Negative Brief: Dark Cables

By “Coach Vance” Trefethen

The AFF case is worried about the vulnerability of sea floor cables that handle internet traffic between North America and Europe. If a Russian submarine were to cut those cables, it could disrupt internet service throughout the country. Plan requires installation of "Dark Cables" - backup cables in secret "classified locations" that would only be activated in case of an outage.

Negative: Dark Cables 3

INHERENCY 3

1. Status Quo Redundancy solves 3

Lots of backup systems already in place. Russia wouldn't be able to significantly damage the internet 3

European cable systems have lots of redundancy and switch over is easy: The average cable only uses 18% of capacity 3

2. Status Quo cable deployment far exceeds AFF plan 3

AFF deploys 3 new cables. Status Quo is deploying dozens 3

HARMS / SIGNIFICANCE 4

1. Cable breaks happen all the time, with no impact 4

100 cable ruptures / year globally already happen (as of 2022) but no one notices 4

200 cable incidents / year (as of 2018) but there's no impact because there's plenty of redundancy and fast repairs 4

Cables to Europe get damaged all the time, but the traffic just gets re-routed, so no impact 4

2. No threat from Russia 5

Russia has more to lose than we do, plus there are repair ships always on patrol to fix any damage 5

Russian attack wouldn't cause much impact and wouldn't take everything down 5

Even if Russia did somehow chop every single cable to the U.S., the internet wouldn't go out 5

3. A/T "Military at risk" 5

No real threat: Military has satellite backup 5

Military threat is exaggerated 6

4. Pacific cables. Harms / Solvency dilemma 6

US has cables in the Pacific that connect globally. So either 1) There's no threat, no harm. Or 2) there is a threat but AFF doesn't solve, since they only solve for Europe 6

SOLVENCY 6

1. AFF's "Dark" cables won't stay dark 6

"Dark" cables AFF thinks they are hiding will be easy to find 6

2. "Secret location" cables will be damaged accidentally 6

If location isn't published, cables will be damaged accidentally by boating activity 6

3. Landing stations 7

Landing stations are where the cables finish their transit of the ocean and reach the shoreline 7

All cables are still vulnerable at the landing site, and they're not hard to find 7

Even if the AFF Plan did create new landing sites, nerds on the internet would find them and publish the location [and if a nerd can find them, so can a terrorist or a foreign country] 7

DISADVANTAGES 8

1. Solvency & Disadvantage Dilemma: Shortage of undersea cable maintenance technicians 8

AFF either 1) won't have the people needed to maintain the new cables (Solvency failure) OR 2) Will hire them away from working systems to manage systems no one is using (Disadvantage - outages get worse without qualified maintenance) 8

2. Masking Disadvantage: AFF case distracts us from the real threats 8

"Threat" of deliberate attack is exaggerated. We need to focus on the real threats: Marine activities and natural disasters 8

Negative: Dark Cables

INHERENCY

1. Status Quo Redundancy solves

Lots of backup systems already in place. Russia wouldn't be able to significantly damage the internet

Mark Scott 2022 (journalist) 29 Sept 2022 "Will Russia attack undersea internet cables next?" POLITICO (accessed 2 Oct 2022) https://www.politico.eu/article/everything-you-need-to-know-about-the-threat-to-undersea-internet-cables/

No one denies Moscow has the ability to attack these targets. But what it lacks is the capacity to carry out worldwide attacks at a scale to significantly hobble the West's internet infrastructure. In recent years, companies have built multiple redundancies into their undersea networks, primarily to ensure any short-term damage won't materially affect people's online activity. As internet usage has skyrocketed, so too have these deep-sea pipes that now connect disparate parts of the world via multiple alternative routes.

European cable systems have lots of redundancy and switch over is easy: The average cable only uses 18% of capacity

Christian BUEGER, Tobias LIEBETRAU, Jonas FRANKEN 2022 (Christian BUEGER, Professor of International Relations, Department of Political Science, University of Copenhagen, Denmark. Tobias LIEBETRAU, Postdoctoral Researcher, Centre de Recherches Internationales (CERI), *Paris Institute of Political Studies*, France. Jonas FRANKEN, Research Assistant, Science and Technology for Peace and Security, Technical University of Darmstadt, Germany) June 2022 (accessed 2 Oct 2022) Security threats to undersea communications cables and infrastructure – consequences for the EU https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO\_IDA(2022)702557\_EN.pdf

The continental EU Member States are connected by a tight network of terrestrial and submarine connections. All continental EU Member States are linked to at least two other members either by land or sea cable systems. On average, non-island EU Member States have 4.5 internal cross-border cable systems available. During partial failures of components, internet traffic is rerouted so that dysfunctions are circumvented, making state-wide internet blackouts highly improbable for the EU Member States. On average, submarine cables have only used 18 % of their maximum capacity.

2. Status Quo cable deployment far exceeds AFF plan

AFF deploys 3 new cables. Status Quo is deploying dozens

Justin Sherman 2021. (non-resident Fellow, Atlantic Council Cyber Statecraft Initiative; currently earning his MA in Security Studies from Georgetown University’s School of Foreign Service. He earned his BS in Computer Science and his BA in Political Science from Duke University) Cyber defense across the ocean floor: The geopolitics of submarine cable security 13 Sept 2021 (accessed 25 Sept 2022) https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/

By these numbers, the rate of submarine cable deployment is increasing. In 2016, fifteen new cables were ready for service around the world. In 2020, twenty-eight new cables entered service around the world, representing an almost twofold increase in just four years. This uptick is no accident—there are several drivers at play. More traffic is sent over the global Internet every year (discussed further in the third trends chapter). More countries are also looking to expand Internet penetration within their borders (e.g., how many people have Internet access) as well as to expand the bandwidth available to those Internet users.

HARMS / SIGNIFICANCE

1. Cable breaks happen all the time, with no impact

100 cable ruptures / year globally already happen (as of 2022) but no one notices

Christian BUEGER, Tobias LIEBETRAU, Jonas FRANKEN 2022 (Christian BUEGER, Professor of International Relations, Department of Political Science, University of Copenhagen, Denmark. Tobias LIEBETRAU, Postdoctoral Researcher, Centre de Recherches Internationales (CERI), *Paris Institute of Political Studies*, France. Jonas FRANKEN, Research Assistant, Science and Technology for Peace and Security, Technical University of Darmstadt, Germany) June 2022 (accessed 2 Oct 2022) Security threats to undersea communications cables and infrastructure – consequences for the EU https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO\_IDA(2022)702557\_EN.pdf

Multiple causes potentially render submarine data cables incapable of data transmission. Around 100 cable ruptures happen each year globally. End users hardly notice those faults because the data traffic is usually rerouted through alternative cable paths. Total internet outages only occur when there is no broadband redundancy available.

200 cable incidents / year (as of 2018) but there's no impact because there's plenty of redundancy and fast repairs

Garrett Hinck 2018 (PhD student in political science at Columbia University, studying international relations and the political economy of security. He was previously a research assistant with the Technology and International Affairs and Nuclear Policy programs at the Carnegie Endowment for International Peace) 5 Mar 2018 (accessed 25 Sept 2022) Evaluating the Russian Threat to Undersea Cables https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables

 Although each undersea cable transmits huge quantities of data, the cable network has significant [redundancy](http://searchnetworking.techtarget.com/feature/Undersea-cables-keep-global-enterprise-networks-afloat) capacity. Rupturing one cable can cause temporary disruptions but does not cut off service. When a major cable to Vietnam [failed](https://dyn.com/blog/cuba-up-vietnam-down-recent-subsea-cable-developments/) last year, customers in Ho Chi Minh City briefly lost connectivity. Because internet routing protocols direct data around points of failure, traffic flows [adjust](https://blog.cloudflare.com/not-one-not-two-but-three-undersea-cables-cut-in-jersey/) to the lost connection and send data over other cables to the same endpoint. Wayward anchors and storms regularly cause [cable faults](https://www.weforum.org/agenda/2015/11/how-can-we-protect-the-internets-undersea-cables/), about 200 a year; repair ships are readily available to mend broken lines. Cutting the United States off from the rest of the world would require severing a large number of cables: at least 18 in the North Atlantic alone, according to Telegeography’s [cable map](https://www.submarinecablemap.com/#/), and many more connecting the U.S. to Latin America and Asia.

Cables to Europe get damaged all the time, but the traffic just gets re-routed, so no impact

Louise Mitsakis 2018 (journalist) 5 Jan 2018 " What Would Really Happen If Russia Attacked Undersea Internet Cables" (accessed 1 Oct 2022) https://www.wired.com/story/russia-undersea-internet-cables/

For one, ruptures aren’t exactly an anomaly. One of the [estimated](https://blog.telegeography.com/frequently-asked-questions-about-undersea-submarine-cables) 428 undersea cables worldwide is damaged every couple of days. Nearly all faults aren’t intentional. They’re caused by underwater earthquakes, rock slides, anchors, and boats. That’s not to say that humans are incapable of purposefully messing with the cables; off the coast of Vietnam in 2007, fishermen [pulled up](https://www.computerworld.com/article/2541664/networking/fishermen-pull-the-plug-on-vietnam-s-web--steal-cable-for-scrap.html) 27 miles of fiber cords, disrupting service for several months. (It wasn't cut off completely, because the country had one more cable that kept the internet going.) You don’t notice when a cable faults, especially if you live somewhere like the United States, because your Instagram message or Google Voice call is instantly re-routed. If you’re Skyping with a friend in Romania for instance, and a fishing boat or anchor ruptures a cable—as causes two-thirds of faults—your conversation simply goes over another line. Many regions, like Europe, the United States, and East Asia have numerous cables running over the same path.

2. No threat from Russia

Russia has more to lose than we do, plus there are repair ships always on patrol to fix any damage

Louise Mitsakis 2018 (journalist) 5 Jan 2018 " What Would Really Happen If Russia Attacked Undersea Internet Cables" (accessed 1 Oct 2022) (brackets in original) https://www.wired.com/story/russia-undersea-internet-cables/

Because faults happen so frequently, cable repair ships patrol nearly all of the world’s waters. Even if Russia did start snipping, there are crews equipped to rapidly repair them. Besides, Russia’s epic hypothetical cable attack would primarily harm its own people, as another Telegeography analyst pointed out in a [video](https://blog.telegeography.com/can-russian-submarines-attack-submarine-cables). “It would hurt the Russians perhaps even more than it would hurt [Americans]. They’re far more dependent on international networks than we are, because so much of our content is stored locally” says senior analyst Jonathan Hjembo.

Russian attack wouldn't cause much impact and wouldn't take everything down

Mark Scott 2022 (journalist) 29 Sept 2022 "Will Russia attack undersea internet cables next?" POLITICO (accessed 2 Oct 2022) https://www.politico.eu/article/everything-you-need-to-know-about-the-threat-to-undersea-internet-cables/

If the Kremlin did attack, for instance, it could possibly take down part of a regional network connecting the Baltic countries with the rest of Europe. But to have a long-term impact on the world's network of undersea cables, Russia — or any other aggressor — would have to act at a scale that would likely be easily detectable to Western national security agencies. It would also damage its own citizens' access to the internet. "We're no longer in the position that once we were where you cut one cable and everything goes down," said Chatham House's Giles.

Even if Russia did somehow chop every single cable to the U.S., the internet wouldn't go out

Louise Mitsakis 2018 (journalist) 5 Jan 2018 " What Would Really Happen If Russia Attacked Undersea Internet Cables" (accessed 1 Oct 2022) https://www.wired.com/story/russia-undersea-internet-cables/

Even in a hypothetical, Black Mirror-esque world in which Russia somehow chops every cable that connects to the United States from every side, the internet would not go out like a light. Americans would still be able to utilize land networks that connect the continent; it would just be impossible to communicate overseas.

3. A/T "Military at risk"

No real threat: Military has satellite backup

Mark Scott 2022 (journalist) 29 Sept 2022 "Will Russia attack undersea internet cables next?" POLITICO (accessed 2 Oct 2022) https://www.politico.eu/article/everything-you-need-to-know-about-the-threat-to-undersea-internet-cables/

Almost two years ago, Jens Stoltenberg, NATO secretary general, [told reporters](https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en) undersea cables were vital not just for civilian society purposes — such as the functioning of financial markets — but also "for different military capabilities." Most Western military can quickly turn to backup satellite communications if these undersea cables become compromised. So far, the concerns over the vulnerability of these seabed cables have yet to be borne out in reality.

Military threat is exaggerated

Louise Mitsakis 2018 (journalist) 5 Jan 2018 " What Would Really Happen If Russia Attacked Undersea Internet Cables" (accessed 1 Oct 2022) https://www.wired.com/story/russia-undersea-internet-cables/

The idea of the global internet going dark because some cables were damaged is frightening. But if Russia or anyone else were to snip a handful of the garden hose-sized lines, experts say that the consequences would likely be less severe than the picture the military paints. The world’s internet infrastructure is vulnerable, but Russia doesn't present the greatest threat. There are plenty of more complicated problems, that start with understanding how the cable system actually works. “The amount of anxiety about somebody sabotaging a single cable or multiple cables is overblown,” says Nicole Starosielski, a professor at New York University who spent six years studying internet cables to write the [The Undersea Network](https://www.dukeupress.edu/the-undersea-network%22%20%5Ct%20%22_blank). “If somebody knew how these systems worked and if they staged an attack in the right way, then they could disrupt the entire system. But the likelihood of that happening is very small. Most of the concerns and fears are not nearly a threat at all.”

4. Pacific cables. Harms / Solvency dilemma

US has cables in the Pacific that connect globally. So either 1) There's no threat, no harm. Or 2) there is a threat but AFF doesn't solve, since they only solve for Europe

Louise Mitsakis 2018 (journalist) 5 Jan 2018 " What Would Really Happen If Russia Attacked Undersea Internet Cables" (accessed 1 Oct 2022) https://www.wired.com/story/russia-undersea-internet-cables/

Many regions, like Europe, the United States, and East Asia have numerous cables running over the same path. You can check out a map of them all [here](https://www.submarinecablemap.com/). That means Russia snipping a handful of cables in the Atlantic, where its submarines have been spotted, would disturb the global internet very little. In fact, even if it ruptured every single cable in the Atlantic Ocean, traffic could still be re-routed the other way, across the Pacific.

SOLVENCY

1. AFF's "Dark" cables won't stay dark

"Dark" cables AFF thinks they are hiding will be easy to find

Bryan Clark 2016. (senior fellow with the Center for Strategic and Budgetary Assessments, in Washington) Undersea cables and the future of submarine competition 15 June 2016 (accessed 2 Oct 2022) https://www.tandfonline.com/doi/full/10.1080/00963402.2016.1195636?src=recsys

Tapping today’s fiber-optic cables is theoretically possible, but it is easier to cut or damage them and significantly impact the cables’ users. And while the exact location of cables is not publicly available, improvements to “bottom survey” equipment and unmanned undersea vehicles are making finding cables easier and faster.

2. "Secret location" cables will be damaged accidentally

If location isn't published, cables will be damaged accidentally by boating activity

Christian BUEGER, Tobias LIEBETRAU, Jonas FRANKEN 2022 (Christian BUEGER, Professor of International Relations, Department of Political Science, University of Copenhagen, Denmark. Tobias LIEBETRAU, Postdoctoral Researcher, Centre de Recherches Internationales (CERI), *Paris Institute of Political Studies*, France. Jonas FRANKEN, Research Assistant, Science and Technology for Peace and Security, Technical University of Darmstadt, Germany) June 2022 (accessed 2 Oct 2022) Security threats to undersea communications cables and infrastructure – consequences for the EU https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO\_IDA(2022)702557\_EN.pdf

The vulnerability of the cable component differs depending on its position. In coastal and shallow waters, the location of cables is usually publicly available to prevent accidents by anchoring and dredging. Positions are marked on navigational charts to ensure awareness of marine users.

3. Landing stations

Landing stations are where the cables finish their transit of the ocean and reach the shoreline

And the AFF plan doesn't create any new landing stations, so they'll just have to use the existing ones.

All cables are still vulnerable at the landing site, and they're not hard to find

Bryan Clark 2016. (senior fellow with the Center for Strategic and Budgetary Assessments, in Washington) Undersea cables and the future of submarine competition 15 June 2016 (accessed 2 Oct 2022) https://www.tandfonline.com/doi/full/10.1080/00963402.2016.1195636?src=recsys

In addition to the cables themselves, their onshore termination points are particularly vulnerable – and easier to find than a submerged cable. Sometimes consisting of a non-descript building on a beach or marshland, these locations are often the junction of several cables that are then connected with terrestrial phone and cellular networks. An accident or attack on one of them could have the same effect, in the short-term, of cutting multiple cables at once.

Even if the AFF Plan did create new landing sites, nerds on the internet would find them and publish the location [and if a nerd can find them, so can a terrorist or a foreign country]

Christian BUEGER, Tobias LIEBETRAU, Jonas FRANKEN 2022 (Christian BUEGER, Professor of International Relations, Department of Political Science, University of Copenhagen, Denmark. Tobias LIEBETRAU, Postdoctoral Researcher, Centre de Recherches Internationales (CERI), *Paris Institute of Political Studies*, France. Jonas FRANKEN, Research Assistant, Science and Technology for Peace and Security, Technical University of Darmstadt, Germany) June 2022 (accessed 2 Oct 2022) Security threats to undersea communications cables and infrastructure – consequences for the EU https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO\_IDA(2022)702557\_EN.pdf

In landing stations, undersea network traffic terminates and connects to the terrestrial network of the local operator. Landing stations tend to be close to the shore and are often collocated with submarine electricity networks or other critical infrastructures. Landing stations host servers, routing and switching technologies that provide the bridge to the terrestrial network. They tend to be physically protected by fences or barb wire and remote surveillance equipment, such as cameras and sensors. The precise locations of landing stations are not in the public domain, although there are indicative maps that potentially make these easy to identify. Indeed, a transnational landing station ‘spotting community’ exists that aims to take photographs of landing stations and post their precise location on the internet fora.

DISADVANTAGES

1. Solvency & Disadvantage Dilemma: Shortage of undersea cable maintenance technicians

AFF either 1) won't have the people needed to maintain the new cables (Solvency failure) OR 2) Will hire them away from working systems to manage systems no one is using (Disadvantage - outages get worse without qualified maintenance)

Prof. Nicole Starosielski 2015 (professor of media at Duke Univ., specialist in undersea cables) SCIENTIFIC AMERICAN 27 Mar 2015 " Undersea Cable Network Operates in a State of Alarm [Excerpt]" (accessed 2 Oct 2022) https://www.scientificamerican.com/article/undersea-cable-network-operates-in-a-state-of-alarm-excerpt/

When I ask operators about the vulnerabilities of today’s undersea network, many express concerns about downsizing and retirements. They fear that carefully sustained industry knowledge will be lost and that there will be nobody to take their place that will adhere to the same standards of reliability. Recruiting the next generation of workers is difficult. There is no direct path to the industry and it remains largely invisible to the public. One engineer describes the situation, “Nobody goes to school and says I want to be in the undersea cable business.” In many ways, the operation of the undersea cable system is in opposition to the everyday tech culture: it is built on an ethos of durability, rather than disposability. Many ask who will ensure the continuity of the cable networks, if their industry starts to take a path toward quicker turnover, devalued labor, or planned obsolescence? Who will ensure that the bodies maintaining our undersea networks are as reliable as the cable technology?

2. Masking Disadvantage: AFF case distracts us from the real threats

"Threat" of deliberate attack is exaggerated. We need to focus on the real threats: Marine activities and natural disasters

Christian Bueger and Tobias Liebetrau 2021 (*Christian Bueger is a professor of international relations at the University of Copenhagen, and one of the directors of SafeSeas. Tobias Liebetrau is a postdoctoral researcher at Paris Institute of Political Studies*) 15 Sept 2021 " Beyond Triple Invisibility: Do Submarine Data Cables Require Better Security?" (accessed 2 Oct 2022) https://theglobalobservatory.org/2021/09/beyond-triple-invisibility-do-submarine-data-cables-require-better-security/

While many of the threat scenarios of deliberate attacks to cables are over-exaggerated, there is a need to zoom in on the actual vulnerabilities the network faces, mainly [accidental damage and non-human hazards.](https://www.youtube.com/watch?v=iQZYcdf4VZg) Accidents or malfunctions stemming from marine activities such as fishing and shipping account for at least 40 percent of the damage done to the undersea cable infrastructure. Earthquakes, volcanic eruptions, tsunamis, landslides, and sharks feature among the non-human threats. Much of the protection of the cables will continue to revolve around mundane technical tasks.