

## Meldung

### Rotes Kreuz will digitales Emblem

(BS) Das Rote Kreuz ist ein international be- und anerkanntes Symbol für Krankenhäuser und Rettungseinrichtungen. Besonders in Kriegsgebieten kann diese Kennzeichnung viele Leben retten. Da sich kriegerische Handlungen mittlerweile auch in Teile des Cyber-Raums verlagert haben, soll es eine entsprechende digitale Schutzsymbolik geben.

Das Internationale Komitee vom Roten Kreuz (ICRC) will auch seine digitalen Ressourcen schützen: durch neue digitale Embleme (DIEM). Eine Arbeitsgruppe der Internet Engineering Task Force (IETF) soll die digitale Kennzeichnung ausarbeiten. Dies wurde auf dem 121. IETF-Treffen in Dublin, Irland, beschlossen. Die Arbeitsgruppe soll ein Datenformat sowie Verfahren für die Ausstellung und Integration der digitalen Schutzmarkierungen entwerfen. Anhand des digitalen Roten Kreuzes sollen Dritte in Zukunft prüfen können, ob eine digitale Ressource nach humanitärem Völkerrecht oder anderen Normen gekennzeichnet ist und daher „geschützt und respektiert“ werden müsse, so Samit D’Cunha vom ICRC. Ob das Internationale Rote Kreuz zunächst als einzige Institution ein DIEM erhält, wird noch diskutiert. Es steht auch im Raum, ob Journalistinnen und Journalisten mehr digitalen Schutz bekommen sollen. Mike Christie, Ex-Reuters-Journalist und Experte für Pressesicherheit, hatte sich in der Vergangenheit dafür eingesetzt, dass auch durch „Press“ gekennzeichnete Ausrüstungsgegenstände von Pressemitarbeitenden durch digitale Embleme geschützt werden sollten.

## Silvesterbilanz bleibt gemischt

(BS) Die Silvesternacht bleibt weiterhin ein Ausnahmezustand für Feuerwehr und Rettungsdienst. Nach den Bildern und Meldungen des Jahreswechsel 2023/24 vermeldet die Berliner Feuerwehr ein gemischtes Bild.

Insgesamt mussten 1892 Einsätze zum Jahreswechsel 2024/25 bewältigt werden. Das sind 294 Einsätze mehr als im Vorjahr. Es kam aber auch wieder zu Gewalt gegen Einsatzkräfte. In der Silvesternacht wurden 13 Angriffe und Störungen auf Einsatzkräfte registriert. Erfreulicherweise wurden hierbei nach jetzigem Kenntnisstand keine Rettungskräfte verletzt. Im Vorjahr waren es noch 30 Übergriffe.

„Die Silvesternacht war erneut die einsatzreichste Nacht des Jahres, geprägt von zahlreichen Bränden und Rettungsdienst-einsätzen. Leider gab es auch wieder Übergriffe auf unsere Einsatzkräfte und Fahrzeuge. Glücklicherweise wurden dabei keine Einsatzkräfte verletzt. Diese Vorfälle machen uns dennoch tief betroffen. Jeder einzelne Übergriff wird umfassend ausgewertet und konsequent zur Anzeige gebracht“, erklärte Landesbranddirektor Berlins Dr. Karsten Homrighausen.

Auch andernorts gab es ein gemischtes Bild bzgl. der Einsatzzahlen im Vergleich zum Vorjahr. Während in München die Feu-



Silvester bedeutet für die Einsatzkräfte von Polizei, Feuerwehr und Rettungsdienst mittlerweile Ausnahmezustand.

Foto: BS/ Markus Distelrath, [pixabay.com](https://pixabay.com)

erwehrensätze sanken, (Insgesamt: 190 Einsätze (Vorjahr 209) davon: Brandeinsätze 163 (Vorjahr 183) Technische Hilfeleistungen 27 (Vorjahr 26)) stiegen die Notarztein-sätze (128 Einsätze (Vorjahr 102)).

In Essen wurden glücklicherweise keine Einsatzkräfte durch Übergriffe verletzt, auch wenn es diese gab. Im Vergleich zum Vorjahr 2023/24 verzeichnete die Feuerwehr Essen mehr Brandeinsätze und eine etwas geringere Zahl von Rettungsdienst-einsätzen im Stadtgebiet.



cyber\_sicherheits\_tag  
niedersachsen

30. Januar 2025 // Hannover  
Designhotel + Congresscentrum Wienecke XI.

#cyberNDS

## Rund 340 Tonnen Kampfmittel gefunden

(BS) In Brandenburg sind 2024 rund 340 Tonnen Kampfmittel gefunden worden. Insgesamt konnten 537 Hektar Landesfläche aus dem Kampfmittelverdacht entlassen werden, teilte das Innenministerium in Potsdam in einer vorläufigen Bilanz des Kampfmittelbeseitigungsdienstes (KMBD) mit. Im Vergleich zum Jahr 2023 sind rund 230 Tonnen Kampfmittel weniger gefunden worden. Trotz der enormen Menge bleibt Brandenburg Spitzenreiter unter den Bundesländern, was die Kampfmittelverdachtsflächen angeht.

Der KMBD hat bis Ende November 2024 über 4.300 Anfragen von Grundstückseigentümern auf Kampfmittelbelastung bearbeitet und wurde zudem zu fast 2200 Zufallsfunden im Rahmen der Gefahrenabwehr gerufen. Außerdem beauftragte er über 200 Kampfmittelräummaßnahmen auf landeseigenen, kommunalen und privaten Liegenschaften. Insgesamt hat der KMBD ca. 500 Tonnen Kampfmittel und -teile im vergangenen Jahr fachgerecht vernichtet.

Unter den rund 340 Tonnen gefundenen Kampfmitteln und -teilen befanden sich circa 900 Stück Nahkampfmittel, 90 Stück Minen, 48.000 Stück Granaten, 500 Stück Brandbomben, 450 Stück Sprengbomben über 5 kg, 2.500 Stück Panzerabwehrraketen/Raketen, 1.500 Stück Waffen/Waffenteile sowie 330.000 Stück Handwaffenmunition. Brandenburg musste für die Kampfmittelräumung bis Ende November



*Auch bald 80 Jahren dem Ende des Zweiten Weltkrieges kämpfen Kampfmittelräumdienste mit den Altlasten des Krieges.*

*Foto: BS/Feldmann*

2024 insgesamt 12,8 Millionen Euro aufwenden – darunter fielen unter anderem 5,3 Millionen Euro für die Beseitigung von Kampfmitteln, 5,3 Millionen Euro für Personalkosten und 2,2 Millionen Euro für sonstige Sachkosten.

Brandenburgs Innenministerin Katrin Lange (SPD) erklärte zu den Zahlen: „Diese Rangliste anzuführen, ist trauriges Erbe unserer Geschichte. Über Generationen hinweg wird unser Land noch mit dieser explosiven Last leben müssen.“ Im vergangenen Jahr sei kein Mitarbeiter des KMBD bei der Arbeit verletzt worden. Noch immer stehen circa 580.000 Hektar der Fläche des Landes unter Kampfmittelverdacht.

## NEWSLETTER & PODCASTS

In den aktuellen Ausgaben unserer weiteren Newsletter und Podcasts finden Sie u. a. folgende Themen:

### NEWSLETTER

#### [Newsletter „Netzwerk Sicherheit“](#)

**16. Dezember:**

- Mit den Drogen kommt die Gewalt

#### [Newsletter „Verteidigung. Streitkräfte. Wehrtechnik“](#)

**7. Januar:**

- U.S.-Army zieht Mikroreaktoren in Betracht
- Wo das Pentagon Investitionsbedarf sieht

#### [Newsletter „Digitaler Staat und Cyber Security“](#)

**8. Januar:**

- Weiteres Verfahren gegen TikTok
- Hohe Cyber-Bedrohung in Hessen

#### [E-JOURNAL FUTURE4PUBLIC:](#)

- Hoch hinaus

### PODCASTS

#### [Podcast „Public Sector Insider“](#)

**7. Januar:**

- Wünsch dir was

#### [Podcast „Public Sector Insider Stichwort“ vom 8. Januar:](#)

- Cyber-Sicherheit auf niedersächsisch

## IT-Sicherheitstag Bayern

5. Februar 2025 | München

### VERNETZT UND SICHER

Gemeinsam für eine digitale Zukunft  
in Bayerns Verwaltung

## ZUKUNFTSKONGRESS BAYERN

06. Februar 2025 | München

### EINE DIGITALE DEKADE VIEL ERREICHT – VIEL ZU TUN!

2015–2025 – Zehn Jahre Zukunftskongress Bayern

## Der schwierige Schutz von maritimen Infrastrukturen

(BS) Ob die Nord-Stream-Pipeline oder Datenkabel auf dem Meeresgrund der Ostsee oder vor Taiwan – Vorfälle und Sabotageakte auf hoher See haben zugenommen. Frank Sill Torres, Direktor des Instituts für Maritimen Infrastrukturschutz am Deutschen Zentrum für Luft- und Raumfahrt (DLR), spricht im Interview über die Herausforderungen beim Schutz von maritimen Infrastrukturen und was das KRITIS-Dachgesetz auslöst. Das Interview führte Bennet Biskup-Klawon.

**Behörden Spiegel:** Was versteht man alles unter Kritischen maritimen Infrastrukturen?

**Frank Sill Torres:** Unter Kritischen Infrastrukturen (KRITIS) versteht man Infrastrukturen, deren Ausfall signifikante Auswirkungen auf die Versorgung der Bevölkerung haben kann. Im maritimen Bereich stehen dabei zuletzt vor allem die viel diskutierten Datenkabel im Fokus. Allerdings gilt für Deutschland, dass die für uns relevanten Datenkabel gar nicht in der Nord- oder Ostsee liegen. Unsere kritischen Datenkabel befinden sich vielmehr in anderen Regionen, wie zum Beispiel im Roten Meer, das eine zentrale Rolle für den Datenverkehr nach Asien spielt.

Weitere wichtige maritime Infrastrukturen sind Pipelines und Offshore-Windparks. Hierbei wird oft vergessen, dass es nicht nur um die Windräder selbst geht, sondern auch um die dazugehörigen Stromkabel und Transformatorstationen, die für die Einspeisung des Stroms an Land entscheidend sind. Auch Öl- und Gasförderplattformen zählen zu den Kritischen Infrastrukturen. In Deutschland gibt es jedoch nur eine Förderplattform, die sich im Wattenmeer befindet. Darüber hinaus existieren in deutschen Gewässern keine weiteren Förderstationen.

Ein weiterer zentraler Aspekt im maritimen Bereich sind die Schifffahrtswege. Viele denken hierbei zunächst an den Suezkanal. Doch für Deutschland wäre eine Blockade des Nord-Ostsee-Kanals weitaus gravierender. Die Auswirkungen eines solchen Ereignisses könnten für uns deutlich schwerwiegender sein als das, was wir bei



Frank Sill Torres ist kommissarischer Direktor des Instituts für Maritimen Infrastrukturschutz am Deutschen Zentrum für Luft- und Raumfahrt (DLR).

Foto: BS/DLR

der Blockade des Suezkanals beobachtet haben.

Schließlich gibt es noch eine oft übersehene Infrastruktur, die eine besondere Rolle spielt, da sie sowohl maritime als auch landgebundene Komponenten verbindet: Häfen. Häfen sind besonders interessant, weil sie diese beiden Welten miteinander verknüpfen und somit eine Schlüsselfunktion für den internationalen Handel und die Logistik darstellen.

**Behörden Spiegel:** Wie ist es um den Schutz von maritimen Infrastrukturen bestellt?

**Sill Torres:** Beim Schutz von Kritischen Infrastrukturen betrachtet man meistens drei Phasen oder Komponenten. In der ersten Phase geht es darum, einen Angriff durch Schutzmaßnahmen zu verlangsamen. Bei landgebundenen Infrastrukturen ist dies vergleichsweise einfach umsetzbar, etwa durch den Bau von Zäunen oder Mauern um das Schutzziel. Dabei muss jedoch klar sein, dass jede Schutzmaßnahme überwunden werden kann – es ist nur eine Frage der Zeit. Ziel ist es, den Angriff so weit wie möglich zu verzögern. Im maritimen Bereich stehen solche Maßnahmen jedoch nur einge-

schränkt zur Verfügung. Die zweite, überaus wichtige Komponente ist die Erkennung. Um einen Angriff abzuwehren und die Infrastruktur zu schützen, muss erkannt werden, dass etwas Ungewöhnliches passiert. Dies lässt sich beispielsweise durch den Einsatz von Sensorik erreichen. Die dritte Komponente ist die Intervention. Das bedeutet, dass Maßnahmen ergriffen werden, um den Angriff aktiv abzuwehren.

Im maritimen Bereich gibt es sowohl Vor- als auch Nachteile beim Schutz von Infrastrukturen: Einerseits sind die großen Distanzen im Offshore-Bereich ein Vorteil, da es in diesen Gebieten wenig Durchgangsverkehr gibt. Dies erleichtert die Erkennung von Anomalien. So können beispielsweise Satellitenbilder genutzt werden, um maritime Infrastrukturen zu überwachen. Der Nachteil hierbei ist jedoch, dass Satelliten nicht konstant Bilder liefern und zeitliche Lücken in der Überwachung entstehen können.

Ein weiteres wichtiges Hilfsmittel im maritimen Bereich ist das Automatische Identifikationssystem (AIS).

Fortsetzung auf Seite 4

Fortsetzung von Seite 3

Dieses System müssen Schiffe ab einer bestimmten Größe aktivieren, damit sie für andere sichtbar sind. Vereinfacht gesagt werden dabei die GPS-Koordinaten mit anderen Schiffen und Überwachungsstellen geteilt. Das Problem ist jedoch, dass das AIS leicht manipuliert oder deaktiviert werden kann. Solche Manipulationen oder Abschaltungen können Hinweise auf potenzielle Bedrohungen sein.

Nach den Anschlägen auf das World Trade Center wurden mit dem sogenannten ISPS-Code (International Ship and Port Facility Security Code) verbindliche Anforderungen definiert, um ein bestimmtes Sicherheitsniveau in der Schifffahrt einzuhalten. Allerdings deckt der ISPS-Code nicht alle Bedrohungen ab, wie etwa Angriffe durch Drohnen oder groß angelegte Cyber-Angriffe.

**Behörden Spiegel:** *Diese Maßnahmen dienen jetzt der Identifikation und Erkennung. Wie sieht es mit der Intervention aus?*

**Sill Torres:** Hier kommt der Aspekt der weiten Distanzen wieder. Hauptverantwortlich ist da die Bundespolizei. Die Marine kann unterstützen, ist aber nicht zuständig. Nach dem Erkennen einer Gefahr braucht es eine zeitnahe Intervention. Im maritimen Bereich kann das aber dauern. Bis ein Polizeiboot oder auch ein Hubschrauber vor Ort ist, kann es eine halbe Stunde bis zu einigen Stunden dauern. Diese Verzögerung ist kritisch, da währenddessen wertvolle Zeit

verloren geht. Um diesem Problem entgegenzuwirken, ist es entscheidend, Gefahren frühzeitig zu antizipieren. Je früher eine potenzielle Bedrohung erkannt wird, desto schneller kann reagiert werden. Genau an dieser Stelle setzt unsere Arbeit beim DLR an: Wir versuchen, diese Reaktionslücke zu verkleinern. Mithilfe der Auswertung von Daten und der Identifikation von Anomalien im Verhalten – beispielsweise wenn ein Schiff in der Nähe von Datenkabeln sich in einer Art bewegt, die darauf schließen lässt, dass es einen Anker hinter sich herziehen könnte, oder es sich ungewöhnlich in der Nähe von Pipelines bewegt – können wir frühzeitig Warnsignale erkennen und Maßnahmen einleiten.

Es gibt eine schöne Aussage: Was wäre gewesen, hätte sich ein Polizeiboot in der Nähe aufgehalten, als die Nord-Stream-Pipeline gesprengt wurde? Schließlich wollen kriminelle oder staatliche Akteure dabei nicht beobachtet werden. Auch ein Geheimhalten der genauen Lage der Datenkabel hilft dabei nicht weiter, diese sind in Seekarten verzeichnet. Aber diese ganze Kette aus Überwachung und Intervention bleibt weiterhin schwierig.

**Behörden Spiegel:** *Welche Vorschriften gibt es zur Sicherung der maritimen Infrastruktur? Und wie bewerten Sie den Gesetzesentwurf zum KRITIS-Dachgesetz?*

**Sill Torres:** Im maritimen Bereich gibt es, abgesehen vom ISPS-Code, der eine solide Grundlage bietet, derzeit keine konkreten Anforderungen. Das KRITIS-Dachgesetz

stößt zunächst lediglich eine grundlegende Diskussion an, dass Handlungsbedarf besteht. Allerdings regelt das Gesetz bislang nicht, welche spezifischen Vorkehrungen die Betreiber treffen müssen. Die Betreiber müssen sich zusammen mit den Behörden Gedanken machen. Denn das Dachgesetz definiert zunächst einmal nur, wer es kontrollieren darf. Der nächste Schritt wird deshalb spannend. Im nächsten Schritt soll dann definiert werden, welche konkreten Anforderungen die Betreiber erfüllen müssen. Die Betreiber sind jetzt in einer unkomfortablen Situation. In unseren Gesprächen mit den Betreibern wird deutlich, dass ihnen die Notwendigkeit des Schutzes ihrer Anlagen bewusst ist. Allerdings ist dies mit erheblichen Kosten verbunden.

Dies wird vor allem durch die momentane geopolitische Lage nicht einfacher, wenn es um hybride Kriegsführung geht. Zudem geht es den Betreibern auch darum, was die Mitbewerber machen. Das heißt, die Betreiber wollen Rechtssicherheit und ein konkretes Sachgesetz, das klare Vorgaben macht.

Dann kommt die große Diskussion dazu: Wo ist der Unterschied zwischen Aufgaben eines Betreibers und des Staates? Es bestehen etwa unterschiedliche Auffassungen über die Verantwortlichkeiten im Zusammenhang mit Staatsterrorismus.



Die vollständige Fassung des Interviews lesen Sie in der aktuellen Behörden Spiegel-Ausgabe auf Seite 33.

FUTURE  PUBLIC

Der Newsletter mit Zukunft.

 SUBSCRIBE

## Die Wahrscheinlichkeit ist nicht Null

(BS/Prof. Frank Reininghaus) Die Liste der Angriffe auf die Wasserversorgung ist lang und hat bereits vor 2.500 Jahren die ersten Erwähnungen gefunden. Bereits im Jahr 430 v. Chr. berichtete der Grieche Thukydides in seinem Werk über den Peloponnesischen Krieg, dass „die Peloponnesier“ verdächtigt worden waren, „Gift in die Zisternen“ geworfen zu haben. Die Wahrscheinlichkeit, dass es zu einem derartigen Anschlag in Deutschland kommen kann, ist nicht nahe Null und schon gar nicht gleich Null. Daher darf und kann diese Option eines terroristischen (oder auch anderweitig motivierten) Angriffs nicht außer Acht gelassen werden,

Der Wissenschaftliche Dienst des Deutschen Bundestages notiert in einer Ausarbeitung über Biowaffen im Jahr 2002, dass schon „im Mittelalter (...) Brunnen mit Leichen vergiftet oder Städte durch pestifizierte Tierkadaver oder Pestopfer ver-seucht“ wurden.

Operation Alberich, bei der Räumung besetzter Teile Nordostfrankreichs durch deutsche Truppen; der russisch-finnische Winterkrieg 1939–1940, die Vergiftung von Brunnen durch Tierkadaver und Kot; Burkina Faso, 2022: die Sabotage von Wasseranlagen und die gezielte Verunreinigung von Wasserstellen; das kanadische Wassereservoir in Rafah im südlichen Gazastreifen, im Juli 2024 gezielt von den Israelis zerstört.

Ein Beispiel eines Landwirts aus dem Raum Ravensburg aus dem November 2005 zeigt auch hier das Potenzial. Er hatte zwei geöffnete Kanister Pflanzenschutzmittel an der Wasserentnahmestelle im westlichen Bodensee bei Sipplingen versenkt; sein Motiv: „Rache an der Justiz“.

### Kunden als Sicherheitsmechanismus

Die mehrstufigen Sicherheitsmechanismen, die von den Wasserversorgungsunternehmen von Flensburg bis Garmisch und von Aachen bis Cottbus eingesetzt werden, sind sicherlich eine geeignete Maßnahme, um dieses Risiko einzuschränken. Wie sehen nun die derzeitigen Schutzmechanismen aus?

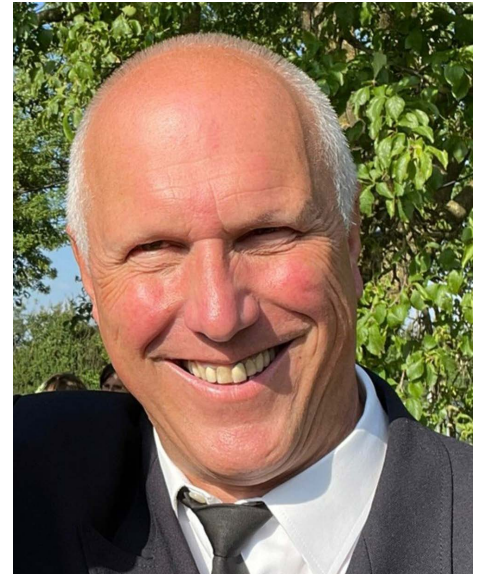
In der Regel findet die Kontrolle der Trinkwasserqualität nach Einbringung ins Versor-

gungsnetz in einem meist mehrwöchigen Zyklus statt: An designierten Probeentnahmestellen (bspw. in Schulen, Kindergärten, Krankenhäusern, Behörden) wird in regelmäßigen Abständen eine Probe gezogen und dem angeschlossenen Labor für eine umfassende Analyse zugestellt.

Darüber hinaus setzen Wasserversorger auf ihre aufmerksame, kritische Kundschaft: Sollte das gelieferte Trinkwasser Veränderungen in Farbe, Geruch und/oder Geschmack aufweisen, so melden sich die Verbraucher im Regelfall sehr schnell bei ihrem Wasserversorgungsunternehmen. Hier findet sich jedoch letztlich die Schwachstelle im System, denn wenn es einer (wie auch immer gearteten) Gruppierung gelingen würde, nach Ausgang aus dem Wasserwerk ein farb-, geschmack- und geruchloses Gift in ausreichender Menge in das Wasserversorgungssystem einzubringen, so könnten die Gemeinde, der Stadtteil, die Region dadurch beeinträchtigt werden, ohne dass dies zeitnah dem Wasserversorger und den Kunden zur Kenntnis gelangen würde.

### Mit genug Wissen ist Sabotage möglich

Die Schwachstellen sind die Zugänge zu den Wassernetzen sowie die Lagerungsstätten des aufbereiteten Trinkwassers. Physische Sicherheit (der Trinkwasserbrunnen und) der Trinkwasserhochbehälter wird in Deutschland in vielen Fällen durch eine geeignete Palette von Maßnahmen generiert. Hierzu gehören bspw. einfache Zäune, vergitterte Fenster, Zugangskontrollen in Form von Codekarten oder Schließsystemen, Videoüberwachung, Bewegungsmeldern u.v.a.m. Diese Maßnahmen reichen generell aus, da in jedem System genügend Redundanzen in Form weiterer Lagerstätten vorhanden sind. Jedoch wäre mit nur wenigen wasserbau- und -versorgungstechnischen Grundkenntnissen eine Manipulation / Sabotage durchaus realisierbar; dies könnte eine Unterbrechung / physische Zerstörung der Anlagen ebenso beinhalten wie die gezielte Einbringung einer kontaminierenden Substanz. Die Folge des ersteren wäre ein Versorgungsengpass (der jedoch sofort von der Bevölkerung bemerkt wer-



Prof. Frank Reininghaus ist Non-Resident Research Fellow am Institut für Friedensforschung und Sicherheitspolitik sowie Fregatkapitän d.R.

Foto: BS/pirvat

den würde), weiteres würde – je nach Substanz – möglicherweise zu einer unbemerkten und schleichenden Kontamination der Verbraucher im betroffenen Gebiet führen.

In den vergangenen Jahren wurden die technischen Möglichkeiten zur permanenten Überwachung der Wasserqualität breitflächig erforscht und teils zur Serienreife entwickelt. So basiert eines der Systeme, welches auf der SafeWater-Konferenz in Zürich im November 2016 vorgestellt wurde, auf dem Vorkoster-Prinzip: biologische Kleinstlebewesen, die in einem Bypass der Trinkwasserleitung ausgesetzt werden, werden per Kamera überwacht, um signifikante Veränderungen ihrer Fluoreszenz bei toxischer Schädigung zu beobachten.

Seit Sommer 2018 kommt ähnliches System bei den Berliner Wasserwerken zum Einsatz: Hier werden Bachflohkrebse als „natürliches Frühwarnsystem“ eingesetzt. Die Krebse werden zu einer Kohorte von je acht Krebsen in einem Kammersystem in einen Wasser-Bypass eingesetzt und reagieren, sobald das Wasser in irgendeiner Weise verschmutzt ist.

Fortsetzung auf Seite 6

Fortsetzung von Seite 5

Diese Tiere reagieren bspw. auf Kupfer und Blei, aber auch auf andere Schad- und Schwebstoffe. Über die installierte Sensorik werden die Veränderungen des Verhaltens der Krebstiere an die Zentrale gemeldet, in der dann die Quelle der Verunreinigung ermittelt und entsprechend vom Netz getrennt wird.

Weitere Systeme für ständige Wasserkontrollen sind bspw. im Wasserwerk in Berlin-Friedrichshagen installiert, wo ein Dutzend Moderlieschen (silberfarbene, bis zu zehn Zentimeter lange Fische) in einem Aquarium leben, oder Coca-Cola in Knetzgau, wo mit Fischen die Qualität des gereinigten

Abwassers getestet wird. Es ist das einzige Werk des Getränkeherstellers in Deutschland, das eine eigene Kläranlage betreibt.

#### Reicht alles aus?

Als Fazit ist festzuhalten, dass die Möglichkeit, Trinkwasserversorgungssysteme zu manipulieren, zu sabotieren oder zu kontaminieren, durchaus gegeben ist. Bei einem malevolenten Eingriff im Bereich des Rohwassers wird möglicherweise im Bereich der Gewinnung, spätestens jedoch im Wasserwerk selbst die Kontamination festgestellt und entsprechende Gegenmaßnahmen ergriffen werden. Für einen malevolenten Eingriff nach Austritt aus der Produktionsstätte (dem Wasserwerk),

wenn sich das vermeintlich unbelastete Trinkwasser im Verteilungsnetz befindet, lassen sich verschiedene Szenarien kreieren, bei denen dieser Eingriff zum Erfolg führen könnte; dies gilt insbesondere für nur einfach gesicherte, oberirdische Lagerstätten, Pumpstationen, etc. Obwohl es in der Vergangenheit nur sehr wenige Versuche gegeben hat, über die Kontamination des Trinkwassers einen terroristischen Akt oder Sabotageakt durchzuführen, bedeutet dies nicht, dass diese Bedrohung gänzlich negiert werden kann.

Es wird empfohlen, die bestehenden Sicherheitsmaßnahmen und Sicherheitsmechanismen einer kritischen Überprüfung zu unterziehen.

## Neue Lehrleitstelle übernommen

(BS) Die neue Lehrleitstelle des Niedersächsischen Landesamtes für Brand- und Katastrophenschutz (NLBK) wurde in Betrieb genommen. Die Lehrleitstelle geht damit offiziell vom Bauherren, dem Staatlichen Baumanagement Lüneburger Heide, in die Hände des Niedersächsischen Landesamtes für Brand- und Katastrophenschutz (NLBK) als Nutzer über.

Die neue Lehrleitstelle dient der Aus- und Fortbildung von Leitstellenbediensteten für die Feuerwehren, den Rettungsdienst, den Mitarbeitenden in Katastrophenschutzstäben und den Technischen Einsatzleitungen in Niedersachsen. Die neue Lehrleitstelle ist Teil einer umfassenden Baumaßnahme auf

der ehemaligen Freiherr-von-Fritsch-Kaserne in Celle-Scheuen. In rund drei Jahren Bauzeit wurde ein bestehendes Gebäude auf dem Gelände des Technik- und Trainingszentrums des NLBK zur Lehrleitstelle umgebaut. Die Gesamtkosten des Bauprojekts belaufen sich auf rund 8,8 Millionen Euro.

#### Lehrleitstelle als Reserve für den besonderen Ernstfall

„Die neue Lehrleitstelle war dringend erforderlich, deshalb freut es mich besonders, heute an der offiziellen Schlüsselübergabe teilnehmen zu dürfen. Die Mitarbeiterinnen und Mitarbeiter in den Leitstellen

stellen sich regelmäßig besonderen Herausforderungen – von deutlich erhöhten Notrufgeschehen bis hin zu Unwetter- und Katastrophenlagen. Genau diese Stress- und Belastungssituationen können hier simuliert und trainiert werden“, erklärte die niedersächsische Innenministerin Daniela Behrens (SPD). In besonderen Einsatzlagen, wenn die vorhandenen Kapazitäten der sich im Regelbetrieb befindenden Leitstellen nicht ausreichen, könne die neue Lehrleitstelle in Zukunft auch für reale Einsätze der Polizei, des Katastrophenschutzes sowie die Autorisierte Stelle Digitalfunk Niedersachsen (ASDN) genutzt werden, so die Ministerin weiter.



#cyberNDS

cyber\_sicherheits\_tag  
niedersachsen

30. Januar 2025 // Hannover  
Designhotel + Congresscentrum Wienecke XI.



EUROPEAN POLICE CONGRESS

**NEUER  
TERMIN****20.–21. MAI  
2025** **CityCube Berlin**[www.european-police.eu](http://www.european-police.eu)**Impressum**

Herausgeberin und Chefredakteurin von „Behörden Spiegel Newsletter Rettung. Feuer. Katastrophe.“: Dr. Eva-Charlotte Proll.

Redaktionelle Leitung: Bennet Biskup-Klawon. Redaktion: Jonas Brandstetter, Christian Brecht, Guido Gehrt, Dr. Barbara Held, Ann Kathrin Herweg, Mirjam Klinger, Scarlett Lüsser, Lars Mahnke, Sven Rudolf, Paul Schubert, Anna Ströbele, Anne Mareile Walter. Online-Redaktion: Tanja Klement. Redaktionsassistentin: Kerstin Bauer (Berlin); Produktionsassistentin: Wiebke Werner.

ProPress Verlagsgesellschaft mbH, Friedrich-Ebert-Allee 57, 53113 Bonn, Telefon: 0049-228-970970

E-Mail: [redaktion@behoerderspiegel.de](mailto:redaktion@behoerderspiegel.de); [www.behoerden-spiegel.de](http://www.behoerden-spiegel.de). Registergericht: AG Bonn HRB 3815. UST-Ident.-Nr.:DE 122275444 - Geschäftsführer: Dr. Fabian Rusch. Herausgeber- und Programmbeirat: Uwe Proll (Vorsitz). Der Verlag hält auch die Nutzungsrechte für die Inhalte von „Behörden Spiegel Newsletter Rettung. Feuer. Katastrophe.“ Die Rechte an Marken und Warenzeichen liegen bei den genannten Herstellern. Bei direkten oder indirekten Verweisen auf fremde Internetseiten („Links“), die außerhalb des Verantwortungsbereiches des Herausgebers liegen, kann keine Haftung für die Richtigkeit oder Gesetzmäßigkeit der dort publizierten Inhalte gegeben werden.