GLOBAL NETWORK & INTELLIGENCE

CII DEEP-DIVE

Hybride Bedrohungen Teil 1/3

Angriffsarten im Überblick

Dr. Christopher Nehring

CYBER|INTELLIGENCE
.Institute

Vorwort

Diese dreiteilige CII-Deep-Dive-Reihe bietet einen Überblick über aktuelle hybride Angriffsszenarien und -hintergründe. Der erste Teil widmet sich den „Hybriden Bedrohungen“, der zweite Teil dem aktuellen Stand der „Drohnenabwehr“, während sich der dritte Teil den angreifenden Akteuren mit einem Fokus auf Russland widmet.

Mit dieser Reihe möchte das CII zum besseren Verständnis der allgemeinen Ausgangslage aktueller hybrider Bedrohungen beitragen. Der Anspruch liegt nicht auf Vollständigkeit oder der Darstellung umfangreicher Quellennachweise, sondern der Orientierung und Förderung des Risikoverständnisses für Entscheider in Organisationen, um sich dieser Gefahrenlage und möglicher Handlungserfordernisse bewusst zu werden und in einen Dialog zu kommen.

Ich wünsche eine aufschlussreiche Lektüre.

Dr. Christopher Nehring
CII-Intelligence Director

Über den Autor

Dr. Christopher Nehring, Intelligence Director des cyberintelligence.institute in Frankfurt am Main. Er ist Forscher, Analyst und Experte für verschiedene Medien in Deutschland und Europa. Sein Themengebiet umfasst die Arbeit von Geheimdiensten, Desinformation, Hybride Kriegsführung und KI-Cyberrisken (insbesondere Deepfakes und Manipulationen). Er war Gastdozent und Experte für Desinformation des Medienprogramms der Konrad-Adenauer-Stiftung, wissenschaftlicher Leiter des Spionagemuseums Berlin sowie Senior Analyst des Institute for Global Analysis. Dr. Nehring ist regelmäßiger Gastautor und Experte für zahlreiche Medien (z.B. ARD, Tagesspiegel, Spiegel, NZZ, Welt etc.), als Speaker, Trainer, Kursleiter und Berater ist er für verschiedene Unternehmen, IHKs, Stiftungen und Medienorganisationen tätig.

Kontakt: christopher.nehring@cyberintelligence.institute

Hybride Bedrohungen. Teil 1: Angriffsarten im Überblick

Das Wichtigste in Kürze:

- Hybride Angriffe gegen KRITIS-Einrichtungen und Mittelstand nehmen rapide zu: rund ein Angriff pro Tag im Durchschnitt der letzten drei Jahren.
- Dieses Papier identifiziert zwölf verschiedene Angriffsvektoren hybrider Angriffe.
- Deutsche KRITIS-Einrichtungen müssen gegen die Vielzahl dieser Angriffe und ihre Wirkungen physische und mentale Resilienz aufbauen.
- Das neue KRITIS-Dachgesetz verpflichtet alle betroffenen Einrichtungen zu konkreten Maßnahmen („Resilienzpflichten“).
- Menschliche Resilienz durch Vorbereitung, Frühwarnsysteme, Sensibilisierung und Schulungen ist essentiell.

Konkreter Mehrwert für KRITIS-Betreiber, CSOs, CISOs, Sicherheitsmitarbeiter und Dienstleister:

Dieses Deep-Dive-Paper …

- … bietet eine praxisnahe Ergänzung und übersetzt abstrakte Resilienzvorgaben in konkrete Beobachtungen und Bedrohungsszenarien.
- …identifiziert typische Vorgehensweisen hybrider Angriffe und dient dadurch der Früherkennung und Musterschärfung in Risikoanalysen.
- …dient dem Taktikverständnis hinsichtlich feindlicher Akteure.
- …kann die Planung von Schutzmaßnahmen gemäß KRITIS-DachG (insb. § 13 KRITIS-DachG) erleichtern und ergänzen.
- …trägt zur Förderung psychologischer Resilienz und Awareness bei.
- …bietet Impulse für branchenspezifische Resilienzstandards (nach § 14 Abs. 2 KRITIS-DachG).
- …kann die Reaktionsfähigkeit bei Vorfällen erhöhen (§ 18 KRITIS-DachG).
- …trägt durch seine Verbreitung zur Stärkung der Gesamtresilienz bei.

Inhalt

Was sind hybride Angriffe?

Hybride Bedrohungen oder hybride Kriegsführung umfassen vielfältige Angriffsformen, die staatliche und nichtstaatliche Akteure einsetzen, um Gesellschaften, Staaten oder Unternehmen zu destabilisieren, ihre Sicherheitssysteme zu unterlaufen, wirtschaftlichen Schaden anzurichten, Gesellschaften zu polarisieren und politischen Einfluss zu nehmen.[1] Dabei werden konventionelle und unkonventionelle Methoden kombiniert, um größtmöglichen Schaden anzurichten und Unsicherheit zu erzeugen. Grundsätzlich umfassen hybride Bedrohungen:

(1) physische (oder „kinetische“) Angriffe wie Sabotagen oder Personenanschläge,

(2) Cyberangriffe wie Ransomware oder „DDoS“-Angriffe,

(3) klassische Spionage und

(4) Informationsangriffe wie Desinformation.[2]

Die Besonderheit hybrider Bedrohungen liegt in ihrer Kombination aus mehreren Angriffsvektoren, die gleichzeitig oder aufeinander abgestimmt zum Einsatz kommen. Diese Verbindung von physischen, digitalen, geheimdienstlichen und psychologischen Methoden erschwert die klare Zuordnung zu einem Urheber und Aggressor. Zu dieser Art der Verschleierung gehört auch, dass oft Stellvertreter (z.B. eigentlich staatsferne, private Hackergruppen oder Kriminelle) oder getarnte Militär- und Spionageeinheiten zur Ausführung benutzt werden. Dadurch werden auch angemessene Reaktionen (z.B. Zuweisung, rechtliche Verfolgung, Sanktionen, Ächtung, Abschreckung, Gegenschläge) erheblich behindert.

Hybridität bedeutet, dass es um – teils gewalttätige – Aktionen geht, die unterhalb der Schwelle einer offenen Aggression und Konfrontation liegen. Dabei werden offene und verdeckte, reguläre und irreguläre, symmetrische und asymmetrische, militärischen und nicht-militärischen Aktionen und Mittel flexibel miteinander gemischt.[3]

Die Grenzen zwischen Frieden und Krieg, zwischen ziviler und militärischer Auseinandersetzung verschwimmen somit. Die psychologische Wirkung solcher Aktionen – Angst, Unsicherheit, Blockaden, Chaos, Spannungen und Polarisierung – ist ein wesentliches Element und ein intendiertes strategisches Ziel.

1 Siehe einführend: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

2 Siehe z.B.: https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefaehrdung-russische-spionage-sabotage-desinformation.html#doc2129880bodyText3.

3 Siehe z.B.: https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen.

Vorgehen, Angriffsvektoren und Beispiele

Seit 2022 sind in Deutschland zahlreiche Aktionen und Vorfälle hybrider Angriffe zu beobachten. Insgesamt kann eine Vielzahl verschiedener Angriffsarten identifiziert werden, die aktuell in Deutschland (und insb. für KRITIS-Einrichtungen) eine Bedrohung darstellen. Diese werden im Folgenden anhand von Fallbeispiele erläutert:

1. Drohnen und unbemannte Fahrzeuge

Drohnen (Flugdrohnen ebenso wie Unterwasserdrohnen) werden zu gezielten Aufklärungs- und Überwachungsoperationen, aber auch bei Sabotageakten eingesetzt. Ähnlich wurde auch die Nutzung von mit Spionageausrüstung ausgestatten Tieren (z.B. Wale oder Delfine im Meer) dokumentiert.

> **Drohnenüberflüge über Deutschland haben seit dem russischen Angriff auf die Ukraine stark zugenommen.**

Drohnenüberflüge über Deutschland haben seit dem russischen Angriff auf die Ukraine stark zugenommen. Ihre genaue Zahl ist unbekannt, übersteigt jedoch 500. Über Bundeswehrstandorten, den am stärksten betroffenen kritischen Einrichtungen, wurden allein im Jahr 2023 446 (2022: 172; 2021: 9) Drohnenüberflüge gemeldet.[4] Dazu kommen zahlreiche Überflüge über zivile kritische Infrastruktur, wovon Energieunternehmen, Bahn und Rüstungsunternehmen besonders betroffen sind.[5] Die Art der dabei eingesetzten Drohnen variiert stark – von großen, vermutlich von Schiffen aus Nord- und Ostsee gesteuerten Militärdrohnen mit großer Spannweite und Geschwindigkeit bis zu kleineren „Jedermannsdrohnen“ (z.B. Quadrocopter), die von Personen am Boden gesteuert werden.[6] Sowohl die Attributierung (also das Erkennen des Urhebers) als auch das Ermitteln der konkreten Absichten hinter einem Drohnenüberflug sind schwierig und bislang wenig fortgeschritten.

Bei großen Militärdrohnen ist der Kreis potenzieller Täter wesentlich kleiner, eine feste Zuweisung jedoch ohne weitergehende Informationen (z.B. audiovisuelle Aufnahmen, Rückverfolgung, Peilung etc.) schwierig. Russland zählt dabei oft zu den aktivsten Akteuren (vor allem bei großen Militärdrohnen). Bislang ist nur ein Abschuss einer solchen Drohne über einem Bundeswehrstützpunkt in Sachsen-Anhalt bekannt.[7]

Bei den Motiven und Zielen hinter den Drohnenflügen gibt es ebenfalls wenig Klarheit. Viele dienen offenbar der militärischen Aufklärung und Spionage, andere (gerade gegen zivile KRITIS-Einrichtungen) wohl auch der Aufklärung potenzieller Angriffsziele. Gleichzeitig spricht besonders die hohe Anzahl der Überflüge auch für ein ständiges Austesten von Reaktionen und Abläufen seitens Behörden, Armee und betroffener Einrichtungen. Darüber hinaus steht – typisch für hybride Angriffe – die psychologische Wirkung im Fokus: Gerade die Unklarheit hinsichtlich des Urhebers und seiner Intentionen verunsichert Entscheidungsträger, KRITIS-Einrichtungen und die Gesellschaft. Dass auch nach fast drei Jahren und einer stetig steigenden Anzahl an Vorfällen keine wirkliche Antwort bzw. wirksame Gegenmaßnahmen erfolgen, trägt weiter zur Verunsicherung und dem vom Angreifer intendierten psychologischen Schaden bei.

Ausführliche Darstellung zur Drohnenabwehr im zweiten Teil der CII-Deep-Dive-Reihe „Hybride Bedrohungen“

4 Siehe: https://www.tagesschau.de/investigativ/ndr-wdr/zunahme-drohnensichtungen-100.html.

5 Siehe z.B.: https://www.tagesschau.de/investigativ/ndr-wdr/drohnen-ueberfluege-100.html.

6 Siehe auch: Frank Christian Sprengel: Drones in hybrid warfare: Lessons from current battlefields, hg.: Hybrid CoE, 2021 (https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-10-drones-in-hybrid-warfare-lessons-from-current-battlefields/).

7 Siehe: https://www.tagesschau.de/investigativ/ndr-wdr/zunahme-drohnensichtungen-100.html.

Unterwasserdrohnen

Bei Unterwasserdrohnen ebenso wie bei zur Unterwasseraufklärung eingesetzten Tieren (z.B. Delfine oder kleinere Walarten) sind die Dunkelziffer und das gesicherte Wissen noch geringer. Vor der norwegischen und schwedischen Küste soll es z.B. zu mehreren dokumentierten Fällen von mit Spionageausrüstung ausgestatteten Belugawalen gekommen sein.[8] Auch hier blieben

Abgestürzte russische „Orlan 10"-Aufklärungsdrohne in der Ukraine; Quelle: Ukrainischer Geheimdienst SBU.

der genaue Zweck sowie die Urheber unbekannt. Unterwasserdrohnen kommen sowohl durch die Ukraine als auch durch Russland für Kamikaze-Bombenangriffe und Spionage im Schwarzen Meer zum Einsatz.[9] Ihr Einsatz in Nord- und Ostsee ist bislang schlecht dokumentiert, jedoch förderten Untersuchungen über 400 Fahrten (davon 60 in deutschen Gewässern) auffälliger russischer Spionageschiffe zutage, die Ausrüstung zum Aussetzen und Aufsammeln von Unterwasserdrohnen beherbergten.[10] Vermutet wird hierbei, dass solche Unterwasserdrohnen zur Sabotage an maritimer KRITIS (z.B. Unterwasserkabel und -leitungen) benutzt werden. Das chinesische Militär verfügt hierzu über sabotagefähige Unterwasserdrohnen, die in bis zu 4.000 Metern Tiefe operieren können.[11]

2. Sabotage gegen Datenkabel und maritime KRITIS

Sabotageangriffe auf Unterseekabel und -leitungen der kritischen Infrastruktur (insb. Daten- und Internetkabel) zählen mit Drohnenüberflügen zu den häufigsten Arten hybrider Angriffe der letzten Jahre.[12] Auch hier ist die genaue Anzahl der Vorfälle in Nord- und Ostsee unklar. Durchgeführt werden diese Angriffe oft durch Ankerschleifen vorgeblich ziviler Schiffe und mutmaßlich auch durch sabotagefähige Unterwasserdrohnen. Sowohl die sog. russische Schattenflotte, die Embargo und Sanktionen unterläuft, als auch chinesische Schiffe werden solcher Angriffe verdächtigt.[13] Im November 2024 wurde z.B. das chinesische Schiff „Yi Peng 3" in der Ostsee festgesetzt und durchsucht. Das Schiff war zuvor rund 180 Kilometer mit abgeschaltetem Ortungssystem AIS und gelassenem Anker im Umkreis von zwei beschädigten Kabelverbindungen (C-Lion 1 zwischen Finnland und Deutschland sowie East-West Interlink zwischen Litauen und der schwedischen Insel Gotland) gefahren.[14]

3. GPS- und ILS-Spoofing

„Spoofing" meint das gezielte Stören und Verfälschen, in diesem Fall von GPS-Daten, die der Standortbestimmung dienen. Konkret kommt es im Nord- und Ostseeraum zu einer starken Zunahme solcher Signalstörungen seit 2022.[15] Dies betrifft sowohl den Luftverkehr als auch die Schifffahrt in den jeweiligen Regionen. Störungen dieser Art können sowohl von Schiffen als auch von Flugzeugen oder von Sendern am Boden ausgestrahlt werden. Besonders gefährlich sind solche Angriffe, weil sie nicht nur GPS-Signale zum Ausfall bringen, sondern diese teilweise manipulieren und falsche GPS-Daten anzeigen lassen. GPS-Spoofing ist somit ein konkreter

8 Siehe: https://www.rnd.de/panorama/wal-unter-spionageverdacht-beluga-taucht-vor-schweden-auf-PVKJE6DQWVJXHLN3ZA6ALWLZSA.html.

9 Siehe z.B.: http://www.hisutton.com/Russia-Ukraine-USVs-2024.html.

10 Siehe: https://www.tagesschau.de/investigativ/ndr-wdr/russland-ostsee-spionage-100.html.

11 Siehe: https://geopoliticsunplugged.substack.com/p/chinas-deep-sea-cable-cutter-a-new?utm_campaign=post&utm_medium=web.

12 Siehe z.B.: https://internationalepolitik.de/de/unterseekabel-kritisch-ungeschuetzt; und: https://www.kas.de/de/analysen-und-argumente/detail/-/content/unterseekabel-als-kritische-infrastruktur-und-geopolitisches-machtinstrument; auch: Christian Schaller: Spionage und Sabotage vor Europas Küsten – Kritische Infrastruktur im Fadenkreuz. Völkerrechtliche Spielräume für Abwehrmaßnahmen (SWP-Studie 2024/S 08), 28.02.2024 (https://www.swp-berlin.org/publikation/spionage-und-sabotage-vor-europas-kuesten-kritische-infrastruktur-im-fadenkreuz).

13 Siehe: ebd.; auch: https://www.deutschlandfunk.de/unterseekabel-sabotage-schattenflotte-russland-estlink-2-ostsee-finnland-100.html.

14 Siehe z.B.: https://carnegieendowment.org/emissary/2024/12/baltic-sea-internet-cable-cut-europe-nato-security?lang=en.

15 Siehe z.B.: https://www.deutschlandfunk.de/unterseekabel-sabotage-schattenflotte-russland-estlink-2-ostsee-finnland-100.html.

Angriff und eine Gefahr für Versorgungs- und Handelslinien sowie für militärische und zivile Verkehrsinfrastruktur. Im Frühjahr 2025 kam es z.B. zu einem gezielten GPS-Störangriff auf den Hamburger Hafen.[16]

Ein ähnliches Angriffsmuster ist das gezielte Stören des Funks zwischen Piloten und Bodenpersonal an Flughäfen (Instrumentenlandesystem ILS). Solche Störungen können dazu führen, dass Piloten und Tower einander nicht mehr hören können und so Abläufe gestört und verwirrt werden. Russische Geheimdienste, so legen Untersuchungen nahe, arbeiten bereits seit Jahren an solchen Angriffen, um Routinen und Abläufe zu stören und vor allem psychologisch auf kritische Infrastruktur einzuwirken.[17]

4. Spionage

Klassische Spionage zählt ebenfalls zum Instrumentarium hybrider Angriffe. Zwar ist Spionage eine dauerhafte Erscheinung, wird jedoch zunehmend von Russland nicht nur für politische und militärische Aufklärung, sondern auch für hybride Angriffe eingesetzt. Spionage kann und soll dabei psychologisch wirken und verunsichern sowie Verwundbarkeit signalisieren.

> **Spionage findet dabei mit verschiedenen Methoden statt – durch Cyberspionage, Drohnen und Spionageschiffe in Ost- und Nordsee, …**

Spionage findet dabei mit verschiedenen Methoden statt – durch Cyberspionage, Drohnen und Spionageschiffe in Ost- und Nordsee,[18] aber auch durch angeworbene Spione oder das Abhören von Kommunikation.

Bei der Spionage mit Menschen zeichnet sich ein neuer Trend ab: Statt gut getarnter, geheim gehaltener und vorsichtiger professioneller Rekrutierung von Agenten zur Informationsbeschaffung setzen russische Geheimdienste in der jüngeren Vergangenheit auf unprofessionelle „Hobby-“, „Einmal-“ oder „Wegwerf-Agenten“.[19]

Zur Arbeit russischer Geheimdienste mit menschlichen Agenten siehe den dritten Teil der CII-Deep-Dive-Reihe „Hybride Bedrohungen“

Diese kennen ihre anleitenden Geheimdienstkontakte oft nicht persönlich, werden über Messengerdienste (insb. Telegram) für Aufgaben gegen Bezahlung rekrutiert und erhalten keine professionelle Ausbildung. Beispiele dafür waren z.B. die Agenten, die kurz vor der Bundestagswahl Hunderte Pkw mit Bauschaum attackierten.[20] Diese Art von „Wegwerf-Agenten“ gilt in der Geheimdienstwelt als brachiale, kurzfristige Methode und kommt seit Kriegsbeginn z.B. in der Ukraine sehr oft zum Einsatz.

Der Einsatz dieser Methode durch russische Geheimdienste in Deutschland und Europa stieg infolge der umfänglichen Ausweisung russischer Diplomaten und damit der an Botschaften untergebrachten Geheimdienstoffiziere sowie der Einschränkung der Bewegungs- und Reisemöglichkeiten für russische Diplomaten und Geheimdienstler seit 2022 an. Dabei hat auch der Einsatz von „Wegwerf-Agenten“ eine spezielle psychologische Komponente: Sie senden Signale und Botschaften von Ruchlosigkeit, Brutalität und Enthemmung aus. Andererseits sind solche Agenten gerade im kriminellen Milieu verhältnismäßig leicht zu gewinnen und auch für Sabotageaktionen zu mobilisieren. Gerade wenn es sich dabei um Einmalaktionen handelt, sind diese, ähnlich wie terroristische Angriffe, nur schwer zu erkennen und abzuwehren.

Das gezielte Unterwandern von Behörden und KRITIS-Einrichtungen (ebenso wie „Wegwerf-Agenten“) hat also nicht nur den Zweck der Informationsbeschaffung, sondern auch der psychologischen Einwirkung. Dies gilt ebenso für andere Formen der Spionage gegen KRITIS-Einrichtungen. Drohnenüberflüge, Spionageschiffe oder

16 Siehe: https://www.tagesschau.de/inland/gesellschaft/bedrohung-haefen-versorgungslage-100.html.

17 Siehe: https://www.tagesschau.de/investigativ/ndr-wdr/russland-sabotage-106.html.

18 Siehe z.B.: https://www.ndr.de/nachrichten/mecklenburg-vorpommern/Spionage-und-Sabotage-Voller-Schutz-kritischer-Infrastruktur-illusorisch,ostseemarkritis100.html; auch: Christian Schaller: Spionage und Sabotage vor Europas Küsten – Kritische Infrastruktur im Fadenkreuz. Völkerrechtliche Spielräume für Abwehrmaßnahmen (SWP-Studie 2024/S 08), 28.02.2024 (https://www.swp-berlin.org/publikation/spionage-und-sabotage-vor-europas-kuesten-kritische-infrastruktur-im-fadenkreuz).

19 Siehe z.B.: https://www.zeit.de/2024/41/russische-sabotage-wegwerf-agenten-geheimdienst-sicherheitsbehoerde; oder: https://www.spiegel.de/ausland/russland-wie-das-land-wegwerf-agenten-fuer-propagandazwecke-einsetzt-a-8ba38bab-701c-4c10-9ad0-84518e40e3be.

20 Siehe z.B.: https://www.swr.de/swraktuell/baden-wuerttemberg/ulm/sabotage-autos-bauschaum-verdaechtige-100.html.

Cyberspionage sollen eben nicht nur Informationen beschaffen, sondern auch Abwehrmechanismen, Abläufe und Antworten der Ziele austesten und dabei immer die Botschaft der Verwundbarkeit aussenden.

5. Personenanschläge

Morde und sonstige Anschlagspläne gehören seit jeher ins Repertoire geheimdienstlicher Einflussnahme. Bereits vor dem Angriff auf die Ukraine kam es zu mindestens 20 Fällen im In- und Ausland, bei denen russische Geheimdienste als Urheber vermutet werden;[21] diese Zahl stieg seit Februar 2022 um ein Vielfaches. Auch mehrere Fälle in Deutschland, etwa Vergiftungen von russischen Exilanten und Oppositionellen, stehen hier im Verdacht. Im Sommer 2024 schlugen Meldungen über angeblich aufgedeckte Mordpläne gegen Rheinmetall-CEO Armin Pappenberger hohe Wellen.[22]

Bei geheimdienstlichen Mordanschlägen geht es neben der gezielten Tötung von Menschen auch darum, auf diesem Wege psychologische Botschaften und Signale zu senden. Insbesondere die russischen Geheimdienste hinterlassen so z.B. immer wieder auffällige Spuren und Hinweise, die Angst verbreiten, Nachahmer abschrecken und ein Zeichen der Stärke senden sollen.[23]

6. Sabotage

Neben Anschlägen auf Personen gehören Anschläge auf Objekte, Gebäude, Fahrzeuge etc. zu den sog. kinetischen (oder physischen) hybriden Aktionen. Insbesondere Brand- und Bombenanschläge, wie Paketbomben, die mutmaßlich angeheuerte „Wegwerf-Agenten“ im Auftrag des russischen Militärgeheimdienstes GRU aus dem Baltikum nach Deutschland, England und Polen schickten, kommen dabei zum Einsatz.[24] Ähnliche Pläne verfolgte die vom ehemaligen Wirecard-Vorstand Jan Marsalek angeleitete Agenten-Gruppe, die einen Militärstützpunkt in Deutschland mit einer selbstgebauten Bombe angreifen wollte.[25] Im April 2024 sowie im Mai 2025 wurden mehrere Personen festgenommen, die Militäreinrichtungen, Bahnstrecken und andere Infrastruktur ausgespäht sowie Testpakete verschickt hatten, um Sprengstoffanschläge vorzubereiten.[26] In Marine-Werften wiederum kam es offenbar zu Sabotageakten an der Fregatte „Hessen“ und der Korvette „Emden“, wobei zum einen die Trinkwasseranlage mit Altöl vergiftet werden sollte und zum anderen kiloweise Metallspäne in den Antrieb geschüttet wurden.[27]

Vor der Bundestagswahl 2025 kam es gleichfalls zu mehreren Hundert Sabotageangriffen gegen private Pkw, wobei offenbar eine Gruppe von Kleinkriminellen, die über den Messengerdienst Telegram rekrutiert wurden, Bauschaum in Auspuffe sprühte und Aufkleber mit Wahlwerbung der Grünen anbrachte.[28] Diese Fälle demonstrieren die große Bandbreite an Sabotageakten sowie das unterschiedliche Ausmaß an Professionalität und Komplexität. Insbesondere Sabotageakte mit vergleichsweise einfachen Mitteln (z.B. Bauschaum oder Metallspäne) verdeutlichen ein neues Level der Eskalation sowie gleichfalls die intendierte psychologische Dimension solcher Anschläge (v.a. Angst).

7. Cyberangriffe

Cyberattacken sind ein häufiges Mittel hybrider Angriffe, die aus der Ferne ausgeführt, schwer konkreten Urhebern zugeordnet („attributiert“) werden können und deren im Ausland sitzenden Tätern oftmals unmöglich beizukommen ist. Gerade hier ist die Dunkelziffer hoch, da Opfer häufig gar nicht oder erst mit größerer Verzögerung realisieren, dass sie angegriffen wurden.

Angreifer benutzen eine Vielzahl unterschiedlicher Angriffsarten:

- Computer Network Exploitation (CNE)-Operationen, also das Eindringen in fremde IT-Systeme, werden zur Gewinnung sensibler Daten und Informationen (Spionage) eingesetzt. Solche CNE-Operationen können

21 Siehe ausführlich: Christopher Nehring: Geheimdienstmorde: Wenn Staaten töten – Hintergründe, Motive, Methoden, München 2022.

22 Siehe: https://www.tagesschau.de/inland/rheinmetall-anschlagsplan-papperger-100.html.

23 Siehe: Christopher Nehring: Geheimdienstmorde, S. 195–201.

24 Siehe: https://www.tagesschau.de/investigativ/ndr-wdr/russland-sabotage-106.html.

25 Siehe: https://www.sueddeutsche.de/politik/jan-marsalek-agenten-us-kaserne-deutschland-li.3192861.

26 Siehe: https://www.tagesschau.de/investigativ/russland-sabotage-100.html.

27 Siehe: https://www.tagesschau.de/investigativ/marine-kriegsschiff-sabotageverdacht-100.html; und: https://www.tagesschau.de/investigativ/ndr-wdr/sabotage-marine-ostsee-100.html.

28 Siehe: https://www.swr.de/swraktuell/baden-wuerttemberg/ulm/sabotage-autos-bauschaum-verdaechtige-100.html.

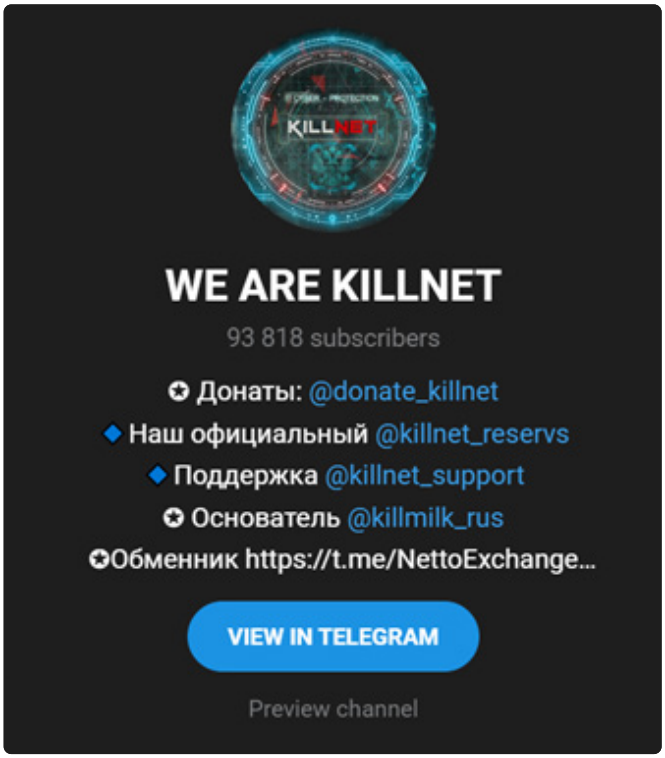
auch die Basis bilden für verschiedene Cyber-Sabotage-Angriffe, bei denen Angreifer nicht nur in Systeme eindringen, sondern auch die Kontrolle über Systeme und Prozesse übernehmen.

- Industrial Control Systems (ICS)-, Operational Technology (OT)- oder Cyber-Physical System (CPS)-Attacken sind für KRITIS-Einrichtungen die wohl größte Gefahr. In den USA z.B. geschah solch ein Angriff auf Kontrollsysteme von Kraftwerken durch die Russland zugeschriebene Gruppe Seashell Blizzard im Frühjahr 2024.[29] China wiederum soll in direkten Gesprächen mit der US-Regierung im Frühjahr 2025 zugegeben haben, wiederkehrende Cyberangriffe (Volt Typhoon) auf kritische Infrastruktur (Kraftwerke, Wasserversorgung etc.) als Vergeltung für US-amerikanische Unterstützung für Taiwan durchgeführt zu haben.[30]

Einer der wohl folgenreichsten Cyberangriffe auf kritische Infrastruktur war die NotPetya-Ransomware-Attacke von 2017. Dieser Angriff, der der Sandworm-Hackgruppe des russischen Militärgeheimdienstes GRU zugeschrieben wird, griff gezielt und flächendeckend kritische Infrastruktur (Kraftwerke, Bahn, staatliche Einrichtungen) in der Ukraine an, von wo aus er auch auf zahlreiche westliche Unternehmen wie Reedereien und Logistikunternehmen übergriff und Hunderte Millionen Euro an Schaden verursachte, da er nicht nur Daten verschlüsselte, sondern auch löschte.[31]

Tatsächlich ist diese Art der Angriffe eher selten (und aufwendig), oftmals führen jedoch CNE-Spionage-Operationen dazu, dass viele Systeme und Prozesse sicherheitshalber präventiv gestoppt werden.

Darüber hinaus gibt es auch niedrigschwellige Cyber-Sabotage-Angriffe, die weitaus häufiger zum Einsatz kommen. Dazu gehören vor allem Überlastungsangriffe (Distributed Denial of Service, DDoS) auf IT-Systeme, wobei Websites oder Services in kurzer Zeit mit einer riesigen Menge an Anfragen überlastet und damit ausgeschaltet werden. Solche Angriffe sind in den vergangenen Jahren zu einem festen Bestandteil vor allem russischer hybrider Kriegsführung geworden. In der Ukraine wurden sie z.B. 2025 gegen das Ticketsystem und andere Services der staatlichen Bahn eingesetzt,[32] in Deutschland hingegen kam es 2024 zu solchen Angriffen gegen verschiedene Flughäfen[33] und Krankenhäuser[34]. Im Frühjahr 2025 griffen russische Gruppen mit solchen Attacken die Seiten zahlreicher Kommunal- und Stadtverwaltungen in Deutschland flächendeckend an, angeblich als Warnung und Vergeltung, weil die Bundesregierung neue Militärlieferungen an die Ukraine erwog.[35] Solche DDoS-Angriffe wurden von verschiedenen russischen Hackergruppierungen in den vergangenen Jahren als „Vergeltung“ für westliche Unterstützung und Militärhilfe für die Ukraine gefahren.



Screenshot des Telegram-Kanals der russischen „Killnet“-Hacker.

Hier taten sich insb. die Gruppen Killnet und Noname hervor, die sich teils über Telegram-Kanäle zu gezielten Angriffen verabreden.[36]

29 Siehe: https://www.csoonline.com/article/3823955/russian-hacking-group-targets-critical-infrastructure-in-the-us-the-uk-and-canada.html.
30 Siehe: https://www.telegraph.co.uk/us/politics/2025/04/11/china-admits-cyber-attacks-us-infrastructure-secret-meeting/.
31 Siehe z.B.: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
32 Siehe: https://industrialcyber.co/transport/ukrzaliznytsia-detects-russian-trace-in-recent-cyberattack-as-90-of-passenger-services-restored/.
33 Siehe: https://www.tagesspiegel.de/politik/hacker-angriffe-websites-von-flughafen-und-behorden-lahmgelegt-9247941.html.
34 Siehe: https://www.bitdefender.com/de-de/blog/hotforsecurity/killnet-hacker-greifen-europaische-krankenhauser-an.
35 Siehe z.B.: https://www.golem.de/news/wegen-taurus-prorussische-hacker-attackieren-deutschland-2504-195622.amp.html.
36 Siehe zu Killnet: https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/; https://www.theregister.com/2023/11/27/lea-

Screenshots gezielter Falschnachrichten auf Facebook über Werksschließungen in Deutschland, Bildquelle: Correctiv.

Eine dritte Art der Cyber-Sabotage sind auch sog. Ransom-Angriffe, bei denen Angreifer in ein IT-System eindringen und es handlungsunfähig machen oder sensible Daten verschlüsseln und Lösegeldforderungen stellen (Ransomware). Solche Angriffe sind nicht nur darauf gerichtet, Lösegeld zu erzielen, sondern legen in der Zwischenzeit eben auch Systeme und Prozesse lahm, weswegen sie im hybriden Krieg einen doppelten Nutzen haben. Gerade seit Beginn des russischen Krieges gegen die Ukraine haben sich einige bekannte Ransomware-Gruppen (z.B. Conti) offen in den Dienst Russlands gestellt,[37] andere wiederum werden als Stellvertreter benutzt.[38]

8. Desinformation und Informationsangriffe

Desinformation, also die gezielte Erstellung und Verbreitung falscher, verfälschter, irreführender und aus dem Zusammenhang gerissener Informationen und Nachrichten, ist ein wesentlicher Bestandteil hybrider Bedrohungen. Ausländische Akteure wie Russland oder China zielen darauf ab, andere Gesellschaften, politische Systeme und für deren Funktionieren zentrale Einrichtungen zu destabilisieren, zu schwächen, zu verwirren und zu blockieren sowie Angst zu verbreiten.[39] Dies betrifft keineswegs ausschließlich politische oder staatliche Einrichtungen, sondern auch private Organisationen und Unternehmen, insb. der kritischen Infrastruktur. 2022 z.B., nach der russischen Invasion der Ukraine, verbreiteten russische Akteure in einer gezielten Aktion Falschmeldungen als gekaufte Werbung über angebliche Werksschließungen und drohenden Konkurs deutscher Großkonzerne, u.a. aus dem KRITIS-Bereich. Betroffen waren u.a. BASF, Siemens, VW und die Salzgitter AG, die, so die Desinformationskampagne, Werke und Einrichtungen in Deutschland wegen Energieknappheit schließen müssten.[40]

der_of_prorussia_ddos_crew/; zu Noname: https://press.avast.com/noname05716-pro-russian-hacker-group-targeting-sites-in-ukraine-and-supporting-countries-with-ddos-attacks; https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/.

37 Siehe z.B.: https://www.stern.de/digital/computer/ukraine--hacker-stellten-sich-hinter-russlands-angriff---und-duerfte-das-nun-schwer-bereuen-31667056.html.

38 Siehe z.B.: https://www.tagesschau.de/investigativ/ndr-wdr/hacker-attacken-russland-101.html; Justin Sherman: Untangling the Russian web: Spies, proxies, and spectrums of Russian cyber behavior, hg.: Atlantic Council, 2022 (https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/); T. Reinhold /C. Reuter: Zur Debatte über die Einhegung eines Cyberwars: Analyse militärischer Cyberaktivitäten im Krieg Russlands gegen die Ukraine. Zeitschrift für Friedens- und Konfliktforschung 12, 135–149 (2023). https://doi.org/10.1007/s42597-023-00094-y.

39 Siehe wiederum: https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefaehrdung-russische-spionage-sabotage-desinformation.html#doc2129880bodyText3.

40 Siehe: https://correctiv.org/faktencheck/2022/12/08/fake-kampagne-werke-von-basf-siemens-oder-vw-werden-nicht-wegen-energiekrise-geschlossen/?utm_source=substack&utm_medium=email.

Diese Art hybrider Angriffe kann auch durch personalisierte Schmierenkampagnen und Image-Angriffe, durch inszenierte Protestaktionen gekaufter und organisierter „Aktivisten“ oder durch Boykott-Aufrufe gegen exponierte Einzelpersonen oder Unternehmen der kritischen Infrastruktur erfolgen.

9. (Anschlags-)Drohungen

Der psychologische Aspekt hybrider Aktionen wie Sabotage wird oft durch falsche Drohungen und Ankündigungen von Anschlägen verstärkt. Solche Aktionen können auch als Unter- und Spezialform von Desinformation gesehen werden und werden oft recht einfach per E-Mail oder Telefon ausgesprochen. Sie sollen nicht nur gezielt Angst verbreiten, sondern auch Ereignisse und geregelte Abläufe stören und blockieren sowie Unzufriedenheit erzeugen. In den letzten Jahren waren solche falschen Drohungen besonders oft im Kontext von Wahlen, aber auch von Großereignissen wie Olympia 2024 zu beobachten. Sowohl in den USA, als auch in Island oder Bulgarien gingen vor Wahlen bei Behörden per E-Mail Bombendrohungen mit russischem Ursprung ein;[41] vor und während der Sommer-Olympiade in Paris 2024 kam es zu ähnlichen Drohungen sowie zu Online- und Offline-Aktionen, mit denen gezielt die Furcht vor islamistischen Terrorangriffen auf die Olympiade geschürt werden sollte, die aber russischen Ursprungs waren.[42] Solche Aktionen müssen sich keineswegs auf den Online-Raum beschränken, sondern finden auch in der physischen Welt statt: So stufen französische Sicherheitsbehörden z.B. eine Aktion, bei der 60 Davidsterne an Hauswände in Paris gesprüht wurden, um Terror-Angst zu schüren, als gezielten hybriden Angriff Russlands ein, für den ein Pärchen aus Moldau bezahlt wurde.[43]

> **In den letzten Jahren waren solche falschen Drohungen besonders oft im Kontext von Wahlen, aber auch von Großereignissen wie Olympia 2024 zu beobachten.**

Weitere Formen hybrider Kriegsführung mit (in) direkten Auswirkungen auf KRITIS-Einrichtungen sowie zur Verunsicherung der Gesellschaft:

10. Gesteuerte Migration als Mittel hybrider Angriffe

Künstlich erzeugte Migrationsströme werden von einigen Staaten als Instrument in Auseinandersetzungen benutzt. Durch kurzfristige und organisierte Migration großer Menschenmassen sollen Länder, Grenz-, Sicherheits- und Migrationssysteme gezielt und strategisch überfordert werden. Solche Beispiele ereigneten sich in der jüngeren Vergangenheit sowohl an der belarussisch-polnischen als auch an der russisch-finnischen Grenze. In beiden Fällen wurden von den russischen und belarussischen Behörden gezielt Migranten gesammelt, teilweise eigens eingeflogen, um dann Tausende Menschen auf einmal über die Grenze zu schicken.[44]

11. Hybride Angriffe durch sonstige Netzwerke

Transnationale kriminelle Netzwerke bieten vielfältige Ressourcen für staatlich organisierte hybride Kriegsführung. Feindliche Staaten unterstützen und nutzen transnationale kriminelle Aktivitäten, um andere Gesellschaften gezielt zu destabilisieren.

Diese Netzwerke können z.B. die logistische Basis für hybride Angriffe bilden oder unterstützen. Westliche Sicherheitsbehörden wie Europol gehen von einer gezielten Unterstützung transnationaler krimineller Netzwerke durch russische staatliche Stellen aus, um ihre Aktivitäten in EU- und NATO-Staaten auszuweiten.[45] Diese werden dann bei Bedarf zur Durchführung von Cyberat-

41 Siehe: https://www.zdf.de/nachrichten/politik/ausland/fbi-drohung-russland-desinformation-usa-wahl-100.html; und: https://saltylava.de/spionage-massenmord-und-destabilisierung-island-rueckt-ins-visier-fremder-maechte/.

42 Siehe z.B.: https://www.tagesspiegel.de/olympische-spiele-in-paris-cyberattacken-und-fake-news-olympia-in-paris-im-fadenkreuz-11816060.html; https://www.tagesschau.de/faktenfinder/olympische-spiele-fakes-100.html; und: https://www.zdf.de/nachrichten/digitales/hamas-video-propaganda-russland-israel-100.html.

43 Siehe z.B.: https://www.sueddeutsche.de/politik/paris-davidsterne-ermittlungen-1.6300305.

44 Siehe z.B.: https://germany.representation.ec.europa.eu/news/migration-als-waffe-im-hybriden-krieg-gegen-eu-eu-kommission-verstarkt-unterstutzung-fur-2024-12-11_de.

45 Siehe z.B.: Europol: European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg 2025 (https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf); M. Long: Shadows of power beneath the threshold: where covert action, organized crime and irregular warfare converge. Intelligence and National Security, 40(1) 2024, S. 87–113 (https://doi.org/10.1080/02684527.2024.2417454).

tacken, physischen Gewaltaktionen, zur Tarnung, Kontaktanbahnung, Verschleierung, für Menschenhandel, Schmuggel, Erpressung, Fälschungen, zur Durchführung von Finanztransaktionen und Geldwäsche sowie zur Umgehung von Sanktionen benutzt.

> **Systemische Korruption in Politik, Wirtschaft und Justiz ist in vielen Ländern zu einem Mittel gezielter Einflussnahme geworden.**

12. Einflussnahme durch Korruption

Systemische Korruption in Politik, Wirtschaft und Justiz ist in vielen Ländern zu einem Mittel gezielter Einflussnahme geworden. Entscheidungsträger werden beeinflusst, Institutionen geschwächt und Recht außer Kraft gesetzt, um strategische Vorteile und Kontrolle, z.B. für ausländische Unternehmen in KRITIS-Sektoren, zu erlangen, politische Entscheidungen zu manipulieren und Kontrolle über öffentliche Ressourcen zu übernehmen. Korruption kann also die Grundlage für hybride Angriffsmaßnahmen bieten und diese gleichzeitig verstärken. Ebenso besitzt strategische und systemische Korruption eine psychologische Komponente, die für die Destabilisierung von Gesellschaften und ihren Sicherheitssystemen wichtig ist.[46]

Die gezielte Unterstützung von Oligarchen und Kleptokraten bietet Staaten wie Russland oder China daher viele Vorteile: Sie können sich Zugriff auf Rohstoffe sichern, Länder, Gesellschaften und Regionen gezielt instabil halten, Bevölkerungen und Diskurse ablenken, aber auch logistische Basen für andere Operationen sichern (z.B. durch den Verkauf sog. „goldener Pässe“[47], die russische Agenten und Persönlichkeiten nutzen können).

46 Siehe z.B.: ‘A Deadlier Peril’: The Role of Corruption in Hybrid Warfare, hg.: MCDC Countering Hybrid Warfare Project, Information note, March 2019 (https://assets.publishing.service.gov.uk/media/5caf5dd8e5274a59c06bf116/20190318-MCDC_CHW_Info_note_7.pdf); https://smallwarsjournal.com/2024/12/10/corruption-as-an-enabler-in-the-hybrid-influence-toolbox/.

47 Siehe z.B.: https://www.spiegel.de/politik/deutschland/zypern-und-malta-entziehen-reichen-russen-goldene-paesse-a-3fbfb9a0-079b-4d95-934f-1e6c9f84bd96.

Empfehlungen

Aufgrund der allgemeinen Risikolage kann heute nahezu keine Organisation als potenzielles Ziel oder Kollateralziel hybrider Angriffe ausgeschlossen werden. Einrichtungen mit speziellem Bezug zu den politischen und wirtschaftlichen sowie gesellschaftlichen Anliegen hybrider Angreifer stehen jedoch im besonderen Fokus und sollten zusätzliche Strategien und Maßnahmen ins Auge fassen und einplanen.

- Sensibilisierung & Awareness auf der Führungsebene sowie Trainings und Schulungen als Maßnahmen für Mitarbeiter
- Allgemeines Frühwarnsystem für KRITIS-Einrichtungen, um die Gesamtlage zu erfassen, konkrete Risiken zu kennen, zu bewerten und vor die Lage zu kommen
- Entwicklung ganzheitlicher Sicherheitskonzepte infolge umfänglicher Risikobewertung
- Frühwarnsysteme, Schutzmechanismen, Incident Response zur Steigerung der Reaktionsfähigkeit auf Sicherheitsvorfälle mit regelmäßigen Übungen und Überprüfungen
- Psychologische Resilienz durch Training und Vorbereitung, um Stresseffekten, Angst und psychologischen Effekten hybrider Maßnahmen im Krisenfall entgegenwirken zu können

Weitere Maßnahmen

Das cyberintelligence.institute fördert im Verbund mit seinen Partnern die Resilienz gegen hybride Bedrohungen. Dazu werden regelmäßig neue Studien und Erkenntnisse veröffentlicht sowie konkrete Hilfestellungen auf den Weg gebracht. Hierzu zählen auch aktuelle Initiativen wie der HybridThreatRadar.

Für weitere Informationen sowie Möglichkeiten der Unterstützung bei der Entwicklung wirksamer Strategien und Maßnahmen zur Steigerung der Resilienz gegen hybride Bedrohungen sowie für die Bereitstellung von Materialien, Schulungen und Trainings nehmen Sie gerne Kontakt mit uns auf.

Mehr unter: www.cyberintelligence.institute

Impressum & Kontakt

Autor
Dr. Christopher Nehring
Intelligence Director
christopher.nehring@cyberintelligence.institute

Herausgeberin
cyberintelligence.institute
Geschäftsführer: Clemens Kröger (V.i.S.d.P.)
MesseTurm I Friedrich-Ebert-Anlage 49
D-60308 Frankfurt am Main

www.cyberintelligence.institute
info@cyberintelligence.institute

+49 69 505034602

Über das CII

Neue Zeiten brauchen eine neue Form der Forschung: das cyberintelligence.institute (CII) – ein Ort, an dem sich Innovation, Technologie, Strategie und Resilienz treffen. An der Schnittstelle von Wirtschaft und Wissenschaft, NGO und Start-up entwickelt das CII in Frankfurt am Main neue Lösungen für eine sichere digitale Zukunft. Kerngedanken sind die Kooperation, der Dialog und der interdisziplinäre und globale Informations- und Wissensaustausch, um Staat, Wirtschaft und Gesellschaft resilienter zu machen. Gefragt sind dabei ganzheitliche Konzepte, die Cybersicherheit nicht nur als abstrakte technisch-organisatorische Gewährleistungsverantwortung, sondern als gesamtgesellschaftliche Aufgabe zum Schutz gemeinsamer europäischer Werte verstehen. Damit tritt das cyberintelligence.institute aktiv für mehr digitale Sicherheit in einem Zeitalter neuer digitaler Herausforderungen ein.

Weitere Informationen gibt es auf der Website des CII unter www.cyberintelligence.institute.