Vulnerable kritische Infrastrukturen

Perspektiven auf Resilienz bei Cyber-, Drohnen- und Unterseekabelangriffen

von Christian Reuter, Jonas Franken, Anja-Liisa Krichbaum, Marie Gregor und Marc-André Kaufhold

Beschädigte Unterseekabel in der Ostsee, Drohnensichtungen über Flughäfen oder Cyberangriffe auf Versorgungssysteme: Kritische Infrastrukturen rücken zunehmend in den Fokus geopolitischer Konflikte und hybrider Bedrohungen. Doch wie verwundbar sind modernde Gesellschaften und was macht sie widerstandsfähiger? Anhand von Beispielen aus aktueller Forschung am Lehrstuhl PEASEC der TU Darmstadt beleuchtet dieser Beitrag unterschiedliche Formen infrastruktureller Vulnerabilität und diskutiert, wie Lösungsansätze für Resilienz jenseits militärischer Abschreckung gestärkt werden können.

Kritische Infrastrukturen (KRITIS) spielen in Kriegen und Konflikten seit jeher eine zentrale Rolle. Logistik, Energieversorgung und Kommunikationsnetze bilden die Grundlage für das Funktionieren von Gesellschaften und sind somit auch von erheblicher militärischer Relevanz. Die sicherheitspolitische Relevanz von KRITIS ist daher keineswegs ein neues Phänomen.

Dennoch haben sich einige Rahmenbedingungen verändert. Mit der wachsenden Konnektivität entstehen nicht nur neue Möglichkeiten gesellschaftlicher und wirtschaftlicher Entwicklung, sondern auch zunehmende Abhängigkeiten und zusätzliche Angriffsflächen für staatliche und nichtstaatliche Akteure (Reuter 2024). Besonders deutlich zeigt sich dies im Kontext »hybrider Konflikte«, in denen die Grenzen zwischen Krieg und Frieden sowie militärischen und zivilen Zielen zunehmend verschwimmen. KRITIS geraten dabei auf vielfältige Weise in den Fokus.

Vor diesem Hintergrund stellt sich die Frage, wie die KRITIS-Resilienz gestärkt werden kann, ohne primär auf militärische Abschreckung oder offensive Fähigkeiten zu setzen, mit dem Ziel, die Angriffsfläche bei potenziellen Angriffen zu verringern. Exemplarisch stellen wir in diesem Beitrag unsere Forschungsarbeiten zu Untersee-Datenkabeln, Rüstungskontrolle für Cyberwaffen und zur Cybersicherheitskompetenz von Bürger*innen vor, um unterschiedliche Dimensionen der Verwundbarkeit und Resilienz kritischer Infrastrukturen zu beleuchten.

Vulnerabilität und Resilienz

KRITIS versorgen die moderne Gesellschaft mit essenziellen Gütern und Dienstleistungen. Ausfälle in verschiedenen KRITIS-Sektoren zeigen regelmäßig, wie stark die Abhängigkeit von Stromversorgung und digitaler Konnektivität inzwischen ist. Im Zuge der fortschreitenden Digitalisierung gewinnen insbesondere Informations- und Kommunikationstechnologien (IKT) innerhalb dieser KRITIS-Systeme zunehmend an Bedeutung.

»KRITIS« sind jene grundlegenden gesellschaftlichen Strukturen, deren Funktionieren für Staat, Wirtschaft und Bevölkerung von entscheidender Bedeutung ist. Obwohl der Begriff heute weit verbreitet ist, bestehen weiterhin begriffliche Unschärfen, die eine differenzierte Betrachtung erforderlich machen. So hängt die Kritikalität einer Infrastruktur von diversen kontextuellen Faktoren ab, die im Grunde eine dauerhafte Neubewertung verlangen. Dies steht jedoch im Widerspruch zu der Notwendigkeit einer rechtssicheren Umsetzung durch Definitionen – in der Regel in Form von Schwellenwerten – die objektiv überprüfbar und für die Betreiber*innen als Adressat*innen der entsprechenden Verordnungen nachvollziehbar und praktikabel sind. Ebenso kann es vorkommen, dass KRITIS im Sinne einer Versicherheitlichung instrumentalisiert wird – allein das Framing einer Infrastruktur als »kritisch« kann auf diese Weise politisch instrumentalisiert werden (Franken und Reuter 2024).

Im Forschungsfeld der KRITIS wird häufig der Begriff der »Vulnerabilität« verwendet. Ingenieurwissenschaften verstehen darunter Sicherheitslücken, die durch komplexe Systemabhängigkeiten oder externe Risiken wie Cyberangriffe entstehen (Eifert et al. 2018). Ein hohes Maß an KRITIS-Sicherheit ist grundsätzlich wünschenswert, kann jedoch paradoxerweise zu einer höheren Vulnerabilität führen. Besonders anschaulich wird dies durch das sogenannte »Verletzlichkeitsparadoxon«. Bereits in der deutschen KRITIS-Strategie wurde formuliert: *„In dem Maße, in dem ein Land in seinen Versorgungsleistungen weniger störanfällig ist, wirkt sich jede Störung umso stärker aus“* (BMI 2009). Auf den ersten Blick erscheint dies widersprüchlich: Die hohe Zuverlässigkeit von KRITIS kann dazu führen, dass individuelle und gesellschaftliche Vorsorgemaßnahmen an Bedeutung verlieren. Denn: Je seltener Ausfälle auftreten, desto geringer ist häufig die Bereitschaft, Ressourcen für potenzielle Krisenszenarien vorzuhalten. Kommt es dennoch zu einer Störung, können die Auswirkungen daher besonders schwerwiegend ausfallen. Resilienz hängt folglich nicht allein von der Robustheit technischer Systeme ab, sondern auch von der Fähigkeit von Staat, Wirtschaft und Bevölkerung, mit Störungen umzugehen und sich auf diese vorzubereiten.

»Resilienz« beschreibt die Fähigkeit eines Systems, Krisen und Störungen zu absorbieren, sich von ihnen zu erholen oder sich so anzupassen, dass zentrale Funktionen auch unter veränderten Bedingungen aufrechterhalten werden können (Hollick und Katzenbeisser 2024). Resilienz ist daher kein statischer Zustand, sondern ein fortlaufender

Prozess des Lernens und der Anpassung. Durch die Bewältigung vergangener Krisen können Systeme ihre Vorsorge- und Reaktionsfähigkeit (»Preparedness«) langfristig verbessern. Insbesondere digitale Technologien und IKT eröffnen hierfür neue Möglichkeiten. Sie fördern die Anpassungsfähigkeit und erlauben den Weiterbetrieb einzelner Systembestandteile auch bei Störungen, erhöhen jedoch zugleich die Komplexität und den Aufwand für Schutz- und Sicherheitsmaßnahmen. Daher ist häufig eine Abwägung zwischen Anpassungsfähigkeit und Schutz vor Angriffen erforderlich.

Die abstrakten Konzepte von Vulnerabilität und Resilienz lassen sich anhand unterschiedlicher Ebenen kritischer Infrastrukturen veranschaulichen. Die folgenden Abschnitte stellen daher exemplarisch drei Forschungsfelder unseres Instituts PEASEC an der TU Darmstadt vor, die sich mit infrastrukturellen Verwundbarkeiten und möglichen Resilienzstrategien beschäftigen.

Maßnahmen für ein resilientes Seekabelnetz

99 % des interkontinentalen Datenverkehrs laufen durch etwa 600 Unterseekabel. Maritime Datenkabel stellen somit eine zentrale physische Grundlage der globalen Digitalisierung dar. Entsprechend gehören sie zu den wichtigsten KRITIS moderner Gesellschaften. Gleichzeitig geraten maritime Infrastrukturen – nicht nur, aber auch aufgrund des Stellenwerts dieser Kabel – zunehmend in den Fokus geopolitischer Konflikte, hybrider Bedrohungen und möglicher Sabotageakte (Edwards und Seidenstein 2025, Kavanagh et al. 2025). Spätestens seit den Anschlägen auf die Nord-Stream-Pipelines 2022 sowie mehreren beschädigten Kabelverbindungen in der Ostsee wird der deutschen Öffentlichkeit deutlich, wie verwundbar diese Systeme gegenüber technischen Defekten, Unfällen und potenziell auch gezielten Angriffen sind. Besonders Staaten mit nur wenigen redundanten Verbindungen sind bei Ausfällen erheblich gefährdet (Franken et al. 2022).

Vor diesem Hintergrund haben wir untersucht, welche Faktoren den Ausbau des globalen Netzes von Untersee-Datenkabeln zwischen 1995 und 2025 beeinflusst haben (Franken et al. 2025). Dabei haben wir die bisher dominante Annahme hinterfragt, dass wirtschaftliche Kosten-Nutzen-Abwägungen allein die Planung neuer Kabelverbindungen bestimmen. Unsere Ergebnisse zeigen, dass wirtschaftlich starke und bevölkerungsreiche Staaten deutlich häufiger an das globale Unterseekabelnetz angeschlossen werden. Gleichzeitig wirken sich in signifikantem Maße politische Instabilität und gewaltsame Konflikte negativ auf den Ausbau aus, da Kabelbetreiber fragile Regionen offenbar meiden. Auch geografische Faktoren wie seismische Risiken oder die Anzahl angrenzender Staaten beeinflussen die Planung neuer Verbindungen. Ein Verständnis dieser Präferenz- und Vermeidungsfaktoren kann zu einer besseren Einschätzung führen, unter welchen Umständen öffentliche Förderung für Seekabel als Mittel für eine Diversifizierung der Routen und Landepunkte sorgen kann, um letztlich eine höher Ausfallsicherheit zu erreichen.

In PEASEC-Arbeiten (Bueger et al. 2022, Franken 2025) entwickelte Konzepte wie die jüngst im Bundestag (2026) diskutierte »Kabeldiplomatie« zeigen darüber hinaus, dass digitale Infrastrukturen zunehmend strategische und geopolitische Bedeutung besitzen. Die Ergebnisse unterstreichen daher die Notwendigkeit resilienter, redundanter und diversifizierter digitaler Infrastrukturen für die zukünftige globale Vernetzung.

Für die konkrete regulatorische Umsetzung auf nationaler und internationaler Ebene wurde in einer weiteren Studie erhoben, welche Maßnahmen für tatsächlich mehr Resilienz in diesem Bereich sorgen. Militärische Aktivitäten als Antwort auf vermutete Sabotagen, wie die NATO-Operation »Baltic Sentry« können dabei zwar einen Teil zur responsiven Ebene beitragen – eine nachhaltige Seekabelresilienz erfordert aber viele weitere Aspekte – zum Beispiel den engeren Einbezug der Industrie, die Sicherung der Lieferketten, die Einbindung neuer Sensortechnologien zur Seeraumüberwachung und eine weitestgehend transparente Kartierung der Seekabel zur Unfallprävention (Franken et al. 2026, Kavanagh et al. 2025).

Unbemannte Systeme, Cyberwaffen und Rüstungskontrolle

Die KRITIS-Verwundbarkeit beschränkt sich jedoch nicht auf physische Netze, denn neue digitale und autonome Technologien erweitern diese Möglichkeiten wesentlich.

Neben klassischen Angriffsszenarien auf KRITIS gewinnen auch unbemannte Systeme zunehmend an Bedeutung. Insbesondere Drohnen stellen eine wachsende Bedrohung dar, da sie vergleichsweise kostengünstig, leicht verfügbar und flexibel einsetzbar sind (vgl. auch Suckau in dieser Ausgabe, S. 10). Sie können zur Ausspähung sensibler Anlagen, zur Störung von Betriebsabläufen oder sogar für physische Angriffe auf Energie-, Kommunikations- oder Verkehrsinfrastrukturen genutzt werden. Internationale Vorfälle – etwa Drohnensichtungen über Flughäfen, Industrieanlagen oder militärischen Einrichtungen – verdeutlichen die sicherheitspolitische Relevanz dieser Entwicklung. Verschärft wird dies durch den Einsatz zunehmend autonomer Systeme.

Durch die voranschreitende Vernetzung und Digitalisierung kritischer Systeme entstehen hybride Bedrohungslagen, in denen physische und digitale Angriffe ineinandergreifen. Drohnen fungieren dabei nicht nur als eigenständige Angriffsplattformen, sondern können auch cyberphysische Operationen unterstützen und umgekehrt, etwa durch die Einschleusung von Schadsoftware in isolierte Netzwerke oder die Störung drahtloser Kommunikationssysteme. Die Regulierung solcher Technologien gestaltet sich jedoch schwierig, da viele Komponenten einen »Dual-Use«-Charakter besitzen, weil sie sowohl zivile als auch militärische sowie sowohl offensive als auch defensive Anwendungen ermöglichen. Damit stellen Drohnen, ähnlich wie Cyberwaffen, eine Herausforderung für bestehende Rüstungskontroll- und Sicherheitsmechanismen dar.

Vor diesem Hintergrund gewinnt auch die Frage nach Rüstungskontrolle bzw. Regulierung von autonomen Systemen und im Cyberraum zunehmend an Bedeutung – nicht nur für die Sicherheit von KRITIS. Insbesondere im Kontext solcher Waffensysteme beobachten wir eine zunehmend fragmentierte Regulierungslandschaft bei gleichzeitig stagnierenden Verhandlungen in einschlägigen Gremien wie den »Groups of Governmental Experts« zu Cyberspace und zu autonomen Waffen. Daher haben wir untersucht (Gonsior et al. 2026), inwiefern bestehende Mechanismen klassischer Rüstungskontrolle als Vorbild für die Regulierung von Cyberwaffen dienen können. Dabei zeigen sich zentrale Parallelen zu diesen klassischen Mechanismen, insbesondere in den Herausforderungen für die Regulierung, etwa hinsichtlich des Dual-Use-Charakters der Technologien, die Schwierigkeit eindeutiger bzw. ein-

heitlicher Definitionen sowie die Problematiken von Verifikation und Attribution. Insofern sind klassische Mechanismen zwar nicht direkt übertragbar, bieten jedoch wichtige Anknüpfungspunkte. Für die Rüstungskontrolle bedeutsam ist, dass immer deutlicher wird, welch zunehmend zentrale Rolle nicht-staatliche Akteure spielen, unter anderem durch ihren Einfluss auf Forschung und Entwicklung sowie die Etablierung informeller Regulierungsstandards in Bereichen, in denen es derzeit keine formelle Regulierung gibt. Dies zeigt sich insbesondere auch im Kontext von autonomen Systemen (Riebe et al. 2025).

Die Ergebnisse legen nahe, dass sich zukünftige Cyber-Rüstungskontrolle weniger auf die Regulierung konkreter Technologieanwendungen als vielmehr auf deren Nutzungskontexte fokussieren sollte. Zugleich verdeutlichen die Studien, dass politische Interessen, unterschiedliche technische Ansätze sowie die hohe Innovationsgeschwindigkeit digitaler Technologien erhebliche Hürden für dauerhafte und multilaterale Vereinbarungen darstellen.

Die Regulierung von Cyberwaffen adressiert nur eine Ebene digitaler Sicherheit. Ebenso relevant dafür ist die Frage gesellschaftlicher Resilienz.



Claudius Förster (2026): **Schwerter zu Pflugscharen – Mahnmal VIII (Ausschnitt)**

Cybersicherheitskompetenz der Bevölkerung

Angesichts der zunehmenden Verwundbarkeit der Gesellschaft gegenüber Cyberangriffen haben wir in Deutschland in den Jahren 2021 bis 2024 repräsentative Bevölkerungsumfragen mit dem Ziel durchgeführt, das Bewusstsein für Cyberbedrohungen, die Nutzung von Schutzmaßnahmen sowie bevorzugte Informationskanäle besser zu verstehen (Kaufhold et al. 2025).

Die Ergebnisse dieser Umfragen zeigen, dass ein großer Teil der deutschen Bevölkerung ein hohes Maß an Bewusstsein für Cyberbedrohungen besitzt. Jedoch fühlen sich viele Menschen unzureichend darüber informiert, wie sie konkret mit Cyberangriffen umgehen sollen. Zudem besteht nur begrenztes Vertrauen in die Fähigkeit deutscher Sicherheitsbehörden, die Bevölkerung und KRITIS wirksam zu schützen. Insbesondere das Alter wirkte sich auf Wahrnehmung und Verhalten der Befragten aus: Jüngere Menschen berichteten häufiger von Erfahrungen mit Cyberbedrohungen und wiesen zugleich ein höheres Gefahrenbewusstsein als ältere Befragte auf.

Über den Zeitverlauf zeigten sich lediglich geringe Unterschiede zwischen den einzelnen Erhebungen. Die Ergebnisse deuten darauf hin, dass trotz gestiegener öffentlicher Aufmerksamkeit weiterhin erheblicher Informations- und Handlungsbedarf im Bereich Cybersicherheit besteht. Als Empfehlungen können daraus insbesondere Folgende abgeleitet werden:

- Dass Sicherheitsbehörden ihre Kommunikation zu Cyberbedrohungen stärker an den Bedürfnissen und genutzten Informationskanälen der Bevölkerung ausrichten sollten, um Vertrauen, Vorbereitung und Selbsthilfefähigkeiten zu stärken.
- Zudem sollten die staatlichen Reaktionskapazitäten auf großflächige Cyberangriffe ausgebaut und neue Formen der Zusammenarbeit zwischen Behörden und Bürger*innen – etwa durch freiwillige Cyber-Helfer*innen oder Crowdsourcing-Ansätze – gefördert werden.
- Darüber hinaus erscheinen altersorientierte Bildungs- und Präventionsmaßnahmen sinnvoll, da sich Sicherheitsverhalten und genutzte Schutzmaßnahmen zwischen jüngeren und älteren Menschen deutlich unterscheiden.
- Schließlich kann eine intensivere Zusammenarbeit zwischen staatlichen Stellen, Unternehmen und Bildungseinrichtungen helfen, Sicherheitsinformationen wirksamer zu verbreiten und die Cybersicherheitskompetenz der Bevölkerung nachhaltig zu stärken.

Als Grundlage für die Umsetzung dieser Empfehlungen und die Verbesserung des Vertrauens muss das Fähigkeitsspektrum von Sicherheitsbehörden und beteiligten Akteuren gestärkt werden. Zur Identifikation und Behandlung relevanter Cyberbedrohungen und Sicherheitslücken stellen nicht nur das Volumen, sondern auch die variierende Qualität geheimer und öffentlich verfügbarer Informationen eine Herausforderung dar (Riebe et al. 2021). In diesem Zusammenhang untersuchte PEASEC nutzer*innenzentrierte Technologien, die die Lagebilderstellung im Cyberraum durch algorithmische Automatisierung und interaktive Visualisierung kontextadäquat unterstützen. Daraufhin entwickelte und erprobte PEASEC gemeinsam mit deutschen »Computer Emergency Response

Teams« einen Demonstrator, der Cyberbedrohungsinformationen automatisiert bündelt, filtert und aufbereitet, und leitete daraus konkrete Anforderungen und Gestaltungsprinzipien für solche Systeme ab (Kaufhold et al. 2024).

Neben technischen Schutzmaßnahmen für KRITIS bilden also die Vorbereitung der Bevölkerung und das gesellschaftliche Sicherheitsgefühl sowie die Aushandlungsprozesse darum zentrale Voraussetzungen für die Resilienz eines Landes.

Fazit: Vulnerabilität von KRITIS – auch jenseits des Krieges

Die sicherheitspolitische Relevanz von KRITIS ergibt sich heute nicht nur aus ihrer Funktion, sondern vielmehr aus der zunehmenden Komplexität ihrer Verwundbarkeiten. Die rasante Digitalisierung vieler Bereiche hat zusätzliche Vulnerabilitäten geschaffen, die weit über klassische Angriffe auf physische Infrastruktur hinausgehen. Cyberangriffe auf Steuerungssysteme, Störungen digitaler Kommunikationsverbindungen oder die Nutzung kostengünstiger Drohnensysteme erweitern das Spektrum möglicher Bedrohungen. Hinzu kommt, dass sicherheitspolitische Fragen nicht erst im Krisen- oder Kriegsfall relevant werden.

Die drei vorgestellten Forschungsfelder verdeutlichen, dass die KRITIS-Sicherheit heute auf mehreren Ebenen zugleich verhandelt wird. Zusammen betrachtet machen die Ergebnisse deutlich, dass Resilienz weder allein durch technische Schutzmaßnahmen noch durch staatliche Sicherheitsakteure gewährleistet werden kann, sondern aus dem Zusammenwirken infrastruktureller, technologischer und gesellschaftlicher Faktoren entsteht. Gerade im Kontext hybrider Bedrohungen und bewaffneter Konflikte gewinnen präventive Resilienzmaßnahmen an Bedeutung, da sie dazu beitragen können, die Auswirkungen von Angriffen auf KRITIS zu begrenzen und die Handlungsfähigkeit von Staat und Gesellschaft zu erhalten – hierbei auf rein militärisch abschreckende Prävention zu setzen, wäre verkehrt. Die vorgestellten Beispiele verdeutlichen, dass Resilienz nicht nur eine technische, sondern auch eine politische und gesellschaftliche Gestaltungsaufgabe ist.



Danksagung

Diese Arbeit wurde durch die LOEWE Initiative des Landes Hessen im Rahmen des LOEWE Zentrums emergenCITY (Förderkennzeichen: LOEWE/1/12/519/03/05.001(0016)/72) sowie im Rahmen des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE gemeinsam vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) und vom Hessischen Ministerium für Wissenschaft und Forschung, Kunst und Kultur (HMWK) gefördert.

Literatur

Bueger, Ch.; Liebetrau, T.; Franken, J. (2022): Security threats to undersea communications cables and infrastructure – consequences for the EU. Brüssel: Europaparlament.

Bundesministerium des Inneren (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Berlin.

Deutscher Bundestag (2026): Eckpfeiler einer wirksamen und strategischen Kabeldiplomatie. Antrag der Fraktionen der CDU/CSU und SPD. BT-Drucksache 21/5749.

Edwards, C.; Seidenstein, N. (2025): The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure. Berlin: International Institute for Strategic Studies.

Eifert, S.; Knauf, A.; Thiessen, N. (2018): Vulnerability. In: Engels, I. (Hrsg.): Key Concepts for Critical Infrastructure Research. Wiesbaden: Springer VS, S. 21-29.

Franken, J. (2025): Cable diplomacy: Securing influence, data and global rules. Böll EU Brief 3/2025.

Franken, J.; Backes, T.; Reuter, Ch. (2026): Mapping the Maps: Safety-Security Trade-offs in the Charting of Subsea Data Cables. In: Troubitsyna, E. et al. (Hrsg.): SAFECOMP2026 Workshops, LNCS 16869.

Franken, J.; Reinhold, Th., Reichert, L., Reuter, Ch. (2022): The Digital Divide in State Vulnerability to Submarine Communications Cable Failure. International Journal of Critical Infrastructure Protection 38, 100522.

Franken, J.; Reinhold, Th.; Dörnfeld, T.; Reuter, Ch. (2025): Hidden Structures of a Global Infrastructure: Expansion Factors of the Subsea Data Cable Network. Technological Forecasting and Social Change 215, 124068.

Franken, J.; Reuter, Ch. (2024): Secure Critical Infrastructures. In: Reuter, Ch. (Hrsg.): Information Technology for Peace and Security. Wiesbaden: Springer Vieweg, S. 279-301.

Gonsior, A.-L.; Pleil, H.; Reuter, Ch. (2026): Difficult but possible: an exploratory approach to the regulation of cyber weapons using lessons learned from chemical weapons arms control, Journal of Cyber Policy, DOI: doi.org/10.1080/23738871.2026.2665269.

Hollick, M.; Katzenbeisser, S. (2024): Resilient Critical Infrastructures. In: Reuter, Ch. (Hrsg.): Information Technology for Peace and Security. Wiesbaden: Springer Vieweg, S. 75-83.

Kaufhold, M.-A.; Bäumler, J.; Bajorski, M.; Reuter, Ch. (2025): Comparative Cybersecurity Survey: Citizens' Cyber Threat Awareness, Protective Measures, and Trust in Security Authorities in Germany. Proceedings CHI, Yokohama, Japan: ACM, DOI: doi.org/10.1145/3706598.3713795.

Kaufhold, M.-A.; Riebe, Th.; Bayer, M.; Reuter, Ch. (2024): 'We Do Not Have the Capacity to Monitor All Media': A Design Case Study on Cyber Situational Awareness in Computer Emergency Response Teams. Proceedings CHI, Honolulu. USA: ACM, DOI: doi.org/10.1145/3613904.3642368.

Kavanagh, C.; Franken, J.; He, W. (2025): Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure. Genf: UNIDIR.

Reuter, Ch. (2024): Information Technology for Peace and Security. Wiesbaden: Springer Vieweg.

Riebe, Th.; Gonsior, A.-L.; Reichert, L.; Reuter, Ch. (2025): Envisioning Human-Machine Interaction in Future Warfare: Defence Industry Narratives on Human Control of Autonomous Weapon Systems. Global Society 39(4), S. 421-445.

Riebe, Th.; Kaufhold, M.-A.; Reuter, Ch. (2021): The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study. Proceedings of the ACM: Human-Computer Interaction (PACM): CSCW, ACM. DOI: doi.org/10.1145/3479865.

Prof. Dr. Dr. Christian Reuter *leitet den interdisziplinären Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) der TU Darmstadt.*
Jonas Franken*, M.A., ist wissenschaftlicher Mitarbeiter und Doktorand bei PEASEC und forscht zu Seekabeln, maritimer Sicherheit und kritischen Infrastrukturen.*
Anja-Liisa Krichbaum*, M.A., ist wissenschaftliche Mitarbeiterin und Doktorandin bei PEASEC und forscht zu Rüstungskontrolle im Cyberraum und autonomer Waffensysteme.*
Marie Gregor*, B.A., arbeitet als studentische Mitarbeiterin am Institut PEASEC.*
Dr. Marc-André Kaufhold *forscht bei PEASEC als Post-Doktorand zu nutzerzentrierter Gestaltung digitaler Krisentechnologien.*