* (中国海洋报)[51] published an article that argued for the construction of an undersea surveillance system, which the article called the Undersea Great Wall. According to the article, the Undersea Great Wall should increase maritime safety and monitoring capabilities by building underwater target detection, surveillance and early warning systems. The undersea surveillance system should not be limited to territorial waters, but could also be implemented in coastal waters, deep and far seas, around island and strategic passages all around the world.[52]

In 2016, the SOE China Shipbuilding Industry Corporation (中船重工集团) acquired CEC CoreCast Corporation (中电广通股份有限公司) to advance military-civil fusion and improve capabilities in maritime acoustics. The aim of the acquisition was to accelerate the construction of the Undersea Great Wall.[53] Military-civil fusion is a long-term CCP, policy dating back to the Mao era, to use linkages between the military and the civilian sector to build up China's economic and military strength. Military-civil fusion has been promoted to a national strategy under Xi Jinping, who personally oversees the Central Commission for the Development of Military-Civil Fusion (中央军民融合发展委员会).[54]

[49] Anne-Marie Brady, "Facing Up to China's Military Interests in the Arctic", *China Brief* 19:21, 10 December 2019.

[50] Ryan D. Martinson, "The Role of the Arctic in Chinese Naval Strategy", *China Brief* 19:22, 20 December 2019.

[51] *China Ocean News* (中国海洋报) was published by the State Oceanic Administration (SOA, 国家海洋局), subordinate to the Chinese Ministry of Land and Resources (国土资源部), and currently by the Ministry of Natural Resources, which absorbed SOA's functions upon its dissolution in 2018. The author of the article, Wang Fang 王芳, is a researcher at the China Institute for Marine Affairs (CIMA, 海洋发展战略研究所), that is China's only research institute under a ministry specialising in marine strategy, policy and legal issues ("所简介" [Introduction], CIMA, 15 January 2019). Since 2013, Wang Fang has been working on the strategy for building China into a Maritime Power (海洋强国) ("专家介绍" [Expert introduction], CIMA).

[52] Wang Fang 王芳, "构建我国海洋水下观测体系的思考" [Reflection on the construction of China's undersea surveillance system], *China Ocean News*, 2 December 2015.

[53] "中船重工资产证券化率将升至 70%" [China Shipbuilding Industry Corporation assets securitization rate will increase to 70%], Xinhua, 13 October 2017.

[54] Alex Joske, "The China Defence Universities Tracker", ASPI, 2019.

In June 2017, the PRC central government approved the construction of the Underwater Science Observation Network (海底科学观测网), which will take 5 years to finish and was expected to cost 2.1 billion RMB. The project will be led by Tongji University and carried out in collaboration with the Institute of Acoustics of the Chinese Academy of Sciences (中国科学院声学研究所). The Underwater Science Observation Network will provide real-time high-resolution 3-dimensional monitoring of the ecosystem and sea maritime accidents both underneath and above the East and South China Seas. The data collected will be transferred through undersea fibre-optic cables to a data centre in Shanghai, were it will be analysed.[55]

In December 2019 Chinese company Zhongtian Marine Systems (中天海洋系统) announced a breakthrough by reaching a depth of 2000 m with indigenous underwater connector (水下连接器) technology, which links together the different parts of the underwater surveillance system and enables the transmission of optical and electrical signals.[56] Zhongtian Marine Systems is a joint venture between Jiangsu Zhongtian Science and Technology (江苏中天科技) and Zhejiang University (浙江大学) established in 2015 to help carry out the 863 Plan, building China into a maritime power by providing the necessary equipment and services for undersea monitoring and environmental protection.[57] Amongst the list of products on Zhongtian Marine Systems' website are underwater observation networks (水下观测网) consisting of a shore base, an underwater transmission system, an underwater junction box system and an underwater sensor system. Underwater observation networks equipped with water-quality sensors, cameras and sonars can be used for military purposes, as advertised on the website.[58]

China Shipbuilding Industry Corporation (CSIC, 中国船舶重工集团) is engaged in the research, development, design and manufacturing of ships and maritime equipment for both military and civilian use. As the main supplier for the PLA Navy, CSIC produces aircraft carriers, submarines, surface combat vessels, amphibious assault vessels and support ships. By late 2018, CSIC had 18 subsidiaries and the majority of them had a military industry production licence.[59] CSIC together with China State Shipbuilding Corporation (CSSC, 中国船舶集团) account for almost three quarters of China's overall shipbuilding capacity and have also produced all domestic navy vessels recently introduced into the Chinese Navy.[60] In October 2019, the State-owned Assets Supervision and Administration Commission approved the merger of CSIC and CSSC, in order to increase the competitiveness of China's shipbuilding industry. The merged company is called China Shipbuilding Group (中国船舶集团). The chairman

[55] "我国将建设国家海底科学观测网" [China will build Underwater Science Observation Network], Government of the People's Republic of China, 8 June 2017.

[56] Chen Yu 陈瑜, "我国有了 2000 米水下插拔电连接器" [China obtained underwater electric connector technology that can reach a depth of 2000 m], Xinhua, 25 December 2019.

[57] "公司概述" [Company overview], Zhongtian Marine Systems (中天海洋系统); "行业深度系列之六-海底长城——海底监测网行业深度研究" [Industry in depth series nr 6 – Underwater Great Wall - In depth analysis of the underwater surveillance network market], Industrial Securities Co (兴业证券), 24 September 2017; "海底监测网行业深度研究" [In depth analysis of the underwater monitoring network market], 科塔学术 (sciping.com), 2 February 2019. Authorship belongs to Industrial Securities Co (兴业证券) that is a Chinese securities company registered in Fuzhou. Its three biggest shareholders are the Fujian provincial government 20.27%, Fujian Investment Group (7.98%), Shanghai Shenxin Group (3.14%). "兴业证券股份有限公司" (Industrial Securities Co), 企查查 (Qichacha).

[58] "水下观测网" [Underwater observation networ], Zhongtian Marine Systems.

[59] "公司简介" [Company introduction], China Shipbuilding Industry Corporation (CSIC, 中国船舶重工集团).

[60] "How is China modernizing its navy?", CSIS, 16 October 2019.

of the board, Li Fanpei 雷凡培, and the CEO, Yang Jincheng 杨金成, previously held the same positions at CSSC.[61]

The former CSIC's 705th department focuses on developing underwater drones that can be used for exploration of natural resources, laying, repairing and defending underwater cables and pipelines and conducting research and rescue missions. In 2017, the 705th department established strategic cooperation with one of the biggest Chinese engineering companies, SANY Heavy Industry (三一重工股份有限公司) to co-develop amphibious equipment under military-civil fusion.[62] The biggest shareholder of SANY Heavy Industry, with a 30.2% stake, is SANY Group (三一集团有限公司).[63] SANY Group's biggest shareholder is company's founder, Liang Wengen 梁稳根, with 56.7% of the shares.[64]

China has improved its undersea surveying and scientific observation capabilities through the development of underwater drones. In 2008 the underwater Arctic Autonomous / Remote Vehicle (ARV), developed by the Chinese Academy of Sciences' Shenyang Institute of Automation (CAS-SIA, 中国科学院沈阳自动化研究所) was deployed for the first time in the Arctic. In 2014, a second-generation ARV joined the *Xue Long* research vessel in the Arctic to conduct underwater monitoring.[65] In 2017, the *Sea Wing* (海翼) glider set a world record by diving into the Mariana Trench to the depth of 6329 metres. The *Sea Wing* glider can be equipped with sensors measuring the temperature, salinity, oxygen saturation, turbidity, content of chlorophyll and nitrate, water current velocity, acoustic profiles. In 2018 *Sea Wing* was first used for scientific research in the Arctic.[66] Besides the Arctic, *Sea Wing* has been used for scientific purposes in the South China Sea and in the Indian Ocean, but due to its low acoustic signature, which enables it to detect foreign submarines, it could be used to strengthen the PLA's anti-submarine warfare capabilities.[67] In 2018 the *Sea Swallow X* (海燕 - X) glider took the record in the Mariana Trench even farther, to a depth of 8213 metres. *Sea Swallow – L* has set the record of undisrupted voyage to 141 days with a total distance of 3619 kilometres and maximum depth of 1010 metres.[68]

Another participant in the government-approved project for the construction of the of Underwater Science Observation Network (海底科学观测网) is the Institute of Acoustics of the Chinese Academy of Sciences, which specialises in the research of acoustic information processing and has undertaken many military projects in this field.[69] In 2009, the Institute of Acoustics opened an acoustic-sensing test site in Hainan

[61] "南北船正式合并中国船舶集团启航" [South and North Shipbuilders officially merge into China Shipbuilding Group to set sail], Xinhua, 26 October 2019.
[62] "海底监测网行业深度研究", op. cit.
[63] "三一重工股份有限公司 2019 年半年度报告摘要" [SANY Heavy Industry's 2019 interim repot summary], SANY Group.
[64] "三一集团有限公司" [SANY Group], 企查查 (Qichacha).
[65] "北极 ARV" [Arctic ARV], Chinese Academy of Sciences, 13 December 2015.
[66] Chen Lianzeng 陈连增 and Lei Bo 雷波, "海洋技术与装备研发取得长足发展" [Long term development of maritime technology's and equipment research and development], *China Ocean News* (中国海洋报), 3 December 2019.
[67] Elsa B. Kania, "Chinese Military Innovation in Artificial Intelligence", Centre for American New Security, 7 June 2019, pp. 12, 18-19.
[68] Chen Lianzeng, op. cit.
[69] "海底监测网行业深度研究", op. cit.

on the South China Sea coast.[70] In 2013, they built a model underwater observation system in the South China Sea near Hainan.[71]

Tongji University is the leading participant in the Underwater Science Observation Network project and has the only State Key Laboratory of Marine Geology (海洋地质国家重点实验室).[72] In 2010 Tongji University signed a cooperation agreement with the Ministry of Education and the State Oceanic Administration (SOA) to develop marine science and technology in collaboration with 16 other universities.[73] Under the supervision of SOA, Tongji University conducted polar research of national importance and it housed a Ministry of Education laboratory dedicated to defence research by the name of Ministry of Education National Defence Science and Technology National Key Laboratory on Advanced Microstructure Materials (先进微结构材料教育部国防科技重点实验室).[74]

Tongji University also houses the Centre for Polar and Oceanic Studies, which was established in 2009 with a research focus on polar studies in international organisations, politics, security policy, the environment, natural resources and society.[75] In 2018, SOA was dissolved and its duties were divided between the Ministry of Natural Resources (自然资源部), the Ministry of Ecology and Environment (生态环境部) and the People's Armed Police (PAP). Under the reform, SOA's coast guard duties were transferred to PAP and polar research and strategic planning, maritime economy, island affairs and maritime space became the responsibility of the Ministry of Natural Resources.[76]

In 2019 Tongji University was added to the US Unverified List, which restricts exports to the university due to the difficulty of carrying out end-user checks.[77] In 2009 Tongji University built the first Xiaoqu Mountain Underwater Observation test site (海底观测小衢山试验站) on Hangzhou Bay in the East China Sea.[78] In 2012, Tongji University started operating a shallow-water undersea observation network in the East China Sea. With its underwater observation networks, Tongji University has researched wireless acoustic communication transmission and achieved deep-sea long-distance data transmission capabilities.[79]

In June 2019, Huawei announced that it would sell its 51% stake in Huawei Marine Systems to Hengtong Optic-Electric (江苏亨通光电股份有限公司).[80] Hengtong Optic-Electric sells products and provides services in the domain of fibre-optic communication and power transmission. Hengtong looks forward to capitalising from

[70] "中国科学院声学研究所" 南海声学与海洋综合观测试验站" 正式挂牌" [The Institute of Acoustics of the Chinese Academy of Sciences officially opened South China Sea Acoustics and Comprehensive Maritime Monitoring Test Site], Institute of Acoustics of the Chinese Academy of Sciences, 3 December 2009.

[71] "海底监测网行业深度研究", op. cit.

[72] "Tongji University 同济大学", China Defence University Tracker, ASPI.

[73] "高校要为国家实施海洋战略做出新贡献" [Chinese higher education institutions want contribute to the implementation of the maritime strategy], Ministry of Education, 16 September 2010.

[74] "科研基地名单" [Research Units List], Tongji University, 15 August 2014.

[75] "Center for Polar and Oceanic Studies, Tongji University", China-Nordic Arctic Research Centre.

[76] Zhang Chun, "Shake-up for China's ocean management", China Dialogue Trust, 16 April 2018,

[77] "Tongji University 同济大学", op. cit.

[78] Zhang Yanwei 张艳伟, Fan Dadou 范代读 and Xu Huiping 许惠平, "东海海底观测网小衢山试验站记录的 2010 年智利海啸信号分析", State Key Laboratory of Marine Geology (海洋地质国家重点实验室), Chinese Science Bulletin, 32, 2011.

[79] "海底监测网行业深度研究", op. cit.

[80] Gao Chao 高超, "亨通光电拟收购华为海洋 51% 股权", 通信产业网 (CCIDCOM), 3 June 2019; Yuan Yang, Louise Lucas, "Huawei to offload undersea telecoms cable business", *Financial Times*, 3 June 2019.

the internationalisation of Chinese companies under the Belt and Road Initiative.[81] Hengtong Optic-Electric's biggest share of 15.66% belongs to Hengtong Group and its second biggest shareholder, with 14.95%, is Cui Genliang 崔根良.[82] Cui Genliang is with 58.70% also the majority stakeholder in Hengtong Group.[83]

Arctic Connect is planned to be built on a platform provided by submarine-cable network supplier Huawei Marine, a joint venture established by Huawei Technologies Co., Ltd and Global Marine Systems Limited.[84] Media reports have claimed that Huawei is planning to sell its majority stake in Huawei Marine Systems due to American pressure over security concerns. It was just in August 2018 that Huawei gained a majority stake in Huawei Marine, while British Global Marine retained a 49% non-controlling interest.[85] If this deal goes through, Hengtong Optic-Electric, through its majority stake in Huawei Marine, will have ultimate control over the supplier of the technology used in the undersea cable network platform that Cinia plans to use for the construction of Arctic Connect.

In 2016, Hengtong Group's subsidiary Jiangsu Hengtong Marine Cable Systems (江苏亨通光电股份有限公司) and Tongji University's School of Ocean and Earth Science jointly established a Marine Engineering Technology Research and Development Centre (海洋工程技术研发中心) to research the technologies needed for creating marine observation networks. In 2017 Hengtong Optic-Electric and Tongji University set up Hengtong Marine Equipment (上海亨通海洋装备有限公司) to combine each side's industrial and scientific strengths in order to industrialise undersea observation technology for both civilian and military use and contribute to the creation of underwater observation networks.[86] Hengtong Marine Equipment's majority stakeholder (70%) is Hengtong Group and 9% of the shares belong to Tongji Innovation and Entrepreneurship Holdings Ltd (同济创新创业控股有限公司), whose sole owner is Tongji University.[87]

The implementation of the Arctic Connect project could potentially give China the opportunity to put the capabilities gained in developing the Undersea Great Wall to use in the distant Arctic Sea, which holds great geostrategic importance in nuclear deterrence, because rockets launched there will travel the shortest distance to any major city in the Northern hemisphere. In addition, if the Chinese Undersea Great Wall extends to the Arctic, it will significantly hinder the undetected manoeuvrability of Western powers' submarines.

[81] "我们是谁", Hengtong Optic-Electric (江苏亨通光电股份有限公司).
[82] "江苏亨通光电股份有限公司"(Hengtong Optic-Electric), 企查查 (Qichacha).
[83] "亨通集团有限公司" (Hengtong Group), 企查查 (Qichacha).
[84] "About Huawei Marine Networks Co., Ltd.", Huawei Marine.
[85] "Huawei to sell off undersea cable business to Chinese firm after U.S. reportedly cited security risk", *Japan Times*, 3 June 2019.
[86] "行业深度系列之六-海底长城——海底监测网行业深度研究", op. cit.
[87] "上海亨通海洋装备有限公司" (Shanghai Hengtong Marine Equipment), 企查查 (Qichacha).

5 Conclusion

Arctic Connect could hinder Europe's strategic autonomy in the field of telecommunications and increase Chinese offensive and defensive intelligence collection capabilities. If in the future the majority of the EU's data with Asia travels through Chinese fibre-optic cables, then in case of a conflict China could cut off European countries from its Asian partners.

If the core technology of the undersea cable network were provided by a Chinese company, which is obliged by the National Security Law to collaborate with the Chinese intelligence services, then Chinese offensive intelligence capabilities would increase due to having access to the vast amounts of data transferred between Europe, Russia and Asia.

Chinese defensive intelligence collection capabilities would increase with the construction of Arctic Connect, because Chinese and Russian data would not travel through a cable network owned by a foreign power, enabling them to shield their data from foreign interception.

Arctic Connect gives China an opportunity to put into use undersea surveillance capabilities developed through a multitude of military-civilian fusion projects, which, besides being of commercial value, enhance the capabilities of the Chinese military in the undersea warfare domain. Undersea data cables with or without sensing equipment accompanied by undersea drones could be used to detect foreign vessels along the Northern Sea Route, which would lose the strategic advantage of being undetected in a strategically important region.

Internet cables, meant to connect people in cyberspace, can become a dividing factor, if countries participating in the Artic Connect project want to protect the cable from outside intrusion and the outsiders try to improve their capabilities to have access to the data transferred through them. This could lead to the militarisation of the Arctic and increase the probability of conflict in the region.

6 Policy recommendations

1. As vast amounts of European data are planned to travel through the Arctic Connect data cable, in the light of the potential security threats mentioned above, there should be another survey to evaluate the political perception of the EU member states.
2. In order to avoid potential overdependence from one service provider, which could lead to a disruption of the service in case of conflict, the EU should incentivise the private sector to better compete with foreign data cable service providers in order to ensure strategic autonomy in the strategic communications infrastructure.
3. EU member states should consider developing similar legislation to Australia, allowing the government to refuse a licence to a telecommunications service provider on the basis of a security assessment.
4. In order to improve defensive intelligence gathering capabilities, additional funds should be allocated for the improvement of encryption, in order to keep up with the development of quantum computing and to guarantee data privacy even if sensitive data travels through cables controlled by a third party.
5. A feasibility study for the Arctic Connect project should be conducted in a way that takes into consideration, besides the economic benefits, also the potential security threats and the cost of hindered privacy, loss of sensitive data etc.
6. Procurement for the best service provider for the Arctic Connect project should take into consideration potential security threats: the service provider's relations with a foreign government and its security apparatus, as well as its previous behaviour.

Frank Jüris *is a Junior Researcher at the Estonian Foreign Policy Institute. His research focuses on China's domestic and foreign policy, EU-China relations, China's relations with the Central and Eastern European countries in the 16+1 format, and Sino-Russian relations. His recent paper "The Talsinki Tunnel: Channelling Chinese Interests into the Baltic Sea" discusses the possible involvement of Chinese investors and SOEs in a project to build an undersea rail tunnel between Helsinki and Tallinn in the context of China's interests in the Arctic and highlights potential security risks.*

Sinopsis *is a collaborative project between the Institute of East Asian Studies at Charles University in Prague and the non-profit AcaMedia Institute. The conference "Beyond Huawei: Europe's adoption of PRC technology and its implications", organised by Sinopsis, was held on 27 November 2019 at the Czech Academy of Sciences. Full video and audio recordings of the presentations are available here. Previously published: Łukasz Sarek, "5G and the Internet of Things: Chinese companies' inroads into 'digital Poland'".*