CII DEEP-DIVE

Hybride Bedrohungen Teil 2/3

Drohnenabwehr und kritische Infrastruktur

Ein Maßnahmenkatalog

Dr. Christopher Nehring

CYBER|INTELLIGENCE
.Institute

Vorwort

Diese dreiteilige CII-Deep-Dive-Reihe bietet einen Überblick über aktuelle hybride Angriffsszenarien und -hintergründe sowie über Gegenmaßnahmen. Der erste Teil widmet sich den „Hybriden Bedrohungen“, der zweite Teil dem aktuellen Stand der „Drohnenabwehr“, während sich der dritte Teil den Methoden russischer Geheimdienste mit Fokus auf Agenten 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 2: Drohnenabwehr und kritische Infrastruktur

Das Wichtigste in Kürze:

- Unerlaubte Drohnenüberflüge sind seit 2022 ein stetig wachsendes Sicherheitsproblem mit nahezu täglichen Vorfällen insbesondere gegen KRITIS-Einrichtungen.
- Zur Drohnenabwehr gibt es sog. „Hard kill-“ und „Soft kill“-Maßnahmen, die unterschiedliche Vor- und Nachteile bieten.
- Resilienzbildung – sowohl bauliche und technische als auch psychische Resilienz – ist ein essenzieller Bestandteil ganzheitlicher Sicherheitskonzepte.
- Bislang dürfen nur Polizei und Bundeswehr fremde Drohnen abschießen (und dies nur unter sehr strengen Bedingungen).
- Zur Drohnenabwehr und Resilienzbildung bedarf es spezifischer technischer sowie menschlicher Fähigkeiten und Kapazitäten, die aufgebaut werden müssen.

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

Dieses Deep-Dive-Paper …

- … bietet einen konzisen Überblick über Gegen- und Resilienzmaßnahmen bei Drohnenangriffen.
- … übersetzt abstrakte Risikoanalysen und Resilienzvorschriften in handlungsleitendes, maßnahmenzentriertes Wissen.
- … unterstützt bei Planungen von Schutzmaßnahmen gemäß § 13 KRITIS-DachG.
- … kann die Reaktionsfähigkeit bei Vorfällen erhöhen entsprechend § 18 KRITIS-DachG.
- … trägt durch seine Verbreitung zur Stärkung der Gesamtresilienz bei.

Inhalt

Drohnen als Instrument hybrider Angriffe

Flugdrohnen (Unmanned Aerial Vehicles, UAV) werden zu gezielten Aufklärungs- und Überwachungsoperationen, aber auch zu Sabotageakten eingesetzt und sind aktuell ein weit verbreitetes Instrument hybrider Angriffe in Deutschland. Die genaue Zahl von unerlaubten Drohnenüberflügen über KRITIS-Einrichtungen ist unbekannt, übersteigt jedoch 500 bei Weitem (alleine über Bundeswehrstandorten wurden 2023 mindestens 446 Drohnenüberflüge gemeldet).[1] Dabei kommen viele verschiedene Drohnen zum Einsatz – von großen, vermutlich von Schiffen in der Nord- und Ostsee aus gesteuerten Militärdrohnen mit großer Spannweite und Geschwindigkeit bis zu kleineren „Jedermann-Drohnen“ (z.B. Quadrocoptern), die von Personen am Boden gesteuert werden.[2] Russland ist dabei aufgrund eines genuinen Interesses oft der mutmaßliche Akteur (vor allem bei Militärdrohnen).

Motive & Ziele der Angreifer

Die Motive und Ziele hinter den Drohnenflügen sind oft nicht klar erkennbar, viele dienen offenbar der militärischen Spionage und Aufklärung potenzieller Angriffsziele. Gleichzeitig geht es auch um ein ständiges Austesten von Reaktionen und Abläufen von Sicherheitsbehörden, Armeeeinheiten und den betroffenen 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.

Ukrainische PD-2-Aufklärungsdrohne;
Quelle: Ukrainischer Geheimdienst SBU.

Damit stellen Drohnenüberflüge eine neue sicherheitstechnische Herausforderung dar; dass auch nach fast drei Jahren und einer stetig steigenden Anzahl an Vorfällen keine strategische Antwort bzw. wirksame Gegenmaßnahmen erfolgen, trägt zur Verunsicherung und dem vom Angreifer intendierten psychologischen Schaden bei.

Ein ausführlicher Überblick über Angriffsarten hybrider Bedrohungen findet sich im ersten Teil der CII-Deep-Dive-Reihe „Hybride Bedrohungen“.

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

2 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/).

Aggressive und aktive Abwehrmaßnahmen[3]

1. Abschuss von Drohnen

Eine aktive und zugleich aggressive Möglichkeit der direkten Neutralisierung (sog. hard kill) unbefugter Drohnen ist der Abschuss. Dies kann durch den Einsatz traditioneller Schusswaffen, etwa Gewehre oder Schrotflinten, und sowohl vom Boden als auch aus der Luft (z.B. aus Helikoptern) erfolgen. Rüstungsunternehmen wie z.B. Rheinmetall arbeiten hierzu an mobilen Anti-Drohnen-Kampf-Fahrzeugen, die sowohl über Detektionstechnik als auch Abschussvorrichtungen und Geschütze verfügen.[4]

Auch speziell entwickelte Geschosse oder Kampf- und Abfangdrohnen, die feindliche Drohnen durch Abschuss, Rammen oder gezielten Aufprall (auch mit kleineren Sprengvorrichtungen) angreifen, werden eingesetzt. Das Rüstungsunternehmen Airbus hat hierzu erst 2025 eine spezielle Abwehrdrohne zur Verteidigung gegen Kamikaze-Angriffsdrohnen („LOAD“) vorgestellt;[5] diese dürfte jedoch zunächst nur für den militärischen Einsatz und nicht für zivile Zwecke zum Schutz von KRITIS geeignet sein.

Diese Hard-kill-Methoden bergen jedoch auch Risiken, da z.B. herabfallende Teile oder unkontrolliert abstürzende Drohnen eine Gefahr darstellen. Nach aktueller Rechtslage sind gleichfalls ausschließlich Behörden bzw. die Bundeswehr berechtigt, illegale Drohnen abzuschießen (und dies nur als Ultima Ratio bei unmittelbarer Gefahr).[6]

a. Laser und EMP: Hochenergetische Effektoren

Zu den technologisch fortschrittlichsten Abwehrmethoden gehören Laser- und Mikrowellenwaffen. Diese sind ebenfalls sog. Hard-kill-Verfahren. Laserwaffen können eine Drohne durch einen präzisen, gebündelten Lichtstrahl innerhalb weniger Sekunden beschädigen oder entzünden. Systeme wie das israelische Drone Dome oder das US-amerikanische Athena nutzen diese Technologie[7] und in Deutschland arbeitet Rheinmetall an Laser-basierten Anti-Drohnen-Systemen (Laser-Testbed).[8]

Andere Systeme basieren auf Hochleistungs-Mikrowellen (HPM), die durch einen elektromagnetischen Impuls oder Mikrowellenstrahl die Bordelektronik der Drohne angreifen oder zerstören (wie z.B. das US-System THOR[9]). Diese Systeme wirken mit großer Geschwindigkeit und können auch mehrere Drohnen nacheinander neutralisieren. Ihr Einsatz erfordert jedoch hohe Investitionen in Technik und Personal und kann unerwünschte Nebeneffekte auf andere elektronische Systeme und Flugobjekte in der Umgebung haben.

b. Jamming und Spoofing: Signalstörungen

Eine vergleichsweise sanftere Methode (sog. soft kill) sind Signalstörungen. Durch den Einsatz gerichteter Störsender (Jammer) können Steuerfrequenzen oder GPS-Signale anfliegender Drohnen gezielt blockiert werden. Moderne Systeme verwenden dabei breitbandige, reaktive Jammer, die Steuersignale und Telemetrie

3 Für einen ausführlichen Überblick zu Anti-Drohnen-Maßnahmen siehe: House Committee on Transportation and Infrastructure, Subcommittee on Aviation hearing entitled, “Counter-Unmanned Aircraft Systems”, 07.02.2025: https://www.youtube.com/watch?v=rQ70gD1VAR8; US Department of Defense: Department of Defense Counter Unmanned Aircraft Systems: Background and Issues for Congress, 31.03.2025 (https://www.congress.gov/crs-product/R48477); Miriam McNabb / Jim Magill: Strengthening Airport Defenses: The Growing Need for Better Counter-Drone Measures (https://dronelife.com/2025/02/19/strengthening-airport-defenses-the-growing-need-for-better-counter-drone-measures/), 19.02.2025; P. Hansen / R. Pinto Faria: Protection against unmanned aircraft systems – Handbook on UAS protection of critical infrastructure and public space – A five phase approach for C-UAS stakeholders, Publications Office of the European Union, 2023 (https://data.europa.eu/doi/10.2760/18569); Dawn Zoldi: Act Now to Protect Critical Infrastructure Against Drones, ed.: Sentrycs (https://sentrycs.com/wp-content/uploads/2023/09/White-paper-Act-Now-to-Protect-Critical-Infrastructure-Against-Drones_FINAL.pdf).

4 Siehe z.B.: https://www.rheinmetall.com/de/produkte/flugabwehr/flugabwehrsysteme/drohnenabwehr-toolbox.

5 Siehe: https://www.heise.de/news/Airbus-zeigt-preisguenstige-LOAD-Abwehrdrohne-gegen-Kamikazedrohnen-10329120.html.

6 Siehe: https://www.lto.de/recht/hintergruende/h/illegale-drohnen-abschuss-kabinett-luftsicherheitsgesetz-bundeswehr.

7 Siehe z.B.: https://militaryembedded.com/unmanned/counter-uas/athena-laser-weapon-system-defends-uas-threat.

8 Siehe: https://www.rheinmetall.com/de/media/news-watch/news/2022/2022-05-19_laserwaffe-gegen-drohnen.

9 Siehe z.B.: https://afresearchlab.com/technology/thor.

unterbrechen.[10] Systeme wie das Drone Dome in Israel oder das Rheinmetall U-CAS-System[11] verfügen über stationäre und mobile Störsender, die im Umkreis mehrere Drohnen gleichzeitig durch Blockade von Funk und Satellitennavigation neutralisieren. In den USA werden auch tragbare Vorrichtungen wie der Drone Defender entwickelt, die per Knopfdruck den Steuerfunk einer anfliegenden Drohne auf mehrere Hundert Meter unterbrechen können.[12]

Eine andere Methode ist das Signal-Spoofing: Hierbei senden Abwehrsysteme gefälschte Navigationssignale, die die anfliegende Drohne in die Irre führen oder zur Landung zwingen sollen. Manche Systeme, wie das israelische EnforceAir, zielen sogar darauf, die Steuerung und Navigation der anfliegenden Drohne zu übernehmen.[13]

c. Kinetische Neutralisierung („Abfangen und Einsammeln“)

Eine andere Methode ist die sog. „kinetische Neutralisierung“, bei der Drohnen physisch abgefangen werden. Hierzu gehören Netzwerfer, wie z.B. das britische SkyWall-System[14], ein Bazooka-ähnlicher Werfer, der eine Kapsel mit einem großen Netz bis zu 100 Meter weit schießt. Das Netz soll die Rotoren von Drohnen verwickeln, ein kleiner Fallschirm lässt die eingefangene Drohne dann kontrolliert zu Boden sinken. Von solchen Netzwerfern gibt es stationäre und tragbare Varianten. Eine andere Methode sind Jagd- oder Abfangdrohnen, wie z.B. DroneCatcher[15] oder Fortem DroneHunter[16]. Größere Drohnen fangen die Zieldrohne mit einem ausgesetzten Netz oder einem Greifmechanismus in der Luft. So nutzt z.B. das niederländische DroneCatcher-System (Delft Dynamics) eine Abfangdrohne mit Netzwerfer. Ähnlich arbeitet das US-System Fortem DroneHunter, das autonom Feinddrohnen mit einem Netz einfängt. Diese Drohne-gegen-Drohne-Taktik wurde an einigen Flughäfen und militärischen Einrichtungen erprobt.[17] Alternativ werden auch Kampfdrohnen

Aufnahmen einer mit einem Netz gefangenen Kleindrohne im Rahmen des Forschungsprojektes „FALKE“ der Bundeswehr-Universität Hamburg, (C) HSU / Jan Cornils.

eingesetzt, um anfliegende Drohnen zu rammen (z.B. Anduril Anvil in den USA[18]).

d. Weitere Methoden

Abweichend von den genannten Maßnahmen können auch weitere Instrumente eingesetzt werden, um die anfliegende Drohne entweder von ihrem Kurs abzubringen oder ihre Navigation bzw. Sicht einzuschränken. Dazu gehören Blend-Laser, starke Scheinwerfer sowie Wasser- und Nebelwerfer, um die Sensorik oder die Sicht der Drohne zu beinträchtigen oder zu zerstören. Diese Maßnahmen eignen sich jedoch vor allem auf kurze Distanzen („auf Sicht“) und erfordern eine entsprechend breitflächige physische Infrastruktur, schnelle Reaktionszeiten sowie geschultes Personal.

Aufgrund rechtlicher Beschränkungen dürfen viele dieser Methoden in Deutschland nur von staatlichen Stellen eingesetzt werden. Darüber hinaus sind sie oft kostenintensiv und ihr Erfolg hängt von Reaktionszeiten und der Umsetzung durch Mitarbeiter ab. Betreiber kritischer Infrastruktur müssen daher eng mit den Behörden kooperieren und sind auf deren Unterstützung angewiesen!

10 Siehe: army-technology.com.

11 Siehe z.B.: https://www.rheinmetall.com/de/produkte/flugabwehr/flugabwehrsysteme/drohnenabwehr-toolbox.

12 Siehe: https://de.dedrone.com/solutions/dedrone-defender-2.

13 Siehe z.B.: https://www.unmannedsystemstechnology.com/video/enforceair2-rf-cyber-takeover-anti-drone-system-benefits/.

14 Siehe: https://techcrunch.com/2016/03/04/the-skywall-100-bazooka-captures-drones-with-a-giant-net/#:~:text=Other%20devices%20use%20radio%20waves,drones%20to%20capture%20smaller%20drones.

15 Siehe: https://dronecatcher.nl/#Introduction.

16 Siehe: https://fortemtech.com/products/dronehunter-f700/.

17 Siehe: Miriam McNabb / Jim Magill: Strengthening Airport Defenses: The Growing Need for Better Counter-Drone Measures (https://dronelife.com/2025/02/19/strengthening-airport-defenses-the-growing-need-for-better-counter-drone-measures/), 19.02.2025.

18 Siehe: https://www.anduril.com/hardware/anvil/.

2. Resilienzmaßnahmen

a. Baulicher Schutz

Die robuste und risikominimierende Bauweise von KRITIS-Anlagen ist eine grundlegende Schutz- und Resilienzmaßnahme. Dazu gehören z.B. Netze über offenen Bereichen, verstärkte Dachkonstruktionen oder der Einbau von Gittern, Schutzhauben, Dächern, Sichtschutz etc. über empfindlichen Anlagenteilen. Weiterhin können unterirdische Anlagen für besonders sensible Bereiche, die Gleichförmigkeit von Bauten und Anlagen sowie weitere bauliche Maßnahmen dazu beitragen, die Resilienz gegen Drohnenüberflüge und -aufklärung zu erhöhen.[19]

b. Sichtschutz, Tarnung, Abschirmung und gezielte Täuschung

Darüber hinaus können sensible Bauten und Anlagen durch Sichtschutzmaßnahmen und/oder spezielle Tarnungen resilienter gegen Drohnenüberflüge gemacht werden. Um Ausspähung zu verhindern, sollten Gebäude z.B. keine sichtbaren Hinweise wie Beschriftungen auf sensible Bereiche enthalten. Außerdem können sensible Bauten und Räume getarnt und abgeschirmt werden. Fenster, Glastüren oder Dachluken können

> **Um Ausspähung zu verhindern, sollten Gebäude z.B. keine sichtbaren Hinweise wie Beschriftungen auf sensible Bereiche enthalten. Außerdem können sensible Bauten und Räume getarnt und abgeschirmt werden.**

mit Jalousien, Vorhängen oder reflektierenden Folien versehen werden, Netze, Folien, Gitter o.Ä. hingegen über Anlagen angebracht werden. Das BSI empfiehlt beispielsweise, keine erkennbaren äußeren Anzeichen (z.B. Beschriftungen oder baulich-räumliche Hervorhebung) für kritische Räume zu hinterlassen.[20] Weiterhin sollte auch nicht nur der visuellen Aufklärung durch Drohnen, sondern auch Abhörmaßnahmen vorgebeugt werden. Elektromagnetische Abschirmungen durch metallbeschichtete Fenster oder Gitter verhindern z.B, dass Funksignale durch Drohnen abgehört oder gestört werden können.[21]

Umgekehrt können jedoch auch strategisch erkennbare Tarnungen, Beschriftungen o.Ä. angebracht werden, die die Aufmerksamkeit von Drohnen und Drohnenführern gezielt auf sich lenken, ohne jedoch tatsächlich sensible Bereiche zu sein. Solche Maßnahmen der strategischen Täuschung erfordern Spezialwissen, Risikobereitschaft und Geduld.

c. Einnebeln und Verblenden

Nebelmaschinen oder Rauchgeneratoren können kurzfristig und akut bei einem Drohnenüberflug eingesetzt werden, um sensible Bauten, Gebäude, Anlagen, Geräte und Bereiche zu verhüllen und die Sicht von Drohnen zu blockieren. Diese Technik ist aus dem militärischen Bereich bekannt. Weiterhin ist es möglich, anfliegende Drohnen gezielt zu blenden und durch starke Scheinwerfer oder LED- und Laser-Dazzler die Kamerasensoren von Drohnen übersteuern zu lassen.[22] Solche Maßnahmen erfordern eine kurze Reaktionszeit und eine automatisierte Verfolgung der Drohne und bergen das Risiko, andere Flugobjekte zu beeinträchtigen.

d. Organisatorische Maßnahmen

Klare Notfall-, Ablauf- und Reaktionspläne seitens betroffener Einrichtungen sind entscheidend. Dazu gehören Meldeketten, Reaktionen, Eskalationsstufen und festgelegte Verantwortlichkeiten. Mitarbeitende sollten regelmäßig geschult und in Übungen auf Drohnensichtungen vorbereitet werden. Das betrifft einerseits Reaktionen und Abwehrmaßnahmen, andererseits auch vorbeugende Prävention zur Verhinderung z.B. von Abhören. Checklisten, Aushänge und Verhaltensregeln

19 Siehe z.B.: Federal Office for Information Security (BSI): Overview of drone-based cyber threats and aspects of defence, Bonn 2024 (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Drohnen/drone_cyber_threats_defence.pdf?__blob=publicationFile&v=10#:~:text=Avoid%20marking%20or%20publication%20of,are%20also%20accessible%20by%20drones); P. Hansen / R. Pinto Faria: Protection against unmanned aircraft systems – Handbook on UAS protection of critical infrastructure and public space – A five phase approach for C-UAS stakeholders, Publications Office of the European Union, 2023 (https://data.europa.eu/doi/10.2760/18569).

20 Siehe wiederum: Federal Office for Information Security (BSI): Overview of drone-based cyber threats and aspects of defence, Bonn 2024 (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Drohnen/drone_cyber_threats_defence.pdf?__blob=publicationFile&v=10#:~:text=Avoid%20marking%20or%20publication%20of,are%20also%20accessible%20by%20drones.

21 Siehe ebd.

22 Siehe z.B.: https://www.twz.com/land/laser-dazzlers-for-defending-tanks-against-marauding-drones-are-an-untapped-countermeasure.

tragen dazu bei, die Risiken von Drohnenüberflügen zu minimieren. Enge Abstimmung mit Behörden und regelmäßige gemeinsame Übungen verbessern ferner die Reaktionsfähigkeit.

e. Geofencing und Luftraumbeschränkungen

Betreiber kritischer Infrastruktur können ferner behördliche Flugverbotszonen beantragen und mit Drohnen-Herstellern kooperieren, damit ihre Standorte in sog. Geofencing-Datenbanken integriert werden. Die dort hinterlegten Geodaten dürfen von kommerziellen „Jedermann-Drohnen" nicht angesteuert werden. So verhindern einige Drohnenmodelle automatisch den Start in gesperrten Zonen oder deren Einfliegen.[23] Geofencing bietet daher vor allem Schutz vor versehentlichen Überflügen und Überflügen mit kommerziell leicht verfügbaren Drohnen, ist aber gegenüber manipulierten oder spezialisierten Drohnen (z.B. Militärdrohnen) wirkungslos.

3. Voraussetzungen und Herausforderungen bei der Drohnenabwehr

Eine Grundvoraussetzung für effektive Abwehrmaßnahmen gegen Drohnen sind **gute und aktuelle Informationen** über eingesetzte Drohnentypen und deren Technik, über typische Vorgehensweisen, Flugzeiten, Routen etc. Dazu sind Kooperationen und Wissensaustausch genauso unabdingbar wie Spezialtechnik zur Detektion. Diese Informationen sind im Einzelfall entscheidend, um Abwehrmaßnahmen überhaupt durchführen zu können (Signal-Jammer oder Spoofer müssen z.B. unbedingt zu den jeweiligen Systemen der Drohne passen, um wirkungsvoll zu sein).

> **Drohnenüberflüge dauern oft nur wenige Minuten – werden sie spät erkannt, bleibt fast keine Zeit zum Reagieren.**

Insbesondere ist die **Früherkennung** entscheidend. Drohnenüberflüge dauern oft nur wenige Minuten – werden sie spät erkannt, bleibt fast keine Zeit zum Reagieren. Aktuelle und funktionierende Detektionssysteme wie Radar, Funkpeilung sowie optische oder akustische Sensoren sind erforderlich, um Drohnen frühzeitig und genau zu erkennen. Dazu gehören auch die Art und die Größe der anfliegenden Drohne, die unterschiedliche Abwehrmaßnahmen bedingen können. Hier kommen Radar (erfasst Flugobjekte und ihre Position), RF-Sensoren (detektieren Funkverbindungen der Drohne), Kameras (visuelle/IR-Erkennung) und akustische Sensoren (Erkennen von Rotorengeräuschen) zum Einsatz.[24] Das israelische System Drone Dome nutzt z.B. 360°-Radare und elektro-optische Infrarotsensoren, gekoppelt mit RF-Scannern, um kleine Drohnen auf mehrere Kilometer zu entdecken.[25] Auch andere Systeme setzen auf die Fusion von Kameras, Funkpeilung und Audiomonitoring, um unautorisierte Drohnen z.B. über Kraftwerken oder Flughäfen frühzeitig zu erkennen.

Darauf aufbauend braucht es zur Drohnenabwehr eine ganze Reihe an **Ausrüstung, Fähigkeiten und Personal**. Für Abschuss, Signalstörung, Blendung oder kinetische Neutralisierung werden jeweils spezielle Gerätschaften sowie qualifiziertes Personal (z.B. Piloten, Hacker, Schützen, Jammer, Operatoren) zur Bedienung benötigt. Dasselbe gilt für Abwehr- oder Angriffsdrohnen oder Hubschrauber zum Abfangen, Einfangen und Neutralisieren. Dazu können/müssen ggf. auch externe Dienstleister engagiert und koordiniert sowie mit Behörden kooperiert werden. Schließlich braucht es auch einen klaren, flexiblen und multidimensionalen Reaktions- und Ablaufplan bei Vorfällen.

Besondere **Herausforderungen** bestehen derzeit auch in rechtlichen Einschränkungen, Unwissen über Art und Verhalten der anfliegenden Drohnen, begrenzten Reaktionszeiten, unsicheren Wetterbedingungen und der Gefahr von Kollateralschäden. Darüber hinaus sind viele bestehende Detektions- und Abwehrsysteme ihrem Ursprung nach für den militärischen Einsatz in Gefechtszonen und nicht für den Einsatz unter zivilen Bedingungen konzipiert. Unklarheiten über die Absichten oder die Gefährlichkeit einer Drohne erschweren fernerhin die Entscheidungsfindung zusätzlich.

23 Siehe: https://eudroneport.com/de/blog-de/verstehen-der-unterschiede-zwischen-geocaging-und-geofencing/; ebenso: https://sentrycs.com/de/the-counter-drone-blog/the-potential-effects-of-djis-geofencing-removal-on-counter-uas-efforts/.

24 Siehe z.B.: Dawn Zoldi: Act Now to Protect Critical Infrastructure Against Drones, hg.: Sentrycs (https://sentrycs.com/wp-content/uploads/2023/09/White-paper-Act-Now-to-Protect-Critical-Infrastructure-Against-Drones_FINAL.pdf).

25 Siehe z.B.: https://www.army-technology.com/projects/drone-dome-counter-uncrewed-aerial-system-c-uas-israel/#:~:text=In%20the%20hard,seconds%20to%20destroy%20the%20target.

Empfehlungen

Aktiv werden

Aufgrund der allgemeinen Risikolage gilt für „interessante Zieleinrichtungen“ heute, dass das Risiko von feindseligen Drohnenangriffen nicht mehr als Einzelfall, sondern als Bestandteil des organisationellen Alltags zu zählen ist. Dabei gilt auch hier: Einrichtungen mit besonderem Bezug zu den politischen und wirtschaftlichen sowie auch gesellschaftlichen Anliegen stehen im besonderen Fokus und sollten zusätzliche Strategien und Maßnahmen ins Auge fassen und einplanen.

- Betreiber von KRITIS-Einrichtungen sowie von potenziellen Zielobjekten sollten eigene Kapazitäten (Technik und Geräte, Personal, Software, Fähigkeiten, Ressourcen, Wissen, Experten und Kooperation) zur Drohnenabwehr aufbauen.
- Diese sollten enge und stehende Kooperationen mit Behörden zur aktiven Drohnenabwehr aufbauen und pflegen.
- Aktuelles Detail- und Fachwissen über Technik und Strategien von Drohnenüberflügen (Threat Intelligence) sind essenziell, um Abwehr- und Resilienzmaßnahmen effektiv zu gestalten.
- Zielobjekte der Drohnenangriffe brauchen Sicherheitsstrategien und organisatorische Ablaufpläne für Drohnenvorfälle.
- Gesetzliche Regelungen müssen auf Praxistauglichkeit überprüft und gegebenenfalls angepasst werden.
- Bewusstsein für die Bedrohungslage, mögliche Angriffstaktiken und deren Auswirkungen ist auf allen relevanten Ebenen innerhalb von KRITIS-Einrichtungen zu fördern.
- Zielobjekte sollten internationale Kooperationen, Netzwerke und Erfahrungsaustausch mit anderen Betroffenen anstreben, um auf dynamische Entwicklungen vorbereitet zu sein.

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 und Angebote auf den Weg gebracht.

Für weitere Informationen und Möglichkeiten der Unterstützung bei der Entwicklung wirksamer Strategien und Maßnahmen zur Steigerung der Resilienz gegen hybride Bedrohungen durch Drohnen 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.