Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 189 (2023)

Heft: 7

Artikel: Was EU und NATO gegen Cyberattacken und Desinformationskampagnen leisten können

Autor: Goertz, Stefan

DOI: https://doi.org/10.5169/seals-1052758

Was EU und NATO gegen Cyberattacken und Desinformationskampagnen leisten können

Die hybride Kriegsführung Russlands bedroht neben der Ukraine auch Staaten der EU und der NATO. Es zeigt sich, dass die vorhandenen Abwehrmittel im Westen noch nicht ausreichen.

Stefan Goertz

Ein wesentliches Element einer hybriden Kriegsführung ist die Verschleierung. Hybride Kriegsführung ist erfinderisch und koordiniert. Ein entscheidender Kriegsschauplatz von Hybridkriegsführung ist der Cyber- und Informationsraum. Die Kriegsführung Russlands im neuen Ost-West-Konflikt bedroht neben der Ukraine auch zahlreiche Staaten der EU und der NATO, auf verschiedenen Ebenen, mit verschiedenen Akteuren.

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

Cyberattacken gegen westliche Staaten

Im Zusammenhang mit dem russischen Angriffskrieg gegen die Ukraine hat das Cyberpeace-Institut in Genf für das Jahr 2022 mehr als 850 Cyberattacken registriert. Sie wurden demnach von pro-russischen Hackern respektive von russischen Geheimdiensten gegen Ziele in der Ukraine, Russland und rund drei Dutzend anderen Ländern ausgeführt. Prorussische oder von russischen Geheimdiensten gesteuerte Hackernetzwerke würden durch immer stärkere Vernetzung immer unberechenbarer, erklärte das Genfer Institut Anfang 2023.[1]

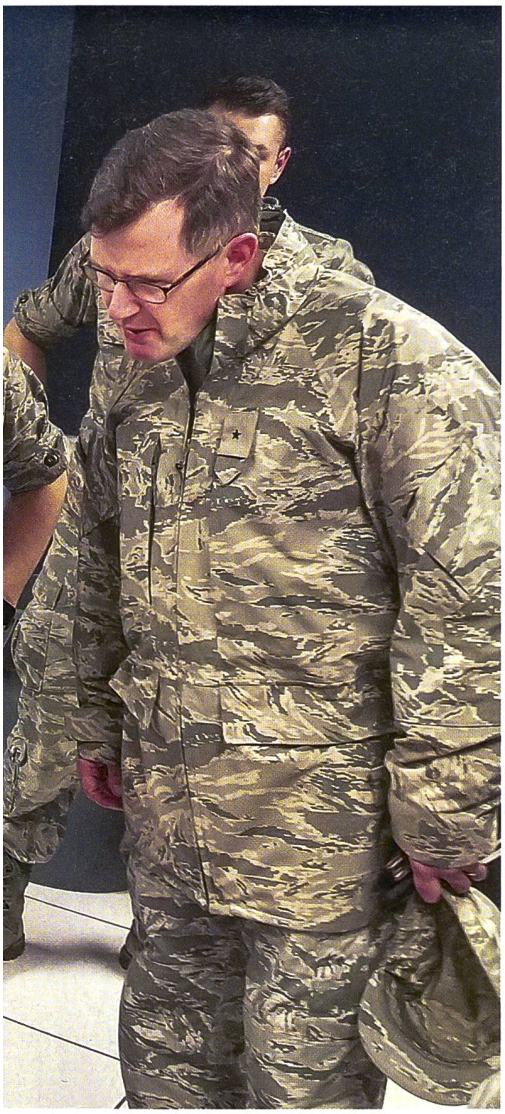
Beispielsweise gab es im September 2022 an zwei Tagen fünf Cyberattacken gegen Deutschland, die Ziele waren dabei etwa Ministerien, Banken, Internetanbieter und Flughäfen. Das Genfer Institut entdeckte im Herbst 2022 neue Trends bei Cyberattacken. So nutzte die prorussische Hackergruppe «Fancy Bear», die von russischen Geheimdiensten gesteuert wird, ein Störprogramm auf Basis von Konni-Malware, die bislang von nordkoreanischen Hackern benutzt wurde. Aktuell ist festzustellen, dass sich von russischen Geheimdiensten gesteuerte Hackernetzwerke immer stärker vernetzen.[2]

Spätestens seit Frühjahr 2022 warnen deutsche Sicherheitsbehörden und diejenigen anderer westlicher Staaten vor russischen Cyberattacken. Dazu gehören im Wesentlichen drei Arten: Einerseits ist das Cyberspionage, also das Eindringen in fremde Rechner und Netzwerke mit dem Ziel, sensible Daten zu stehlen. Daneben gibt es Cyberattacken, die Teil von Desinformationskampagnen sind, beispielsweise wenn Websites oder bekannte Social-Media-Accounts gehackt werden, um darüber Falschinformationen zu verbreiten. Drittens Cybersabotage, Hackerangriffe mit dem Ziel,

► **Ausbildung von US-Soldaten der Air Force im Bereich der Cyberabwehr in West Point.** Bild: Wikimedia

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, wenn die Telekommunikation, die Energie- oder die Wasserversorgung einer ganzen Region lahmgelegt wird.[3]

Der Vizepräsident des deutschen Bundesamtes für Sicherheit in der Informationstechnik, Gerhard Schabhüser, erklärte im November 2022: «Die Bedrohungslage im Cyberraum ist angespannt, dynamisch und vielfältig und damit so hoch wie nie».[4] Eine weltweite Welle von Cyberattacken mit Erpressungssoftware legte zu Beginn des Jahres 2023 auch deutsche Unternehmen und öffentliche Einrichtungen lahm. Nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik lag der geographische Schwerpunkt der Cyberattacken auf Frankreich, den USA, Deutschland und Kanada.[5]



Russische Desinformationskampagnen

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.[6]

Die russischen Desinformationskampagnen gegen westliche Staaten sind spätestens seit dem 24. Februar 2022 im Bereich der strategischen Desinformation anzusiedeln und sollen mit ihren inkohärenten Narrativen das Misstrauen in etablierte Medien und Politik schüren. Damit soll der Rückhalt der westlichen Politik im Ukraine-Krieg in der Bevölkerung minimiert werden. Die deutsche Bundesinnenministerin Nancy Faeser erklärte im Mai 2022, «die Bedrohung unserer Sicherheit durch den neuen Krieg in Europa» sei real. Desinformationskampagnen fremder Staaten, um aggressive Interessenpolitik unterhalb der militärischen Schwelle zu betreiben, bezeichnete sie als «hybride Bedrohungen», denn «Desinformation als staatliches Instrument» sei «ressourcenstark und so besonders wirkmächtig».[7]

Drei Themenblöcke im Ukraine-Krieg

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. 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.[8]

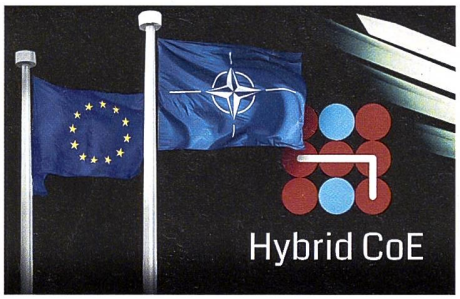
Weiter erläutert Güllner, dass zahlreiche Zielgruppen in Deutschland und Europa von den russischen Desinformationskampagnen angesprochen werden und bezeichnet die Instrumente dafür als «Werkzeugkasten». Erstens sind die offiziellen Kanäle, Reden und Statements des russischen Präsidenten selbst sowie seiner Minister und seines Kremlsprechers zu nennen, zweitens die russischen Staatsmedien und drittens die sogenannten Informationsportale, die häufig sehr eng mit russischen Behörden, auch mit den russischen Geheimdiensten verbunden sind. Viertens gibt es einen klandestinen Bereich in den sozialen Medien, wo teilweise falsche Identitäten im Einsatz sind, deren Reichweiten wiederum künstlich verstärkt werden.[9]

Die Zielgruppen der russischen Desinformationskampagnen sind nach Angaben der EU, die russische Bevölkerung im Inland, dann die Bevölkerung in der Ukraine – die Ukrainer sollen glauben, dass der Westen sie aufgegeben hat – und schliesslich die westlichen Demokratien, vor allem Staaten der Europäischen Union. Zum Erfolgsgrad der Desinformationskampagne erklärt Güllner, dass man in den sozialen Medien zwar sehen könne, wie oft ein Beitrag geteilt wird. Der Erfolg bemesse sich aber auch darin, ein Narrativ so lange zu wiederholen, bis es «kleben» bleibt.[10]

Drei wesentliche Abwehrakteure

Die drei wesentlichen Akteure der EU und der NATO im Bereich der Abwehr von Desinformationskampagnen sind aktuell das NATO Strategic Communications Center in Riga, das European Centre of Excellence for Countering Hybrid Threats in Helsinki sowie die Abteilung Strategische Kommunikation im Europäischem Auswärtigen Dienst. Dazu kommen stark unterschiedlich ausgeprägte Kapazitäten und Fähigkei-

ten der Mitgliedsstaaten der EU und der NATO, wobei auch entscheidend ist, wie stark die dortigen Fähigkeiten im Bereich zivile und militärische Nachrichtendienste respektive Geheimdienste sind.



Die Website des European Centre of Excellence for Countering Hybrid Threats. Bild: PD

Nach Angaben der Autoren Eleonora Heinze und Manuel Steudle stehe «Deutschland russischen Desinformationskampagnen relativ unvorbereitet gegenüber». Eines der Probleme sei, «neben fehlender Ausbildung staatlicher Institutionen, die mangelhafte öffentliche Kommunikation vonseiten der Politik, obwohl Politik und Sicherheitsbehörden nach Expertenmeinung genau wüssten, wer hinter diesen Desinformationskampagnen steckt».[11] Dabei könnte sich die deutsche Politik an Tschechien und Estland orientieren, die sich mit einem Zusammenspiel aus staatlichen und zivilgesellschaftlichen Mitteln in erprobter Weise erfolgreich gegen russische Desinformationskampagnen behaupten. So verfüge beispielsweise Tschechien über eine Spezialeinheit innerhalb des Innenministeriums, die auf das Erkennen und Analysieren von Desinformationskampagnen spezialisiert ist und in kurzer Zeit in Abstimmung mit anderen Ministerien und Nichtregierungsorganisationen Gegenmassnahmen in Stellung bringen kann. Eine ähnliche Spezialeinheit findet sich auch in Estland.

Der Rat der Europäischen Union billigte am 21. März 2022 das Dokument «Ein Strategischer Kompass für Sicherheit und Verteidigung – Für eine europäische Union, die ihre Bürgerinnen und Bürger, Werte und Interessen schützt und zu Weltfrieden und internationaler Sicherheit beiträgt».[12] Dieser «Strategische Kompass» soll ein Aktionsplan für die Stärkung der Sicherheits- und Verteidigungspolitik der Europäischen Union bis zum Jahr 2030 sein.

Dieser Rat stellte knapp einen Monat nach dem Beginn des russischen Angriffskrieges gegen die Ukraine fest, dass das «feindlichere Sicherheitsumfeld» von der EU einen «Quantensprung nach vorn» erfordere und die EU ihre «Handlungsfähigkeit und -bereitschaft erhöhen», ihre «Resilienz stärken sowie mehr und besser» in ihre Verteidigungsfähigkeiten investieren müsse.[13] So solle dieser «Strategische Kompass» als Aktionsplan «die strategische Autonomie der EU und ihre Fähigkeit stärken, mit Partnern zusammenzuarbeiten, um ihre Werte und Interessen zu wahren». «Eine stärkere und fähigere EU im Bereich Sicherheit und Verteidigung» solle «einen konstruktiven Beitrag zur globalen und transatlantischen Sicherheit leisten» und «eine Ergänzung zur NATO» bilden, «die für ihre Mitglieder das Fundament der kollektiven Verteidigung» bleibe.[14]

In Zeiten der zunehmenden Abhängigkeit von digitalen Technologien sei der Cyberraum zum Schauplatz eines strategischen Wettbewerbs geworden, in welchem die EU mit immer ausgefeilteren Cyberangriffen konfrontiert sei. Es gelte daher «unbedingt, einen offenen, freien, stabilen und sicheren Cyberraum aufrechtzuerhalten». Mehr Resilienz und die Abwehr hybrider Bedrohungen, von Cyberangriffen und Desinformationskampagnen sind weitere wichtige Handlungsfelder des Strategischen Kompasses. Gemeinsam wollen die Mitgliedstaaten einen Instrumentenkasten zur Abwehr hybrider Bedrohungen (EU Hybrid Toolbox) entwickeln, um Mitgliedsstaaten und auch Partnerländer schneller und wirksam bei der Abwehr hybrider Bedrohungen unterstützen zu können.[15]

Bisherige Mittel reichen nicht aus

Die vom deutschen Bundeskanzler Scholz postulierte «Zeitenwende» konzentriert sich auf neue Kampfpanzer und Kampfflugzeuge, übersieht aber, dass die russische Hybridkriegsführung einen neuen Ost-West-Konflikt begonnen hat, der ausserhalb der Ukraine, in der EU, sehr stark in den sozialen Medien geführt wird, durch Fake News und Desinformationskampagnen. Diejenigen Telegramgruppen, die bis zum 24. Februar 2022 russische Narrative der Kritik an den Corona-Hygienemassnahmen der westlichen Regierungen transportiert haben, verbreiten nun Narrative und Fake News des Systems Putin. Kurz gesagt: Seit dem Beginn des russischen Angriffskrieges sind Kampfpanzer und Kampfflugzeuge in Europa zwar wieder wichtig geworden, die russische Hybridkriegsführung gegen den Westen wird aber nicht mit Kampfpanzern auf Territorium von EU-Staaten gestoppt werden müssen, sondern mit Kampfpanzern auf ukrainischem Territorium und gleichzeitig mit neuen Akteuren im Kampf gegen russische Desinformationskampagnen im Internet.

Absolut richtig ist daher die vom «Strategischen Kompass» angeregte Aufwertung der nachrichtendienstlichen Auswertung und der Hybrid Fusion Cell im Europäischen Auswärtigen Dienst. Es ist offensichtlich, dass die bisherigen Institutionen und Massnahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU und der einzelnen EU-Mitgliedsstaaten gegen Cyberattacken und Desinformationskampagnen nicht ausreichen. Die EU-Mitgliedstaaten benötigen Zentren zur Analyse und Abwehr von Desinformationskampagnen. Zusätzlich sollten sie umgehend Fähigkeiten anschaffen, um in die Online-Propagandasysteme der Hacker des Systems Putin einzudringen und diese dort zu bekämpfen. ■

Dieser Beitrag stellt die persönliche Auffassung des Autors dar.

1 Vgl. https://www.zdf.de/nachrichten/politik/cyber-angriffe-hacker-deutschland-ukraine-krieg-russland-102.html (5.6.2023).
2 Vgl. ebd.
3 https://www.nzz.ch/technologie/russische-cyberangriffe-wie-gross-ist-die-gefahr-von-schweren-hackerattacken-fuer-den-westen-ld.1678530 (5.6.2023).
4 Behörden Spiegel: Gefahr so hoch wie nie. BSI-Lagebericht 2022. In: Behörden Spiegel November 2022, S. 35.
5 Vgl. https://www.tagesschau.de/inland/gesellschaft/cyberattacke-deutschland-101.html (5.6.2023).
6 Vgl. Goertz, S. (2022): Der Krieg in der Ukraine und die Folgen für Deutschland und Europa, S. 173.
7 Vgl. https://www.bmi.bund.de/SharedDocs/reden/DE/2022/faeser-19052022-bfv-symposium.html (5.6.2023).
8 Vgl. https://www.bundesregierung.de/breg-de/themen/umgang-mit-desinformation/desinformation-interview-ead-2010706 (5.6.2023).
9 Vgl. ebd.
10 Vgl. ebd.; Goertz, S. (2022): Der Krieg in der Ukraine und die Folgen für Deutschland und Europa, S. 177–178.
11 Vgl. www.hss.de/news/detail/russlands-einsatz-von-desinformationen-news8625 (5.6.2023).
12 https://www.consilium.europa.eu/de/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/ (5.6.2023).
13 Vgl. ebd.
14 Vgl. ebd.
15 Vgl. ebd.

Oberstlt d.R. Stefan Goertz
Prof. Dr.
Hochschule des Bundes
Fachbereich Bundespolizei
D-23562 Lübeck