Unterwasserinfrastruktur : verwundbare Zivilisation

Autor(en): **Kürsener, Jürg**

Objekttyp: **Article**

Zeitschrift: **Schweizer Soldat : die führende Militärzeitschrift der Schweiz**

Band (Jahr): **97 (2022)**

Heft 11

PDF erstellt am: **10.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-1045862

Unterwasserinfrastruktur – verwundbare Zivilisation

Bei den Pipelines, welche Kontinente miteinander verbinden, geht es um weit mehr als Öl. Die Globalisierung hat Unterwasserkabel zu einer wichtigen Infrastruktur gemacht. Ein gezielter Angriff auf Unterwasserkabel wäre nicht der erste in der Geschichte der Kriegsführung.

Jürg Kürsener

Das Thema ist nicht neu. Aber der Zwischenfall um den mutmasslichen Anschlag auf die Nord-Stream-2-Pipeline in der Ostsee hat vor Augen geführt, wie verwundbar die Errungenschaften der Zivilisation sind.

Dass dieses Ereignis so viel Publizität erhält, ist wohl eher auf den herrschenden Konflikt zwischen Putins Russland, dessen Angriff auf die Ukraine, die Spannungen mit der westlichen Welt sowie die drohende Versorgungslücke im kommenden Winter zurückzuführen als auf das Thema an sich. Norwegen, Schweden und Grossbritannien haben seither mit der Entsendung von Fregatten den Schutz ihrer Unterwasserinfrastruktur und Ölbohrplattformen verstärkt.

Mehr als Erdgas

Es geht allerdings um weit mehr als bloss um die Erdgas-Pipeline. Die Globalisierung der Welt hat einen massiv gestiegenen Handel zur See, eine rasante Steigerung der Mobilität weltweit, sowie eben auch einen steigenden Rohstoff-, Daten- und Informationstransfer zur Folge. Informationen werden zwar auch über weltraumgestützte Systeme ausgetauscht, welche ihrerseits verwundbar sind.

Dieser Anteil beträgt allerdings bloss etwa sieben Prozent des gesamten Aufkommens, während in den Unterseekabeln weit über 90 Prozent des Informationsaufkommens ausgetauscht werden. Swift-Finanztransaktionen zum Beispiel werden fast ausschliesslich über Unterwasserkabel abgewickelt.

Die Unterwasserinfrastruktur umfasst im Wesentlichen:

- Rohstoff- und Energieleitungen (Gas, Öl, Energie, Wasser etc.)
- Kommunikationsleitungen (Telefon, Daten, Bild, Internet etc.)
- Rohstoff Abbauvorrichtungen mit entsprechenden Leitungen (Ölplattformen, Gasplattformen etc.)
- militärische Infrastruktur (Unterwasserortung etc.)
- Windparks mit zugehörigen Leitungen
- andere (z.B. Gezeitenkraftwerke).

Informationsträger

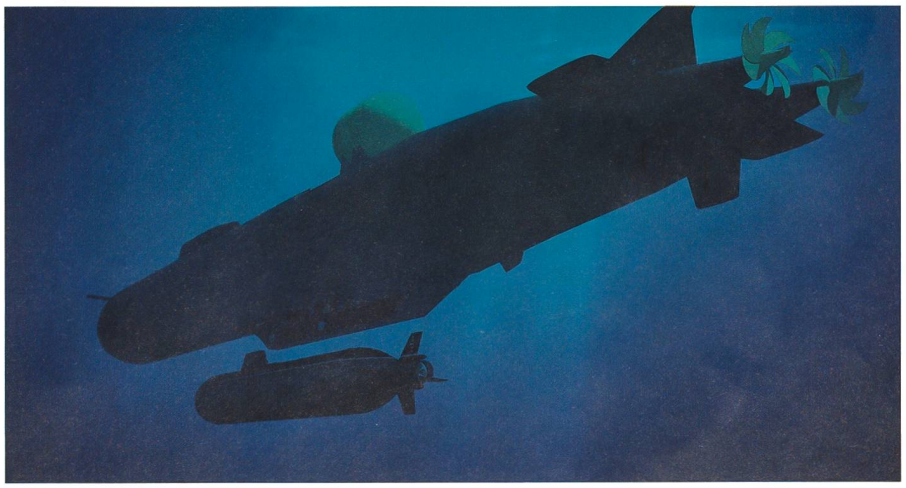
Von grösster Bedeutung sind die Informationen, die meist über leistungsstarke physische Netze unter Wasser transportiert werden. So geht man davon aus, dass weltweit täglich finanzielle Transaktionen im Wert von etwa 10 Trillionen Dollars (10 000 Billionen) getätigt werden.

Allein diese unglaubliche Summe macht deutlich, wie gefährlich Anschläge auf die Unterwasserinfrastruktur sind und wie verwundbar die westliche Wirtschaft ist.

Weltweit soll es heute rund 420 Unterwasserkabel mit einer Gesamtlänge von 1,3 Mio. Kilometern Länge geben. Allein das Kabel «Sea-Me-We 3», welches Südostasien durch das Rote Meer, den Suezkanal und das Mittelmeer mit Europa verbindet, misst 39 000 Kilometer.

Das einzelne, meist aus Glasfaser gefertigte und mit Lichtgeschwindigkeit übertragende Kabel ist in der Regel nicht dicker als ein normaler Gartenschlauch. Ein solches Kabel soll aus bis zu 200 Glasfasern bestehen, welche je 400 Gigabyte Daten pro Sekunde zu übertragen imstande sein sollen.

Die wichtigsten Kabelverbindungen liegen im Atlantik, der «Great Pacific Highway» verbindet die USA mit Japan, China und andere asiatische Staaten, wäh-



Bilder: Tass, Internet, U.S. Navy

Russland verfügt über eine beträchtliche geheime Flotte zur Aufklärung und zum Einsatz gegen die Unterwasserinfrastruktur des Westens. Die Aufnahme zeigt ein Tochter-Uboot «Losharik» und ein nukleares Mutterschiff der «Belogorod»-Klasse.

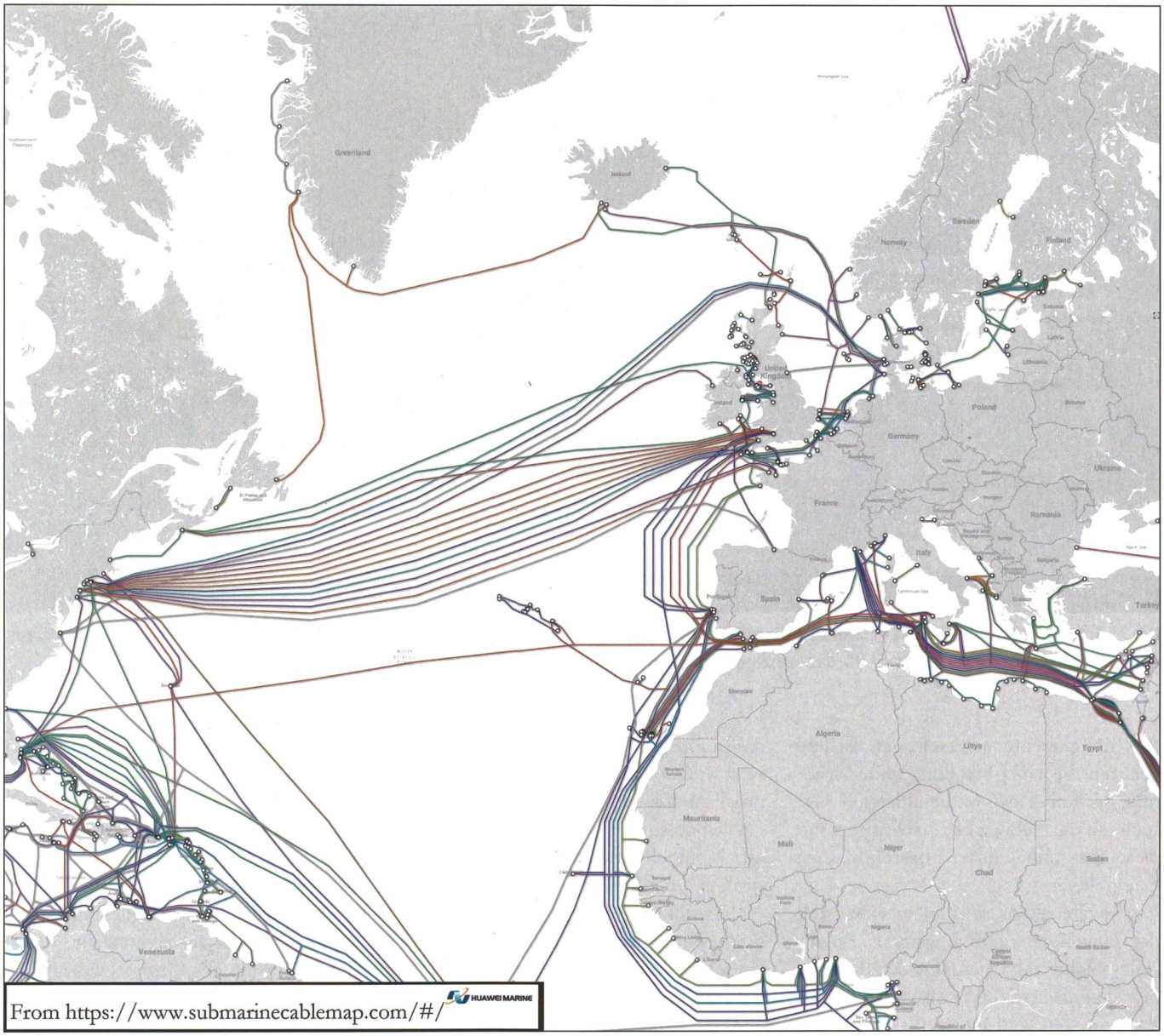


Bild: www.submarinecablemap.com

Karte mit Unterwasserkabel-Verbindungen im Atlantik, zwischen Europa und den USA, in der Nordsee und dem Mittelmeer.

rend von Miami aus viele Staaten über den Golf von Mexiko in Zentral- und Südamerika erreicht werden.

Die Herstellung, Verlegung und der Betrieb von Unterwasserkabeln sind weitgehend in privaten Händen, die vier wichtigsten Akteure stammen aus den USA, China, Frankreich und Japan. So sollen Google, Facebook, Amazon, Verizon, Microsoft und AT&T über eigene Netze verfügen und diese bauen.

Operationsraum Wasser

Unter Wasser befinden sich auch wertvolle und begehrte Rohstoffvorkommen. Zudem wird der «Operationsraum Wasser» – insbesondere der Unterwasserraum – für weitere wichtige Systeme, wie beispielsweise für militärische Zwecke besonderer Bedeutung, genutzt.

Zu ihnen zählte das bereits im Kalten Krieg installierte fixe SOSUS («Sound Surveillance System») zwischen Grönland-Island und Grossbritannien, welches jetzt modernisiert und mobiler als «Integrated Undersea Surveillance System» (IUSS) auf dem Grund des Atlantiks vor allem Uboot-Bewegungen Russlands orten und melden soll.

Russland seinerseits versucht, mit dem Unterwasserortungssystem Harmony vor allem den Zugang zur Arktis zu überwachen. Dieses soll mit einer Serie von kleinen mobilen nuklearen, auf dem Seegrund installierten Reaktoren gespeist werden.

Unterwasserinfrastruktur

Jährlich werden im Schnitt zwischen 100 und 200 Zwischenfälle mit Unterwasserkabeln registriert. Dabei ist es nicht immer einfach, zwischen Unfall oder absichtlich herbeigeführten Pannen zu unterscheiden. Unbestritten ist, dass viele Zwischenfälle durch Fischereiboote sowie Ankerketten verursacht werden.

Daneben gibt es die gezielte Bedrohung, die eine physikalische und eine digi-

Die U.S. Navy verfügt über sehr wenige Einheiten zur Aufklärung und zum Einsatz gegen Unterwassereinrichtungen. Die über 8000 Tonnen grosse USNS Zeus ist das einzige Kabellege- und Reparaturschiff der Navy.

tale Komponente unterscheidet. Erstere geht auf die Unterbrechung und Zerstörung der Kabel aus, während letztere versucht, in die Netzwerke einzudringen, um diese abzuschöpfen, zu kopieren bzw. zu manipulieren.

Solche Aktionen könnten damit Teil der Cyberkriegführung werden. Hauptziele solcher Aktionen sind letztlich die Schädigung der Volkswirtschaft und des Bankensystems im internationalen Wettbewerb oder aber auch Spionage, Beeinträchtigung oder gar Unterbindung der gegnerischen Kommunikation bzw. der Führungsfähigkeit.

Seit etwa 2014 fällt auf, dass sich verschiedene Aktivitäten von «Fischerei»-, «Forschungs»- oder «Ozeanographischen»-Schiffen verdächtig oft entlang von Unterwasserkabeln bewegen, beispielsweise zwischen Grossbritannien-Irland bzw. Frankreich und den USA. Zu diesen auffälligen Bewegungen gehören beispielsweise jene der russischen Yantar, eines Schiffs für angeblich ozeanische Forschungszwecke, welches über zwei Drohnen, eine Art bemannte Mini-Uboote des Typs AS-37 verfügt.

Dieses soll 2021 vor der irischen Küste, in der Nähe eines Transatlantikkabels, das Europa mit den USA verbindet, eingesetzt worden sein. Russland ist gemäss Admiral Andrew Lennonen, Kommandant der Ubootstreitkräfte der NATO, ganz offensichtlich an der Unterwasserinfrastruktur der NATO interessiert.

Es soll über neun bemannte nuklearbetriebene Mini-Uboote für solche Sonderoperationen verfügen, wozu u.a. die bis auf eine Tiefe von angeblich 1000 Meter einsetzbare «Poseidon» sowie die verunfallte und nun wieder reparierte «Losharik» gehören. Diese Kräfte operieren von Olenya Guba auf der Kola-Halbinsel aus.

Solche Drohnenfahrzeuge werden von umgebauten nuklearen Ubooten der «Belogorod»-Klasse (umgebaute «Oscar» Uboote) sowie von zwei umgebauten und verlängerten ballistischen Lenkwaffen-Ubooten der «Delta IV»-Klasse als Mutterschiffe eingesetzt.

Seewölfe

Auch die USA waren und sind in diesem Bereich nicht untätig. Wie bei anderen Nationen ist hierzu allerdings sehr wenig bekannt. Früher sind vor allem die Uboote USS «Parche», «NR-1» und USS «Halibut» für diese Art der Unterwasserkriegführung eingesetzt worden. Heute ist einzig erwiesen, dass die drei Uboote der Seawolf-Klasse, vor allem die gestreckte USS Jimmy Carter, auch für Zwecke - in enger Zusammenarbeit mit Special Forces der Navy (Seals) - der verdeckten Kriegführung eingesetzt werden.

Zudem gibt es spezielle Fahrzeuge, die beispielsweise zur Hebung von verunfallten Ubooten des Gegners aus grossen Tiefen eingesetzt werden können. Hier hat die CIA-Operation «Jennifer» Berühmtheit erlangt, als die USA 1974 erfolglos versuchten, mit dem speziell gebauten Schiff «Glomar Explorer» in der Region von Hawaii das 1968 verunfallte sowjetische Uboot «K-129» der «Golf II»-Klasse mit Nuklearraketen an Bord aus einer Tiefe von 5000 Metern zu heben.

Erste ernsthafte Attacken der Neuzeit gegen Unterwasserkabel gibt es seit 2017, oft sind sie der Öffentlichkeit aber nicht bekannt.

Die Einsatztiefe der Drohnen bis zu 1000 Meter lässt den Schluss zu, dass vor allem bis in diese Tiefen gegen Unterwasserkabel vorgegangen wird.

Damit lässt sich zumindest teilweise ausschliessen, dass diese Art der verdeckten Kriegführung in den grossen Tiefen der Ozeane stattfindet.

Zudem liegt es auf der Hand, dass vor allem Leitungen in seichten Gewässern anfällig sind, auch die Infrastruktur in der Ostsee mit ihrer geringen Tiefe ist entsprechend verwundbar.

Gegnerische Aktionen zu nahe an der Oberfläche fallen allerdings auf und ihr Erfolg ist deswegen höchst fraglich. Exponiert sind auch jene Stellen, wo die Tiefseekabel an die Oberfläche gelangen.

Das gewaltsame Vorgehen gegen Tiefseekabel ist Teil der hybriden Kriegführung und interessanterweise sind gewaltsame Vorgehensweisen gegen die Unterwasserinfrastruktur im Seerecht nicht oder nur unzureichend geregelt. Dies, obschon es Bemühungen gibt, solche Normen zu schaffen. Erste Bemühungen dieser Art gab es übrigens bereits 1884, als der bisher letzte Versuch unternommen wurde, die internationalen Telegraphenkabel vor illegalen Zugriffen zu schützen. Dort waren sich die Unterzeichner scheinbar sogar einig, dass es im Kriegsfalle durchaus zulässig sei, gegen die Unterwasserkabel des Gegners vorzugehen.

Massnahmen

Um all diesen gegnerischen Massnahmen in der Unterwasserkriegführung zu begegnen, wird eine ganze Zahl von möglichen Massnahmen propagiert:

- Vermehrter Austausch von Daten und Erfahrungen in Sachen Unterwasserbedrohung zwischen den Alliierten und Befreundeten.
- Obschon viele Kabelprojekte ziviler Natur sind, drängen sich eine nationale, besser noch internationale Bedrohungsanalyse und eine koordinierte Zusammenarbeit durch den bzw. mit dem Staat auf. Denn nur dieser verfügt über die Mittel zur Bekämpfung.
- Der private Sektor sollte auf die möglichen Gefahren ihrer Unterwassernetze aufmerksam gemacht und sensibilisiert werden. Die Erkenntnis, dass die Zusammenarbeit mit dem Staat letztlich allen dient, sollte gefördert werden.
- Es drängt sich auf, dass die Staaten die Vorkommnisse rund um die kritische Unterwasserinfrastruktur genauestens verfolgen und aufzeichnen sowie ra-

Das Spezial-Uboot USS «Jimmy Carter», ein Jagd-Uboot der Seawolf-Klasse ist für spezielle Operationen, u.a. mit Spezialkräften, umgebaut und verlängert worden. Man geht davon aus, dass es auch für Einsätze gegen Unterwasserinfrastrukturen eingesetzt wird.

Frankreich verfügt mit der Teliri über ein Kabellegeschiff, das u.a. die Verbindung zwischen Frankreich und Singapur aufgebaut hat.

sche koordinierte Reparaturfähigkeiten aufbauen.
- Vorbereitung von Notmassnahmen für den Fall, dass wichtige Netzwerke beschädigt oder unterbrochen werden.
- Schliesslich drängt sich auf, dass die gesamte Problematik der Verwundbarkeit der Unterwasserinfrastruktur im Rahmen von internationalen Verhandlungen wieder aufgenommen und vertraglich verbindlich geregelt wird.

Schlusswort

Die Unterwasserinfrastruktur ist ein Bereich, der Nationen empfindlich treffen kann. Gestörte, missbrauchte oder unterbrochene Verbindungen können den Ausgang von Auseinandersetzungen in Kriegen und Konflikten entscheidend beeinflussen.

Die Verwundbarkeit der Kommunikationen ist enorm. Die Erkenntnis, dass die klandestine und gewaltsame Beeinträchtigung von Unterwasserinfrastruktur integraler Teil des internationalen Wettbewerbs und Teil hybrider militärischer Auseinandersetzungen sein kann und zunehmend sein wird, setzt sich nur langsam durch. Hier tut ein kombinierter zivil-militärischer, ganzheitlicher und kooperativer Ansatz Not, wobei alle Nutzniesser, auch Binnenstaaten, gefordert sind.

Im Alleingang sind Ortung, Feststellung des Schadenausmasses, eine Reparatur bzw. Gegenmassnahmen nur schwerlich zu bewerkstelligen. Die Mittel dazu, vor allem auf westlicher Seite, fehlen bzw. sind führungsmässig und organisatorisch nicht optimal aufgestellt.

Es fehlt auch an Redundanzen. Private Aktivitäten und sicherheitspolitisch relevante Vorkehrungen müssen besser koordiniert werden. Noch geben sich viele Nationen bedeckt und verweigern sich der Schaffung von Transparenz. Zudem drängt sich eine internationale Regelung der Fragen im Bereich der Unterwasserinfrastruktur als Teil des See- bzw. Völkerrechts auf.

Diese Aufnahme zeigt ein Internetkabel, das ins Meer verlegt worden ist.