Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Herausgeber: Verlagsgenossenschaft Schweizer Soldat
Band: 98 (2023)
Heft: 1

Artikel: Bedrohung für Europa
Autor: Goertz, Stefan
DOI: https://doi.org/10.5169/seals-1047579

Bedrohung für Europa

Obwohl viel über die konventionelle Kriegsführung im Ukrainekrieg berichtet wird, heisst das nicht, dass die hybride Kriegsführung Russlands gegen den Westen beendet wurde. Die europäischen Staaten bleiben verwundbar gegenüber Angriffen auf ihre Infrastruktur und Desinformationskampagnen.

Prof. Dr. Stefan Goertz, Bundespolizei, Hochschule des Bundes, Lübeck

Dieser Beitrag stellt die persönliche Auffassung des Autors dar.

Die Kriegsführung Russlands gegen die Ukraine ist hybrid, und dies spätestens seit der illegalen Annexion der Krim 2014. Die Kriegsführung Russlands im neuen Ost-West-Konflikt bedroht auch zahlreiche Staaten der westlichen Welt, Europas, auf verschiedenen Ebenen, mit verschiedenen Akteuren.

Das System Putin kombiniert klassische Militäreinsätze, wirtschaftlichen Druck, (potenzielle) Angriffe auf kritische Infrastrukturen (KRITIS), Cyberattacken sowie Desinformationskampagnen in den Medien und sozialen Netzwerken. Nach der Logik des russischen Generalstabschefs Waleri Gerassimow ist diese Kriegsführung Russlands «entgrenzt».

Die europäischen Staaten, ihre Streitkräfte, Sicherheitsbehörden und die politischen Entscheidungsträger müssen diese hybride Kriegsführung Russlands ebenso wie Institute und Thinktanks umfassend auswerten und ihre Analysen abgleichen, weil diese Kriegsführung Russlands noch für viele Jahre eine Bedrohung für Europa und die Welt darstellen wird.

Russische Cyberattacken

Russische Cyberattacken auf europäische Energieunternehmen haben seit dem Beginn des russischen Angriffskrieges gegen die Ukraine massiv zugenommen, zeigt eine Analyse der Strategieberatung Macro Advisory Partners aus dem Oktober 2022. Danach habe sich die Zahl von Cyberattacken mehr als verdoppelt, bis Oktober 2022 kam es zu mindestens 21 Attacken, im Jahr 2021 waren es zehn. Von den zwischen April und Oktober 2022 mindestens zehn verübten Attacken gegen europäische Energieunternehmen waren sechs deutsche Firmen betroffen.

Nach Angaben einer aktuellen Studie des deutschen Digitalverbands Bitkom aus dem Sommer 2022, für die mehr als 1000 Unternehmen quer durch alle Branchen befragt wurden, entstand deutschen Unternehmen im Jahr 2021 ein jährlicher Schaden von mindestens 203 Milliarden Euro durch Cyberangriffe, Spionage und Sabotage.

Hierbei verzeichneten die deutschen Unternehmen einen starken Anstieg der Angriffe aus Russland und China, 36 Prozent der befragten deutschen Firmen verorteten den Ursprung der Attacke in Russland, im Jahr 2021 waren dies noch 23 Prozent.

Spätestens seit Frühjahr 2022 warnen deutsche Sicherheitsbehörden und diejenigen anderer westlicher Staaten vor russischen Cyberattacken. Dazu gehören im Wesentlichen drei Arten, einerseits Cyberspionage, also das Eindringen in fremde Rechner und Netzwerke mit dem Ziel, sensible Daten zu stehlen, wie im Jahr 2015 im Deutschen Bundestag geschehen.

Daneben gibt es Cyberattacken, die Teil von Desinformationskampagnen sind, beispielsweise wenn Websites oder bekannte Social-Media-Accounts gehackt werden, um darüber Falschinformationen zu verbreiten – so geschehen 2020 bei diversen bekannten Twitter-Usern. Drittens Cybersabotage, Hackerangriffe mit dem Ziel, einzelne Computer oder ganze Netzwerke lahmzulegen.

Dies kann mit kleineren Ransomware-Angriffen beginnen, bei denen einzelne Rechner durch Schadsoftware verschlüsselt und nur gegen Zahlung von Lösegeld wieder entschlüsselt werden. Eskalieren kann dies aber auch mit koordinierten Angriffen auf Kritische Infrastrukturen (KRITIS), wenn die Telekommunikation, die Energie- oder die Wasserversorgung einer ganzen Region lahmgelegt wird.

Bild: Bundeswehr

Krieg wird in Europa weiterhin auch hybrid geführt. Hier im Bild: NATO-Truppen während einer Übung im Dezember.

Bild: Kremlin.ru

Präsident Putin zusammen mit Verteidigungsminister Shoigu (links) und Chef des Generalstabes Gerassimow. Das System Putin kombiniert klassische Militäreinsätze, wirtschaftlichen Druck, (potenzielle) Angriffe auf Kritische Infrastrukturen (KRITIS), Cyberattacken sowie Desinformationskampagnen in den Medien und sozialen Netzwerken.

Der Vizepräsident des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI), Gerhard Schabhüser, erklärte im November 2022: «Bedrohungslage im Cyber-Raum ist angespannt, dynamisch und vielfältig und damit so hoch wie nie.»

Das deutsche BSI führt in seinem aktuellen Lagebericht «Die Lage der IT-Sicherheit in Deutschland 2022» aus dem November 2022 aus, dass es in Deutschland seit Beginn des russischen Angriffskriegs gegen die Ukraine in Deutschland zu zusätzlichen IT-Sicherheitsvorfällen gekommen sei, so beispielsweise zu einem Ausfall der satellitengestützten Kommunikation zur Fernwartung von Windenergieanlagen in Teilen Europas. Auch waren Betreiber kritischer Infrastrukturen Angriffsziele von Hacktivisten.

Kritische Infrastruktur

Kritische Infrastrukturen (KRITIS) sind nach Angaben des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI): «Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.» Sektoren Kritischer Infrastrukturen sind Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Medien und Kultur, Wasser, Ernährung, Finanz- und Versicherungswesen, Siedlungsabfallentsorgung sowie Staat und Verwaltung.

Am 26. September 2022 wurden mehrere Lecks an der Pipeline Nord Stream 2 (KRITIS, Energie) entdeckt. Die insgesamt vier Explosionen in der Ostsee vor der dänischen Insel Bornholm hatten mehrere Lecks in die Nord-Stream-Pipelines gerissen. Erste Unterwasser-Untersuchungen erhärteten den Verdacht auf Sabotageakte. Die Nord-Stream-Pipelines waren zum Zeitpunkt ihrer Beschädigung ausser Betrieb, jedoch mit Gas gefüllt.

Die NATO geht von einem «vorsätzlichen und unverantwortlichen Sabotageakt» aus. Laut Recherchen eines US-Fachmagazins befanden sich in den Tagen vor Bekanntwerden der Lecks, zwei «dunkle Schiffe» in der Nähe des Bereichs, in dem die Explosionen erfolgten.

Als «dunkle Schiffe» werden grosse Schiffe bezeichnet, die mit ausgeschalteten Trackern unterwegs sind.

Dies ist laut internationalem Recht verboten. Die beiden fraglichen Schiffe sollen zwischen 95 und 130 Meter lang gewesen sein und sich nur wenige Kilometer von den Leckstellen entfernt befunden haben. 90 Tage hatte die Firma SpaceKnow Satellitenbilder des Gebietes durchsucht und nutzte dabei auch 38 spezifische Algorithmen, die in der Lage sind, militärisches Gerät zu erkennen. Die Ergebnisse der Untersuchung wurden an die NATO weitergeleitet.

Anfang Oktober 2022 lag der Schienenverkehr im Norden Deutschlands lahm. Der Grund war ein möglicher Sabotage-Akt, Unbekannte hatten wichtige Kommunikationskabel zerstört. Mehrere Regierungspolitiker der Ampel-Koalition im Bundestag sprachen von einem Sabotage-Akt.

An mindestens zwei Stellen wurden Lichtwellenleiterkabel durchtrennt, in Berlin-Hohenschönhausen sowie in Nordrhein-Westfalen, auch das Backup-System war damit ausgefallen. Nach Angaben der Deutschen Bahn waren von diesem Sabotageakt auch Schleswig-Holstein, Niedersachsen, Bremen und Hamburg betroffen. Von dort oder nach dort konnten keinerlei ICE-, IC- oder EC-Züge fahren.

Die Ausfälle hatten daher Folgen für den gesamten Fernverkehr in Deutschland. Bundesverkehrsminister Volker Wissing sprach am Nachmittag des Sabotageaktes von einem, wie er mehrfach betonte, «mutwilligen und gezielten Vorgehen»: Es handle sich «eindeutig um eine vorsätzliche Tat», bei der wichtige Kabel an zwei Stellen «bewusst und gezielt durchtrennt» worden seien.

Nach dem Sabotageakt auf den Schienenverkehr in Norddeutschland erklärte der Generalbundesanwalt (GBA) am 13. Oktober 2022, dass es sich um verfassungsfeindliche Sabotage gehandelt haben könnte.

Hintergrund der Übernahme der Ermittlungen durch den GBA ist der mögliche Straftatbestand der «verfassungsfeindlichen Sabotage» (Paragraf 88 StGB) und die besondere Bedeutung des Falls. Mit den weiteren Ermittlungen beauftragte die Bundesanwaltschaft das Bundeskriminalamt.

Desinformationskampagnen

Die deutsche Bundesregierung definiert Desinformationskampagnen aktuell wie folgt: «Desinformation ist falsche oder irreführende Information, die gezielt verbreitet wird. Davon zu unterscheiden sind falsche oder irreführende Informationen, die irrtümlich bzw. ohne Täuschungsabsicht entstehen und verbreitet werden. →

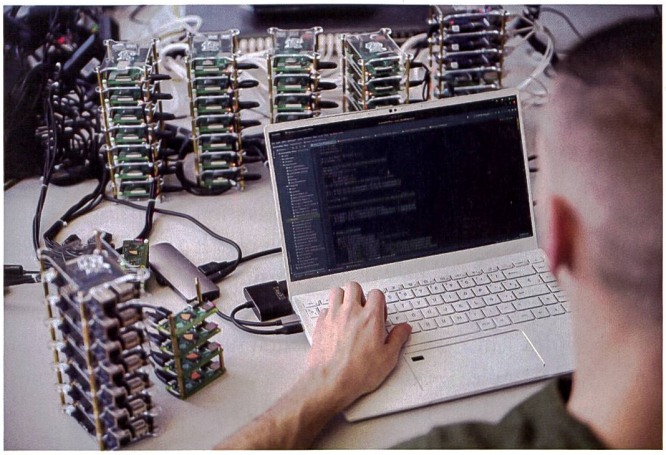

Bild: VBS

Im Jahr 2021 entstand ein jährlicher Schaden von mindestens 203 Milliarden Euro durch Cyberangriffe, Spionage und Sabotage für deutsche Unternehmen.

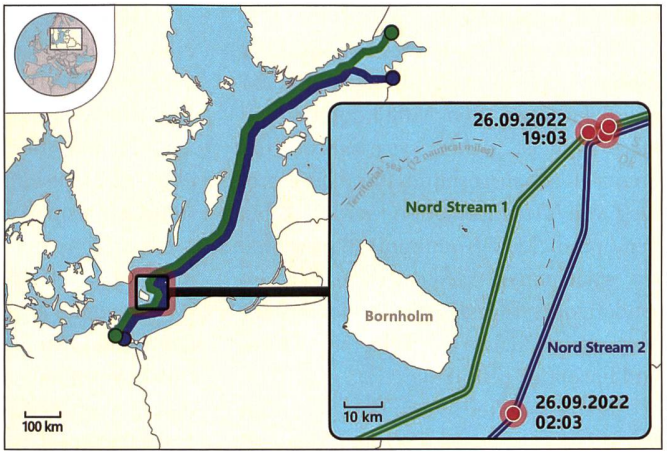

Bild: Factswithoutbias1/wikimedia

Die NATO geht von einem «vorsätzlichen und unverantwortlichen Sabotageakt» bei den Beschädigungen der Pipelines Nord Stream 1 und 2 aus.

Bild: Wikimedia/Rolf Heinrich

Sabotage bei der Deutschen Bahn: Unbekannte hatten wichtige Kommunikationskabel zerstört.

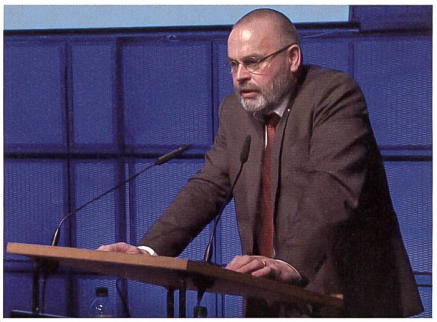

Bild: ZKM

Der Vizepräsident des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI), Gerhard Schabhüser, erklärte im November 2022: «Bedrohungslage im Cyber-Raum ist angespannt, dynamisch und vielfältig und damit so hoch wie nie.»

Bild: Steffen Prössdorf

Die deutsche Bundesinnenministerin Nancy Faeser erklärte in einer Rede im Rahmen eines Symposiums des Bundesamtes für Verfassungsschutz zum Thema «Bedrohung der inneren Sicherheit Deutschlands», «die Bedrohung unserer Sicherheit durch den neuen Krieg in Europa» sei real.

Desinformation wird von nicht-staatlichen Akteuren aus dem In- und Ausland sowie von ausländischen staatlichen Akteuren aus unterschiedlichen Motivationen heraus eingesetzt. Die Absender von Desinformation setzen darauf, die Empfänger zu täuschen und dazu zu verleiten, falsche und irreführende Informationen weiterzuverbreiten.

Wird Desinformation von einem fremden Staat verbreitet, um dadurch illegitim Einfluss auf einen anderen Staat auszuüben, handelt es sich um eine hybride Bedrohung. Beabsichtigt wird die Verunsicherung der Öffentlichkeit, Beeinflussung der öffentlichen Meinungsbildung, Verschleierung und Ablenkung von eigenen Aktivitäten, Emotionalisierung von kontroversen Debatten und Verstärkung gesellschaftlicher Spannungen sowie das Schüren von Misstrauen in staatliche Institutionen und Regierungshandeln.»

Die aktuellen russischen Desinformationskampagnen, die weltweit angelegt sind, stellen kein genuin neues Phänomen dar. Doch seit der völkerrechtswidrigen Annexion der Krim 2014 hat das System Putin die Intensität und Reichweite der Desinformationskampagnen drastisch erhöht.

Dabei wird die «Informationskriegsführung» als ein explizit anerkannter Bereich der russischen Militärdoktrin definiert und ist daher systematisch und finanziell gut ausgestattet. Für die Verbreitung von Desinformation werden neben herkömmlichen Kommunikationsmitteln wie staatsnahen oder -eigenen Fernsehsendern oder Tageszeitungen auch Instant-Messaging-Dienste wie Telegram, Twitter und Facebook genutzt.

Die russischen Desinformationskampagnen in europäischen Staaten sollen seit spätestens dem 24. Februar 2022 – in Bezug auf die Corona-Hygienemassnahmen der Bundesregierung schon seit dem Frühjahr 2020 – mit ihren propagandistischen Narrativen das Misstrauen in etablierte Medien und Politik schüren. Damit soll der Rückhalt der europäischen Russlandpolitik in der Bevölkerung minimiert werden.

Zu Beginn des russischen Angriffskrieges Ende Februar 2022 nahmen die russischen Desinformationskampagnen vor allem die russischsprachige Bevölkerung in Deutschland als Zielgruppe ins Visier.

Dafür wurden neben Telegram, Facebook und Twitter vor allem bei älteren Rezipienten E-Mail-Verteiler verwendet, die extrem schwer bis gar nicht einsehbar sind. Eine weitere Zielgruppe stellt die über die letzten zwei Jahre der Pandemie immer medienkritischer aufgestellte «Querdenker»-Gruppierung in Deutschland dar, die vor allem über Telegram mit diversen russischen Desinformationen adressiert wird und diese weiterverbreitet.

Die deutsche Bundesinnenministerin Nancy Faeser erklärte am 19. Mai 2022 in einer Rede im Rahmen eines Symposiums des Bundesamtes für Verfassungsschutz zum Thema «Bedrohung der Inneren Sicherheit Deutschlands – von Delegitimierung bis Desinformation» «die Bedrohung unserer Sicherheit durch den neuen Krieg in Europa» sei real.

Das gelte «sowohl für Spionageaktivitäten und Cyberangriffe als auch für Einflusskampagnen fremder Mächte, die durch Propaganda, Lügen und gezielte Desinformation unsere Demokratie destabilisieren sollen». Desinformationskampagnen fremder Staaten, um aggressive Interessenpolitik unterhalb der militärischen Schwelle zu betreiben, bezeichnete Innenministerin Faeser als «hybride Bedrohungen», denn «Desinformation als staatliches Instrument» sei «ressourcenstark und so besonders wirkmächtig».

Die Corona-Pandemie und die damit verbundenen Desinformationskampagnen durch Russland und China gegen Deutschland führt Faeser als Beispiel an, verweist aber auf eine «neue Dimension», die seit dem Beginn des russischen Angriffskrieges gegen die Ukraine erreicht worden sei.

Hierbei hätten Putin und seine Regierung von Beginn an versucht, «ihren völkerrechtswidrigen Angriffskrieg durch Unwahrheiten zu rechtfertigen», beispielsweise wurde verbreitet, dass die Ukraine im Donbas einen Genozid verüben würde oder dass die Ukraine geplant hätte, Russland anzugreifen.

Daneben wolle das System Putin das Narrativ einer angeblichen «Russophobie» des Westens verfestigen, um damit die russischsprachige Bevölkerung in Deutschland zu beeinflussen.

Lutz Güllner, Leiter der Strategischen Kommunikation im Europäischen Auswärtigen Dienst (EAD), die sich mit der Aufdeckung und Bekämpfung von ausländischer Desinformation beschäftigt, führt zu aktuellen russischen Desinformationskampagnen und deren Narrative aus, dass es sich um drei grosse Themenblöcke handele.

Innerhalb der NATO befasst sich das NATO Strategic Communications Centre of Excellence mit den Auswirkungen von Informationsoperationen.

Bilder: NATO

Unsere europäischen Demokratien benötigen starke Abwehrkräfte gegen Desinformationskampagnen, Fake News, Propaganda und diese Abwehrkräfte müssen in uns gestärkt werden.

Einerseits Falschinformationen zum Kriegsverlauf, beispielsweise falsche Verlust- oder Erfolgsmeldungen. Zweitens gehe es um die Frage Ursache und Wirkung. Wer ist der Aggressor? Wo kommt die Gefahr her? Hier würden Tatsachen entweder falsch oder verdreht dargestellt. Immer wieder werde die NATO oder «der Westen» als Aggressor genannt, gegen den sich Russland wehren müsse.

Der dritte grosse Bereich beziehe sich schliesslich auf die Ukraine selbst, deren Existenzrecht abgesprochen werde. Die politische Führung der Ukraine werde diskreditiert, eine gemeinsame Historie konstruiert. Russland spricht von Entnazifizierung und einer Friedensmission.

Weiter erläutert Güllner, dass zahlreiche verschiedene Zielgruppen in Deutschland und Europa von den russischen Desinformationskampagnen angesprochen werden und bezeichnet die Instrumente dafür als «Werkzeugkasten».

Erstens die offiziellen Kanäle, Reden und Statements des russischen Präsidenten selbst sowie seiner Minister und seines Kremlsprechers. Zweitens die russischen Staatsmedien.

Drittens die sogenannten Informationsportale, die häufig sehr eng mit russischen Behörden, auch mit den russischen Geheimdiensten verbunden sind. Und viertens gibt es einen klandestinen Bereich in den sozialen Medien, wo teilweise falsche Identitäten im Einsatz sind, deren Reichweite wiederum künstlich verstärkt wird.

Eine Datenauswertung des WDR, des NDR und der Süddeutschen Zeitung zeigte bereits im April 2022, dass Facebook nicht gegen die russischen Desinformationskampagnen in Deutschland ankommt.

Eine Vielzahl von Fake News, beispielsweise über die Massaker und Gräueltaten russischer Soldaten an Ukrainerinnen und Ukrainern von Butscha, verbreiteten sich im April 2022 auf Facebook rasant. Videos mit Fake News russischer Desinformationskampagnen wurden in Deutschland Tausende Male angeschaut.

Die Auswertung einer Stichprobe von Facebook-Seiten durch den WDR, den NDR und die Süddeutsche Zeitung zeigte, «Postings und Seiten, die die Gräueltaten in Zweifel ziehen, verzeichnen hohe Wachstumsraten und Views – ohne gelöscht oder als falsch markiert zu werden».

Die Massaker und Gräueltaten von Butscha wurden in jenen russischen Fake-News-Videos mit «Das inszenierte Blutbad von Butscha» oder «Die Lüge von Butscha» betitelt.

Genannt werden vermeintliche «Beweise» wie, es sei «kein Blut an ukrainischen Autos» gefunden worden, die Körper der zum Teil gefesselten Menschen hätten «keine Leichenstarre» aufgewiesen, oder es seien «gar keine Leichen gefunden worden», behaupten andere.

Das deutsche Bundesinnenministerium zeigte sich Ende August 2022 beunruhigt über gefälschte und täuschend echt aussehende Medien-Websites mit pro-russischen Desinformationen rund um den Ukraine-Krieg.

So teilte ein Sprecher des Bundesministeriums des Innern und für Heimat mit: «Wir haben mit Sorge zur Kenntnis genommen, dass über Fake-Accounts in bestimmten sozialen Medien täuschend echt aussehende, allerdings gefälschte Webauftritte von etablierten Nachrichtenseiten verlinkt werden.

Dort werden demnach erfundene Nachrichten und gefälschte Videos – Teil der russischen Desinformationskampagnen – verbreitet.

«Diese verfolgen das Ziel, Vertrauen in Politik, Gesellschaft und staatliche Institutionen zu untergraben», erklärte der Sprecher des Bundesinnenministeriums. Unter anderem wurden Seiten der grossen und auflagenstärksten Tageszeitung «Bild» und des auflagenstarken Wochenmagazins «Spiegel» nachgebaut.

Fazit

Die Kriegsführung Russlands im neuen Ost-West-Konflikt des 21. Jahrhunderts ist hybrid, gemäss dem russischen Generalstabschef Gerassimow «entgrenzt», sie wendet «alle Mittel» an, wobei der Einsatz von strategischen Atomwaffen eher unwahrscheinlich bleibt.

Im Kampf gegen den Westen, im neuen Ost-West-Konflikt des 21. Jahrhunderts, nutzt das System Putin Cyberattacken und (potenzielle) Angriffe auf KRITIS sowie Desinformationskampagnen gegen europäische Staaten.

Unsere europäischen Demokratien benötigen starke Abwehrkräfte gegen Desinformationskampagnen, Fake News, Propaganda, und diese Abwehrkräfte müssen in uns gestärkt werden.

Dafür benötigen die EU-Staaten schnellstmöglich staatliche Zentren bzw. Beauftragte für die Analyse von Desinformationskampagnen und effektive Counter-Narratives. Verbunden damit muss die Medienkompetenz der Schülerinnen und Schüler an den Schulen, ihre Resilienz gegen Fake News, Propaganda und Desinformationskampagnen professionell und umfassend gestärkt werden.