Sicherheit kritischer Infrastrukturen im Bereich grüner Energie: Maßnahmen zur Bekämpfung von Sabotage und Cyberangriffen.

Die Art der globalen Energie verlagert sich hin zur Nachhaltigkeit, wobei erneuerbare Energien als alternative Energiequelle dienen, um den Klimawandel zu mildern. Dennoch bringt diese Veränderung Schwächen wie das Risiko von Sabotage und Cyberangriffen in der Infrastruktur des grünen Sektors mit sich, was zu Stromausfällen, wirtschaftlichen Störungen und Umweltkatastrophen führen kann. Dieser Artikel untersucht die Herausforderungen im Bereich der grünen Energiewirtschaft in Bezug auf Sabotage und Cyberangriffe auf ihre kritische Infrastruktur [1]. Grüne Energie wird derzeit in das Stromnetz integriert, doch diese Anlagen werden zunehmend zu potenziellen Zielen für Angreifer. Der Artikel untersucht die spezifischen Schwachstellen und Risiken von grünen Anlagen sowie die erforderlichen Sicherheitsmaßnahmen, um sie vor möglichen Angriffen zu schützen. Durch die Analyse bestehender Sicherheitsstandards und -richtlinien werden bewährte Verfahren aufgezeigt, die im Bereich der grünen Energiewirtschaft angewendet werden können. Anhand von Beispielen wie den Cyberangriffen in Israel und der Ukraine werden die mögliche Relevanz und die Konsequenzen des Themas verdeutlicht. Abschließend werden die besten Ansätze für Krisenmanagement und die Reaktion auf Zwischenfälle erörtert, um eine effiziente Reaktion auf Sabotage und Cyberangriffe zu gewährleisten.

Lars Arnold Ritter und Marco Barenkamp

Wirtschaftsinformatik & Management
https://doi.org/10.1365/s35764-024-00527-0
Angenommen: 30. Mai 2024

Published online: 23 July 2024

Die Welt setzt vermehrt auf grüne Energiequellen, was bedeutet, dass sich auch die Infrastrukturdynamik im Energiesektor ändert und einen bedeutenden Schritt im Kampf gegen den Klimawandel darstellt [2]. Der Kampf gegen den Klimawandel hat angesichts der ländlich-urbanen Migration eine besondere Bedeutung erlangt. Diese Übergänge haben zu einem steigenden Energiebedarf in städtischen Gebieten geführt. Eine Studie, die in Städten über die letzten 30 Jahre durchgeführt wurde, hat gezeigt, dass die urbane Bevölkerung stark zunimmt und dadurch Druck auf die Energieversorgung ausgeübt wird [3]. Die Umstellung auf nachhaltige Energie zielt darauf ab, den Verbrauch von Ressourcen, Umweltauswirkungen und die übermäßige Abhängigkeit von Energie zur Stimulierung des wirtschaftlichen Wachstums zu reduzieren. Derzeit wird der Energiesektor hauptsächlich durch die starke Nutzung fossiler Brennstoffe belastet. Die übermäßige Ausbeutung natürlicher Ressourcen zur Sicherstellung ausreichender fossiler Brennstoffe ist langfristig schädlich für die Energieziele von Staaten und unterstreicht die Bedeutung des Übergangs zu nachhaltiger Energie als Alternative. Diese Umstellung ist von entscheidender Bedeutung für die Bemühungen um Nachhaltigkeit, steht jedoch der Gefahr von Störungen durch mögliche Sabotage und Cyberangriffe gegenüber. Dies unterstreicht die Notwendigkeit einer sicheren, lebenswichtigen Infrastruktur im Bereich der grünen Energie. Die kritische Infrastruktur in diesem Zusammenhang umfasst die Erzeugung, Verteilung und Übertragung von Strom, was für das Funktionieren der Gesellschaft von entscheidender Bedeutung ist. Da die meisten dieser Anlagen digitalisiert und weitverbreitet sind, sind sie anfällig für Risiken und verdeutlichen die Herausforderungen im Bereich der Cybersicherheit [4].

Die Smart-Grid-Technologie unterstützt den Paradigmenwechsel im Energiesektor. Diese Technologie bietet Ländern beispiellose Möglichkeiten, ihre Netzwerke zu modernisieren, was zu intelligenten, reaktionsschnellen und kooperativen Stromerzeugungs-, -übertragungs- und -verteilungssystemen führt. Die Betriebsmodi innerhalb des Smart-Grid-Systems sind netzgebunden (grid-tied) und eigenständig (standalone) [5]. Die Autarkieleistung des intelligenten Stromnetzes findet Anwendung im eigenständigen Modus, indem sie die Stromversorgung in abgelegenen Gebieten mithilfe von grünen Energiequellen wie Wind und Sonne zusammen mit Energiespeicherung verwaltet. Im netzgebundenen Modus ist das intelligente Stromnetz mit dem Hauptstromnetz verbunden, was einen bidirektionalen Stromfluss ermöglicht und die Stabilität durch den Export und Import von Strom unterstützt. Die Wahl zwischen diesen beiden Modi hängt von den Energiezielen, der Infrastruktur und dem Standort ab. Das intelligente Stromnetz unterstützt ein bidirektionales Automatisierungssystem, das jedoch aufgrund seiner vielfältigen Funktionalitäten anfällig für Cyberangriffe und Sabotage ist. Es ermöglicht Anwendungen, die die Energieeinschränkung sowie eine effiziente Energieintegration und -speicherung aufrechterhalten. Neben externen Bedrohungen sind diese Netze auch Insidersabotage und menschlichen Faktoren ausgesetzt. Soziale Manipulation, Schulungen und Sensibilisierungsprogramme spielen ebenfalls eine Rolle bei der Resilienz von intelligenten Stromnetzen gegenüber Cyberangriffen und Sabotage. Reale Beispiele belegen das Vorhandensein von Cyberangriffen und Sabotage im Bereich der nachhaltigen Energieindustrie. Die Integration von Künstlichen-Intelligenz-Techniken wie Deep Learning (DL), genetischen Algorithmen (GA), maschinellem Lernen (ML) und Schwarmintelligenz

Mag. Lars Arnold Ritter MBA[1] (✉)
ist ein erfahrener Experte im Bereich Cybersicherheit mit einem besonderen Fokus auf die Implementierung von Informationssicherheitsmanagementsystemen (ISMS) und Business-Continuity-Management-Systemen (BCMS) im Consulting. Er ist zudem als Dozent an mehreren Hochschulen tätig, wo er den Bereich des wissenschaftlichen Arbeitens lehrt. Seine Forschungsinteressen konzentrieren sich auf das zukunftsweisende Thema Green Energetics. Er kombiniert praxisorientiertes Consulting mit akademischer Expertise und trägt damit maßgeblich zur Entwicklung und Implementierung sicherheitsrelevanter und nachhaltiger Systeme bei.
lars.ritter@epubg.eu

Prof. Dr. Marco Barenkamp[2]
ist promovierter Wirtschaftsinformatiker und studierter Wirtschaftsjurist. Als Gründer und ehemaliger Vorstandsvorsitzender der LMIS AG mit Hauptsitz in Osnabrück ist er nunmehr im Aufsichtsrat der Gesellschaft tätig. Er wurde 2022 in die Bundesfachkommission für Künstliche Intelligenz und Wertschöpfung 4.0 im Wirtschaftsrat Deutschland berufen, ist Mitglied des Herausgeberbeirats der Fachzeitschrift ‚Wirtschaftsinformatik und Management' und unterstützt als Vorsitzender des wissenschaftlichen Beirats der Studiengesellschaft für Künstliche Intelligenz die Förderung des öffentlichen Diskurses rund um gesellschaftliche Fragestellungen der KI. An der Schnittstelle von Politik und Wirtschaft engagiert er sich aktiv bundespolitisch für die Etablierung zukunftsorientierter Rahmenbedingungen für KI in Deutschland und der Europäischen Union. Er agiert auf nationalen und internationalen Kongressen als Referent und Moderator und publiziert regelmäßig zu wissenschaftlichen und unternehmerisch-praktischen Fragestellungen aus dem Bereich der KI. Er forscht und lehrt an verschiedenen Hochschulen im In- und Ausland im Bereich der Künstlichen Intelligenz.
Marco.Barenkamp@LMIS.de

[1]*European Polytechnical University, Pernik, Bulgarien*

[2]*Hochschule Osnabrück, Osnabrück, Deutschland*

Zusammenfassung

- Schwachstellen:
  Grüne Energieinfrastruktur ist anfällig für Cyber- und physische Angriffe.
- Richtlinien:
  Es braucht angepasste Sicherheitsstandards für erneuerbare Energien.
- Krisenmanagement:
  Internationale Zusammenarbeit und Übungen sind entscheidend.

eröffnet weitere Möglichkeiten für Cyberangriffe und Sabotageversuche von intelligenten Stromnetzen (**Abb. 1**).

Dieser Artikel zielt darauf ab, eine dreifache These zu präsentieren, die Sicherheitslücken im Bereich erneuerbarer Energien aufdeckt. Zunächst wird in der ersten These die Analyse der Schwachstellen bei Cyber- und physischen Bedrohungen vorgenommen, die mit der Exposition oder Sichtbarkeit der kritischen Infrastruktur im grünen Sektor verbunden sind. Die zweite These untersucht die aktuellen Sicherheitsrichtlinien und -standards und prüft, ob diese Richtlinien ausreichenden Schutz für die grüne Energieinfrastruktur bieten, um potenzielle Angriffe abzuwehren. Abschließend wird die Bedeutung von Best Practices in der grünen Energie hervorgehoben, um den aufgezeigten Lücken und Schwachstellen in den Richtlinien entgegenzuwirken, die die kritische Infrastruktur im Bereich der grünen Energie beeinträchtigen könnten [6]. Die vorliegenden Ansätze umfassen die Integration technologischer Innovationen, Krisenmanagementstrategien und politischer Interventionen, um die Risiken von Cyberangriffen und Sabotage zu mindern. Auf diese Weise wird ein robustes und umfassendes Konzept für Cybersicherheit bereitgestellt [7].

Diese Einführung legt den Grundstein für eine detaillierte Untersuchung der These, die durch ein umfassendes theoretisches Rahmenwerk gestützt wird, das sich auf Cybersecurity-Doktrinen und Risikomanagementprinzipien stützt. Durch diese Perspektiven zielt der Artikel darauf ab, wichtige Erkenntnisse und logische Lösungen gegen aufkommende Bedrohungen im Bereich der grünen Energie zu liefern.

Die Komplexität kritischer Infrastruktur

Die kritische Infrastruktur bezieht sich auf die kollektiven Netzwerke und Systeme, die von einer Regierung als wichtig für die Sicherheit der Bevölkerung und ihr Funktionieren angesehen werden [8, 9]. Die kritische Infrastruktur im Bereich

der grünen Energie, wie beispielsweise die Produktion von Elektrizität, die Stromerzeugung und die Wasseraufbereitung, sind miteinander verbunden, um das Energieversorgungsnetz zu bilden [10, 11]. Obwohl das grüne Energieversorgungsnetz der Öffentlichkeit zugutekommt, ist es anfällig für Terroristen und Cyberangriffe. Diese kritische Infrastruktur ist komplex und stützt sich auf ein Netzwerk verbundener Geräte. Zuverlässige Elektrizität ist entscheidend für die Annehmlichkeiten der Moderne und wichtig für die Sicherheit und Wirtschaft eines Landes [12, 13]. Dies hat Länder dazu veranlasst, so weit zu gehen, in grüne Energie zu investieren, um den Elektrizitätsbedarf ihrer Bevölkerung zu decken [14–16]. In den letzten Jahren haben Stromnetze und andere kritische Infrastrukturen isoliert voneinander operiert. Doch derzeit arbeiten sie gemeinsam, und ein Ausfall in einer der kritischen Infrastrukturen wirkt sich auf die anderen aus [17, 18]. Die meisten Informationen in der Öffentlichkeit über die Anfälligkeiten von Versorgungsunternehmen für Cyberangriffe stammen aus gemeldeten Vorfällen von Cyberangriffen sowie aus kontinuierlicher Forschung, die zusätzliche Angriffsvektoren und Schwachstellen für ein bestimmtes System untersucht [19, 20]. Verteilungssysteme im Netz haben sich als anfällig erwiesen, unter anderem weil ihre Betriebstechnologie Fernverbindungen und Zugangspunkte zu Geschäftsnetzwerken aufweist [21, 22]. Dies ermöglicht es Kriminellen und Angreifern, auf die Systeme zuzugreifen und möglicherweise den Betrieb zu stören. Die Betriebstechnologie der Netzver-

Kernthesen

- Die Infrastruktur der grünen Energie ist anfällig für sowohl Cyber- als auch physische Bedrohungen, die die Sicherheit und Zuverlässigkeit der Energieversorgung gefährden können.
- Die vorhandenen Sicherheitsrichtlinien für grüne Energie müssen einer eingehenden Analyse unterzogen werden, um sicherzustellen, dass sie ausreichenden Schutz bieten und potenzielle Angriffe abwehren können.
- Es bedarf innovativer Ansätze und Strategien, um die Risiken von Cyberangriffen und Sabotage in der grünen Energie zu mindern. Dies umfasst die Entwicklung und Implementierung von robusten Sicherheitslösungen sowie die Förderung eines proaktiven Krisenmanagements.

Abb. 1 Eine schematische Darstellung des intelligenten Stromnetzes könnte wie folgt aussehen, Quelle: [5]

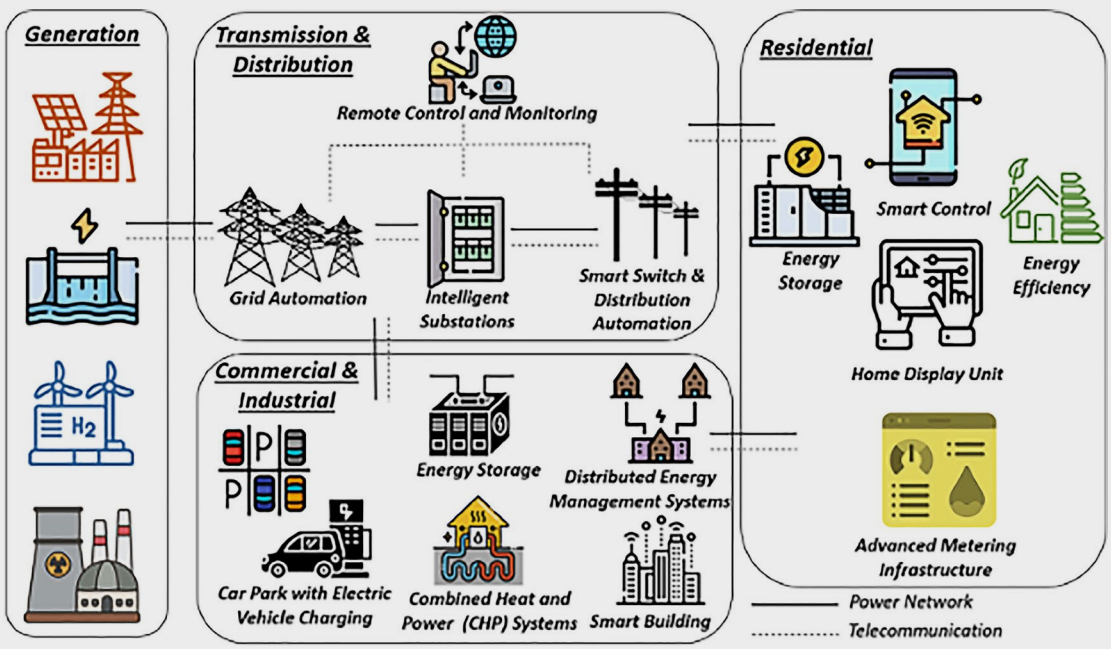
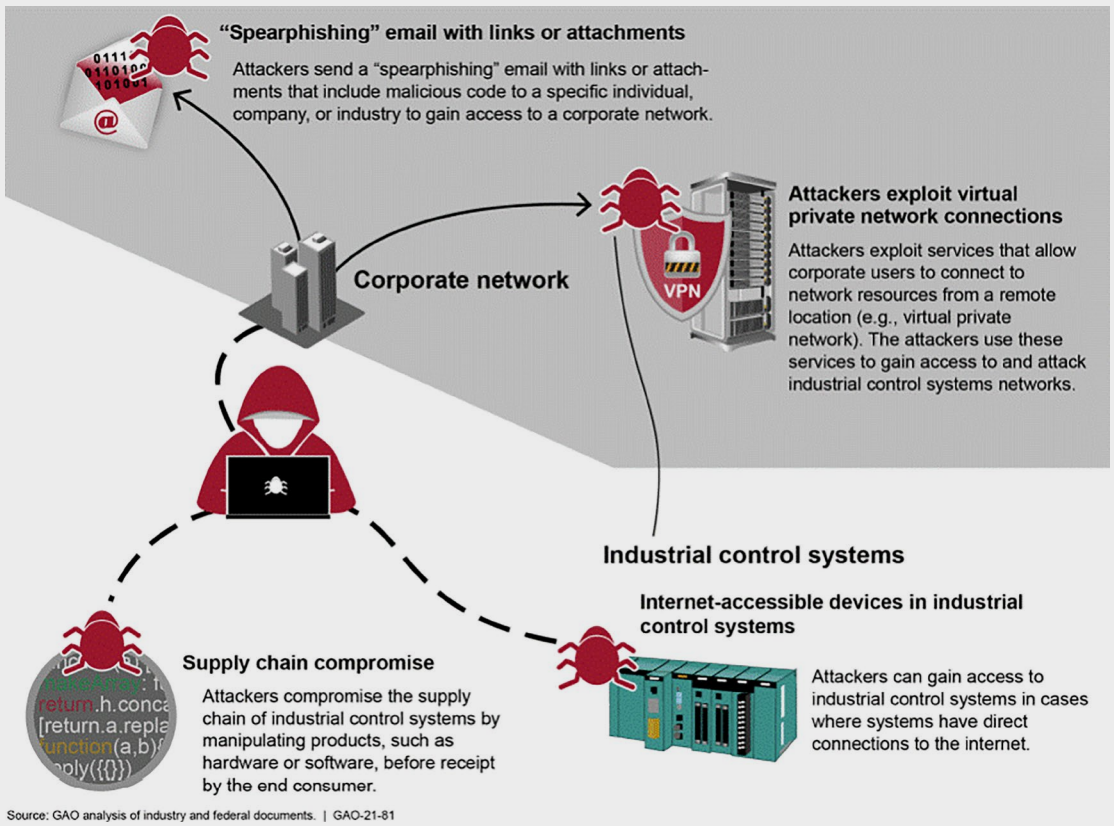


Abb. 2 Cyberangriffe und ihre Ursprungsorte. Quelle: [25]



teilung hat sie zunehmend verwundbar gemacht, indem sie Fernverbindungen und Zugang ermöglicht [23]. Kriminelle Gruppen und Nationen stellen die höchsten Cyberbedrohungen für das Stromnetz eines Landes dar, was sie abhängig und schwach macht (**Abb. 2**; [24]).

Es ist nicht überraschend festzustellen, dass technische Ausfälle und die Anfälligkeit für Cyberangriffe zunehmende Bedenken darstellen, und aktuelle Ereignisse haben diese Befürchtungen verstärkt. Zum Beispiel waren 2015 die Stromverteilungsunternehmen in der Ukraine Cyberangriffen ausgesetzt. Es wird berichtet, dass die Malware Black Energy in den Computernetzwerken der Energieunternehmen gefunden wurde [26]. Gemäß den Angaben des Unternehmenspersonals ereigneten sich die Cyberangriffe in regelmäßigen Abständen von 30 min und betrafen verschiedene Standorte. Während dieser Angriffe führten verschiedene Personen bösartige Remote-Operationen durch, entweder durch das industrielle Steuerungssystem oder das Administrationswerkzeug im Betriebssystem über das virtuelle private Netzwerk. Die Angreifer erlangten Zugriff auf legitime Zugangsdaten des Unternehmens, um Remote-Zugriff und Angriffe zu ermöglichen. Am Ende des Angriffs wurden die meisten Systemdaten des Unternehmens durch die Ausführung der KillDisk-Malware gelöscht. Diese Malware kann Dateien löschen und den Master-Boot-Record beschädigen, was das System stark beeinträchtigt. Dies führte dazu, dass weite Teile des Landes im Dunkeln blieben [27].

Eine weitere Form der Komplexität in der Infrastruktur ist Sabotage. Dies wurde kürzlich im Rahmen des russisch-ukrainischen Krieges beobachtet, bei dem Einrichtungen für grüne Energie zerstört wurden. Das Energieversorgungsunternehmen Centrenergo in der Ukraine berichtete, dass Russland am 23. März das Zmiiv-Wärmekraftwerk in der Region Charkiw zerstört hat. Dieser Luftangriff war laut Russland eine Vergeltung für den kürzlichen Angriff innerhalb Russlands [28]. Die Folgen dieses Angriffs waren verheerend, da weite Teile des Landes im Dunkeln lagen, wirtschaftliche Aktivitäten unterbrochen wurden und Menschenleben zu beklagen waren. Zu

guter Letzt gab es einen Vorfall von Cyberangriffen auf das israelische Wassersystem Mitte 2020. Diese Angriffe legten das Kontrollsystem und die ICS-Befehle für die Pumpstationen, Kläranlagen und Abwassersysteme lahm. Obwohl ihr Plan scheiterte, zielten die Angriffe darauf ab, den Chlorgehalt und andere Chemikalien im Wasser auf toxische Werte zu erhöhen und die Wasserverteilung während der COVID-19-Pandemie und einer Hitzewelle zu stören. Die Angreifer nutzten veraltete Legacy-Systeme und unzureichende Passwortrichtlinien innerhalb dieser Einrichtungen. Die Ereignisse in der Ukraine und in Israel dienen als deutliche Warnung für die Zukunft jedes Landes. Die häufigen Sabotageakte und Cyberangriffe, die mit Ländern in Verbindung gebracht werden, sind von großer Besorgnis. Diese Cyberangriffe werden durch die heimliche Natur von Cyberoperationen motiviert, die gegenüber herkömmlichen Kriegsführungsmethoden den Vorteil haben, dass sie kostengünstig und unauffindbar sind. Länder nutzen Cyberangriffe, um politische und wirtschaftliche Vorteile zu erlangen, die sie zuvor nicht hatten [29].

Die Angriffe auf den Sektor der grünen Energie verdeutlichen die sich wandelnde Natur dieser Bedrohung und ihre direkte Verbindung zu bestehenden geopolitischen Beziehungen.

Die aktuellen Sicherheitsrichtlinien und -lücken

Obwohl die Bedrohungen für die Sicherheit der grünen Energie hervorgehoben wurden, befinden sich erkennbare Sicherheitsrichtlinien und -standards noch in ihren Anfängen im Vergleich zum konventionellen Energiesektor. Diese These betrachtet diese Unzulänglichkeiten, indem sie Lücken identifiziert und bestehende Rahmenbedingungen überprüft, die erneuerbare Energieanlagen anfällig für mögliche Cyberangriffe und Sabotage machen. Sie zeigt auch Lücken in den bestehenden Richtlinien auf und betont die Notwendigkeit spezifischer Leitlinien für den Sektor, um diese Schwachstellen der grünen Energieinfrastruktur anzugehen. Der weltweite Umfang der Herausforderungen im Bereich der Cybersicherheit hat zur Bildung verschiedener nationaler und internationaler Richtlinien geführt, um die Widerstandsfähigkeit der kritischen Infrastruktur zu fördern. In der Europäischen Union (EU) ist die Richtlinie für die Netz- und Informationssicherheit (NIS) eine Darstellung der wichtigsten gesetzlichen Rahmenbedingungen, die darauf abzielen, das gesamte Sicherheitsniveau der Cybersicherheit in den Mitgliedsländern zu stärken [30]. Auf der anderen Seite hat in den Vereinigten Staaten die Cybersecurity and Infrastructure Agency (CISA) die Richtlinien für kritische Infrastrukturen wie Energie festlegt. Diese Rahmenwerke haben das gleiche Ziel: eine Grundlage für Sicherheitspraktiken zu schaffen, die von Betreibern kritischer Infrastrukturen eingehalten werden müssen [31].

Trotz lobenswerter Bemühungen bleiben die Anwendbarkeit und Spezifität bestehender Rahmenwerke im Bereich der grünen Energie unklar. Angesichts der Cybersicherheit stellen grüne Energiequellen wie Wind und Wasser im Vergleich zu traditionellen Energiequellen einzigartige Herausforderungen dar. Die wesentlichen Lücken in den aktuellen Sicherheitsrichtlinien umfassen unklare Anleitungen, die auf die technologischen und betrieblichen Feinheiten des Sektors für grüne Energie zugeschnitten sind. Die meisten Richtlinien werden mit einer Mentalität für traditionelle Energiesysteme verfasst, wodurch die einzigartigen Eigenschaften erneuerbarer Energien übersehen werden. Diese Annahme macht grüne Energieanlagen anfällig für Cyberangriffe und Sabotage, die durch die aktuellen Sicherheitsmaßnahmen nicht adressiert werden. Darüber hinaus übersteigt das schnelle Tempo der Technologieentwicklung im Bereich der grünen Energie oft die Entwicklung entsprechender regulatorischer Standards. Aufgrund dessen kann es bei der Entstehung neuer Schwachstellen zu erheblichen Verzögerungen kommen, bevor Richtlinien aktualisiert werden, um das Problem zu lösen. Dies ist die Zeit, in der diejenigen, die sabotieren, dies ausnutzen [32].

Bewährte Verfahren zur Sicherung kritischer Infrastruktur

Der Schutz kritischer Infrastruktur befasst sich hauptsächlich mit unverzichtbaren Objekten für das Funktionieren des politischen und sozialen Lebens. Dennoch liegen die Analyse materieller Objekte und die Diskussion über den Schutz kritischer Infrastruktur größtenteils im Zuständigkeitsbereich von Managementantworten [33].

Cybersicherheitsrisiken und Sabotage sind sich weiterentwickelnde Bedrohungen für den grünen Energiesektor in seiner Fähigkeit, seine Ziele zu erreichen und seine Funktionen auszuführen. Das Cybersicherheitsumfeld muss sich von dem der IT-Experten auf das des Topmanagements verlagern, wo deren Minderung und Überlegungen mit den von ihnen dargestellten Risiken korrespondieren. Eine effektive Cybersicherheit erfordert einen ganzheitlichen Ansatz für das Risikomanagement entlang der Lieferkette, Ökosysteme und Organisationsnetzwerke [34].

Handlungsempfehlungen

- Technologische Lösungen:
- Einsatz fortschrittlicher Cybersicherheitstechnologien, z. B. Secure Socket Layer (SSL), Intrusion Detection and Prevention Systems (IDPS), Blockchain für sichere Energietransaktionen, Nutzung von REMS (Erneuerbare-Energie-Managementsystem) zur Überwachung und Erkennung von Bedrohungen.
- Politische Maßnahmen und internationale Zusammenarbeit:
- Entwicklung sektorübergreifender Sicherheitsstandards, Förderung der internationalen Zusammenarbeit zur Bedrohungsabwehr.
- Incident Response und Krisenmanagement:
- Regelmäßige Simulationen und Übungen, Erstellung eines umfassenden Incident-Response-Plans, Implementierung eines Krisenkommunikationsplans.

Angesichts der Schwachstellen und der aktuellen Richtlinien schlägt dieser Abschnitt mehrere bewährte Verfahren vor, um die Sicherheit der kritischen Infrastruktur innerhalb der grünen Energie zu gewährleisten. Diese Empfehlungen drehen sich um technologische Lösungen, internationale Zusammenarbeit, politische Maßnahmen und Strategien zur Incident Response, um eine umfassende Grundlage zur Verbesserung der Sicherheit und Resilienz der kritischen grünen Energieinfrastruktur bereitzustellen.

Technologische Lösungen

Fortgeschrittene Cybersicherheitstechnologien: Die Grundlage zur Sicherung kritischer Infrastruktur liegt in der Verwendung fortschrittlicher Technologien. Dazu gehören Secure Socket Layer (SSL), Intrusion Detection and Prevention Systems (IDPS), Verschlüsselung und Firewall-Protokolle, die Daten während der Übertragung und im Ruhezustand schützen. Darüber hinaus könnten die Implementierung von Sicherheitsinformations- und Ereignismanagementsystemen Echtzeitwarnungen und Analyse von Sicherheitsmeldungen bieten, die von Netzwerk- und Anwendungssoftware erstellt wurden [35].

Blockchain für Energietransaktionen: Die Blockchaintechnologie bietet eine manipulationssichere und dezentrale Methode zur Aufzeichnung von Transaktionen. Dies verbessert die Sicherheit des Datenaustauschs und des Energiehandels innerhalb des Sektors für grüne Energie. Dadurch werden Betrug und Manipulation minimiert [36].

Erneuerbare-Energie-Managementsystem (REMS): Die Verwendung von REMS, das Cybersicherheit von vornherein berücksichtigt, kann Schwachstellen erheblich reduzieren. Das System sollte kontinuierlich nach ungewöhnlichen Aktivitäten suchen, die auf Cyberbedrohungen hinweisen könnten, und dabei maschinelles Lernen verwenden, um Muster zu erkennen, die auf Cyberangriffe hinweisen.

Politische Maßnahmen und internationale Zusammenarbeit

Sektorübergreifende Sicherheitsstandards: Die Schaffung und Durchsetzung von Sicherheitsstandards, die auf den grünen Energiesektor abzielen, ist entscheidend. Diese Standards müssen Cyber- und physische Bedrohungen berücksichtigen und dabei die einzigartigen Aspekte und Schwachstellen erneuerbarer Energieanlagen berücksichtigen.

Internationale Zusammenarbeit: Cyberangriffe sind ein grenzüberschreitendes Problem. Daher ist internationale Zusammenarbeit wichtig, um diesen Herausforderungen zu begegnen. Länder müssen Bedrohungsintelligenz und Reaktionsstrategien teilen, um die weltweite Widerstandsfähigkeit des grünen Energiesektors zu verbessern [37].

Incident Response und Krisenmanagement

Simulationen und regelmäßige Übungen: Die Durchführung regelmäßiger Simulationen und Übungen von Cyberangriffen ist wichtig, um die Effizienz des Incident-Response-Plans zu testen und das Personal auf tatsächliche Vorfälle vorzubereiten. Die Übungen sind wichtig, um Lücken in den Reaktionsstrategien zu identifizieren und einen Zustand der Bereitschaft bei den Reaktionsteams zu fördern. Incident-Response-Plan: Ein durchdachter Plan ist entscheidend für eine schnelle und effiziente Reaktion auf Sicherheitsbedrohungen. Der Plan sollte Verfahren zur Eindämmung, Erkennung und Beseitigung von Bedrohungen hervorheben.

Krisenkommunikationsplan: Ein Krisenplan sollte interne und externe Kommunikationsmethoden mit Stakeholdern, Regulierungsbehörden und der Öffentlichkeit definieren, um Transparenz und Vertrauen sicherzustellen. Ein ganzheitlicher Ansatz ist erforderlich, wenn diese bewährten Verfahren implementiert werden. Er umfasst Bildung, Richtlinien, Technologie und Zusammenarbeit. Durch Priorisierung der Sicherheit kritischer Infrastrukturen im grünen Sektor können Risiken gemindert und eine zuverlässige Stromversor-

gung verbessert werden. Die Reise zur Sicherung der grünen Energieinfrastruktur entwickelt sich ständig weiter und erfordert kontinuierliche Wachsamkeit und Anpassung an sich wandelnde Cyberbedrohungen [38].

Conclusio

Die Untersuchungen zur Sicherung kritischer Infrastrukturen im Bereich der grünen Energie haben eine Situation voller Komplexitäten aufgezeigt. Die Erkundung des grünen Energiesektors offenbart Schwachstellen in der dezentralen Natur und Technologie der grünen Energieinfrastruktur. Die Überprüfung der aktuellen Sicherheitsrichtlinien und -standards hebt den dringenden Bedarf an Maßnahmen hervor, um die Einzigartigkeit der grünen Energie zu berücksichtigen, die sie anfällig für Angriffe und Sabotage macht. Die Untersuchung dieses Artikels verdeutlicht die Notwendigkeit besserer Sicherheitsmaßnahmen zur Risikominderung und Gewährleistung der Sicherheit und Integrität wichtiger Vermögenswerte in der grünen Energie.

Der grüne Sektor hat einzigartige Schwächen, wie beispielsweise die Nutzung digitaler Technologie im dezentralen System, was Wachsamkeit und ausgefeilte Cybersicherheitsmaßnahmen erfordert. Die aktuellen Richtlinien und Standards weisen einen erheblichen Unterschied zwischen den Infrastrukturanforderungen und den Rahmenbedingungen im grünen Energiesektor auf. Diese Studie unterstreicht den dringenden Bedarf an verstärkten Sicherheitsmaßnahmen zur Kontrolle von Bedrohungen und Gewährleistung der Integrität und Flexibilität kritischer Infrastrukturen im Bereich der grünen Energie.

Die Stakeholder im grünen Energiesektor werden dazu aufgerufen, kritische Infrastrukturen priorisieren. Energieanbieter und andere Interessengruppen müssen zusammenarbeiten, um fundierte Entscheidungen zum Schutz kritischer Infrastrukturen zu treffen. Grüne Energie entwickelt sich und expandiert, daher ist es wichtig, dass ihre Vermögenswerte gesichert sind, um Kontinuität und Sicherheit für eine grüne Zukunft zu gewährleisten.

Literatur

[1] Aradau, C. (2010). Security that matters: critical infrastructure and objects of protection. *Security Dialogue*, *41*(5), 491–514.

[2] Gielen, D., Boshell, F., Syagin, D., Bazilian, M. D., Wagner, N., & Gorini, R. (2019). The role of renewable energy in the global energy transformation. *Energy Strategy Reviews*, *24*, 38–50.

[3] Cirella, G. T., Russo, A., Benassi, F., Czermanski, E., Goncharuk, A. G., & Oniszczuk-Jastrzabek, A. (2021). Energy re-shift for an urbanizing world. *Energies*, *14*(17), https://doi.org/10.3390/en14175516.

[4] Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in power grids: challenges and opportunities. *Sensors*, *21*(18), https://doi.org/10.3390/en14175516.

[5] Bouramdane, A.-A. (2023). Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *Journal of Cybersecurity and Privacy*, *3*(4), 662–705.

[6] Chipangamate, N. S., & Nwaila, G. T. (2024). Assessment of challenges and strategies for driving energy transitions in emerging markets: a scio-technological systems perspective. *Energy Geoscience*, *5*(2), 1–20.

[7] Haber, E., & Zarsky, T. (2016). Cybersecurity for infrastructure: a critical analysis. *Fla. St. UL Rev*, *44*(515), ISSN: 0096-3070

[8] Bruder, M., & Baar, T. (2024). Innovation in humanitarian assistance—A systematic literature review. *Journal of International Humanitarian Action*, *9*(2), https://doi.org/10.1186/s41018-023-00144-3

[9] Khan, K. A., Quamar, M. M., Al-Qahtari, F. H., Asif, M., Alqahtani, M., & Khalid, M. (2023). Smart grid infrastructure and renewable energy deployment: a conceptual review of Saudi Arabia. *Energy Strategy Reviews*, *50*, https://doi.org/10.1016/j.esr.2023.101247

[10] Jasiunas, J., Lund, P. D., & Mikkola, J. (2021). Energy system resilience—A review. *Renewable and Sustainable Energy Reviews*, *150*, https://doi.org/10.1016/j.rser.2021.111476

[11] Onyeji, I., Bazilian, M., & Bronk, C. (2014). Cyber security and critical energy infrastructure. *The Electricity Journal*, *27*(2), 52–60.

[12] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186.

[13] Collier, S. J., & Lakoff, A. (2014). Vital systems security: Reflexive biopolitics and the government of emergency. *Theory, Culture and Society*, *32*(2), https://doi.org/10.1177/02632764135100

[14] Jayachandran, M., Gatla, R. K., Rao, K. P., Rao, G. S., Mohammed, S., Milyani, A. H., Azhari, A. A., Kalaiarasy, C., & Geetha, S. (2022). Challenges in achieving sustainable development goal 7: Affordable and clean energy in light of nascent technologies. *Sustainable Energy Technologies and Assessments*, *53*, Part C.

[15] Aleluia, J., Tharakan, P., Chikkatui, A. P., Shrimali, G., & Chen, X. (2022). Accelerating a clean energy transition in Southeast Asia: role of governments and public policy. *Renewable and Sustainable Energy Reviews*, *159*, https://doi.org/10.1016/j.rser.2022.112226

[16] Kumar, C. R., & Majid, M. A. (2020). Renewable energy for sustainable development in India: current status, future prospects, challenges, employment, and investment opportunities. *Energy, Sustainability and Society*, *10*(2), https://doi.org/10.1186/s13705-019-0232-1

[17] Amir, M., & Khan, S. Z. (2022). Assessment of renewable energy: status, challenges, COVID-19 impacts, opportunities, and sustainable energy solutions in Africa. *Energy and Built Environment*, *3*(3), 348–362.

[18] Felice, F. D., Baffo, I., & Petrillo, A. (2022). Critical infrastructures overview: past, present and future. *Sustainability*, *14*, 4.

[19] Aros-Vera, F., Gillian, S., Rehmar, A., & Rehmar, L. (2021). Increasing the resilience of critical infrastructure networks through the strategic location of microgrids: a case study of Hurricane Maria in Puerto Rico. *International Journal of Disaster Risk Reduction*, *55*, https://doi.org/10.1016/j.ijdrr.2021.102055

[20] Stergiopoulos, G., Gritzalis, D. A., & Limnaios, E. (2020). Cyber-attacks on the oil & gas sector: a survey on incident assessment and attack patterns. *IEEE Access*, *8*, 128440–128475.

[21] Aslan, O., Aktug, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of Cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), https://doi.org/10.3390/electronics12061333

[22] Zografopoulos, I., Hatziargyriou, N. D., & Konstantinou, C. (2023). Distributed energy resources cybersecurity outlook: vulnerabilities, attacks, impacts, and mitigation. *IEEE Systems Journal*, *17*(4), 6695–6709.

[23] Rivas, A. E. L. (2020). Faults in smart grid systems: monitoring, detection and classification. *Electric Power Systems Research*, *189*, https://doi.org/10.1016/j.epsr.2020.106602

[24] Abir, S. M. A. A., Anwar, A., Choi, J., & Kayes, A. S. M. (2021). IoT-enabled smart energy grid: applications and challenges. *IEEE Access*, *9*, 50961–50981.

[25] GAO (2024). Critical infrastructure protection: challenges and efforts to secure control systems. https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-04-354/html/GAOREPORTS-GAO-04-354.htm. Zugegriffen: 15. März 2004.

[26] Admass, W. S., Munase, Y. Y., & Diro, A. A. (2024). Cyber security: state of the art, challenges and future directions. *Cyber Security and Applications*, *9*, https://doi.org/10.1016/j.csa.2023.100031

[27] Gjevski, L., & Szulecki, K. (2023). Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout. *European Security*, *32*(1), 104–124.

[28] Jazeera, A. Two killed as Russia escalates attacks on Ukraine's energy infrastructure, Al Jazeera, 31 March 2024. https://www.aljazeera.com/news/2024/3/31/2-dead-as-russia-escalates-attacks-on-ukraines-energy-infrastructure. Zugegriffen: 3. Apr. 2024.

[29] Whyte, C. (2020). Cyber conflict or democracy "hacked„? How cyber operations enhance information warfare. *Journal of Cybersecurity*, *00*(0), 1–17.

[30] Koppa, M. (2022). The new resonance of European „holistic security. In *The evolution of the common security and defence policy: critical junctures and the quest for EU strategic autonomy* (S. 105–122). Cham: Springer.

[31] Alshemeili, A., Hertelendy, A., Hart, A., Alburaidi, A., Benmoussa, G., DiGregorio, D., & Ciottone, G. (2023). Assessment of statewide communication Interoperability plans (SCIP) across the United States using the cybersecurity & infrastructure security agency (CISA) Interoperability marker. *Prehospital and Disaster Medicine*, *38*(S1), S95.

[32] Kariuki, D. (2018). *Barriers to renewable energy technologies development*. Keele University.

[33] Harašta, J. (2018). Legally critical: defining critical infrastructure in an interconnected world. *International Journal of Critical Infrastructure Protection*, *21*, 47–56.

[34] Patel, A., & Suthar, A. (2023). *Cyber security techniques PGDCS103*. Madhya Pradesh Bhoj Open University.

[35] Yilmaz, E. (2020). *Firewall and intrusion detection and prevention concept for automotive ethernet*. Uppsala: Uppsala Universitet.

[36] Damisa, U., & Nwulu, N. I. (2022). Blockchain-based auctioning for energy storage sharing in a smart community. *Energies*, *15*(6), https://doi.org/10.3390/en15061954

[37] Mishra, A. Y., Alzoubi, I., Anwar, M. J., & Gill, Q. A. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers and Security*, *120*, https://doi.org/10.1016/j.cose.2022.102820

[38] Chowdhury, N., & Gkioulos, V. (2023). Cybersecurity training for critical infrastructure protection. *Computer Science Review: A literature review*, *40*(7), https://doi.org/10.1016/j.cosrev.2021.100361