6. Nov. 2012

von fgrunert

in Außenpolitik, Cyber Security, Sicherheitskultur, Strategie

Kommentare (1)

Drohnen und SWIFT unter Wasser – Die Relevanz von Unterseekabeln

von Florian Grunert

95% unseres weltweiten Datenverkehrs werden von Unterseekabeln transportiert, nur ein Bruchteil über Satelliten (~5%). Das macht sie zu einer zentralen, kritischen Infrastruktur. Die Kabel verbinden Menschen und Regierungen, ermöglichen eine globale Datenkommunikation und damit auch unsere moderne und vernetzte Gesellschaft. Das derzeitige, alltägliche Leben vieler Menschen wäre ohne diese Kabel nicht möglich. Ein moderner Staat und seine Armee wären nicht handlungsfähig.

Unterseekabel sind relevant für das **Militär**, beispielsweise wenn die USA ihre Drohnen bei Irak Missionen fliegt. Die Piloten sitzen oft mehrere 1000km entfernt von der Drohne. Die Übertragung benötigt eine hohe Bandbreite, da sie in Echtzeit passieren muss, sodass die Drohne fehlerfrei gesteuert werden kann. Hierzu werden die Unterseekabel stark in Anspruch genommen. Allein wegen der hohen Latenz wären Satelliten hier die schlechtere Wahl. Eine moderen Armee beruht auf dem Gedanken der Vernetzung, alles ist miteinander verbunden: Konzepte wie das *Network-Centric-Warfare*, das *C4ISR* oder *die vernetzte Operationsführung (NetOpFü)* zeigen dies. Doch gerade die ungeschützen Unterseekabel, die diese Konzepte erst ermöglichen, könnten im Falle eines Konfliktes zu großen Problemen führen.

Einen ebenfalls sehr wichtigen Faktor stellen Unterseekabel für den Hoch-Frequenz-Handel an den **Börsen** dar. Dieser Handel macht einen großen Teil des Tagesgeschäftes aus, wurde aber ebenfalls erst möglich durch moderne Seekabel. Alleine die SWIFT agiert über diese Kabel in über 200 Ländern. Man geht davon aus, dass mehrere Billionen US-Dollar jeden Tag darüber gehandelt werden. Im September 2011 wurde zwischen der New Yorker und der Londoner Börse ein neues Unterseekabel gelegt, um 6 Millisekunden Zeit beim Handel zu sparen. Der Bau kostete ungefähr 300 Millionen Dollar – die Kosten haben sich nach kurzer Zeit wieder rentiert.

Kurze Geschichte der Vernetzung

Das erste Unterseekabel, das jemals zur Kommunikation genutzt

SOCIAL MEDIA

SUCHE

Suche...

Suche

TWITTER FEED

Ben Kamis: The concept of #cyberpeace is linguistic trolling. Cyberpeace: post-war is war, only more so http://t.co/fkaHhcgekK #cyberwar
ungefähr 21 Stunden her von &s

Wer wissen will was #cyberpeace ist, sollte wissen was dieser sog. #cyberkrieg ist: Matthias Schulze dazu bei uns http://t.co/LyvFdE29dN
8. Dezember 2014, 11:08 von &s

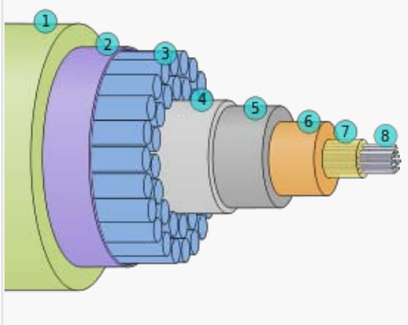
Neue #Jobs für Politikwissenschaftler_innen! http://t.co/f3vSzfJpMG
5. Dezember 2014, 9:03 von &s

TAGS

bundeswehr China Cyber Security cybersicherheit Cyber Spionage Cyberwar Deutschland diplomatie Ethik EU Europa Japan job jobs Jobsuche Krim Leaking Leaks Netzpolitik nsa Obama Politikwissenschaft Politikwissenschaften protest Putin R2P Resilienz Responsibility to Protect russland Sanktionen

The Eastern Telegraph Co.: System and its general connections. Chart of submarine telegraph cable routes, showing the global reach of telecommunications at the beginning of the 20th century (A.B.C. Telegraphic Code 5th Edition)

worden ist, befand sich im Ärmelkanal und verband Großbritannien und Frankreich. Die Kommunikation fand damals noch über einen Telegraphen statt; viele Nationen erkannten schnell den Vorteil dieser Technologie und beauftragten Unternehmen und Wissenschaftler damit, Lösungen für eine Kommunikation über Kabel zu erarbeiten. Im 19. Jahrhundert war nicht nur die Übertragung an sich eine technische Herausforderung, sondern auch der physische Schutz der Kabel. Man merkte schnell, dass ein offenes Kabel über Land bei Trockenheit relativ stabil funktionierte, die Übertragungsqualität jedoch massiv eingeschränkt wurde, wenn Nässe hinzukam. Es mussten also andere Techniken für die Überquerung der Ozeane entwickelt werden. Man begann, die Kabel mit immer widerstandsfähigeren Ummantellungen zu umgeben.



Typischer Aufbau eines modernen Seekabels/ Nachrichtenkabel (http://1.usa.gov/RwmfHd)

Zu Beginn waren die Kabel meist aus Kupfer. Ein Kupferkabel konnte anfangs nur ein, später mittels modulierter Übertragung etwa 40 Telefone verwalten. Der Aufwand war sehr hoch für lediglich 40 Leitungen. Erst mit der Erfindung der Glasfaserkabel konnten größere Datenmengen transportiert werden. Diese schafften zunächst nur 1000-mal mehr als die herkömmlichen Kupferleitungen. Die schnellsten Kabel der Welt übertrugen schon testweise im Bereich von 100 Petabits pro Sekunde und Kilometer (100.000.000 Gigabits pro Sekunde und Kilometer). Diese technische Entwicklung hat die Kupferkabel schnell abgelöst, denn durch den Transport von Information über Licht in Glasfaserkabeln war man nicht nur viel schneller, sondern die Kabel konnten dünner und sicherer konstruiert werden. Mittlerweile sind alle Kontinente, außer der Arktis, an Glasfaser-Unterseekabel angeschlossen. Diese Entwicklung vollzog sich in 150 Jahren. Das längste Unterseekabel ist im Moment das SEA-ME-WE 3-Kabel mit 39.000km.

Sicherheitspolitische Diagnose

Schutzverantwortung Sicherheit Sicherheitskonferenz snowden Stellenangebote Stellenanzeigen Syrien Transparenz Ukraine USA Versicherheitlichung Wikileaks Wissenschaftsblogs Workshop Überwachung

WP Cumulus Flash tag cloud by Roy Tanck requires Flash Player 9 or better.

BELIEBT KOMMENTARE NEU

Hell yeah, it's Political Science! Wissenschaftliche Podcasts

Das Internet darf ein cyberfreier Raum sein

Deutschlands Irak-Politik – Verantwortung nach außen, Intransparenz nach innen.

Wir haben Geburtstag!

It's not Cyberwar, stupid!

Peter
Dem Fazit kann nur zugestimmt werden, es sind dringend Dialoge notwendig die deeskalierend auf die...

Stellenangebote Sucher
Echt interessante Stellenangebote. Mich persönlich sprechen ja die Kaderstellen „Project Manager Berlin“ und die Studentenjobs...

seditioni
Danke Jochen! :3

Jochen
Na dann aber herzlichen Glückwunsch zum Geburtstag! Und

Die gemeinsame Kooperation

Schon 1884 erkannte die internationale Gemeinschaft, dass die Kabel eine kritische Infrastruktur darstellen, die es zu schützen gilt. Mit der INTERNATIONAL CONVENTION FOR THE PROTECTION OF SUBMARINE CABLES zeigten die damaligen Staaten, dass eine gemeinsame Abhängigkeit von dieser kritischen Infrastruktur besteht. Dies hat zu einem zukunftsweisenden Vertragswerk geführt, welches bis heute Bestandteil der United Nations Convention on the Law of the Sea (UNCLOS) ist. Auf internationaler Ebene gibt es kaum vergleichbare Kooperation auf diesem Niveau zu dieser Zeit. Eine wichtige Institution ist das International Cable Protection Comitee, welches als Schnittstelle zwischen Unternehmen und staatlichen Akteuren fungiert. Interessanterweise werden die meisten Kabel sowohl von privaten Investoren finanziert, gebaut als auch gewartet. Dieser Markt hat einen starken Wettbewerb, da sowohl Ausbau als auch Wartung der Kabel ein langfristiges Geschäft sind. Es werden jedoch klare Anweisungen der Internationalen Gemeinschaft für den Ausbau gemacht, so wie es Generalsekretär Dr. Hamadoun I. Touré von der International Telecommunication Union (ITU) am vierten August 2009 für die Unterseekabel SEACOM formuliert hat. Durch das Projekt SEACOM, über das Touré spricht, soll Afrika an die Infrastruktur des weltweiten Unterseekabelnetzes anschließen, da so der Wohlstand ganz Afrikas vergrößert werden könne. Durch SEACOM soll der ganze afrikanische Kontinent mit verschiedenen Kabeln umrundet werden. Von den Meeren aus sollen die Leitung wie ein Spinnennetz in das Land wachsen, hofft die ITU. Die weltweite Vernetzung gilt als ein Beschleuniger für die Weiterentwicklung vieler Bereiche von Gesellschaften. So wird es auch für Afrika prognostiziert.

Krieg, Spionage und Unterseekabel

Nicht nur die moderne Kriegsführung mit ihren Drohnen nutzt die Unterseekabel. Schon im Kalten Krieg wurde versucht, Informationen in diesen Netzen abzuhören. Die NSA hat mithilfe verschiedener Technologien die ungeschützten Kabel der UdSSR im Meer erfolgreich abgehört. Die Operation Ivy Bells war dabei wohl nicht der einzige Versuch, die Kabel anzuzapfen. Bei Längen von mehreren 1000km scheint es mit dem nötigen Equipment ein leichtes zu sein, die Kabel abzuhören. Auch das Abhören der Bürger ist möglich, wobei dies nicht auf dem Meer passieren muss. Denn die Kabel begeben sich irgendwann aufs Land, was aus rechtlicher Sicht eine nicht international regulierbare Sache ist.
Des Weiteren wird der Datenverkehr oft auch unterschiedlich durch die Netze geleitet, was vor einigen Jahren zu diplomatischen Verstimmungen zwischen den USA und China geführt hat. Ein chinesischer Internet Service Provider (ISP) mit dem Namen IDC China Telecommunication hatte einen großen Teil des weltweiten Internetverkehrs über sich geleitet. Für größere Staaten ist es also kein gößeres Problem, Informationen aus den weltweiten Datenkabeln zu erfassen und zu verarbeiten.

auf die nächsten drei Jahre! Schönes/r Blog!...

Sicherheits-Experte
Guter Artikel zur Sicherheitspolitik!

Cyberpeace: post-war is war, only more so

It's not Cyberwar, stupid!

Stellenanzeigen November 2/2

Ankündigung: Blogforum zum Thema Cyberpeace

Konferenzbericht aus Göttingen: Politisches Handeln in digitalen Öffentlichkeiten

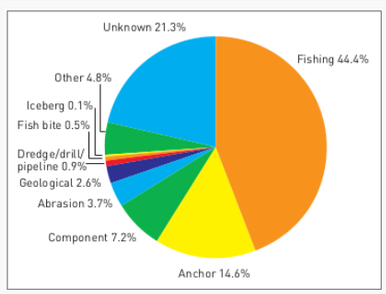
KATEGORIEN

Außenpolitik (59)
Bürgerkriege (16)
Cyber Security (42)
Demokratisierung (9)
Drohnen (15)
Humanitäre Interventionen (15)
Innere Sicherheit (24)
Interviews (10)
Katastrophen (4)
Konferenz (20)
Militär (28)
Pandemien (2)
Podcast (7)
Popkultur (21)
Sanktionen (8)
Security Culture (14)

Der Kabelriss

Global pattern of external aggression cable faults, 1959–2006. (Tyco Telecommunications (US) Inc.)

Die größten Gefahren für Unterseekabel sind Fischerei und Seefahrt, Meeresbewohner mit scharfen Zähnen und natürlich das Meer und die Bewegung des Meeresbodens. Von 1959 bis 2006 gab es 2162 Vorfälle, bei denen Unterseekabel beschädigt worden sind. Viele von diesen Vorfällen wurden von der breiten Gesellschaft nicht wahrgenommen, da sie vor der Entwicklung des Internets stattgefunden haben. Einer der Vorfälle, und wohl einer der spektakulärsten in den letzten Jahren, passierte im Jahre 2008. Im Mittelmeer hat ein Boot geankert und dabei ein Kabel (SEA-ME-WE 4 und FLAG Telecom) zerstört. Ein einzelner Anker unterbrach somit damals 70% des Internetverkehrs von und nach Ägypten und 60% des Internetverkehrs in Indien. Die Reparaturarbeiten dauerten ungefähr eine Woche, was deutlich macht, wie anfällig diese Kabel sind. Wie fatal die Auswirkungen wären, wenn dies an mehreren Stellen passiert, ist kaum vorzustellen. Die Schwierigkeit ist, dass zunächst über verschiedene Verfahren herausgefunden werden muss, wo die zerstörte Stelle ist – dann müssen Boote und Taucher dort hinfahren und sie finden und reparieren. Zusätzlich muss das Wetter auf hoher See mitspielen. Dieser Unfall zeigte deutlich, wie anfällig und verwundbar unsere vernetzte Gesellschaft doch ist.



Proportion of cable faults by cause, from adatabase of 2,162 records spanning 1959–2006 (Tyco Telecommunications (US) Inc.)

Die vernetzte Zukunft

Auch in zukünftigen Konflikten können Schäden an strategischen Knotenpunkten dieses Netzes die Internet-Infrastruktur eines Landes lahmlegen. Zwischen Europa und den USA scheint dies eine schwierige Aufgabe zu sein, da dort viele redundante Kabel liegen – aber in Ländern, in denen die Netze nicht so weit ausgebaut sind, können Angriffe auf Unterseekabel ein erhöhtes Risiko darstellen. Strategische und operative Manöver der Armeen zum Schutz dieser Kabel sind notwendig und ratsam.

Sicherheits-Kommunikation (14)
Sicherheitskultur (205)
Sozialwissenschaft Online (57)
Stellenangebote (42)
Strategie (10)
Terrorismus (14)
Theorie (2)
Umwelt (1)
Versicherheitlichung (22)
Visualisierung (5)
Whistleblowing (8)
WikiLeaks (17)
WMD (10)
Zivilgesellschaft (48)

BLOGROLL

Arbeitskreis soziale Bewegungen
Augen geradaus
Dan Drezner
Dart-Throwing Chimp
David Campbell
de.hypotheses.org
Demokratieforschung Göttingen
Duck Of Minerva
Future and Politics
Hylaean Flow
Internet und Politik
IR Blog
Just Security Blog
justsecurity.org
Killer Apps
Kings Of War

Ob schon terroristische Attacken oder Erpressungen stattgefunden haben, ist aus den öffentlich zugänglichen Quellen nicht zu beantworten. Die Weiterentwicklung und der Ausbau der Unterseekabel werden weiter fortschreiten, und da die Menschheit immer mehr Bandbreite braucht, werden die Kabel länger und die Geschwindigkeit, mit denen die Daten transportiert werden, immer höher. Weitere Sicherheitsmechanismen werden implementiert werden: Hier wird die Quantenkryptografie einen großen Beitrag dazu leisten, die Informationen vor Dritten besser zu schützen. Auch der Einsatz von automatisierten Geräten, die sowohl die Kabel kontrollieren als auch reparieren können, werden immer häufiger zum Einsatz kommen. Die kritisch diskutierten, autonomen Systeme übernehmen heute schon Reparaturaufgaben, die früher Taucher machen mussten.

Die internationale Politik hat zwar bisher einige Verträge zum Schutz dieser bedeutenden Infrastruktur auf den Weg gebracht, aber die wenigen genannten Beispiele zeigen bereits, dass das nicht reicht. Dass hier noch mehr Zusammenarbeit geleistet werden muss, damit dieses Netz sicher bleibt und die vernetzte Gesellschaft ungefährdet bleibt.

Links zu spannendem Zeug

1. [Spannend]Mother Earth Mother Board – The hacker tourist ventures forth across the wide and wondrous meatspace of three continents, chronicling the laying of the longest wire on Earth. By Neal Stephenson Link: http://www.wired.com/wired/archive/4.12/ffglass_pr.html

2. Gregs Cable Map http://www.cablemap.info/

3. [Informativ]Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N. (2009). Submarine Cables and the Oceans – Connecting the World. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC. http://www.iscpc.org/publications/ICPC-UNEP_Report.pdf

   [Vertiefend][CYBERSPACE IN DEEP WATER: PROTECTING UNDERSEA COMMUNICATION CABLES
   By Creating an International Public-Private Partnership Prepared by:
   Michael Sechrist Harvard Kennedy
   School http://belfercenter.ksg.harvard.edu/files/PAE_final_draft_-_043010.pdf

Florian Grunert aka @zeroskillor schließt gerade

netzpolitik.org
percepticon
shabka.org
Terrorismus in Deutschland
theorieblog.de
Verfassungsblog
Vom Bohren harter Bretter
whistleblower-net.de

ARCHIV

Wähle den Monat

sein Politikwissenschafts- und Philosophie-Studium an der Universität Osnabrück ab. Er beschäftigt sich seit Jahren mit Cyber War und Cyber Security und betreibt die Website http://www.study4cyberpeace.com/. Wir veröffentlichten bereits einen seiner Vorträge.

Tags: diplomatie, politik, sicher, unterseekabel, vernetzung, vertrag

« Neusprech – ›Humanitäre Intervention‹ Podcast #1: Die Wahl in den USA »

Trackbacks/Pingbacks

1. **Angreifbarkeit von Unterseekabeln « Florian's Blog** - 7. Nov. 2012

   [...] Beim lesen auf Twitter stieß ich vorhin auf folgenden Tweet von @SipoBlog: #Drohnen und #SWIFT unter Wasser – @zeroskillor über die Relevanz von #Unterseekabeln http://www.sicherheitspolitik-blog.de/2012/11/06/drohnen-und-swift-unter-wasser/“ [...]

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Kommentar senden

☑ Benachrichtige mich über nachfolgende Kommentare per E-Mail.