What happens if submarine cables in Hormuz go down?

Maria Cattini | 21/03/2026 | CYBERSECURITY

Submarine Cables Hormuz Risk. A tanker drifts. An anchor drops. No explosion, no headlines at first. Then banks slow down, cloud services lag, and half the internet feels… off.

This is not a hypothetical scenario. It already happened in the Red Sea in 2025, when multiple fiber optic cables were cut, disrupting connectivity across Asia and the Middle East.

Now place that same event in the Strait of Hormuz—one of the most sensitive geopolitical chokepoints on the planet.

The question is simple: **how fragile is global internet infrastructure when it runs through a war zone?**

The hidden backbone of the internet

Most people imagine satellites when thinking about the internet. That’s outdated.

97% of global data travels underwater

Submarine cables carry almost all international data traffic. Not satellites, not wireless networks. Physical cables, lying on the ocean floor.

• Around 1.7 million kilometers of submarine cables exist worldwide
• The Red Sea–Persian Gulf corridor handles over 20% of global traffic
• Up to 95% of Asia–Europe data flows through these routes

This makes Hormuz more than an energy chokepoint. It’s a digital artery.

Big Tech knows this. Google, Meta, Amazon, and Microsoft have invested billions in these routes—and slowed projects when security risks increased.

Not for budget reasons. For survival.

A disruption doesn’t kill the internet—but it hurts

Let’s drop the Hollywood version. No total blackout.

Reality is messier.

What actually happens during cable damage

When cables fail:

• Traffic reroutes automatically
• Alternative paths handle overflow
• Latency increases sharply
• Costs spike

During previous incidents, rerouting via longer paths—like around the Cape of Good Hope—cost up to **six times more** and added significant delay.

The internet bends. It doesn’t break.

But some regions suffer more.

Who gets hit the hardest?

Countries with limited redundancy:

• India
• Pakistan
• East Africa

These regions depend heavily on a few key routes. When those fail, performance drops fast.

Streaming buffers. Cloud services lag. Financial systems slow down.

And timing matters.

The real bottleneck: repair time

Cutting a cable is easy.

Fixing it? That’s another story.

Weeks… or months

Under normal conditions:

• A repair ship takes weeks to fix one cable

In conflict zones:

• Repairs can take 6 months or more

In 2024, repair operations in contested waters were delayed due to security threats. Ships simply couldn’t approach safely.

Now imagine Hormuz during escalation.

No access. No repairs. Just degraded service for months.

Hybrid warfare: the silent threat

No missiles required.

How cables get damaged in modern conflicts

Recent events show a pattern:

• Anchors dragging across the seabed
• Ships drifting without control
• GPS jamming disrupting navigation
• Small boats operating in gray zones

One notable case involved a drifting vessel damaging kilometers of cable simply by dragging its anchor.

No advanced weapon. Just physics.

That’s the uncomfortable truth:
critical infrastructure can be disrupted without triggering a formal war response.

Hormuz: from oil corridor to digital battlefield

Historically, Hormuz meant energy.

• 20% of global oil passes through it
• 25% of liquefied natural gas flows here

Now, add data.

A new layer of strategic importance

Recent tensions (2026) include:

• Drone activity
• Fast-boat harassment
• GPS interference

These actions affect more than shipping. They complicate:

• Cable monitoring
• Repair missions
• Surveillance operations

Digital infrastructure becomes collateral damage—or a deliberate target.

Europe’s late response

After years of incidents, policymakers reacted.

[The EU Submarine Cable Security Toolbox]

In 2026, the European Commission introduced a plan focused on:

• Prevention
• Detection
• Rapid response
• Diplomatic deterrence

Budget: **€347 million**

A key initiative:
a reserve fleet of cable repair vessels

A good move. Late, but necessary.

Because the pattern is clear:

Damage first. Response later.

The risk nobody wants to price

Every year, **150–200 cable incidents occur globally**. Most are accidental. Some aren’t.

Add geopolitical tension to that baseline, and the equation changes.

What’s really at stake?

• Financial markets (slower transactions)
• Cloud infrastructure (higher latency)
• Real-time systems (trading, logistics)
• National security communications

SWIFT and global payment systems won’t collapse. They’re designed with redundancy.

But performance degradation? That’s inevitable.

And expensive.

Practical takeaway: test your resilience now

This isn’t just a geopolitical story.

It’s a business continuity issue.

If your infrastructure depends on:

• Cloud services
• Real-time data
• Cross-region connectivity

You are exposed.

What you can do

Start with the EU framework. It’s public and actionable.

Map your dependencies. Identify single points of failure. Stress-test your network assumptions.

Because the next disruption won’t announce itself.

It will feel like “the internet is slow today.”

Want to go deeper?

If this topic caught your attention, explore real OSINT techniques to monitor maritime risk, cable routes, and digital infrastructure in near real time.

Join the community:

• Newsletter → https://projectosint.substack.com/
• Telegram → https://t.me/osintaipertutti
• Telegram Group → https://t.me/osintprojectgroup

The infrastructure is invisible—until it fails.

Submarine Cables Hormuz Risk. A tanker drifts. An anchor drops. No explosion, no headlines at first. Then banks slow down, cloud services lag, and half the internet feels… off.

This is not a hypothetical scenario. It already happened in the Red Sea in 2025, when multiple fiber optic cables were cut, disrupting connectivity across Asia and the Middle East.

Now place that same event in the Strait of Hormuz—one of the most sensitive geopolitical chokepoints on the planet.

The question is simple: **how fragile is global internet infrastructure when it runs through a war zone?**

The hidden backbone of the internet

Most people imagine satellites when thinking about the internet. That’s outdated.

97% of global data travels underwater

Submarine cables carry almost all international data traffic. Not satellites, not wireless networks. Physical cables, lying on the ocean floor.

- Around 1.7 million kilometers of submarine cables exist worldwide
- The Red Sea–Persian Gulf corridor handles over 20% of global traffic
- Up to 95% of Asia–Europe data flows through these routes

This makes Hormuz more than an energy chokepoint. It’s a digital artery.

Big Tech knows this. Google, Meta, Amazon, and Microsoft have invested billions in these routes—and slowed projects when security risks increased.

Not for budget reasons. For survival.

A disruption doesn’t kill the internet—but it hurts

Let’s drop the Hollywood version. No total blackout.

Reality is messier.

What actually happens during cable damage

When cables fail:

- Traffic reroutes automatically
- Alternative paths handle overflow

• Latency increases sharply
• Costs spike

During previous incidents, rerouting via longer paths—like around the Cape of Good Hope—cost up to **six times more** and added significant delay.

The internet bends. It doesn’t break.

But some regions suffer more.

Who gets hit the hardest?

Countries with limited redundancy:

• India
• Pakistan
• East Africa

These regions depend heavily on a few key routes. When those fail, performance drops fast.

Streaming buffers. Cloud services lag. Financial systems slow down.

And timing matters.

The real bottleneck: repair time

Cutting a cable is easy.

Fixing it? That’s another story.

Weeks… or months

Under normal conditions:

• A repair ship takes weeks to fix one cable

In conflict zones:

• Repairs can take 6 months or more

In 2024, repair operations in contested waters were delayed due to security threats. Ships simply couldn’t approach safely.

Now imagine Hormuz during escalation.

No access. No repairs. Just degraded service for months.

Hybrid warfare: the silent threat

No missiles required.

How cables get damaged in modern conflicts

Recent events show a pattern:

• Anchors dragging across the seabed
• Ships drifting without control
• GPS jamming disrupting navigation
• Small boats operating in gray zones

One notable case involved a drifting vessel damaging kilometers of cable simply by dragging its anchor.

No advanced weapon. Just physics.

That’s the uncomfortable truth:
critical infrastructure can be disrupted without triggering a formal war response.

Hormuz: from oil corridor to digital battlefield

Historically, Hormuz meant energy.

• 20% of global oil passes through it
• 25% of liquefied natural gas flows here

Now, add data.

A new layer of strategic importance

Recent tensions (2026) include:

• Drone activity
• Fast-boat harassment
• GPS interference

These actions affect more than shipping. They complicate:

• Cable monitoring
• Repair missions
• Surveillance operations

Digital infrastructure becomes collateral damage—or a deliberate target.

Europe’s late response

After years of incidents, policymakers reacted.

[The EU Submarine Cable Security Toolbox]

In 2026, the European Commission introduced a plan focused on:

• Prevention
• Detection
• Rapid response
• Diplomatic deterrence

Budget: **€347 million**

A key initiative:

a reserve fleet of cable repair vessels

A good move. Late, but necessary.

Because the pattern is clear:

Damage first. Response later.

The risk nobody wants to price

Every year, **150–200 cable incidents occur globally**. Most are accidental. Some aren’t.

Add geopolitical tension to that baseline, and the equation changes.

What’s really at stake?

• Financial markets (slower transactions)
• Cloud infrastructure (higher latency)
• Real-time systems (trading, logistics)
• National security communications

SWIFT and global payment systems won’t collapse. They’re designed with redundancy.

But performance degradation? That’s inevitable.

And expensive.

Practical takeaway: test your resilience now

This isn’t just a geopolitical story.

It’s a business continuity issue.

If your infrastructure depends on:

• Cloud services
• Real-time data
• Cross-region connectivity

You are exposed.

What you can do

Start with the EU framework. It’s public and actionable.

Map your dependencies. Identify single points of failure. Stress-test your network assumptions.

Because the next disruption won’t announce itself.

It will feel like “the internet is slow today.”

Want to go deeper?

If this topic caught your attention, explore real OSINT techniques to monitor maritime risk, cable routes, and digital infrastructure in near real time.

Join the community:

• Newsletter → https://projectosint.substack.com/
• Telegram → https://t.me/osintaipertutti
• Telegram Group → https://t.me/osintprojectgroup

The infrastructure is invisible—until it fails.