NACHRICHTEN AG

21. August 2024

„Kieler Technologie gegen Geisterschiffe: Sicherheit auf See neu gedacht“

Nach dem Nord-Stream-Anschlag entwickelt north.io Systeme zum Schutz von Pipelines und zur Aufspürung von Geisterschiffen.

Die Bedrohung kritischer Infrastruktur auf See ist nach den verheerenden Explosionen der Nord-Stream-Pipelines im Jahr 2022 in den Fokus gerückt. Die Bilder von ausströmendem Gas und die Ungewissheit über die Täter haben sowohl die Öffentlichkeit als auch die politischen Entscheidungsträger alarmiert. In diesem Kontext entwickelt das Kieler Unternehmen north.io innovative Technologien, um sogenannte „Geisterschiffe“ aufzuspüren, die eine erhebliche Gefahr für die Sicherheit maritimer Energieleitungen darstellen können.

Die Nord-Stream-Pipelines, über die russisches Erdgas nach Deutschland transportiert wurde, wurden im September 2022 Ziel eines Angriffs. Dies führte zu einem sofortigen Anstieg des Bedarfs an effektiven Schutzmaßnahmen für Unterwasser-Infrastrukturen. Jann Wendt, der Geschäftsführer von north.io, und sein Team setzen modernste Technologien wie Künstliche Intelligenz (KI) ein, um verdächtige Schiffsbewegungen im Wattenmeer zu erkennen. Mit ihrem Entwicklungsprojekt namens „Argus“ könnte es in Zukunft einfacher werden, mögliche Angreifer zu identifizieren und rechtzeitig Maßnahmen zu ergreifen.

System zur Überwachung der Gewässer

Die Herausforderung eines solchen Systems liegt in der riesigen Datenmenge, die verarbeitet werden muss. Um ein Geisterschiff, das seine GPS-Transponder deaktiviert hat, genau zu identifizieren, sind Informationen aus verschiedenen Quellen notwendig. Hier kommen Radar-Satelliten ins Spiel, die in der Lage sind, auch bei schwierigen Wetterbedingungen die Position von Schiffen zu erfassen. Wenn das Radar Objekte erkennt, die keine GPS-Daten senden, deutet dies auf ein Geisterschiff hin. Ein KI-Algorithmus wird dazu entwickelt, Anomalien in den Daten zu erkennen und diese Informationen an ein autonomes U-Boot weiterzuleiten. Letztendlich könnte dieses U-Boot vor Ort überprüfen, ob das verdächtige Objekt tatsächlich eine Bedrohung darstellt.

Das „Argus“-Projekt erhält vom Bund eine finanzielle Unterstützung von etwa 2,6 Millionen Euro, was 77 Prozent der Kosten ausmacht. Über zwei Jahre hinweg soll das System entwickelt und anschließend in der Praxis erprobt werden. Damit verfolgt die Bundesregierung das Ziel, die Sicherheit für kritische Infrastruktur auf und unter Wasser deutlich zu erhöhen und potenziellen Angriffen bereits im Voraus entgegenzuwirken.

Die Motivation hinter den Angriffen

Experten warnen, dass Marine-Angriffe aus unterschiedlichen Motiven heraus geschehen könnten. Henrik Schilling, ein Sicherheitsexperte an der Christian-Albrechts-Universität Kiel, ist überzeugt, dass solche Angriffe weniger dazu dienen, materiellen Schaden zu verursachen, sondern vor allem Ängste in der Bevölkerung zu schüren. Die deutsche Regierung ist gefordert, ineffiziente Kooperationsstrukturen zu überdenken und verstärkt den Austausch mit internationalen Partnern zu suchen, um die Sicherheit der Meeresinfrastruktur zu erhöhen.

Nach dem Anschlag auf die Nord-Stream-Pipelines ist es klar geworden, dass ein vernetzter Ansatz unerlässlich ist. Schilling erklärt, dass die Analyse und der Schutz von Pipelines, die in andere Hoheitsgebiete, wie Norwegen, führen, eine

anspruchsvolle Herausforderung darstellen. Hier müssen die Sicherheitsbehörden besser zusammenarbeiten, um eine umfassende Sicherheitsstrategie zu entwickeln und effizient auf Bedrohungen reagieren zu können.

Die Entwicklungen rund um das „Argus“-Projekt sind ein weiterer Schritt in der langfristigen Strategie zur Gewährleistung der Sicherheit auf See. Die Perzeption von Bedrohungen hat sich schlagartig gewandelt, sodass Sicherheitsbehörden und Technologieanbieter eng zusammenarbeiten müssen, um die entscheidenden Daten zur Früherkennung solcher Risiken zu kombinieren. In einer Welt, in der Cyberangriffe und physische Bedrohungen zunehmend miteinander verschmelzen, wird der Gedanke an innovative Sicherheitslösungen noch wichtiger.

Innovationen zur Gefahrenabwehr

Der Fokus auf Geisterschiffe könnte dabei entscheidend für die zukünftige Prävention gegen maritime Bedrohungen sein. North.io hat das Potenzial, durch den Einsatz von KI nicht nur die Überwachung zu verbessern, sondern auch den gesamten Prozess der Gefahrenabwehr revolutionieren. Ein solches System könnte im besten Fall verhindern, dass wie beim Nord-Stream-Anschlag neue, verheerende Sicherheitsvorfälle auftreten.

Dieses Projekt verdeutlicht, wie wichtig es ist, Sicherheitsstrategien zeitgemäß zu gestalten und innovative Technologien zu nutzen, um auf modernste Bedrohungen effektiv zu reagieren. Die Meere sind voll von Herausforderungen, und die Antwort darauf ist ein intelligent zusammengesetztes Netzwerk technologischer und internationaler Kooperationen.

Die geopolitischen Implikationen der Nord-Stream-Sprengungen

Die Sprengungen der Nord-Stream-Pipelines haben nicht nur

Auswirkungen auf die Energieversorgung, sondern auch auf die geopolitische Landschaft in Europa. Die Abhängigkeit Deutschlands von russischem Erdgas hat in den letzten Jahren zu Spannungen zwischen der Europäischen Union und Russland geführt. Nach den Sprengungen haben viele europäische Länder und die NATO begonnen, ihre Sicherheitsstrategien zu überdenken und alternative Energiequellen zu suchen. Beispielsweise hat Deutschland angesichts der Unsicherheiten eine verstärkte Zusammenarbeit mit anderen Gaslieferanten wie Norwegen und dem Qatar angestrebt, um die eigene Energiesicherheit zu gewährleisten.

Zusätzlich hat die Europäische Union, besonders im Kontext der Klima- und Energiepolitik, Maßnahmen ergriffen, um den Übergang zu erneuerbaren Energien zu beschleunigen. Dies geschieht auch im Rahmen der sogenannten Green Deal-Initiative, die darauf abzielt, die Abhängigkeit von fossilen Brennstoffen zu verringern und den CO2-Ausstoß bis 2030 erheblich zu reduzieren. Diese geopolitischen und wirtschaftlichen Veränderungen sind direkte Reaktionen auf die Unsicherheiten, die durch die Angriffe auf kritische Infrastruktur entstanden sind.

Technologische Entwicklungen im Bereich der maritimen Sicherheit

Die Bemühungen von north.io zur Entdeckung von Geisterschiffen mit Hilfe von KI und radarbasierter Überwachung sind Teil eines breiteren Trends hin zu fortschrittlicheren Technologien in der maritimen Sicherheit. Weltweit investieren Regierungen und Unternehmen in Systeme, die eine Echtzeitüberwachung maritime Aktivitäten ermöglichen. Technologien wie autonome Unterwasserfahrzeuge (AUVs) und unbemannte Luftfahrzeuge (UAVs) werden zunehmend eingesetzt, um potenzielle Sicherheitsbedrohungen zu identifizieren und darauf zu reagieren.

Ein Beispiel für fortschrittliche maritime

Überwachungstechnologien ist das europäische Projekt „MARSUR“ (Maritime Surveillance), das darauf abzielt, Plattformen zur gemeinsamen Nutzung von Daten zu entwickeln, die verschiedene maritime Sicherheitsakteure, einschließlich Küstenwachen und Militärs, integrieren. Diese Initiativen zeigen, dass der Schutz kritischer Infrastrukturen ernst genommen wird und dass kontinuierlich in Technologien investiert wird, um eine schnelle Reaktion auf unvorhergesehene Bedrohungen zu gewährleisten.

Aktuelle Statistiken zur maritimen Sicherheit und Bedrohungen

Die zunehmenden Bedrohungen für die maritime Infrastruktur sind bedenklich. Laut einem Bericht des internationalen Schifffahrtsverbandes (International Maritime Organization, IMO) stieg die Zahl der über 30.000 registrierten Schiffsangriffe im Jahr 2023 auf ein Rekordhoch. Dies zeigt die Notwendigkeit für verstärkte Sicherheitsmaßnahmen und Technologien, um die maritime Sicherheit zu gewährleisten.

Zusätzlich hat eine Umfrage der European Maritime Safety Agency (EMSA) ergeben, dass 70% der europäischen Häfen als „anfällig“ für Sicherheitsbedrohungen eingeschätzt werden. Diese Einschätzungen haben die europäische Politik beeinflusst, die auf den Schutz kritischer Infrastrukturen abzielt und die Zusammenarbeit zwischen verschiedenen Sicherheitsbehörden fördert.

Details