Deep Ocean Danger: Unveiling the Threats to Global Connectivity

[00:00:00]

Charles Mok: If I want to disrupt connection into the United States, I don't need to bother about coming all the way to your shore. I would do it in the middle of the ocean. I would do it in the East Asian shores. If I want to disrupt your connectivities to Europe, I would do it around the waters around Ireland, Iceland, rather than coming over to your shores.

[00:00:29] Podcast Welcome

Ryan Vest: Welcome to *Horns of a Dilemma*, the podcast of the *Texas National Security Review*. I'm Ryan Vest, executive editor of *TNSR*, and I'm here with our editor-in-chief, Dr. Sheena Chestnut Greitens. We're pleased to have joining us today Charles Mok, author of "Toward Undersea Cable Resilience: The Case for Global Collaboration," which is featured in Volume 9, Issue 3 of *TNSR*. Charles is a research scholar at the Global Digital Policy Incubator of the Center on Democracy, Development, and Rule of Law at Stanford University. He is also a member of the board of trustees of the Internet Society and formerly an elected member of the Legislative Council in Hong Kong, representing the information technology functional constituency from 2012 to 2020.

As an entrepreneur, in 1994, Charles co-founded HKNet, one of the earliest internet service providers in Hong Kong. He holds a BS in computer and electrical engineering and an MS in electrical engineering from Purdue University. Charles, welcome to *Horns of a Dilemma*.

Charles Mok: Thank you. Thanks for having me.

Sheena Chestnut Greitens: Charles, we're really excited to discuss your article today.

[00:01:32] Why Attacks Rising

Sheena Chestnut Greitens: Early in the article, you start with an observation that we've seen a sharp rise in attacks on undersea infrastructure in the last decade. So to get us started, could you tell our audience a little bit about why you think we've seen this trend accelerating, and what advantages it might provide to the people doing it?

Charles Mok: Well, undersea cable disruption is not new, right? Because we have a lot of cable systems under the sea for, you know, way back when people were using telegrams or even, yeah, long distance telephone. They all rely on undersea cable infrastructure. But of course, with the internet now, the dependence, and the proliferation of cable systems has just become much faster in the last few decades.

But in the past, most of the disruptions were because of natural reasons, right? Because of earthquakes, tsunamis, or even natural accidents that happen with fishing vessels, and so on. But now we're seeing more, and why? I think, first of all, it's because of the global tension that we see in many parts of the world. And there are countries, I believe, that are trying to take advantage of the fact that there are many of these choke points, and also national economies are becoming more and more dependent on the internet, and telecommunications, and data communications, and not to mention AI.

So there is a much more of a tendency, or a reason, for certain actors to use undersea cables as a point of vulnerability, when they want to maybe test the resilience of certain countries, of their adversaries, or just to also conduct experiments about their techniques, about how they can conduct these kinds of disruptions.

[00:03:25] Out of Sight Risks

Ryan Vest: Charles, undersea cables carry about 99% of intercontinental data transmission, yet serious discussions of these operations are often underrepresented in national security circles, and we don't see a lot of talk on this in a lot of journals. Why aren't we talking more about undersea infrastructure, and really more importantly, how to defend it?

Charles Mok: Well, first of all, I think over the last two or three years, there has been quite a bit more of attention on it from the policy research, or national security circle of researchers, and so on.

But I guess the reason why the general public or even in certain respects, authorities, governments, are not as vigilant about the situations with undersea cables is simply because it's out of sight, and it's out of mind. And also, I think, with the proliferation of wireless devices, and people would like to talk about satellites because they're fancy, they're expensive, and they are sexy to talk about.

Versus if you're thinking about undersea cable, this is actually a 100-year-old kind of infrastructure that, you know, we've seen technological advances, but, by and large, we're using this, a lot of the same types of technologies that we've used for decades, or even for the last century. So it's not as sexy to talk about, and I guess people just have a tendency to talk about what they can see.

And even if we look at some of the gray zone tactics that adversaries are using these days, many of them are very similar, whether they are out above water, or undersea. But people tend to talk about what they can see above water, when they are talking about many of these choke points that we see.

Like what we are seeing in Iran right now, people talk about what's above the water. But in fact, the same, I could argue, is also happening under the sea, in terms of the vulnerabilities that exist.

[00:05:27] Supply Chain Weak Links

Sheena Chestnut Greitens: One of the things I really liked about your article is that in discussing the resilience of these undersea cable networks, you talk about how the fact that resilience isn't just a matter of defending the cables themselves, but also of looking at broader supply chains, and the ecosystem around them.

Do you think that democracies are paying enough attention to these broader sets of questions like who manufactures components, controls repair capabilities, provides maintenance to the cables, and shapes the future geography of new cable routes?

Tell us a little bit about that.

Charles Mok: I guess yes and no. They're very reactive unfortunately, and there are reasons for that. I think part of the reason that democracies, or even countries generally in most parts of the world, are not paying enough attention to undersea cables is because as an industry, it is not a particularly profitable industry.

Let me put it this way. It costs a lot of money, a huge amount of investment, a very long-term investment for companies. Traditionally, telecommunications operators, they get into consortiums across different geographies, countries, and then they lay these cables across the ocean and so on, for long distance particularly–if we're talking about the Atlantic or the Pacific. And then, they share the revenues and the operations of these cables for decades.

So the investment is huge, but you wouldn't say that they are very short-term, very quickly, very profitable, compared to a lot of the things that we're talking about today, you know, SpaceX, IPOs and so on. You won't see that for undersea cables. So in a sense, that's actually also why I believe a kind of industrial reason why these kinds of things used to be associated more with traditional telecom operators.

That has been changing, right? Because particularly in recent years, if we think about the United States, most of these investments are coming from the big techs, from the Googles, Amazon, Microsoft and types of companies. So that's changing. That's why when we think about the companies that are going about doing the groundwork of laying the undersea cables, doing the repairs when there is breakage, that's not very profitable.

And that's why when we look at the repair ships, they tend to be very old, worn out, and very difficult to get companies to invest in them. You know, they're not just the kind of things that your VCs would like to invest in. And that's why the industry, in terms of the laying, and maintenance, and repair of undersea cables, is very concentrated into a small number of companies. One US company, one French company, and one Japanese company. Those are traditionally the big three, and then emerging in the last several years more and more a Chinese company, which used to be owned by Huawei.

So that's it, because nobody would really want to jump into it just because it's going to be very profitable. So that makes it difficult, in a sense, from an industrial point of view. And then obviously also because for governments, again, there are a lot of other technology or infrastructure issues that tend to get their attention a lot more. People talk about AI, they set data center build out, and then talk about energy grid, and so on. To them, maybe to the policymakers, that take up more of their attention than some of these issues like undersea cables. That seems a little bit remote to them.

[00:09:20] Who Pays for Security

Ryan Vest: I'd like to pull on that just a little bit more, Charles.

Charles Mok: Sure.

Ryan Vest: It seems like we've identified a seam here that private companies own this infrastructure, but foreign governments are destroying that infrastructure for national security, or international political reasons. Is this something that policymakers should be more involved with by looking and saying–we need to find a better way to support private industry, because they're the ones actually paying the price for these international conflicts, if that makes sense?

Charles Mok: Oh, definitely. That's exactly, you know, kind of one of the arguments that I want to make. And you actually are seeing some kind of activity similar to that, particularly in the EU. Because if you think about the European situation in particular, when they talk about these undersea infrastructures, they are not only for communications, for data, they are also frequently co-located with gas pipes, with electricity undersea cables that has to do with, you know, these countries sharing their electricity grids across different countries.

So that's why when these kinds of infrastructure problems or disruption happens in the Nordic, in the last two or three years, the effect is actually even felt much greater than just data communications. And we did see that in the last several years in terms of the European communities, there has been efforts of using state fundings from the state investment banks, for example, from different countries and for the EU as a whole, to try to identify certain choke points, or identify certain infrastructure, that needs to be strengthened across various member states, to help them create a better investment incentive, and so on.

Now, obviously, that hasn't happened in the US. Maybe this is not the tradition of this country. But I would say that that should be something that we should look at, in terms of incentives that might have a little bit more to do with the economics, rather than in addition to some of the things that they are talking about–they have been talking about–including this country, in the US, about, for example, easing licensing conditions, making it easier for companies to invest in undersea cables, and also very importantly as well, the landing station infrastructures that goes with the undersea infrastructure.

There has been work in that area, including from the FCC, but I guess not particularly in terms of creating a better economic incentive.

[00:11:59] Big Tech Takes Over

Charles Mok: And one of the effects of that is that, at least in the United States, new investment in undersea cables has been dominated by the big techs because of their, you know, data center, AI investment, and so on. But to a much lesser degree, the traditional players like the telecom companies, and so on.

What's the problem with that? Not that we hate the big techs, but they build these infrastructures for their own use, right? Because if Google builds it, it's for Google and for their AI, for their search, and for the data centers. AWS builds it for their own cloud services. Likewise for Microsoft, for Meta, and so on, right? But what about the rest of the users, right? The rest of the applications that are needed, right?

So traditionally that has been the work done by the telecom operators. But the telecom operators are not the most, you know, profitable, or rich companies, around these days. So for them to make the kind of investment to compete with these big tech companies would be relatively difficult. Which means that in the future, the rest of the industry may have a difficult time to get new cable capacities in these countries, unless you buy it from the big techs.

Unless you use Google Cloud, or Microsoft, or AWS cloud services, otherwise you would be out of luck. Is that the situation that we want to see? I think this is actually one of the industrial issues that hasn't gotten a lot of attention.

[00:13:40] AI Needs Connectivity

Sheena Chestnut Greitens: I wanted to ask you a question about kind of looking forward, which is that, AI is a huge topic across all realms of national security today, it seems like. But I actually think that the role of undersea infrastructure in enabling AI is often ignored in these conversations. And so I wanted to ask you if you could tell readers about how you think about this issue.

How important are undersea cables to AI data processing, to what we might be looking at with the role of AI in the future? And, therefore, what should we be thinking about as we approach this problem?

Charles Mok: Yeah. I think it's important. To me at the very least, AI is an infrastructure. It is an application that runs on the internet. Without the internet, if everybody has an isolated machine that is super intelligent and they cannot communicate across distance and so on, what's the use of that, right?

And then it's not a coincidence, I think, that the way you see some of the big AI players today, they're also big in infrastructure, internet infrastructure, including, like we mentioned, you know, Google, Microsoft, and so on. So, these companies actually do have a little bit of advantage, I think, in that sense. But in the future, when we are seeing all these Stargate projects popping up, with data centers all around the world, not just within the United States, you will need to connect them better. You will definitely need connectivity a lot less.

There are also, of course, options of, you know, using satellite communications and so on. But one thing I need to mention is always, that we need to remind people that this is more expensive, tends to be slower, even though that technology is advancing very quickly. And also, there are still certain latency issues that for certain applications, they might present problems if you just send them, you know, all the way up to the sky and come back.

So, but of course, that will always be a backup solution. But it is kind of difficult to imagine that with the, you know, hundreds and thousands of cable systems around the world, and they could be, you know, over a short period of time, let's say a couple decades, be replaced by satellite technologies. That simply is impossible.

[00:16:08] Chokepoints as Terrain

Ryan Vest: In the article, you talk a lot about how many of these incidents that we've seen recently occur around congested choke points and geopolitically sensitive regions. How is that shifting the way that we see national security or international security? Are places like the Baltic Sea or the waters around Taiwan, some of these places in the South China Sea, are these becoming the new key terrain for future conflict?

Charles Mok: Yes, I think even with the war in Ukraine, even though this is not–we're not just–we're talking about more of a landlock situation. But if you remember in the first couple of months or weeks after the invasion, what did Russia do for the territory that they occupied? They cut off the internet. They rerouted the internet to Moscow, rather than to the West, for those areas that they occupied.

So it's the same thing, especially for economies, countries that are surrounded by water, for example, like Taiwan, or in a region where there's a huge concentration of these cables, such as the Nordics. You could either use these cutting undersea cables as a way of blockade, or as well as a way to disrupt your economic activities.

We're seeing examples today–right now–with the Iran war. The Iranian government recently, you know, they actually hinted, they haven't done it. They hinted that, "Oh, maybe we should charge those undersea cables that go under the Strait of Hormuz, because, if we can talk about charging ships going through, why don't we put a higher licensing fee for these cables that go under the water?" So it's the same thing.

It has been, I guess, over the years, or particularly many of the adversarial countries that we have, are discovering that there's this choke point, there's this dependency, and they will take advantage of it. Just like every other choke point, we talk about supply chain, we talk about semiconductors, whatever, and so on.

People would look at where the choke points are and say, "Hey, why don't we try to profit from it, or try to disrupt our adversaries by taking advantage of these choke points and, yeah, to our advantage."

[00:18:33] Attribution and Law

Sheena Chestnut Greitens: So I'm really interested in another point that you raise, about the nature of these incidents that we've seen. And the article points out that some of the vessels implicated in these incidents where cable infrastructure is damaged are owned, or registered, in Russia or China.

But there are some complicated questions around ownership, flagging, sort of corporate opacity, state direction that really complicate the task of assessing responsibility, and basically what we call attribution, right? And so that slows down, or has certain effects on decision processes.

So for folks who might be learning about some of these incidents, or thinking about this for the first time, how does the nature of the ownership, or flagging, or the identity of the vessels involved, create particular challenges for dealing with this as an international security issue?

Charles Mok: Yeah. Aren't we seeing the same thing with the shadow fleets that we're talking about recently, about the vessels that are bypassing the US, or international sanctions on Iranian oil, or gas, and so on, right? They're the same, in many ways, whether you're talking about these shadow fleets that are bypassing some of these sanctions or causing disruption by cutting cables under the water. They might be different kinds of vessels, but the concept is very similar. And usually, often they are registered to either, Russia or China, or even many of these countries that are quite remote, and for authorities, particularly

Western countries, very difficult to trace, and try to follow through with any kind of–if there is an incident, for example.

So sometimes they would be registered to some little countries in Africa and so on. Why? The reason is because under the international laws of the seas currently that we have, which are 100-year-old laws that are still existing, being enforced. If an incident, let's say, happened within your territorial water or your economic zone, you can establish your own law to try to say what the consequence will be. And that's exactly what some countries have been stepping up to do recently, including Taiwan.

But, if it is in international waters, if something happens to, let's say, undersea cables in international waters–it got cut–who gets the jurisdiction of that particular incident legally, or if the owners and so on want to pursue it, or if a national government wants to pursue it? It is actually the ship that caused the damage, and whichever country that they are registered to, rather than the owner of the property under the water, right? So in that case, now what do you do if this is a Chinese ship, or Russian ship, or a Cameroon ship, that is registered? Even if you were able to identify who the perpetrator was. So it's difficult. So that's why there's an extra incentive for many of these vessels to hide their identities, or to register themselves to countries that are probably remote, or difficult, or not very cooperative with Western governments, and so on.

But on the other hand, I think it's also a tendency right now, for example, with, let's say some of the surveillance activities that are being conducted by NATO and EU in Europe, and they are trying to share information across governments to flag these ships. They look very carefully about these ships, where they come from, and where they are registered. And they would probably flag some of these ships from some of these countries as higher risk. And if they see them coming into the international or domestic waters within their jurisdiction, they might try to watch them more closely. But that's about what they can do. But otherwise, if something happens in international waters, it's difficult under current law.

Sheena Chestnut Greitens: So I thought this was a really interesting point that your article brings out, about the potential impact here, not just of the sabotage incident itself, or the sort of physical damage to the infrastructure that can result, but the sort of second-order effect of decision, or process paralysis in terms of what happens afterwards, and what precedents that might set, or expectations that might set about imposing costs on bad actors who are maybe engaged in some of this behavior.

Do you think that it's accurate to be concerned that this is a way that authoritarian actors in the international system might be exploiting not just the dependence and the vulnerability that comes with dependence on this infrastructure, but some of the gaps, or I guess, loopholes in things like UNCLOS–the UN Convention on the Law of the Sea–or these attribution and decision-making processes that were maybe formed when cable infrastructure was first being laid down, but are now being sort of used and employed in a very, potentially very different geopolitical environment?

[00:24:15] Deterrence and Patrols

Charles Mok: I think so. But I also think that actually the fact that within the last two or three years, particularly in the Nordic and in around Taiwan, where we saw many of these incidents occurring, the interesting thing that I observe, I think, is that there was a peak of these activities around 2024 and '25, and then it taper off quite a bit. I think what happened was, these authoritarian countries and their shadow fleets were really conducting exercises to try to figure out, okay, if I want to cut cables, what should I do? How do I do it? I mean, we want practice, right? So they did it.

But at the same time, because of that, I think they provoked the European authorities, and to a large extent also the Taiwan authorities to do something about it. So what did they do? They stepped up some of the laws. In Taiwan, they passed seven marine-related laws by amending some of the existing law to empower the local governments to have more authorities in terms of pursuing some of these perpetrators. But of course, you have to catch them first. So that means they stepped up the patrolling. Very similar situation by stepping up patrolling and information sharing in the Nordics among, you know, countries in that region, and so on. So, there has been more resilience because of these gray zone activities.

So, I think, in a way, you know, UNCLOS is going to be difficult to change in the short term, but countries are trying to do what they can within their own jurisdiction and capabilities, to try to be more vigilant. So maybe the authoritarian governments are figuring out that–okay, we have done our exercise, the more we do, probably, you know–And there were a couple of cases of arrest too, right? In the Nordic, there was one arrest, and that because of the fact that that ship was actually registered to Hong Kong, the person was actually now being arraigned in Hong Kong. Even though I think the–under their existing law, the punishment would be very light, and not to mention Hong Kong is part of China.

And also, there are cases in Taiwan where the captains of the ship were arrested. Even though you might say that to the shadow fleets, these are low bodies and so on. The authoritarian governments probably don't care about them, but so on. But still, there is some effect of some of these cases happening, and that might be a slight deterrent to some of these hired guns continuing to do the work for these governments.

Ryan Vest: A little earlier in our discussion, you mentioned that major US tech firms are starting to get more involved in this space as opposed to traditional telecommunication firms. So we've seen Google, Meta, Microsoft, Amazon–some of these companies that are getting deeply involved in undersea cable projects. Having these big companies with a lot of resources start to get involved, does this create any kind of resilience or advantage strategically for the United States, or does it introduce new strategic dependencies on private companies?

Charles Mok: I think it's probably more of the latter because, as I said, traditionally, undersea cable infrastructure was owned by the telecommunication companies. And telecom companies just simply basically say, you know, "I am going to build this capacity, and I'm going to rent it out to everybody." Now, some of their users have more money than the telecom companies basically, and they're saying, "Why do I want to pay you and rent your facilities? I'm going to build my own facilities. I have the control end to end," and so on.

Which means that the companies that profited from the requirements for this usage, this capacity being the telecom companies, are actually losing business. So the economic case for them to invest is even lower. And then if I am a user, unless I use Google Cloud, AWS, and so on, I would not be able to make use of these new capacities that are being built by the big tech companies.

So I would say that there's a bit of a worry in that area, and particularly because undersea cables typically are consortiums, and between telecom companies, US American telecom companies working with, you know, let's say if they need to connect a cable to Europe, they need to get other European counterparts into their consortiums, and then they share the cost, share the revenues, share the operation, and so on.

Now, that dynamic has been changing a lot, particularly on the American side, but not so much on the other side. I don't even see Chinese big tech investing heavily into undersea cable, only the American big tech. Well, probably one reason is because Chinese big techs are still not state-owned, and China wants to monopolize that to the state-owned China Telecom and so on. So, that's not even happening in China, not to mention Europe, where you don't see a lot of these huge, profitable, big tech companies anyway. So this is only an American phenomenon.

I would say that the worry is that if the American telecom companies are becoming weaker and weaker, and do not have the capacity to participate in many of these consortiums anymore, then when Europe gets connected to Africa, the American companies will be out of the pictures, and so on. So is that something that we want to see? It might cause other problems down the road.

[00:30:07] Allied Strategy Needed

Sheena Chestnut Greitens: Okay, so the proverbial million-dollar question here, and in this case, I suspect it's well more than a million-dollar question at stake, but to use that phrase, I wanted to ask you, how does Washington make this question of undersea cable resilience a genuinely allied project, given the fragmentation across country approaches, jurisdictions, the issue of coordinating with the private sector, the range of private sector actors involved?

What does it look like if that succeeds, right? What does success look like in terms of a strategy for allied undersea cable resistance? And what happens if the effort fails? What's at stake here?

Charles Mok: Yeah. I think for better and for worse, right now the American consideration about the threat in undersea cables is focused on China. For better because there's a real threat, particularly in the East Asia region, particularly we consider the situation around Taiwan. But the problem is that I think, not just this administration, it's actually tradition for a while. We think of the US FCC, a type of the regulatory bodies in the US government that overlook these kinds of activities.

They typically have been looking at this from a point of view of, for example, when I first got interested in this topic, it was back in 2019 and 2020, when the US government decided that they are not going to allow new undersea cable investment from the United States–from US companies into Hong Kong. And that happened actually quite early, around 2020, or just before 2020.

The reason was because of a fear of surveillance, because they said if these US-owned cables are terminating to a, you know, to an adversary's territory, they are worried about surveillance activities. If there are co-investors in these cables that happen to be Chinese companies, they're worried about these infrastructure being compromised and so on. That's fine, but to me, that's still kind of defensive.

More recently, last year, the FCC put out a new rule, basically to clean up–to demand that undersea cable landings in the US need to be number one–there's no Chinese technologies, or Chinese company's investment involved. They want to get rid of that. Again, fine, but to me it is a bit more defensive.

If I am your adversary, if I want to disrupt connection into the United States, I don't need to bother about, you know, coming all the way to your shore and doing it on your, you know, landing stations. What I can do is, if I want to do something about your connection to the Pacific, I would do it in the middle of the ocean. I would do it in the East Asian shores. If I want to disrupt your connectivities to Europe, I would do it around the waters around Ireland, Iceland, rather than coming over to your shores.

So my worry is that many of these policies are still more focused on, you know, don't touch the United States. Don't touch my shores. You know, get out of my territory and so on, which I don't think there's a lot of those here anyway to begin with. So my thinking is that, and part of the reasons that I am looking into these matters, and talking about it, and writing this article is also to try to tell the US policymakers that it is important to work with and to look at your connectivities from a broader perspective, that if something happen in Africa, actually it affects you. If something happens, not to mention in the Pacific and Atlantic that's even closer, it affects you.

So you have to work with your partners, in investment, in information sharing, in hardening the infrastructure, upgrading the regulatory regimes and so on, all of these matters. So that's what I was trying to, you know, get across. And I do worry about the more inward-looking tendencies in the United States. I do understand that, for example, the China Committee had a meeting, or a hearing about a month ago on this particular topic of undersea cable resilience. But I would have to say that is more talking about, just strictly about the situation around Taiwan, and maybe the Chinese investment, and so on. So for better or worse, there's a lot of talk about China, but just don't think about China alone. It's a global issue.

Undersea cables, we worry about being disrupted. It's just like I was just thinking about this morning. It's just like drones. Like, what can we do about drones? How do you stop them from hitting your buildings, right? It's probably very hard to do. They're just out there. And the best you can do is to try to, you know, upgrade all the things that we talked about, your legal infrastructure, your resilience in terms of helping the industry so that they can have better capacity to be more resilient, and working with your allies to share information, to make sure that future routings–

[00:35:52] Rerouting and Resilience

Charles Mok: You mentioned routing. Actually, there are new routings that are being developed recently, and that is in reaction to some of the disruption in the traditional route of the US going to Asia. Typically in the past, they go through from the West Coast to Japan, down to Hong Kong, down to Singapore. But since Hong Kong is taken out of the picture, and Taiwan has become more vulnerable, what has happened?

New investment, including many of the cables that we have mentioned from, you know, companies like Google and Meta, they go through from the West Coast to Guam, to the Philippines, and then down to maybe Indonesia, and back up to Singapore. So they are rerouting themselves naturally around these geopolitical issues recently. The industry is making adjustments. But I think more needs to be done in terms of policymaking to make, you know, all the countries working together, making themselves more resilient.

Taiwan has done some of their part in terms of the laws and it's difficult for them because they don't have the diplomatic channels like the EU has with the Nordic, and so on. So they've done a lot. I think a lot can be learned from the cooperation with the countries around in the Nordic, and in Europe.

But, it's harder in East Asia to do that. And, in the US it is like, you're far away, so you don't really think about it that much. But really, I mean, there's been a little bit more research and attention, for example, around the waters in Iceland and Ireland, and so on. That can affect the US significantly because all the traffic going through to Europe, basically, you know, I don't exactly have the percentage, but it's a huge percentage of it goes through that area.

There's always choke points because, you know, if we don't think about the danger–everybody you go take the same route to work every day, right? So you invest in another cable, you stick it up where you used to put it, and then naturally there are these choke points, and sometimes there are a lot of geological reasons why they go that particular route and not the other one. So yeah, and then they naturally become these choke points that are becoming very vulnerable. So definitely the US government should be talking more to Ireland about what they can do to harden, you know, to make sure that they can be connected to Europe, and so on, and to the rest of the world.

Sheena Chestnut Greitens: I do think there's growing interest, so it's nice to kind of get ahead of this issue. One of the reasons why I was glad to have you write the article and I am glad to have you on the podcast, so.

Charles Mok: Thank you. Thank you.

[00:38:43] Closing and Credits

Ryan Vest: Thanks for joining us on *Horns of a Dilemma* from the *Texas National Security Review*. Our guest today has been Charles Mok, author of "Toward Undersea Cable Resilience: The Case for Global Collaboration," which as always, can be accessed for free on our website. Charles, thank you very much for joining us today.

Charles Mok: Thank you. Thanks for the discussion. Thank you.

Ryan Vest: If you enjoyed this episode, be sure to subscribe and leave a review wherever you listen. We love hearing from you. You can find more of our work at *TNSR*.org. Today's episode was produced by *TNSR* Digital and Technical manager Jordan Morning, and made possible by the *University of Texas System.*

This is Ryan Vest and Sheena Chestnut Greitens. Thanks for listening.