

# *Cyber Achilles? On the Importance of Undersea-Cables in the 21<sup>st</sup> Century*

by

*Vladimir Stosic*

Among those photos, which were sent from Europe across the Atlantic to the USA on July 23, 1962 as the first intercontinental television signal by means of the TELSTAR satellite, is an image of the *Beli Anđeo* (English: White Angel) from the Serbian Orthodox monastery of Mileševa in Serbia. The *White Angel* is a 13th century fresco depicting a young man dressed in white - an angel – and the women who came to the tomb of Jesus Christ on Easter morning to anoint him. It was meant to be a message of peace between the old and new world. If one thinks about transatlantic cyber security today, two developments are surprising: First, satellite has not been able to establish itself as the main medium of international data traffic - 95% of international data traffic runs over undersea cables. And second, discussions about cyber security are narrowing down to mostly autocratic regimes that want to manipulatively gain interpretive sovereignty over certain political actors or campaigns before and during elections, or around the involvement of the Chinese company Huawei in 5G expansion.

It is those undersea cables that represent a critical infrastructure in the field of cybersecurity. Undersea cables, according to the thesis of this essay, represent the digital Achilles heel of transatlantic security in the 21st century. Undersea cables are an understudied area of international relations. 97% of international data traffic and \$10 trillion in daily financial transactions pass through undersea cables that span 1.2 million kilometers.<sup>1</sup> Undersea cables are critical infrastructure, because nearly every communication passes over them; from business contracting to scientific publications to government business.

Three trends are causing undersea cables to receive increased attention. First, authoritarian states are reshaping the physical Internet layout through companies that control infrastructure elements to better direct data, control data bottlenecks, and thus more easily spy on data.<sup>2</sup> Second, more and more companies are using the system of remote management, which is poorly secured and accordingly pose an increased risk of cybersecurity.<sup>3</sup> Third, the increase of cloud computing has increased the volume as well as the sensitivity of data.<sup>4</sup>

These three trends prompt a rethinking of transatlantic cybersecurity and a focus on undersea cables. It is not that the geostrategic relevance of undersea cables is entirely overlooked. However, the way in which critical infrastructure can be cast into an overall strategy in the transatlantic discourse on cybersecurity leaves some questions unanswered. Other actors are better positioned to do so. For example, cybersecurity seems to be a top priority in Russia: meetings between President Vladimir Putin and Mikhail Oseyevsky, president of Rostelecom, to exchange views on the pressing issues of undersea cable development potential are not

---

<sup>1</sup> Colombo, Matteo/ Solfrini, Federico/ Varvelli, Arturo (2021): Network Effects: Europe's Digital Sovereignty in the Mediterranean, European Council on Foreign Relations, Policy Brief, p.2

<sup>2</sup> Sherman, Justin (2021): Cyber Defense Across the Ocean Floor. The Geopolitics of Submarine Cable Security, Atlantic Council, p.1

<sup>3</sup> Ibid.

<sup>4</sup> Ibid.

uncommon. In the recent past, Russian submarines have been located in the Atlantic Ocean near undersea cables.<sup>5</sup>

And the People's Republic of China also weights the issues surrounding security in cyberspace differently than the transatlantic players. The *Belt and Road Initiative* (BRI) - a maritime and terrestrial infrastructure project launched by President Xi Jinping in 2013 - also includes the *Digital Silk Road* (DSR) announced in 2015. In addition to the development and expansion of intercontinental economic sectors by the People's Republic, digital projects are also being specifically pursued. The Chinese company Huawei is often in the spotlight. To stay with the case study of Serbia mentioned in the introduction, a smart city project is being set up in Belgrade using around 1000 Huawei-brand facial recognition cameras.<sup>6</sup>

Probably the most striking example of a Chinese undersea cable project is the Pakistan East Africa Connecting Europe (PEACE) project: starting in China, it is to run via Pakistan and the Strait of Hormuz to Djibouti and through the Bab-al-Mandab and the Suez Canal to Marseille, France. The interlocking of economic and military projects of the People's Republic of China is particularly striking. In Gwadar, Pakistan, and in Djibouti, the People's Republic of China maintains military bases that can provide military protection for the landing stations of the undersea cables. Against this backdrop, it is not surprising that the Strait of Hormuz has been used by China, together with Russia and Iran, for joint naval exercises since 2018. The merging of geostrategic and geoeconomic components illustrates that the People's Republic of China is taking a holistic approach: The critical infrastructure mandatory for China in order to rise economically is being accompanied militarily to ensure the long-term nature of its development.

And what about the North Atlantic Treaty Organization (NATO) and the European Union (EU)? NATO has recently increased its emphasis on the relevance of undersea cables. For example, at a press conference in the fall of 2020, NATO Secretary General Jens Stoltenberg emphasized the importance of undersea cables to the Alliance's deterrence, defense, and resilience.<sup>7</sup> And the communiqué from NATO's Brussels Summit on June 14, 2021, also includes the following note: "We will maintain awareness of any potential threats to our critical undersea infrastructure and will continue to address them nationally and, where needed, collectively."<sup>8</sup> And a similar realization seems to have taken place at the EU. In her *State of the Union Address* on September 15, 2021, Commission President Ursula von der Leyen announced a connectivity strategy as a counter-model to China's BRI with the "Global Gateway."<sup>9</sup> Nevertheless, one looks in vain for concrete plans for action by the EU on the issue of undersea cables.

The growing attention regarding undersea cables is a positive development. But regarding the relevance of undersea cables for the prosperity and economy of the U.S. and Europe, one misses

---

<sup>5</sup> Roblin, Sebastien (2020): Russian Submarines Could Be Tampering With Undersea Cables That Make the Internet Work, *The National Interest*: <https://nationalinterest.org/blog/reboot/russian-submarines-could-be-tampering-undersea-cables-make-internet-work-169587>

<sup>6</sup> Gomez, Julian (2021): Should citizens in Belgrade be concerned by newly installed surveillance cameras?, *Euronews*, <https://www.euronews.com/2021/07/09/should-citizens-in-belgrade-be-concerned-by-newly-installed-surveillance-cameras>

<sup>7</sup> North Atlantic Treaty Organization (2020): Press Conference by NATO Secretary General Jens Stoltenberg, 22. Oct. 2020, [https://www.nato.int/cps/en/natohq/opinions\\_178946.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en)

<sup>8</sup> North Atlantic Treaty Organization (2021): Brussels Summit Communiqué, Press Release (2021) 086, 14. Jun. 2021, para 10

<sup>9</sup> European Commission (2021): 2021 State of the Union Address by President von der Leyen, 15. Sept. 2021, [https://ec.europa.eu/commission/presscorner/detail/en/speech\\_21\\_4701](https://ec.europa.eu/commission/presscorner/detail/en/speech_21_4701)

a coherent transatlantic strategy that includes critical infrastructure. So how can transatlantic cooperation for resilient transatlantic cybersecurity be operationalized?

The first step of such a transatlantic cybersecurity strategy could imply the continuous exchange of information on undersea cables between the U.S. and EU. For example, the U.S. and the U.K. could join France and Germany in regular meetings to initiate an exchange of information on undersea cables. This could also include possible cooperation opportunities and joint fleet exercises to maintain and secure undersea cables and their landing stations.

A second step could be to ensure high safety standards for undersea cables: By setting standards regarding the security of landing stations in coastal regions, the EU can make a sustainable contribution to securing the infrastructure, especially through its regulatory power for the member states.<sup>10</sup>

Third, transatlantic actors could advocate for legal protections for undersea cables. The 1982 United Nations Convention on the Law of the Sea (UNCLOS) does not prohibit states from considering undersea cables as legitimate wartime targets.<sup>11</sup> International legal cover under the UN would be profitable for all actors, regardless of their different interests. The Russian Federation and the People's Republic of China can also have no interest in enormous economic damage and interdiction of communications caused by destroyed cables.

The current situation reveals how vulnerable transatlantic security is. It is to be welcomed that attention around critical infrastructure is increasing even if there is still no talk of a holistic strategy between the transatlantic players. Military-civilian protection of undersea cables within the institutional framework of NATO and the EU can be used as a first step toward legalization within the UN framework. Whether attacking undersea cables in the context of war will be prohibited within the UN framework also depends on Russia and China.

---

<sup>10</sup> Morcos, Pierre/ Wall, Collin (2021): Invisible and Vital: Undersea Cables and Transatlantic Security, in: Center for Strategic & International Studies, <https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security>

<sup>11</sup> Sunak, Rishi (2017): Undersea Cables. Indispensable, insecure, in: Policy Exchange, p.17