

```
procedure FormCreate(Sender: TObject);  
procedure TreeViewChange(Sender: TObject; Node: TTreeNode);  
procedure EditChange(Sender: TObject);  
procedure TreeViewChanging(Sender: TObject; Node: TTreeNode;  
var Allow: Boolean);  
procedure TreeViewQuery(S: string; Sender: TObject; var CanPass: Boolean);  
procedure TreeViewMouseDown(Sender: TObject; var Key: Word;  
Shift: TShiftState);  
procedure TreeViewMouseUp(Sender: TObject; Button: TMouseButton;  
Shift: TShiftState; X: Integer);  
procedure TreeViewMouseDown(Sender: TObject; Node: TTreeNode;  
var S: String);  
procedure TreeViewDragOver(Sender, Source: TObject; X, Y: Integer;  
State: TDragState; var Accept: Boolean);  
procedure TreeViewResize(Sender: TObject);  
procedure FormKeyDown(Sender: TObject; var Key: Word; Shift: TShiftState);  
procedure FormNewKeyPress(Sender: TObject; var Key: Char; Shift: TShiftState);  
procedure FormClose(Sender: TObject; var Action: TCloseAction);  
procedure FormActivate(Sender: TObject);  
procedure FormOn123Click(Sender: TObject);  
procedure FormOn456Click(Sender: TObject);  
procedure FormOn789Click(Sender: TObject);  
  
procedure GetWakeUpMessage(var Message: TMessage); message MW_WAKEUP; WakeUP;  
procedure GetActivateMessage(var Message: TMessage); message MW_ACTIVATEAPP; Activate;  
procedure GetMYNOTIFYMessage(var Message: TMessage); message MW_MYNOTIFY; MYNOTIFY;  
  
procedure mipExitClick(Sender: TObject);  
procedure mipRestoreClick(Sender: TObject);  
procedure StatusBarDrawPanel(StatusBar: TStatusBar;  
Panel: TStatusPanel; const Rect: TRect);  
procedure TreeViewDragDrop(Sender, Source: TObject; X, Y: Integer);  
procedure TreeViewEndDrag(Sender, Target: TObject; X, Y: Integer);
```

## Moving towards an hyper secure world

Deloitte Technology S.A | May 28th, 2021

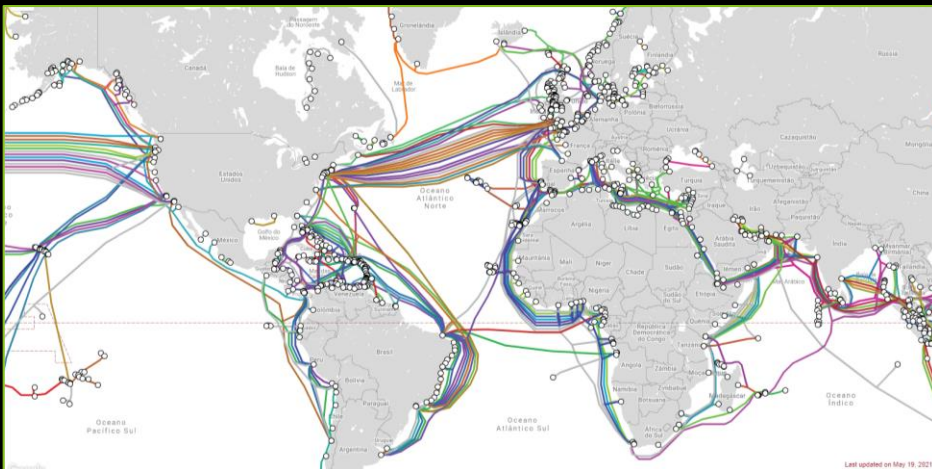
# Moving towards an hyper secure world | Submarine cables

Submarine cables as the backbone of our hyper connected world must be protected at any cost

66  
99

The submarine communication cables form a **vast network on the seabed** and **transmit massive amounts of data** across oceans

As **5G** and **artificial intelligence** transform our societies into highly integrated networks, protecting data will become even more crucial



Source: Telegeography

Submarine cables are a **critical infrastructure worldwide** and a downtime can cause dramatic economical consequences but is **surprisingly vulnerable to interference by hostile actors**

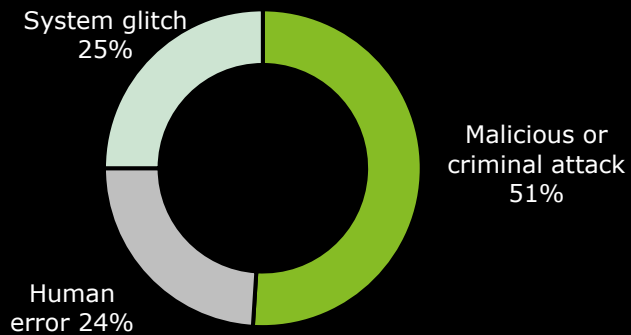
- Carry **99%** of the international communications traffic
- **+400** submarine cables worldwide
- **+1,3M km** of submarine cables in service globally
- **\$10 trillion** in daily financial transactions are transmitted by subsea cables (e.g Google, Microsoft, Facebook)

Source: Telegeography / Information Technology & Innovation Foundation

# Moving towards an hyper secure world | Challenges & Trends

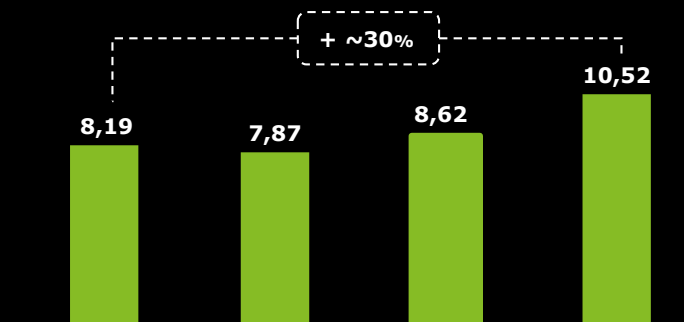
Network attacks have been increasing significantly, which may lead to great costs, whereas, companies should consider protecting their network as top priority

## Causes for data breaches



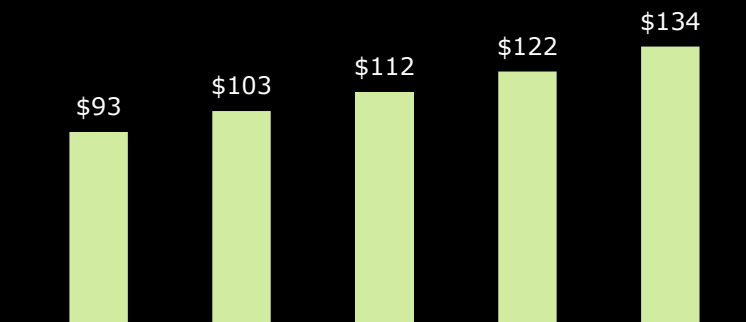
- At least **7.9 billion records**, have been exposed through data breaches in **2019**
- 250 million Microsoft customer records**, were breached in the **beginning of 2020**

## Annual number of malware attacks worldwide (in billions)



- Damage related to network attacks** is projected to hit **\$6 trillion** annually by **2020**
- Globally, the **average size of a data breach** is **25,575 records**

## Worldwide spending on security solutions (US\$ billions)



- Currently, the **average cost per record stolen** is **\$150** and it's expected to grow
- Risk management and privacy concerns** will drive **security services** spending in **2020** for more than **40% of organisations**

Statistics and trends reflect a rampant **increase on the amount of network threats and respective enterprise challenges**, making security top of mind through a **continuous improvement journey**

Source: IBM, IDC, Gartner, Microsoft, CyberSecurity Ventures, Statista

# Submarine communication cable protection | Data and cable protection

There are many possibilities from which cyber attackers could get access into the submarine optical cable systems, to its management and control systems



Cyber attackers, hackers and terrorists can **use artificial intelligence** to enable them to use vulnerabilities in submarine optical cable systems, **in order to penetrate systems and its services**

Submarine Cable Cyber Threat Segment (*)	Land and Beach Area	Near Shore Area ~50 m	Offshore Area ~50 – 100 m	Continental Shelf ~100 – 200 m	Deep Sea ~200 m +
Cyber vandalism	Red	Red	Green	Green	Green
Cyber crime (data theft)	Green	Red	Yellow	Green	Green
Cyber terrorism	Yellow	Red	Yellow	Yellow	Green
Cyber espionage	Green	Yellow	Red	Red	Red
Cyber warfare	Green	Green	Green	Green	Green

**Threat impact level in colors:** **Green** = Low; **Yellow** = Medium **Red** = High

(\*) By use of Intelligence collection device to the cable or to the fibre pair either on the ground, at a landing point, in points where the traffic is amplified or in the seabed.

## How can we protect a submarine cable communication?



### Data protection

Secured encryption based on quantum key distribution method



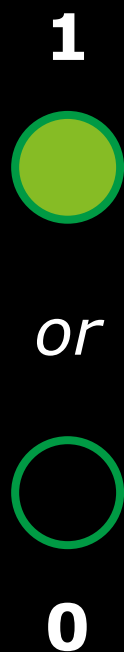
### Cable protection

SMART cables will allow to **enhance the submarine infrastructure safety**

# Submarine communication cable protection | Quantum in the Telecom world

## Quantum technologies will make wiretap, intercept or crack information impossible

Traditional computing is built upon the **bit**

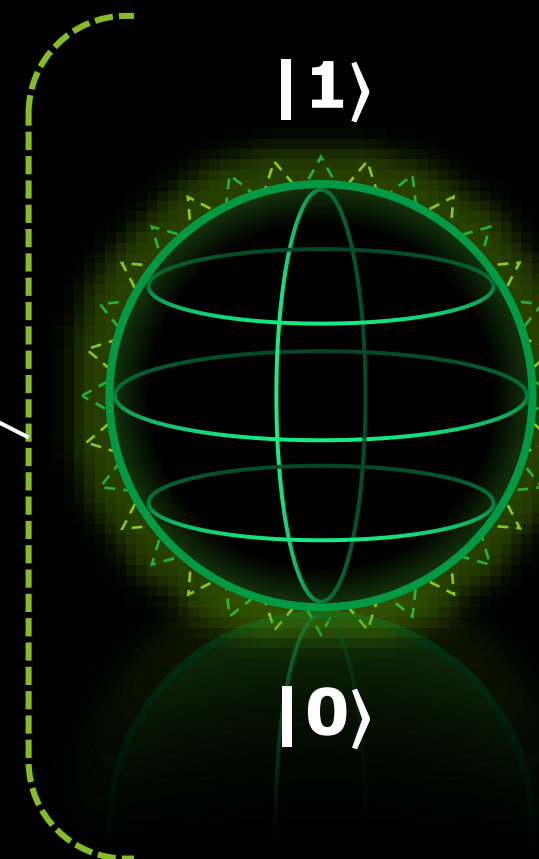


A bit is a Boolean unit – it can assume one of two values: 0 or 1. It is how we currently encode everything in the digital world.

A qubit is the base unit value in quantum computing. It exists solely in the quantum realm and it is also a two-state system. The difference is that it can assume both states simultaneously through a quantum phenomenon called **superposition**.

The main advantage presented by the use of qubits is that by **harnessing properties like superposition**, quantum computers can make operations that would otherwise take an **unpractical amount of resources** and **time for conventional computing**.

Whereas quantum computing uses the quantum bit - **qubit**



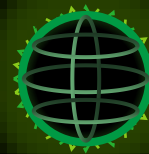
# Submarine communication cable protection | Quantum Key Distribution

QKD can enable submarines to communicate securely both at depth and speed

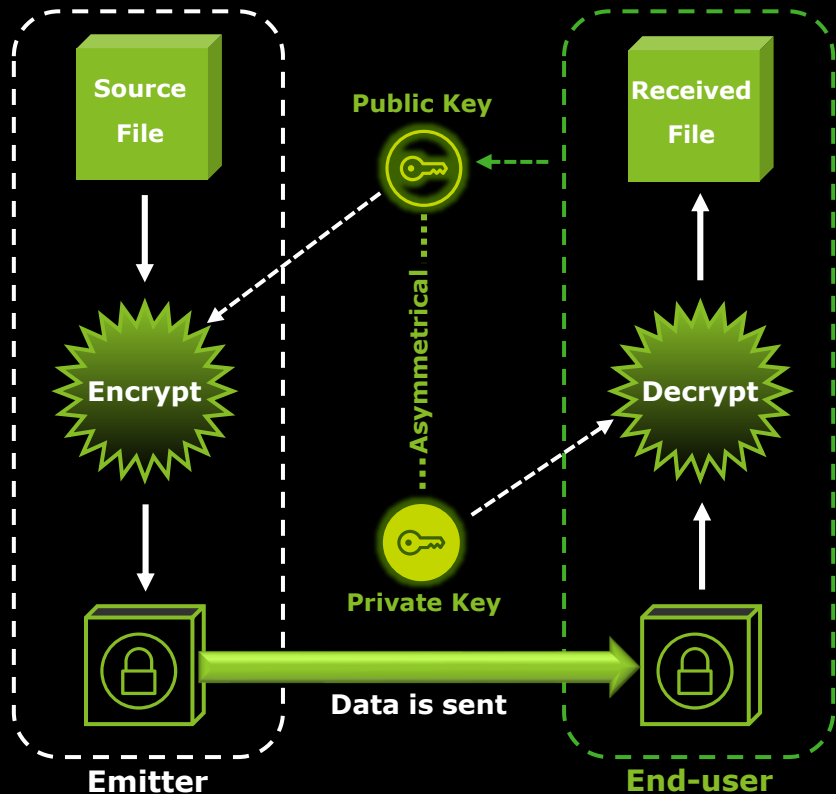
Current communication uses conventional encryption methods to protect information travelling through a communication channel.



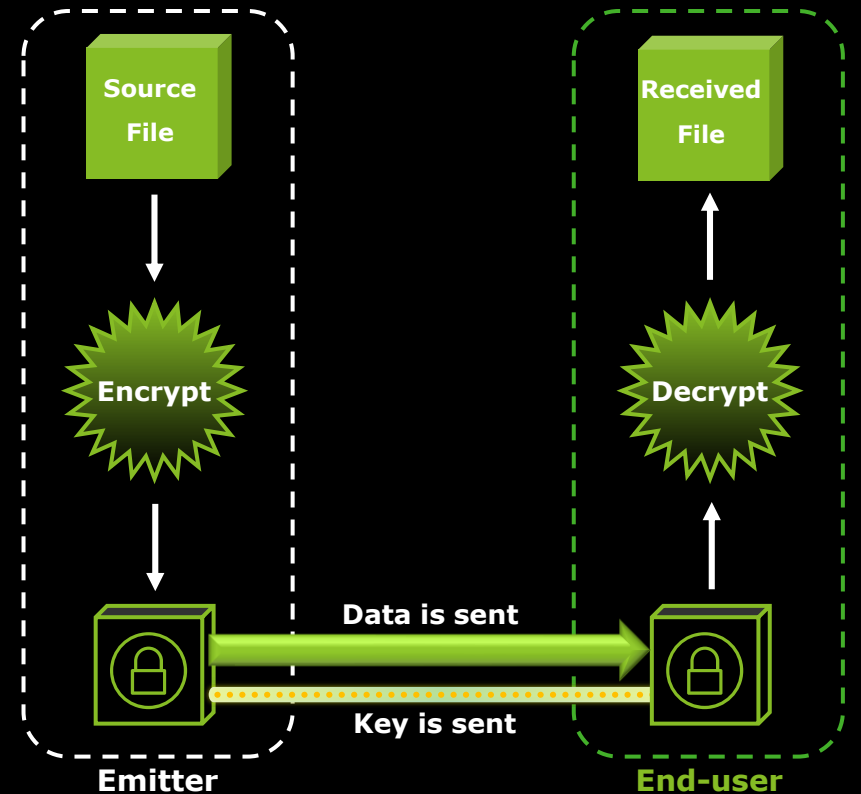
VS.



Whereas QKD networks are provably secure by the laws of physics since it harnesses the quantum domain to transfer information.

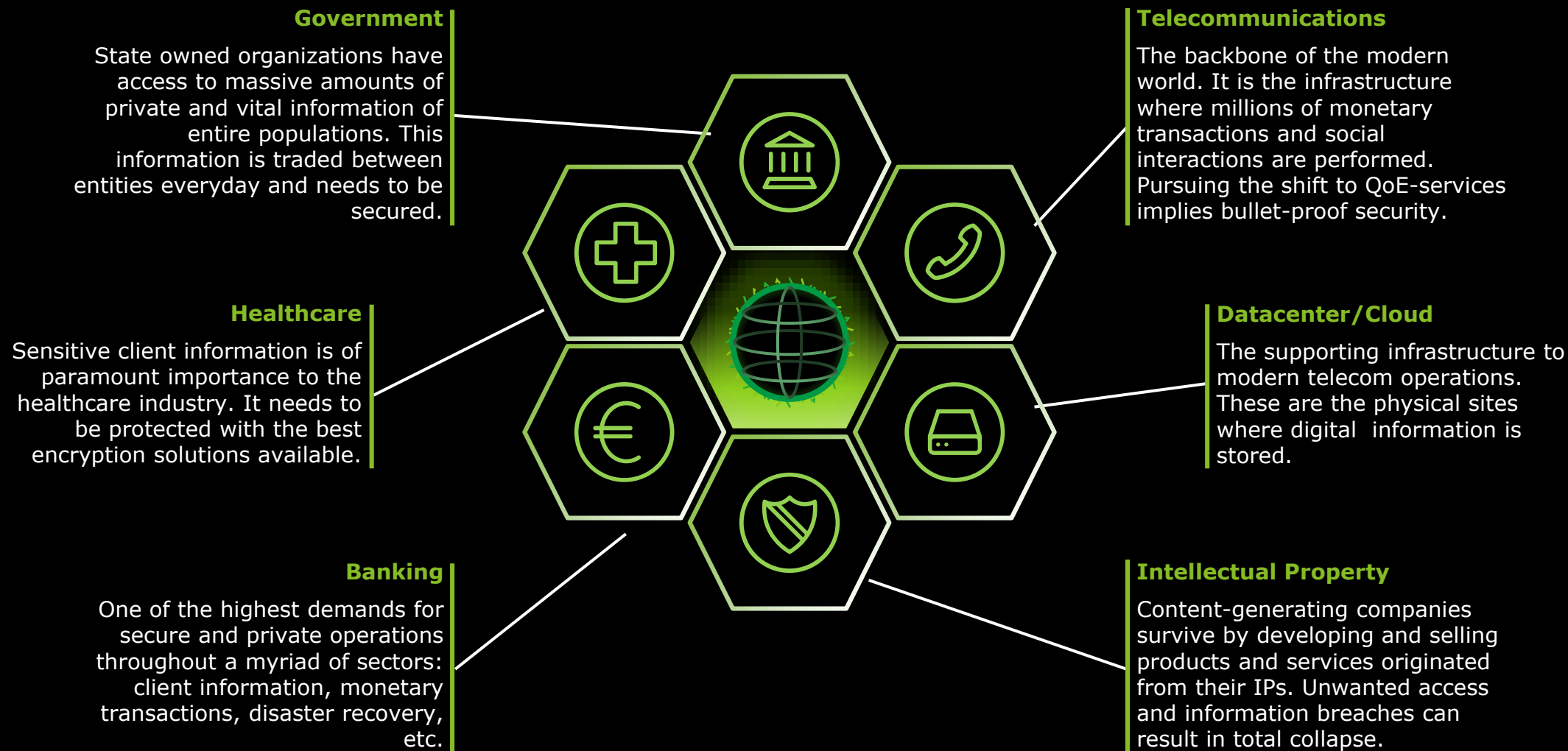


- ✓ There are already quantum algorithms devised that **can break conventional encryption** security systems. These are just awaiting a practical quantum computer to actually run them.
- ✓ QKD networks do not share the inherent vulnerability in mathematical-based security algorithms because the communication link is composed of particles in a state of no-observation.
- ✓ Any attempt to tap into the communication channel destroys it either by disrupting the channel and changing the qubits' states (BB84-based protocols) or by causing a **decoherence of an entanglement state** (E91-based protocols) in which the information is encoded.
- ✓ Can be applied to some existing fiber optic networks.
- ✓ The encrypted message can be transmitted via a public, unsecured, communication channel since the encryption is unbreakable.



# Submarine communication cable protection | Quantum Key Distribution

Any entity or company is looking for a solution that can deliver truly, provably secure communication systems to protect very high-value data in all industry areas



# Submarine communication cable protection | SMART Cables

A SMART component will allow to enhance the submarine infrastructure safety, while enabling science to new and more accurate data of the seabed

66  
99

SMART stands for **Scientific Monitoring and Reliable Telecommunications** and its goal is to integrate sensors into a commercial telecommunications repeater with **negligible impact** and **reliability of the repeaters'** telecommunications functions

**~40%** of all submarine cable faults worldwide are due to **commercial fishing** or caused by vessels **anchoring** in prohibited sea area


## How can SMART cables improve the security of the cable?

*Sensors' information almost instantly (~0,1 ms)*



### Movement detection


Integration of sensor in the cable that can detect the sonar frequencies/ movement detection used by submersibles intent on interference and alert authorities ashore

 Example: Hydrophone, accelometer



### Seismic detection


Use of ground motion sensors in order to detect possible earthquakes and launch the necessary procedures to minimize its consequences

 Example: seismometer, accelometer



### Tsunami detection

Similar to the seismic detection, it is possible to prevent tsunamis with the by measuring the pressure on the seabed

 Example: Absolute pressure gauge

**Source:** JTF SMART Cables, *Listening to Earth in Atlantic (LEA)*, Telegeography



# Submarine communication cable protection | Call for action

Protecting submarine cables must be made a national and international security priority based on both physical and cybernetic protection and regulation is key

66  
99

At a time when ~99% of telecom traffic flows through submarine cables, countries are already focusing on **these deep undersea information pipes as rich sources of intelligence as well as targets in war**

## Tapping or damaging undersea cables is part of the modern warfare



The Yantar, a Russian spy ship, **carries mini-submersibles that can either sever or tap submarine Cables.**



China's People's Liberation Army threat to **sever Taiwan's undersea cables, isolating it from the U.S. and regional allies** during Chinese invasion of the island



## The International Maritime Law shall **include regulations in order to protect against Cyber Attacks**



Opportunity to **legislate laws and regulations for the protection of submarine cables** outside territorial sea, including using new technologies, as well as against new threats with using unmanned and autonomous cyber weapon systems.



"Deloitte" refere-se a uma ou mais firmas membro e respectivas entidades relacionadas da rede global da Deloitte Touche Tohmatsu Limited ("DTTL"). A DTTL (também referida como "Deloitte Global") e cada uma das firmas membro são entidades legais separadas e independentes. A DTTL não presta serviços a clientes. Para mais informação aceda a [www.deloitte.com/pt/about](http://www.deloitte.com/pt/about).

A Deloitte é líder global na prestação de serviços de audit and assurance, consulting, financial advisory, risk advisory, tax e serviços relacionados. A nossa rede de firmas membro compreende mais de 150 países e territórios e presta serviços a quatro em cada cinco entidades listadas na Fortune Global 500®. Para conhecer o impacto positivo criado pelos aproximadamente 312.000 profissionais da Deloitte aceda a [www.deloitte.com](http://www.deloitte.com).

© 2021. Deloitte Technology S.A.