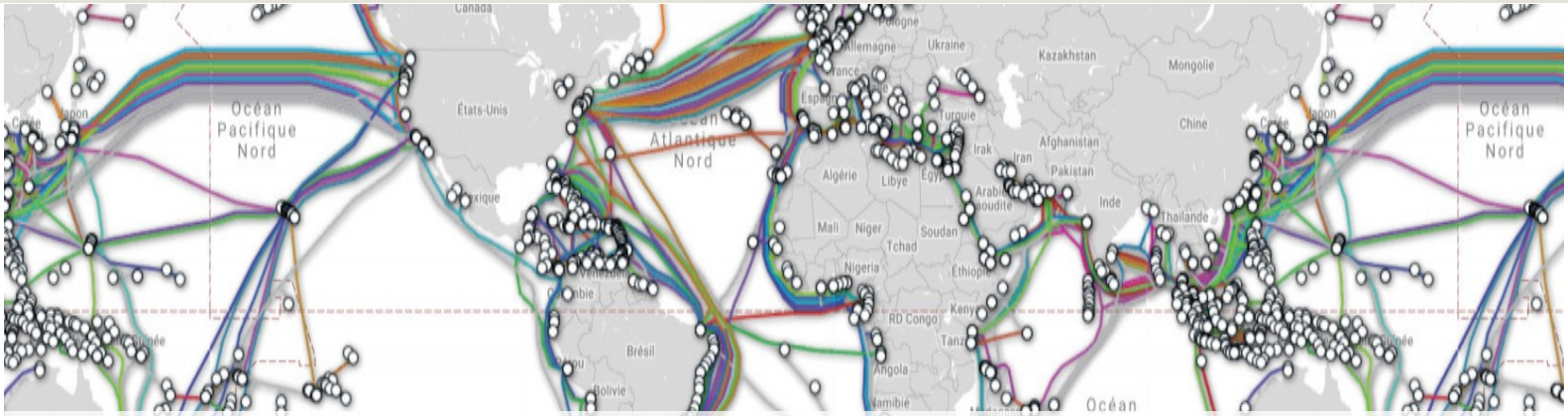

Underwater cables: between vulnerability and strategic stakes

BRENNUS 4.0

le commandant Hélène Gorbéna, officier stagiaire de l'EMSST

Published on 04/04/2020

Sciences & technologies

Since the major computer attacks that have made their mark, (Bronze Soldier in Estonia in 2007, Stuxnet in Iran, discovered in 2010, or Wannacry which affected nearly 200,000 entities worldwide in 2016), cybersecurity is now a growing concern. A significant increase in attacks, mostly related to the world of cybercrime but also to States, has been observed. As a result, many solutions for protection, threat anticipation, detection, anti-virus or other anti-spyware are being proposed by companies that are scrambling to occupy a place in this promising market. However, software protection is incomplete without physical protection.

There are several ways to steal, modify or even delete data, as long as the attacker has physical access to the data carrier. Similarly, it is pointless to protect systems if the spy is positioned upstream of the protection devices to intercept the data. Encryption, which alone can complicate or even prevent the exploitation of data, temporarily secures the data until the algorithms used are broken, which is only a matter of time and computing power. However, not only are the flows still too weakly encrypted, but they pass through submarine cables which are part of the physical architecture of the Internet and allow an attacker to access, not without logistical difficulties, the global data flows, upstream of all software protection systems. They therefore present vulnerabilities that it is important to be aware of in order to try to prevent their alteration or even exploitation for malicious purposes. Beyond these weaknesses, they represent a power issue for States wishing to preserve their sovereignty.

The whole world connected by the seabed

Submarine cables have covered the bottom of the seas and oceans since the 19th century and are still unknown to the general public. Yet, contrary to what is still widely believed, only 1% of Internet traffic passes through satellite networks. The remaining 99%

of data flows pass through these cables. Since the first telegraph cable was laid between France and England in 1851, their number has grown exponentially. The "submarinecablemap.com" site lists more than 430 cables in 2018 that carry data and/or energy using different technologies, with fibre optics now being used massively for telecommunications. Indeed, cables combine many advantages compared to satellites: much lower costs, making it possible to offer competitive rates, high transmission speeds and quality, and a long service life [2].

2] However, there are some drawbacks to this submarine network. If its location makes it difficult for malicious purposes to access it, the same applies to installation and, above all, maintenance. Indeed, these operations are carried out by cable ships, mostly privately owned. The submarine cable market is held by a few large groups. Among others, the French company Nexans, whose Norwegian subsidiary specializes in the manufacture of submarine cable. The Orange Marine group holds 15% of the market with 6 cable ships operating worldwide and 450,000km of cable laid. The latter mainly faces competition from the United States (Subcom), Great Britain (Global Marine Systems Limited), Japan (NEC) and, to a lesser extent, China (Huawei). In particular, Orange Marine has embarked, in cooperation with PCCW global, a division of the Hong Kong telecoms agency, on a 12,000 km cable project called PEACE, which in 2020 will trace the shortest route between China and Europe, via Pakistan, Kenya, Djibouti and Egypt [3].

The laying and maintenance of a cable is a complex operation. First of all, the cable is loaded on board the cable ship, wound in tanks and previously equipped with signal repeaters which are arranged every 50 to 100 km and will ensure that the signal strength is maintained. Depending on the type of bottom and the frequency of use of the site, the cable may be simply laid or buried in a trench dug by a plough fitted to the cable-layers. This technique, which provides better protection for the cable, makes cable maintenance more complex. When it is necessary to repair or change a damaged portion of the cable, once the affected cable has been located, the cable-laying vessel uses a grapple system to try to pull it up.

When the bottom is too deep or the cable is buried, a submersible vehicle is required. Here again, a market is developing which offers prospects that are as interesting as they are worrying. Finally, when the cable reaches the ground, it does so via a landing point. Usually, the cable passes under a beach and ends up in a cable chamber, usually semi-buried, where the connection to the terrestrial network is made [4]. These sites are little known but also poorly protected. The cables therefore have intrinsic vulnerabilities that need to be detailed.

Critical vulnerabilities

In July 2018, the Japanese government updated its cybersecurity strategy, calling for enhanced protection of the physical infrastructure for Internet access, including submarine cables. The dependence of an island country like Japan on this infrastructure is extreme. It was made even more evident following the earthquake and tsunami of 2011, which damaged a large number of cables, necessitating, among other things, the relocation of traffic from the east of the country to the west. The sea bed itself is therefore one of the first weaknesses of the cables, as underwater volcanic eruptions or earthquakes are not uncommon. Shark bites, apparently anecdotal, also contribute, but less significantly than fishing activities (netting or anchoring), to regular damage to the

cables [6]. Although these natural or incidental threats are costly - they represent the vast majority of the problems identified - they are not the most worrisome. Indeed, cables can be coveted by pirates interested in reselling the cable itself. For example, in 2007, in Vietnam, 500km of cables were stolen, causing a nationwide Internet blackout. Sabotage is also a recurring cause of degradation, particularly in Africa. For example, Gabon was cut off from the world for 4 days in 2015 following the deliberate cutting of the Sat3 cable linking the west coast of Africa to Europe. Beyond the cables, the emerging parts of the network may be the target of attack.

For example, a cable ship was attacked by local pirates while laying cable in the Red Sea in 2015, a rare occurrence even today. Landing points are another major point of vulnerability due to their limited number and low level of physical protection. Finally, espionage via the seabed is not a new phenomenon. Already in 1971, the United States had been able to collect intelligence by 'listening in' on the cable used for communications by the Soviet fleet in the Pacific, as part of Operation Ivy Bell [7]. It is also necessary to recall the worrying manoeuvres of the Russian oceanographic research vessel Yantar (or at least declared as such) near the submarine cables, recorded in 2015. All this brings back images worthy of the Cold War. Thus, in the multipolar context in which we find ourselves today, between exponential economic dependence on data flows, terrorist threats and information attacks, the risks weighing on the Internet infrastructure are increasing, and submarine cables and the data transiting through them represent power issues for States.

Power issues and the quest for digital sovereignty

Following Edward Snowden's revelations on the occasion of the opening of the "NET World" summit in 2014, Brazilian President Dilma Roussef has called for a change in Internet governance in order to get out of the tutelage of the United States. She subsequently gave concrete expression to this desire by signing a cooperation agreement with the European Union, including the establishment of a direct submarine cable between Brazil and Europe[8]. 8] This is one of many projects aimed at guaranteeing greater control of data flows for states concerned about the omnipresence of the United States in all management and decision-making bodies. This problem is imposed on States whose Internet access is guaranteed by a small variety of cables. This is the case of many African countries or Lebanon [9]. The resulting means of pressure and listening capacities lead States to seek the diversification of their means of access to the Internet. In France, the problem is posed in a different way, because although the metropolis has several landing and arrival points for cables, it is confronted, through its 11 million km^2 Exclusive Economic Zone (the second largest after that of the United States) and its overseas departments, territories and collectivities, it is faced with a wide variety of situations, interconnections and partnerships.

As a result, France needs to address almost all cable "routes" to ensure Internet access for its overseas citizens. It is also conceivable that the protection of these cables will be played out under the sea using, among other things, underwater drones. Numerous industrialists have embarked on the race to develop this type of device. Thalès and Aquabotix are thus working on a joint project for a multifunctional underwater drone [11]. Finally, although cables today follow the same routes as telegraph cables 100 years ago, because the straits through which commercial maritime traffic passes are not the same as those of 100 years ago, the cables are still in use today.have not changed, global warming and melting ice are opening up new, shorter routes that are also less vulnerable to natural

and accidental hazards. This is a subject of interest, among others, to Russia, which is now heavily dependent on land cables that pass through other states, or to China, which is also looking for alternative routes, as is its "Digital Silk Road" project.

Outlook

In 2017, the Russian Louch-Olymp satellite approached the Franco-Italian secure communications satellite Athena-Fidus in a very suspicious manner. Revealed in September 2018 by the Minister of the Armed Forces Florence Parly, who then specifically accused Russia of attempted espionage [12], this event shows that even supposedly inaccessible vectors of communication are today targeted. Beyond the protection of the infrastructure, it is indeed the protection of sensitive data that is at the heart of the concerns. Complementary protection measures should therefore be sought, in particular through the widespread use of encryption. In France, the law n°2004-575 of 21 June 2004 authorizes the use of cryptological means [13]. Any citizen can therefore freely encrypt his data using encryption software, removable disks and media or files that become easy to use, free and accessible to all. In addition, there are protocols that encrypt data when it circulates over networks (IPSec, TLS) or when the web request leaves the browser (HTTPS). These methods of encrypting communications are still poorly understood and under-used by the general public, making the flows vulnerable to interception.

Moreover, in this field, as in that of cables or satellites, it is tempting for states to develop their own algorithms in order to ensure the absence of "backdoors" , potentially inserted in the code by intelligence agencies[14]. 14] This is also what leads some countries to embark on the development of a "sovereign cloud" in order to guarantee the storage of their citizens' data on their own soil. Russia is thus building huge data centres in Siberia[15]. Finally, the study of a data packet routing strategy[16] that would guarantee, for example, that data coming from and going to the same country does not transit through another country, is also an avenue being studied by some States.

In conclusion, it emerges that submarine cables are a key issue because there are many vulnerabilities and concrete threats. They represent a critical issue, as States are highly dependent on the proper functioning of networks and the integrity of the data that circulates in them. They are therefore a physical component that must be monitored and protected in order to limit vulnerabilities. In light of the struggles for influence in cyberspace, the protection of sensitive data and digital sovereignty are also major issues, of which submarine cables are only one component.

1] Louis Pétiniaud, Cartographier l 'affaire Snowden, Hérodote N°152-153, 2014

[2] http://www.cablesm.fr/2009_C_10-01_cle2c7389.pdf

[3] https://subseaworldnews.com/2018/12/21/pccw-global-and-orange-to-land-peace-cable-in-france/.

[4] http://ifmer.org/assets/documents/files/documents_ifm/Les-cables-sous-marins-et-les-navires-cabliers.pdf

[5] Motohiro Tsuschya - https://www.asiaglobalonline.hku.hk/undersea-cables-cyberspace-stability-security/

[6] Camille Morel, Threats under the seas: vulnerabilities of the global cable system, Herodotus N°163, 2016

[7]http://www.opex360.com/2015/10/27/que-font-les-navires-russes-pres-des-cables-marins-utilises-pour-les-telecommunications/

8] Frédérick Douzet, La géopolitique pour comprendre le cyberespace, 2014

9] Jérémy Robine and Kavé Salamatian, Peut-on pense une cybergéographie, Herodotus N°152-153 , 2014

[10] http://www.opex360.com/2018/12/11/comment- ...communication.

[11] https://subseaworldnews.com/2018/12/21/thales-and-aquabotix-team-up-on-subsea-drones/

[12]https://www.lemonde.fr/international/article/2018/09/07paris-revele-une-tentative-d-espionnage-russe-sur-un-satellite-franco-italien-en-2017_5351908_3210.html

13] Myriam Quéméner, Le droit face à la disruption numérique, Gualino, 2018.

[14] https://www.lemondeinformatique.fr/actualites/lire-la-securite-absolue-n-existe-pas-retour-sur-7-backdoors-63787.html

15] Frédérick Douzet, Kévin Limonier, Jérémy Robine, Kavé Salamatian, Rémi Géraud, Romain Campigotto, Les nouveaux territoires stratégiques du cyberespace : le cas de la Russie, Stratégique N°117, 2017

[16] http://reseaux.blog.lemonde.fr/2012/11/04/routage-enjeu-cyberstrategie/

Title : le commandant Hélène Gorbéna, officier stagiaire de l'EMSST

Author (s) : le commandant Hélène Gorbéna, officier stagiaire de l'EMSST

Release date 19/03/2020

FIND OUT MORE