International journal of Central Eurasia Studies
Scopus
Homepage: jcep.ut.ac.ir
Online ISSN: 2345-3117

EU Energy Security under the Influence of Russian Cyber Threats

Seyed Davood Aghaei[1] and Reza Abdollahi[2]

1. Professor, Department of Regional Studies, Faculty of Law and Political Science, University of Tehran, Tehran, Iran.
2. M. A. in Regional Studies, Faculty of Law and Political Science, University of Tehran, Tehran, Iran.

Email: reza.abdollahi@ut.ac.ir (Corresponding Author)

Article Info.

Article Type:
Research Paper

Article History:
Received:
3 May 2025
Revised:
31 May 2025
Approved:
7 June 2025
Punlished online:
4 August 2025

Key Words:
Cybersecurity, Cyber Threat, Energy Security, European Union, Russia.

ABSTRACT

In today's interconnected digital world, cybersecurity has become a geopolitical challenge. The European Union is vulnerable to cyberattacks, due to its dependence on digital infrastructure and energy networks. These attacks, which mainly target critical energy infrastructure, can lead to economic instability and undermine regional security. Russia, especially after its invasion of Ukraine in 2022, has used cyberattacks as part of its hybrid warfare strategy, threatening the European Union energy security. This article seeks to answer the question of how Russian cyber threats have affected the European Union's energy security and what responses the Union has made. In response, the hypothesis is advanced that Russian cyberattacks have undermined the EU's energy security and that, although the Union's responses are aligned with defensive Neo-realism, their effectiveness has been limited by incoherence. In this research, using a qualitative approach and case study analysis, data were collected from secondary sources and examined based on the framework of defensive Neo-realism. The findings suggest that Russian cyberattacks, such as NotPetya, are part of a strategy to destabilize the European Union. The EU's responses include strengthening cybersecurity policies, but inconsistencies and reliance on outdated systems have reduced their effectiveness. This article emphasizes the need for greater coordination and innovation in cybersecurity.

Cite this article: Aghaei, S. D. and R. Abdollahi (2025), "EU Energy Security under the Influence of Russian Cyber Threats", **Central Eurasia Studies**, Vol. 18, No. 1, pp. 1-28.
http//doi.org/10.22059/JCEP.2025.394596.450321

Publisher: University of Tehran

Introduction: In today's interconnected and increasingly digital world, cybersecurity has emerged as one of the most important geopolitical challenges. The European Union, with its deep reliance on digital infrastructure and interconnected energy networks, finds itself particularly vulnerable to cyberattacks. These attacks, often aimed at disrupting critical energy infrastructure such as power grids, pipelines and industrial control systems, pose significant risks. They can lead to widespread economic instability, a loss of public trust in institutions and the weakening of the regional security framework on which the EU relies. Since Russia's invasion of Ukraine in February 2022, cyberattacks have become a prominent tool in a broader hybrid warfare strategy, designed to destabilize the EU and advance Russia's geopolitical objectives. This escalation of tensions has exposed the European Union's energy security, a vital pillar of its economic prosperity and political stability to an unprecedented threat. Using the theoretical perspective of defense neorealism, this study examines the impact of Russian cyber threats on the energy security of the European Union and critically evaluates the defense measures implemented by the Union. The aim of this research is to examine how these cyber threats endanger critical energy infrastructure, assess the robustness and limitations of the EU's responses and highlight the broader implications for regional stability. Given the foundational role of energy security in maintaining the economic and political cohesion of the European Union, alongside the increasing complexity of cyber threats, this issue requires urgent scientific and political attention.

Research question: How do Russian cyber threats affect the European Union energy security and what strategies has the EU implemented to mitigate these risks?

Research hypothesis: Russian cyber threats, integrated into a hybrid warfare framework, undermine the EU's energy security by targeting critical infrastructure, such as electricity networks and gas pipelines. The EU's defense strategies, including advanced cybersecurity policies and international partnerships, are aligned with the principles of defensive neorealism, emphasizing deterrence and survival in an anarchic system. However, these measures have been limited by political incoherence between member states, reliance on outdated technological systems and the inherently asymmetric nature of cyber

threats, all of which reduce their overall effectiveness.

Methodology and theoretical framework: This research was conducted with a qualitative approach and focused on an in-depth analysis of selected case studies. Data were collected through a systematic review of secondary sources, including peer-reviewed academic articles, official EU reports and key policy documents such as the Network and Information Security (NIS) Directive and the REPowerEU plan. Case studies, including the 2017 NotPetya attack, the 2015 cyberattacks on Ukraine's power grid and the sabotage of the Nord Stream pipeline in 2022, have been deliberately selected to illustrate important and relevant examples of cyber threats targeting the energy sector. The theoretical framework underlying this study is defensive neorealism, rooted in the seminal works of Kenneth Waltz and expanded upon by scholars such as Robert Jervis and Stephen Walt. Defensive neorealism holds that in an anarchic international system, states prioritize security and survival through defensive and deterrent strategies and their goal is to maintain the balance of power rather than pursue aggressive expansion. The analysis focuses on key concepts such as deterrence, security dilemma and defensive posture to assess the patterns of Russian cyberattacks and the EU's counter-responses, providing a structured perspective for understanding this complex interaction.

Results and discussion: The research findings suggest that Russian cyberattacks which have intensified since the invasion of Ukraine in 2022, form a deliberate part of a hybrid warfare strategy aimed at destabilizing the EU. These attacks use sophisticated tools, such as the NotPetya and Industroyer malware, alongside combined tactics such as physical and cyber sabotage of the Nord Stream pipelines. They target critical energy infrastructure, including electricity grids, gas distribution networks and industrial control systems, leading to disruptions in energy supply, reduced public confidence, and instability in energy markets. Specific examples include the NotPetya attack, which paralyzed industries across Europe in 2017 and the Ukrainan power grid attacks that showed the potential for widespread blackouts. The Nord Stream incident further highlighted the vulnerability of physical energy assets to hybrid cyber-physical threats. In response, the EU has strengthened its cybersecurity framework through measures such as updating the NIS Directive,

deepening cooperation with NATO and the United States and imposing targeted economic sanctions on entities linked to these attacks. These actions reflect defensive neorealism's focus on deterrence and the avoidance of direct military confrontation. However, their effectiveness has been undermined by several factors: uncoordinated implementation of policies across member states, reliance on outdated infrastructure vulnerable to abuse and challenges related to attributing attacks to specific actors due to the anonymity of cyberspace. The interconnected nature of Europe's energy systems exacerbates these risks, as seen in the regional consequences of NotPetya. Addressing these vulnerabilities requires greater policy coordination, accelerating infrastructure modernization and integrating advanced technologies like artificial intelligence for threat detection and blockchain to secure data exchanges.

Conclusion: This study concludes that Russian cyber threats, framed within a hybrid warfare paradigm, pose a profound and immediate risk to the EU's energy security. While the EU's defensive actions, from policy enhancements to international collaboration, are aligned with the principles of defense neorealism, their impact has been limited by structural and operational shortcomings. Policy fragmentation among member states, reliance on legacy systems and the ambiguous nature of cyber adversaries limits the Union's ability to fully neutralize these threats. To strengthen its resilience, the EU should adopt binding policy frameworks to ensure cohesive action, invest heavily in modernizing its energy infrastructure with cyber-secure technologies, and expand international cooperation through joint cyber defense exercises and real-time intelligence sharing. Employing advanced tools, such as artificial intelligence for proactive threat detection and blockchain to protect critical communications, is equally essential. In an anarchic global system where hybrid threats are rapidly evolving, the EU's ability to adapt quickly and decisively will determine its capacity to protect energy security and maintain stability. This research highlights the urgent need for a strategic review of the EU's cyber defense to counter the multifaceted risks posed by hybrid warfare.

Key Words: Cybersecurity, Cyber Threat, Energy Security, European Union, Russia.

مجله بین‌المللی مطالعات اوراسیای مرکزی
Scopus
Homepage: jcep.ut.ac.ir
شاپا الکترونیکی: ۲۳۴۵-۲۱۱۷

امنیت انرژی اتحادیهٔ اروپا زیر تأثیر تهدیدهای سایبری روسیه

سید داود آقایی[۱] و رضا عبداللهی[۲]

۱. استاد، گروه مطالعات منطقه‌ای، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران

۲. دانش‌آموخته کارشناسی ارشد مطالعات منطقه‌ای، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران

نویسنده مسئول: reza.abdollahi@ut.ac.ir

اطلاعات مقاله

نوع مقاله: علمی‌پژوهشی

تاریخ دریافت: ۱۴۰۴/۰۲/۱۳

تاریخ بازنگری: ۱۴۰۴/۰۳/۱۰

تاریخ پذیرش: ۱۴۰۴/۰۳/۱۷

تاریخ انتشار برخط: ۱۴۰۴/۰۵/۱۲

واژگان اصلی:
امنیت سایبری،
امنیت انرژی،
تهدید سایبری،
اتحادیهٔ اروپا،
روسیه.

چکیده

در دنیای دیجیتال و به‌هم‌پیوستهٔ امروز، امنیت سایبری به چالشی ژئوپلیتیکی تبدیل شده است. اتحادیهٔ اروپا به‌دلیل وابستگی به زیرساخت‌های دیجیتال و شبکه‌های انرژی، در برابر حمله‌های سایبری آسیب‌پذیر است. این حمله‌ها که بیشتر زیرساخت‌های حیاتی انرژی را هدف قرار می‌دهند، می‌توانند به بی‌ثباتی اقتصادی و تضعیف امنیت منطقه‌ای منجر شوند. روسیه به‌ویژه پس از تهاجم به اوکراین در سال ۲۰۲۲، از حمله‌های سایبری به‌عنوان بخشی از راهبرد جنگ ترکیبی خود بهره برده و امنیت انرژی اتحادیهٔ اروپا را تهدید کرده است. در این نوشتار به‌دنبال پاسخ این پرسش هستیم که تهدیدهای سایبری روسیه چگونه بر امنیت انرژی اتحادیهٔ اروپا تأثیر گذاشته و این اتحادیه چه پاسخ‌هایی ارائه داده است؟ در پاسخ این فرضیه مطرح می‌شود که حمله‌های سایبری روسیه امنیت انرژی اتحادیه را تضعیف کرده و پاسخ‌های اتحادیه، اگرچه با نوواقع‌گرایی تدافعی سازگار هستند، به‌دلیل ناهماهنگی‌ها، اثربخشی محدودی دارند. در این مطالعه با رویکرد کیفی و تحلیل مطالعات موردی، داده‌ها را از منابع دست دوم گردآوری و براساس چارچوب نوواقع‌گرایی تدافعی بررسی می‌کنیم. یافته‌ها نشان می‌دهند که حمله‌های سایبری روسیه مانند نات‌پتیا، بخشی از راهبرد بی‌ثبات‌سازی اتحادیهٔ اروپا هستند. پاسخ‌های اتحادیهٔ اروپا شامل تقویت سیاست‌های سایبری است، اما ناهماهنگی و وابستگی به سیستم‌های قدیمی، کارایی را کاهش داده است. در این نوشتار بر نیاز به هماهنگی بیشتر و نوآوری در امنیت سایبری تأکید داریم.

استناد: آقایی، سیدداود، رضا عبداللهی (۱۴۰۴)، « امنیت انرژی اتحادیهٔ اروپا زیر تأثیر تهدیدهای سایبری روسیه»، **مطالعات اوراسیای مرکزی**، دوره ۱۸، شماره ۱، صص. ۲۸-۱

http//doi.org/10.22059/JCEP.2025.394596.450321

ناشر: دانشگاه تهران

مقدمه

در دنیای دیجیتال و به‌هم پیوستهٔ امروز، امنیت سایبری به یکی از چالش‌های اصلی ژئوپلیتیکی تبدیل شده است. اتحادیهٔ اروپا به‌دلیل وابستگی شدید به زیرساخت‌های دیجیتال و شبکه‌های انرژی، در برابر حمله‌های سایبری آسیب‌پذیر است. این حمله‌ها که بیشتر با هدف اختلال در زیرساخت‌های حیاتی انرژی انجام می‌شوند، می‌توانند به ناپایداری اقتصادی، کاهش اعتماد عمومی و تضعیف امنیت منطقه‌ای منجر شوند (Vasiliu, 2019: 7). روسیه به‌ویژه پس از تهاجم به اوکراین در سال ۲۰۲۲، از حمله‌های سایبری به‌عنوان ابزاری برای پیشبرد هدف‌های ژئوپلیتیکی خود استفاده کرده و امنیت انرژی اروپا را به خطر انداخته است. این حمله‌ها نه‌تنها بخشی از راهبرد گسترده‌تر موسوم به جنگ ترکیبی هستند، بلکه با بهره‌گیری از فناوری‌های نوین، پیچیدگی‌های جدیدی را به امنیت سایبری افزوده‌اند (Lin & Jia, 2023: 4). این تهدیدها که فراتر از جرائم سایبری معمولی هستند، بخشی از راهبرد جنگ ترکیبی روسیه به شمار می‌روند. هدف این حمله‌ها، تضعیف عملکرد شبکه‌های انرژی، اختلال در عرضهٔ انرژی و کاهش اعتماد بازار به توانایی اتحادیهٔ اروپا در حفاظت از زیرساخت‌هایش است (Cao, 2020). پیشرفت فناوری‌هایی مانند اینترنت اشیاء و هوش مصنوعی پیچیدگی این خطرها را افزایش داده و تمایز میان امنیت سایبری و امنیت ملی را کم‌رنگ کرده است.

با توجه به پیچیدگی این تهدیدها و تأثیرهای گستردهٔ آن‌ها بر امنیت ملی، برای تحلیل واکنش‌های اتحادیهٔ اروپا به چارچوب نظری نیاز است. در این نوشتار به‌دنبال پاسخ این پرسش هستیم که تهدیدهای سایبری روسیه چگونه بر امنیت انرژی اتحادیهٔ اروپا تأثیر می‌گذارند و این اتحادیه چه واکنشی به آن‌ها نشان می‌دهد؟ برای این منظور، از چارچوب نوواقع‌گرایی تدافعی استفاده می‌کنیم که کنت والتز مطرح کرده است. این نظریه بر این ایده استوار است که در نظام بین‌المللی آنارشیک، دولت‌ها برای حفظ امنیت و بقای خود به اقدام‌های تدافعی روی می‌آورند و بر بازدارندگی و توازن قدرت تمرکز دارند. بر این اساس، اتحادیهٔ اروپا اقدام‌هایی را برای کاهش تهدیدها و جلوگیری از تشدید تنش‌ها طراحی کرده و با تقویت سیاست‌های امنیت سایبری، گسترش همکاری‌های بین‌المللی و کاربست تحریم‌های اقتصادی به حمله‌های روسیه پاسخ داده است (Maliki, 2022). این اقدام‌های تدافعی نه‌تنها برای کاهش تهدیدهای سایبری حیاتی هستند، بلکه نشان‌دهندهٔ نقش اصلی امنیت انرژی در ثبات اتحادیهٔ اروپا هستند که موضوع اصلی این نوشتار است.

این مطالعه از چند جهت اهمیت دارد. امنیت انرژی، به‌عنوان محور ثبات اقتصادی و

سیاسی اتحادیهٔ اروپا، مستقیم زیر تأثیر حمله‌های سایبری قرار دارد. تحلیل این تهدیدها با نوواقع‌گرایی تدافعی، درک بهتری از رفتار دولت‌ها در برابر چالش‌های امنیتی غیرسنتی ایجاد می‌کند. از سویی، نیاز به سیاست‌های یکپارچهٔ امنیت سایبری و همکاری بین‌المللی بیش‌ازپیش آشکار شده است. برای پاسخ به این نیازها و درک بهتر این پدیده، در این نوشتار ساختاری گام‌به‌گام را دنبال می‌کنیم. ابتدا ادبیات تهدیدهای سایبری و امنیت انرژی را مرور می‌کنیم تا زمینهٔ بحث روشن شود. سپس چارچوب نوواقع‌گرایی تدافعی را توضیح می‌دهیم تا دیدگاه نظری نوشتار مشخص شود. در ادامه، با تحلیل مطالعات موردی مانند حملهٔ نات‌پتیا[1] و دیگر حمله‌های اصلی به زیرساخت‌های انرژی، ابعاد تهدیدها را بررسی می‌کنیم. سرانجام با جمع‌بندی یافته‌ها برای سیاست‌گذاران و پژوهش‌های آینده پیشنهادهایی ارائه می‌دهیم. در این نوشتار از رویکرد کیفی با تمرکز بر تحلیل مطالعات موردی بهره می‌بریم و داده‌ها را با مرور نظام‌مند منابع ثانویه گردآوری کرده‌ایم.

ادبیات پژوهش

پژوهش‌های متعددی به بررسی تأثیر حمله‌های سایبری بر امنیت انرژی پرداخته‌اند و هر یک از زوایای مختلفی به این موضوع نگاه کرده‌اند. در ادامه، به برخی از مطالعه‌های مهم در این حوزه، منابع فارسی و غیرفارسی اشاره می‌شود. رهامی و اژدری (۱۴۰۱) در مقاله‌ای با عنوان «امنیت سایبری اتحادیه اروپا: تهدیدات، فرصت‌ها و اقدامات»، روند سیاست‌گذاری سایبری اتحادیه اروپا را از سال ۲۰۰۷ تا ۲۰۲۱ تحلیل کرده‌اند. این پژوهش نشان می‌دهد که عواملی چون تهدیدهای خارجی، به‌ویژه حمله‌های سایبری منسوب به روسیه، تعارض‌های درونی میان نهادهای اروپایی، چالش‌های حقوقی و انسجام سیاست‌های امنیت سایبری را زیر تأثیر قرار داده‌اند. نویسندگان تأکید دارند که با وجود تدوین راهبردهای متعددی چون راهبردهای امنیت سایبری اروپا در سال‌های ۲۰۱۳ و ۲۰۲۰، ضعف در هماهنگی نهادی، پاسخ‌دهی مؤثر و بازدارندگی در برابر تهدیدهای سایبری همچنان پابرجاست.

در همین راستا، قنبری و خانی (۱۳۹۹) در مطالعه‌ای با عنوان «بازدارندگی سایبری روسیه از منظر اروپا»، اهداف و انگیزه‌های مسکو در بهره‌گیری از ابزارهای سایبری علیه کشورهای غربی را بررسی کرده‌اند. به باور آنان، روسیه با استفاده از فضای مجازی به‌عنوان بستری برای جنگ

1. NotPetya

ناهم‌تراز، به دنبال تضعیف مشروعیت سیاسی دولت‌های اروپایی، گسترش نفوذ در حوزه پساشوروی و افزایش هزینه واکنش‌پذیری غرب است. حمله‌های سایبری به استونی (۲۰۰۷) و گرجستان (۲۰۰۸) به‌عنوان نمونه‌هایی از این راهبرد معرفی شده‌اند. این پژوهش همچنین به ناهماهنگی نهادی و نبود راهبرد بازدارنده مؤثر در اتحادیه اروپا اشاره دارد که این اتحادیه را در موضعی انفعالی قرار داده است. کتانچی و پورقهرمانی (۱۳۹۸) در تحلیل پیمان جرایم سایبری شورای اروپا (کنوانسیون بوداپست)، چالش‌های ساختاری مانند ناهماهنگی قوانین ملی، نبود همکاری بین‌المللی مؤثر و ضعف در اجرا را به‌عنوان موانع بازدارندگی اتحادیه اروپا در برابر تهدیدهای سایبری شناسایی کرده‌اند. این پژوهش نشان می‌دهد که حمله‌های سایبری روسیه به زیرساخت‌های حیاتی اروپا، در شرایط خلأهای نظارتی و حقوقی، شدت یافته است.

فرشاسعید و همکاران (۱۴۰۱) در مقاله «ضرورت همکاری دولت‌ها در تقویت امنیت سایبری»، بر سرشت فرامرزی و پیچیدگی حمله‌های سایبری تأکید کرده و نیاز به پاسخ‌های جمعی و بین‌المللی را برجسته ساخته‌اند. آن‌ها با اشاره به نقش قدرت‌های سایبری مانند روسیه در بهره‌برداری از خلأهای حقوقی، خاطرنشان می‌کنند که نبود هماهنگی نهادی و سازوکارهای بازدارنده مؤثر، امنیت انرژی اتحادیه اروپا را آسیب‌پذیر کرده است. این پژوهش بر ضرورت تقویت چارچوب‌های همکاری بین‌المللی برای مقابله با تهدیدهای سایبری تأکید دارد. بلنک[1] (۲۰۲۴) در کتاب «*چشم انداز امروزین ارتش روسیه*» به بررسی فعالیت‌های سایبری روسیه پرداخته و به حمله‌های این کشور به زیرساخت‌های حیاتی، به‌ویژه بخش انرژی اشاره کرده است. او با استناد به حمله بدافزار *انرژی سیاه*[2] به شبکه برق اوکراین در سال ۲۰۱۵، نشان می‌دهد که کرملین از ابزارهای سایبری پیشرفته برای اختلال در امنیت انرژی اروپا استفاده می‌کند. این پژوهش بر نقش خلأهای حقوقی و نظارتی در تشدید آسیب‌پذیری زیرساخت‌ها تأکید کرده و توافق سایبری روسیه–چین در سال ۲۰۱۵ را به‌عنوان تلاشی برای تقویت چارچوب‌های حقوقی مشابه پیمان جرایم سایبری شورای اروپا معرفی می‌کند.

ویوتوویچ[3] (۲۰۲۴) در مقالهٔ «امنیت انرژی اتحادیهٔ اروپا پس از تهاجم روسیه به اوکراین: محتوا، راهبرد و لابیگری» به‌ویژه بر تهدیدهای سایبری روسیه علیه بخش انرژی اتحادیهٔ اروپا تمرکز کرده و نشان داده است که وابستگی فزایندهٔ سیستم‌های انرژی به فناوری دیجیتال، آن‌ها را

1. Blank
2. BlackEnergy
3. Wójtowicz

در برابر حمله‌ها آسیب‌پذیرتر کرده است. وی تأکید می‌کند که تهاجم روسیه به اوکراین در سال ۲۰۲۲ این تهدیدها را تشدید و امنیت انرژی را به یکی از اولویت‌های اصلی اتحادیهٔ اروپا تبدیل کرده است. الجوهانی[1] (۲۰۲۲) در مقالهٔ «حمله‌های سایبری به زیرساخت‌های انرژی: سلاح‌های نوین جنگ» تأثیر مستقیم حمله‌های سایبری روسیه بر زیرساخت‌های انرژی را بررسی کرده است و استدلال می‌کند که این حمله‌ها با هدف اختلال در شبکه‌های برق، جمع‌آوری اطلاعات و ایجاد هراس عمومی طراحی شده‌اند. همچنین نشان می‌دهد که این تهدیدها نه‌تنها پیچیدگی سیستم‌ها را افزایش داده‌اند، بلکه به بی‌ثباتی بازارهای انرژی و افزایش قیمت سوخت نیز منجر شده‌اند. پیشچیک و آلکسیف[2] (۲۰۲۴) در مقالهٔ «مسائل کنونی امنیت سایبری در روسیه: جنبه‌های جهانی و ملی» با تمرکز بر اوکراین در طول جنگ ۲۰۲۲، نشان داده‌اند که حمله‌های سایبری روسیه، مانند اختلال در ماهوارهٔ کاست[3]، زیرساخت‌های انرژی و ارتباطی را هدف قرار داده و به قطع برق و کاهش تاب‌آوری عملیاتی منجر شده است. آن‌ها همچنین بر تقویت انعطاف‌پذیری اوکراین با همکاری با ایالات متحد تأکید می‌کنند.

ارسلان[4] (۲۰۲۳) در مقالهٔ «تحلیل نوواقع‌گرایانه معضل امنیتی در فضای سایبری؛ مطالعه‌ای کمی» با تحلیل کمی رفتار دولت‌ها در فضای سایبری، نشان می‌دهد که دولت‌های با ظرفیت پیشرفته‌تر امنیت سایبری بیشتر اقدام‌های تهاجمی‌تری انجام می‌دهند، یافته‌ای که با نوواقع‌گرایی تدافعی و مشکل امنیتی نیز هم‌خوانی دارد. مولچانف و ماتوسوا[5] (۲۰۲۰) نیز در پژوهش خود، «امنیت انرژی در عصر دیجیتال‌سازی»، از دیدگاهی دیگر به همبستگی بالای سیستم‌های انرژی در اروپا پرداخته‌اند و می‌گویند که حملهٔ سایبری در یک کشور می‌تواند آثار زنجیره‌ای در دیگر کشورها ایجاد کند. آن‌ها بر ضرورت تدوین چارچوب‌های حقوقی بین‌المللی و تقویت اقدام‌های امنیتی تأکید دارند. کریزکوفسکی[6] (۲۰۲۱) در مقالهٔ «جنبه‌های حقوقی امنیت سایبری در بخش انرژی: وضعیت کنونی و جدیدترین پیشنهادهای تغییرهای قانونی به‌وسیلهٔ اتحادیهٔ اروپا» با نگاهی حقوقی و نظارتی، نبود مقررات هماهنگ در اتحادیهٔ اروپا را مانعی برای سرمایه‌گذاری در امنیت سایبری زیرساخت‌های انرژی دانسته و هشدار داده است که خلأ قانونی می‌تواند تاب‌آوری این سیستم‌ها را کاهش دهند.

1. Aljohani
2. Pishchik and Alekseev
3. KA-SAT
4. Arslan
5. Molchanov and Matusova
6. Krzykowski

در کنار این پژوهش‌ها، برخی پژوهش‌ها از زاویهٔ سیاست‌های کلان انرژی به موضوع نگریسته‌اند. سوتنیک[1] و همکاران (۲۰۲۴) در مقالهٔ «بهای توسعه پایدار بخش انرژی‌های تجدیدپذیر: مورد اوکراین» پیامدهای اقتصادی تهاجم روسیه به اوکراین را بررسی کرده و نشان داده‌اند که این بحران، تورم و بی‌ثباتی بازار انرژی را در اتحادیهٔ اروپا تشدید کرده است. آن‌ها تنوع‌بخشی به منابع انرژی و کاهش وابستگی به روسیه را از راهبردهای اصلی اتحادیهٔ اروپا معرفی می‌کنند. یاکوویک و تسولیخ[2] (۲۰۲۳) با دیدگاهی مشابه در مقالهٔ «امنیت انرژی اتحادیهٔ اروپا در زمینهٔ تجاوز روسیه به اوکراین»، برنامهٔ توانمندسازی انرژی اروپا[3] را تلاشی برای رهایی از وابستگی ژئوپلیتیکی به روسیه دانسته‌اند، هرچند کمتر به حمله‌های سایبری پرداخته‌اند. هارتویگ[4] (۲۰۲۳) در مقالهٔ «پیامدهای اقتصادی و امنیت انرژی سلاح انرژی روسیه» نوسان‌های بازار گاز ناشی از جنگ اوکراین را تحلیل کرده است و بر تسریع استفاده از انرژی‌های تجدیدپذیر تأکید دارد.

گروه دیگری از مطالعات بر راهکارهای فناورانه متمرکز شده‌اند. وو و موخرجی[5] (۲۰۲۱) در مقالهٔ «یادگیری تقویت ایمنی مبتنی بر عملکرد مانع برای کنترل اضطراری سیستم‌های قدرت» نقش سیستم‌های انرژی اضطراری و فناوری‌هایی مانند هوش مصنوعی و فایروال‌های هوشمند را در کاهش آثار حمله‌های سایبری بررسی کرده و یکپارچه‌سازی انرژی‌های تجدیدپذیر را پیشنهاد داده‌اند. صابری و کوهی‌زاد (۲۰۱۸) در مقالهٔ «فناوری بلاک‌چین و ارتباط آن با مدیریت زنجیرهٔ تأمین پایدار» بر استفاده از رمزنگاری و بلاک‌چین[6] برای حفاظت از زیرساخت‌های انرژی تأکید می‌کنند. این پژوهش‌ها نشان‌دهندهٔ تنوع دیدگاه‌ها در رویارویی با تهدیدهای سایبری هستند، اما همچنان شکاف‌هایی در تحلیل عملی این تهدیدها و اثربخشی راهکارها وجود دارد که زمینه را برای این نوشتار فراهم می‌کنند.

در جدول ۱ مطالعات مربوط با تهدیدهای سایبری و امنیت انرژی و نقش آن‌ها در شکل‌دهی به روند قانون‌گذاری اتحادیهٔ اروپا آمده است. هر مطالعه براساس موضوع اصلی، یافته‌های اصلی، حوزهٔ تمرکز و تأثیرش بر سیاست‌ها و قوانین اتحادیه مانند دستورعمل امنیت شبکه و اطلاعات اتحادیهٔ اروپا[7] و برنامهٔ توانمندسازی انرژی اروپا ارائه شده است.

1. Iryna Sotnyk
2. Yakoviyk & Tsvelikh
3. REPowerEU
4. Hartvig
5. Vu, Mukherjee
6. Blockchain
7. NIS Directive

جدول۱. مطالعات مرتبط با تهدیدهای سایبری و امنیت انرژی

پژوهشگر	موضوع اصلی	یافته‌های اصلی	حوزهٔ تمرکز	تأثیر بر قانون‌گذاری اتحادیهٔ اروپا
ویوتوویچ ۲۰۲۴	تهدیدهای سایبری روسیه در بخش انرژی	وابستگی روزافزون شبکه‌های انرژی به سیستم‌های دیجیتال، تشدید تهدیدها پس از تهاجم سال ۲۰۲۲ به اوکراین، تبدیل امنیت انرژی به اولویت سیاستی اتحادیهٔ اروپا	حملات سایبری و امنیت انرژی	تقویت راهبردی توانمندسازی دوبارهٔ انرژی اتحادیهٔ اروپا برای کاهش وابستگی به انرژی روسیه و تسریع تنوع منابع انرژی با قوانین جدید
الجوهانی ۲۰۲۲	تأثیر حمله‌های سایبری روسیه	هدف‌گذاری شبکه‌های برق برای اختلال، جمع‌آوری اطلاعات و القای هراس عمومی، افزایش پیچیدگی حمله‌ها، بی‌ثباتی بازار انرژی و بالارفتن قیمت سوخت	حملات سایبری و پیامدهای اقتصادی	بازنگری آئین‌نامهٔ امنیت اطلاعات و شبکه برای الزام‌های سخت‌گیرانه‌تر در حفاظت از شبکه های حیاتی
مولچانف و ماتوسوا ۲۰۲۰	همبستگی سیستم‌های انرژی	آثار زنجیره‌ای حملهٔ سایبری در کشورهای متصل، ناکارآمدی سیستم‌های قدیمی، نیاز به چارچوب‌های حقوقی بین‌المللی و تقویت دفاع سایبری	حملات سایبری و تاب‌آوری سیستم‌ها	تأکید بر استانداردسازی زیرساخت‌ها در آئین‌نامهٔ امنیت اطلاعات و شبکه و تدوین قوانین برای نوسازی سیستم‌های انرژی قدیمی
کریکوفسکی ۲۰۲۳	امنیت سایبری از دیدگاه حقوقی	نبود مقررات هماهنگ در اتحادیهٔ اروپا، محدودیت سرمایه‌گذاری در امنیت سایبری، کاهش تاب‌آوری زیرساخت‌ها به‌دلیل خلأهای قانونی و نظارتی	سیاست‌گذاری، قوانین و مقررات	تأکید بر استانداردسازی زیرساخت ها در آئین‌نامهٔ امنیت اطلاعات و شبکه و تدوین قوانین برای نوسازی سیستم‌های انرژی قدیمی

پژوهشگر	موضوع اصلی	یافته‌های اصلی	حوزهٔ تمرکز	تأثیر بر قانون‌گذاری اتحادیهٔ اروپا
سوتنیک ۲۰۲۴	پیامدهای جنگ اوکراین	افزایش تورم و بی‌ثباتی بازار انرژی پس از جنگ، تنوع‌بخشی به منابع انرژی و کاهش وابستگی به روسیه به‌عنوان راهبرد اصلی اتحادیهٔ اروپا	سیاست کلان انرژی و امنیت اقتصادی	پشتیبانی از توانمندسازی دوبارهٔ انرژی اتحادیهٔ اروپا و تدوین سیاست‌های مالی برای حمایت از تنوع منابع و کاهش تأثیرهای اقتصادی
یاکوویک و تسولیخ ۲۰۲۳	سیاست خارجی و برنامهٔ توانمندسازی دوبارهٔ انرژی اتحادیهٔ اروپا	استفادهٔ روسیه از انرژی به‌عنوان ابزار ژئوپلیتیکی، برنامهٔ توانمندسازی دوبارهٔ انرژی اتحادیهٔ اروپا برای رهایی از وابستگی، تقویت امنیت عرضهٔ انرژی در بلندمدت	سیاست کلان انرژی و ژئوپلیتیک	فشار برای بازنگری قوانین هماهنگ در قانون تاب‌آوری سایبری[1] برای رفع خلأهای نظارتی در سطح اتحادیه
هارتویگ ۲۰۲۳	پیامدهای اقتصادی جنگ اوکراین	نوسان‌های شدید در بازار گاز پس از جنگ، فشار بر سیاست‌گذاران برای تسریع در استفاده از انرژی‌های تجدیدپذیر، تأثیرهای گسترده بر اقتصاد اروپا	امنیت اقتصادی و انرژی پایدار	تشویق قوانین انرژی پایدار در توافق اروپای سبز[2] و تخصیص بودجه برای تسریع طرح‌های تجدیدپذیر
فندی ۲۰۲۳	فناوری و امنیت سایبری	کاهش آثار حمله‌ها با سیستم‌های انرژی اضطراری، پیشنهاد یکپارچه‌سازی هوش مصنوعی، فایروال‌های هوشمند و انرژی تجدیدپذیر برای افزایش تاب‌آوری	فناوری‌های امنیتی و پایداری انرژی	پشتیبانی از راهبرد توانمندسازی دوبارهٔ انرژی اتحادیهٔ اروپا و تدوین سیاست‌های مالی برای حمایت از تنوع منابع و کاهش تأثیرهای اقتصادی

1. Cyber Resilience Act
2. European Green Deal

پژوهشگر	موضوع اصلی	یافته‌های اصلی	حوزهٔ تمرکز	تأثیر بر قانون‌گذاری اتحادیهٔ اروپا
دینگ ۲۰۲۲	رمزنگاری و بلاک‌چین	استفاده از رمزنگاری پیشرفته و بلاک‌چین برای حفاظت از زیرساخت‌های انرژی، افزایش امنیت در برابر حمله‌های سایبری پیچیده	فناوری‌های نوین و امنیت سایبری	اطلاع‌رسانی به قانون تاب‌آوری سایبری برای گنجاندن رمزنگاری پیشرفته در قوانین حفاظت از داده‌ها
پیشچیک و آلکسیف ۲۰۲۴	تهدیدهای سایبری در جنگ ۲۰۲۲	حمله‌ها به زیرساخت‌های انرژی اوکراین، قطع برق و ارتباطات، تقویت تاب‌آوری با همکاری آمریکا	حمله‌های سایبری و امنیت انرژی	پایه‌گذاری اجرای راهبردی توانمندسازی دوبارهٔ انرژی اتحادیهٔ اروپا و پیشنهاد قوانین الزام‌آور برای کاهش وابستگی ژئوپلیتیکی به روسیه
ارسلان ۲۰۲۳	نوواقع‌گرایی و رفتار سایبری دولت‌ها	دولت‌های با ظرفیت سایبری پیشرفته تهاجمی‌ترند، تأیید مشکل امنیتی با نوواقع‌گرایی تدافعی	نوواقع‌گرایی و امنیت سایبری	هشدار برای تنظیم قوانین بازدارنده در در آئین‌نامهٔ امنیت اطلاعات و شبکه و تقویت سازوکارهای پاسخ‌گویی به حمله‌های تهاجمی

Source: Authers

مفاهیم و چارچوب نظری

برای درک بهتر موضوع لازم است نخست مفاهیم اصلی را تعریف کنیم. «تهدید سایبری» به اقدام‌هایی گفته می‌شود که به‌وسیلهٔ فضای مجازی با هدف اختلال، تخریب یا دسترسی غیرمجاز به سیستم‌های دیجیتال انجام می‌گیرند (Vasiliu, 2019: 11). این تهدیدها در حوزهٔ انرژی بیشتر زیرساخت‌های حیاتی مانند شبکه‌های برق، خطوط لولهٔ نفت‌وگاز و سیستم‌های کنترل صنعتی[1] را هدف قرار می‌دهند که به‌دلیل دیجیتالی‌سازی فزاینده، آسیب‌پذیری بیشتری پیدا کرده‌اند (Limnell, 2018: 4). نمونه‌های برجسته‌ای مانند حملهٔ نات‌پتیا[2] در سال ۲۰۱۷ نشان

1. Industrial control systems
2. یک بدافزار ویرانگر سایبری ,NotPetya

داده‌اند که این تهدیدها می‌توانند پیامدهای فراملی داشته باشند و کل زنجیرهٔ تأمین انرژی را مختل کنند (Watney, 2022: 7).

«امنیت انرژی» به توانایی یک سیستم برای تضمین عرضهٔ پایدار، به‌صرفه و امن انرژی گفته می‌شود که پایهٔ ثبات اقتصادی و سیاسی به شمار می‌رود (Tichy & Dubsky, 2024: 6). این مفهوم در اتحادیهٔ اروپا به‌دلیل وابستگی متقابل شبکه‌های انرژی و تأثیرهای حمله‌های سایبری، اهمیتی دوچندان دارد. از سوی دیگر، «جنگ ترکیبی» راهبردی است که ترکیبی از عملیات سایبری، اقدام‌های نظامی و دیپلماسی فشار را دربر می‌گیرد و روسیه از آن برای تضعیف رقیبان و بی‌ثبات‌سازی زیرساخت‌های حیاتی استفاده می‌کند (Pawlak, 2018: 5). این راهبرد بیشتر با حمله‌هایی نامتقارن گروه‌های هکری وابسته به دولت، مانند ای‌پی‌تی۲۸ [1] و سندوورم [2] اجرا می‌شود که شناسایی منشأ آن‌ها را دشوار می‌کند (Bederrna, 2023). «سیاست‌های امنیت سایبری اتحادیهٔ اروپا» نیز به اقدام‌ها و قوانینی اشاره دارد که برای حفاظت از زیرساخت‌های حیاتی در برابر تهدیدهای سایبری تدوین شده‌اند. از جمله این اقدام‌ها دستور کار امنیت شبکه و اطلاعات [3]، برنامهٔ توانمندسازی انرژی اروپا و فعالیت‌های مرکز تحلیل و اشتراک اطلاعات انرژی اروپا هستند (Kumari, and Others, 2022; Belov, 2023).

در این نوشتار از چارچوب نظری نوواقع‌گرایی تدافعی استفاده می‌کنیم. این نظریه که بر پایهٔ آثار کنت والتز شکل گرفته است و پژوهشگرانی مانند رابرت جرویس و استفن والت آن را توسعه داده‌اند، بر این اصل استوار است که در نظام بین‌المللی آنارشیک، دولت‌ها امنیت و حفظ توازن قدرت را در اولویت قرار می‌دهند (Waltz, 1979). برخلاف نوواقع‌گرایی تهاجمی که بر افزایش قدرت و گسترش نفوذ تمرکز دارد، نوواقع‌گرایی تدافعی بر بازدارندگی و اقدام‌های با کمترین میزان تحریک متقابل تأکید می‌کند. این دیدگاه توضیح می‌دهد که چرا واکنش‌های اتحادیهٔ اروپا به حمله‌های سایبری روسیه بیشتر بر بازدارندگی، دفاع جمعی و اقدام‌های محتاطانه مانند تقویت همکاری‌های امنیتی و کاربست تحریم‌های اقتصادی متمرکز شده است. این نظریه بر چند اصل اساسی استوار است: نخست، نبود مرجع مرکزی در نظام بین‌المللی برای تضمین امنیت، کشورها را در وضعیت اطمینان نداشتن از هدف‌ها و توانمندی‌های یکدیگر قرار می‌دهد (Waltz, 1979). از این‌رو دولت‌ها برای تضمین بقا و امنیت خود به اقدام‌های تدافعی روی می‌آورند و از سیاست‌های

1. Advanced Persistent Threat (APT28)
2. Sandworm
3. Directive on security of network and information systems (NIS Directive)

تهاجمی دوری می‌کنند. دوم، برخلاف نوواقع‌گرایی تهاجمی که بر انباشت قدرت تأکید دارد، نوواقع‌گرایی تدافعی بیان می‌کند که دولت‌ها فقط به میزان لازم برای حفظ بقای خود قدرت به‌دست می‌آورند و به‌دنبال برقراری توازن پایدار در روابط بین‌المللی هستند. سوم، مشکل امنیتی یکی از مفاهیم اصلی این چارچوب است که می‌گوید هر اقدام یک کشور برای افزایش امنیت خود ممکن است از سوی دیگران تهدید براورد شود (Taliaferro, 2000). برای نمونه، تقویت سیستم‌های دفاع سایبری اتحادیهٔ اروپا می‌تواند از سوی روسیه تهدید براورد و به تشدید حمله‌های سایبری منجر شود. به همین ترتیب، توسعهٔ توانمندی‌های سایبری ناتو ممکن است از سوی چین اقدامی تهاجمی تفسیر شود.

از این دیدگاه، حمله‌های سایبری روسیه علیه زیرساخت‌های انرژی اتحادیهٔ اروپا بخشی از راهبردی کلان برای ایجاد بی‌ثباتی و نداشتن اطمینان است. این حمله‌ها که شامل جاسوسی سایبری، انتشار اطلاعات نادرست و نفوذ به سیستم‌های کنترل صنعتی می‌شود، امنیت انرژی اتحادیه را بدون توسل به تهاجم نظامی، مستقیم تهدید می‌کند (Limnell, 2018; Pawlak, 2018). روسیه از این ابزارها برای تضعیف ثبات داخلی کشورهای اروپایی، کاهش اعتماد عمومی به امنیت انرژی و کاربست فشار سیاسی و اقتصادی بهره می‌برد. در برابر، اتحادیهٔ اروپا اقدام‌های دفاعی هم‌راستا با اصول نوواقع‌گرایی تدافعی در پیش گرفته است، از جمله تقویت سیاست‌های امنیت سایبری با ابتکارهایی مانند دستورعمل امنیت شبکه و اطلاعات[1] و برنامهٔ توانمندسازی انرژی اروپا، گسترش همکاری‌های بین‌المللی با ناتو و ایالات متحد و کاربست تحریم‌های اقتصادی علیه عاملان حمله‌های سایبری (EU Policy on Cyber Defence, 2018). نوواقع‌گرایی تدافعی در تحلیل فضای سایبری با محدودیت‌هایی روبه‌رو است. در جنگ‌های سایبری، برخلاف درگیری‌های سنتی، شناسایی منبع دقیق حمله‌ها دشوار است، زیرا این اقدام‌ها را بیشتر گروه‌های هکری وابسته به دولت‌ها انجام می‌دهند. این ویژگی کارایی سازوکارهای بازدارندگی سنتی، مانند تهدید به تلافی نظامی را کاهش می‌دهد (Pawlak, 2018: 5). افزون بر این، پویایی و سرعت تحولات فضای سایبری که ناشی از پیشرفت‌های فناورانه است، با تأکید این نظریه بر ساختارهای ثابت قدرت و امنیت هم‌خوانی ندارد. از این‌رو اتحادیه نمی‌تواند فقط با تکیه بر سیاست‌های تدافعی امنیت سایبری خود را تضمین کند و نیازمند رویکردهای نوآورانه، مانند استفاده از هوش مصنوعی برای تشخیص تهدیدها و

1. Directive on security of network and information systems (NIS Directive)

سیستم‌های سازگار با شرایط متغیر است.

چالش دیگر، وابستگی متقابل زیرساخت‌های انرژی در اتحادیهٔ اروپا است. برخلاف فرض نوواقع‌گرایی تدافعی که کشورها را واحدهایی مستقل می‌بیند، سیستم‌های انرژی اروپا به‌هم‌پیوسته‌اند و حملهٔ سایبری در یک کشور می‌تواند کل زنجیرهٔ تأمین انرژی را مختل کند (Limnell, 2018: 7). بنابراین سیاست‌های امنیت سایبری نیازمند هماهنگی در سطح اتحادیه هستند تا از زیرساخت‌های مشترک محافظت کنند. این چارچوب تبیین می‌کند که چرا اتحادیهٔ اروپا در برابر تهدیدهای سایبری روسیه رویکردی تدافعی در پیش گرفته است. بازدارندگی، تحریم‌های اقتصادی و همکاری‌های بین‌المللی همه با اصول این نظریه سازگارند. با این‌حال، ولی مانند سرشت ناهم‌تراز جنگ سایبری، تحولات سریع دیجیتال و وابستگی متقابل زیرساخت‌ها، کاربرد آن را چالش‌برانگیز می‌کند.

روش پژوهش

این پژوهش از رویکرد کیفی بهره می‌گیرد و بر تحلیل مطالعات موردی متمرکز است تا تأثیر تهدیدهای سایبری روسیه بر امنیت انرژی اتحادیهٔ اروپا و پاسخ‌های این اتحادیه را بررسی کند. داده‌ها با مرور نظام‌مند منابع ثانویه، شامل مقاله‌های علمی، گزارش‌های رسمی اتحادیهٔ اروپا و اسناد سیاست‌گذاری مانند دستور کارهای امنیت شبکه و اطلاعات و راهبردهای تواتمندسازی انرژی اروپا گردآوری شده‌اند. انتخاب مطالعات موردی مانند حملهٔ نات‌پتیا در سال ۲۰۱۷ و حمله‌های سایبری به شبکه‌های برق اوکراین در سال ۲۰۱۵، به‌صورت هدفمند انجام شده است تا نمونه‌هایی برجسته و مربوط با تهدیدهای سایبری در بخش انرژی را پوشش دهد. این موارد به‌دلیل تأثیرهای گستردهٔ فراملی و ارتباط مستقیم آن‌ها با امنیت انرژی اتحادیهٔ اروپا انتخاب شده‌اند.

داده‌ها براساس چارچوب نوواقع‌گرایی تدافعی تحلیل شده است. این چارچوب با تأکید بر اقدام‌های تدافعی دولت‌ها در نظام آنارشیک بین‌المللی، به ارزیابی راهبردهای اتحادیهٔ اروپا در برابر تهدیدهای سایبری کمک می‌کند. فرایند تحلیل شامل شناسایی الگوهای حمله‌های سایبری، بررسی پیامدهای آن‌ها بر زیرساخت‌های انرژی و ارزیابی سیاست‌های مقابله‌ای اتحادیهٔ اروپا از دیدگاه بازدارندگی و افزایش تاب‌آوری است. این رویکرد امکان درک عمیق‌تری از تعامل میان امنیت سایبری و امنیت ملی را فراهم می‌کند و برای سیاست‌گذاری پیشنهادهای عملی ارائه می‌دهد.

مطالعات موردی حمله‌های سایبری روسیه و سیاست‌ها و برنامه‌های متقابل اتحادیهٔ اروپا

در این بخش مطالعات موردی هدفمند را تحلیل می‌کنیم تا تأثیر تهدیدهای سایبری روسیه بر امنیت انرژی اتحادیهٔ اروپا و واکنش‌های این اتحادیه را با استفاده از چارچوب نوواقع‌گرایی تدافعی بررسی کنیم. همان‌گونه که در بخش روش پژوهش بیان کردیم، این موارد به‌دلیل ارتباط مستقیم با زیرساخت‌های انرژی و پیامدهای فراملی انتخاب شده‌اند. این تحلیل‌ها نه‌تنها الگوهای حمله‌های سایبری را روشن می‌کنند، بلکه ظرفیت‌ها و محدودیت‌های رویکرد تدافعی اتحادیهٔ اروپا را در برابر تهدیدهای ناهم‌تراز جنگ ترکیبی آشکار می‌کنند.

۱. حملهٔ بدافزار نات‌پتیا در سال ۲۰۱۷

حملهٔ بدافزار نات‌پتیا در سال ۲۰۱۷ یکی از برجسته‌ترین حمله‌های سایبری در تاریخ محسوب می‌شود. این حمله که ابتدا اوکراین را هدف قرار داد، پیامدهایش فراتر از مرزهای این کشور گسترش یافت و زیرساخت‌های حیاتی اروپا، به‌ویژه شبکه‌های انرژی را تهدید کرد (Limnell, 2018: 5). تحلیل‌های امنیت سایبری نشان می‌دهند که نات‌پتیا بخشی از راهبردی گسترده برای بی‌ثبات‌سازی اقتصادهای غربی بود و ارتباط آن با بازیگران در حمایت دولت روسیه، به‌عنوان بخشی از عملیات جنگ ترکیبی، مورد توجه پژوهشگران قرار گرفته است (Pawlak, 2018: 6). این حمله بر امنیت انرژی اتحادیهٔ اروپا تأثیرهای عمیقی برجای گذاشت. بدافزار نات‌پتیا اختلال‌هایی گسترده در شبکه‌های عملیاتی ایجاد کرد که به زنجیرهٔ تأمین انرژی و سیستم‌های کنترل صنعتی در چندین کشور عضو سرایت کرد. این رویداد نه‌تنها عملیات را متوقف کرد، بلکه اعتماد عمومی به امنیت سایبری شبکه‌های انرژی را کاهش داد و آسیب‌پذیری زیرساخت‌های به‌هم‌پیوستهٔ اروپا را آشکار کرد (Vasiliu, 2019: 11). اتحادیه در پاسخ، دستورکارهای امنیتی خود را به‌سرعت به‌روزرسانی و همکاری با ناتو را تقویت کرد (EU Policy on Cyber Defence, 2018). اصلاح دستورکار امنیت شبکه و اطلاعات و گسترش همکاری‌های دفاع سایبری، واکنشی محتاطانه و تدافعی بود که با اصول نوواقع‌گرایی تدافعی هم‌راستاست. تأخیر در هماهنگی واکنش‌ها نشان‌دهندهٔ ضعف‌هایی در انسجام سیاستی اتحادیهٔ اروپا است. این مورد بر ضرورت سیاست‌های یکپارچهٔ دفاع سایبری در حوزهٔ انرژی تأکید می‌کند تا به‌وسیلهٔ هماهنگی بیشتر و استانداردسازی الزام‌های امنیتی، خطرهای سیستماتیک کاهش یابد. در حالی‌که نات‌پتیا نمونه‌ای از حمله‌های سایبری با دامنهٔ گسترده بود، تهدیدهای منطقه‌ای نیز به همان اندازه امنیت انرژی را به چالش کشیده‌اند، همان‌گونه که در ادامه بررسی می‌کنیم.

۲. حمله‌های سایبری به شبکه‌های انرژی در اروپای شرقی

در سال‌های اخیر، حمله‌های سایبری متعددی علیه بخش انرژی کشورهای اروپای شرقی گزارش شده است. این کشورها که به‌عنوان حائلی راهبردی میان روسیه و اتحادیهٔ اروپا قرار دارند، هدف‌هایی اصلی برای نفوذ سایبری و بی‌ثباتی اقتصادی محسوب می‌شوند (Pishchik & Alekseev, 2024). تحلیل‌های امنیتی نشان می‌دهد که گروه‌های سایبری مرتبط با روسیه از فن‌های پیشرفته‌ای مانند جاسوسی و خراب‌کاری بهره می‌برند که بخشی از راهبرد کلان روسیه برای تضعیف توان دفاعی این مناطق است (Limnell, 2018: 6). این حمله‌ها ضعف‌های ساختاری زیرساخت‌های انرژی منطقه را آشکار کرده است. بسیاری از شبکه‌های برق و سیستم‌های کنترل صنعتی همچنان به فناوری‌های قدیمی وابسته‌اند که در برابر بدافزارهای پیچیده آسیب‌پذیرند. این اختلال‌های زنجیرهٔ تأمین انرژی اتحادیه را زیر تأثیر قرار داده و امنیت سایبری را به اولویت سیاستی تبدیل کرده است (Pawlak, 2018: 4). در پاسخ به این تهدیدها، اتحادیهٔ اروپا استانداردهای امنیت سایبری را هماهنگ‌تر کرد و بودجهٔ دفاع سایبری را افزایش داد. افزایش همکاری با ناتو نقش مهمی نیز در ایجاد دفاع سایبری مشترک داشت (Tichy & Dubsky, 2024: 8). با این‌حال تداوم استفاده از سیستم‌های قدیمی نشان‌دهندهٔ چالش‌هایی در نوسازی زیرساخت‌هاست که باید مورد توجه قرار گیرد.

۳. تکامل عملیات سایبری روسیه پس از سال ۲۰۲۲ و اقدام‌های متقابل اتحادیهٔ اروپا

تهاجم روسیه به اوکراین در سال ۲۰۲۲ نقطهٔ عطفی در تکامل عملیات سایبری این کشور بود. از این زمان، فراوانی و پیچیدگی حمله‌های سایبری علیه زیرساخت‌های حیاتی اتحادیه، به‌ویژه بخش انرژی، افزایش یافت. پژوهش‌ها نشان می‌دهند که گروه‌های سایبری مربوط با روسیه عملیات سایبری را به‌عنوان بخشی از جنگ ترکیبی به کار می‌گیرند (Bouramdane, 2023). این تحولات خطر اختلال گسترده در زنجیرهٔ تأمین انرژی را تشدید کرده است. حمله‌های سایبری روسیه نه‌تنها شبکه‌های انرژی، بلکه سامانه‌های کنترل صنعتی را هدف قرار داده‌اند و برای ثبات کشورهای اروپایی پیامدهای عمیقی داشته‌اند. اتحادیهٔ اروپا برنامهٔ توانمندسازی انرژی اروپا را برای کاهش وابستگی به روسیه برای بازدارندگی اجرا کرد (Tichy & Dubsky, 2024: 7). این اقدام‌های محتاطانه با نوواقع‌گرایی تدافعی هم‌راستاست. با وجود این، موفقیت این اقدام‌ها به هماهنگی سریع‌تر میان اعضای وابسته است. افزایش پیچیدگی حمله‌های سایبری به اقدام‌های ترکیبی مانند خراب‌کاری فیزیکی نیز گسترش یافت که در ادامه بررسی می‌کنیم.

۴. خراب‌کاری خط لولهٔ نورد استریم (سپتامبر ۲۰۲۲)

خراب‌کاری خطوط لولهٔ نورد استریم در سپتامبر ۲۰۲۲ رویدادی اصلی در حوزهٔ امنیت انرژی اروپا بود. تحلیل‌های اولیه نشان می‌دهد که این اقدام بخشی از راهبرد روسیه برای مختل‌کردن شریان‌های انرژی اروپا بوده و برخی آن را به تلاش روسیه برای پاسخ به تحریم‌ها نسبت می‌دهند (Sanderson, 2023). این رویداد نوسان‌های قیمتی شدیدی را در بازار انرژی به‌دنبال داشت و آسیب‌پذیری اتحادیه در برابر حمله‌های ترکیبی را آشکار کرد. در مقابل این اقدام، اتحادیه نظارت بر خطوط لوله را افزایش داد و همکاری با ناتو را برای تقویت امنیت گسترش داد. ولی نبود شواهد قطعی در مورد عاملان، پاسخ‌دهی را دشوار کرده است (Han, S., Zhu, 2023). از دیدگاه نوواقع‌گرایی تدافعی، این رویداد نمونه‌ای از مشکل امنیت است که در آن بازیگران برای حفظ امنیت خود، حتی به قیمت افزایش تنش‌ها و بی‌ثباتی، اقدام‌های پیش‌دستانه انجام می‌دهند تا توازن قدرت را در نظام آنارشیک بین‌المللی حفظ کنند. ترکیب تهدیدهای فیزیکی و سایبری به حمله‌های مالی و بدافزاری نیز کشیده شده است که در ادامه بررسی می‌کنیم.

۵. حمله‌های بدافزاری به شرکت‌های انرژی اتحادیهٔ اروپا

حمله‌های بدافزار به شرکت‌های انرژی در اتحادیهٔ اروپا به نگرانی فزاینده تبدیل شده است و برای امنیت انرژی و اقتصاد منطقه تهدیدهای قابل توجهی ایجاد می‌کند. حملهٔ انرژی سیاه[1] به شبکهٔ برق اوکراین در سال ۲۰۱۵ به خاموشی برای ۸۰ هزار مشتری منجر شد و نشان داد که زیرساخت‌های حیاتی به چه میزان آسیب‌پذیر هستند(Kavocs, 2016). یک سال بعد، حملهٔ سایبری دیگری به نام اینداستروییر[2] سبب قطع برق یک ساعته حدود یک‌پنجم شهر کی‌یف شد. همچنین حملهٔ نات‌پتیا در سال ۲۰۱۷ که به‌عنوان پرهزینه‌ترین حملهٔ سایبری در تاریخ شناخته می‌شود، با به‌روزرسانی نرم‌افزار حسابداری در اوکراین منتشر شد و سیستم‌های کامپیوتری هزاران شرکت را نابود کرد و حدود ۱۰ میلیارد دلار خسارت وارد کرد(Wright, 2017).

در سال‌های اخیر حمله‌های بدافزار متعددی علیه شرکت‌های انرژی اتحادیه گزارش شده است که عملیات را مختل و خسارت‌های مالی ایجاد کرده‌اند. شواهد حاکی از ارتباط برخی از

1. BlackEnergy
2. Industroyer

این حمله‌ها با گروه‌های سایبری مرتبط با روسیه است (Fedotenko, 2023). حملهٔ *انرژی سیاه* به شبکه برق اوکراین در سال ۲۰۱۵ نمونه‌ای از راهبرد جنگ ترکیبی روسیه است که با بهره‌گیری از خلأهای نظارتی، زیرساخت‌های انرژی را هدف قرار داد(Blank, 2019). این حمله‌ها اعتماد عمومی را کاهش داده و آسیب‌پذیری‌های نظام‌مند را تشدید کرده‌اند (Vasiliu, 2019: 12). در برابر این حمله‌ها، اتحادیه پروتکل‌های پشتیبان را بهبود داده و همکاری‌های دولتی‌خصوصی را تقویت کرده است (Smith, 2018). اتحادیهٔ اروپا همچنین چارچوبی به نام جعبهٔ ابزار دیپلماسی سایبری[1] را در سال ۲۰۱۷ تصویب کرد که بر بهبود همکاری، جلوگیری از درگیری، کاهش تهدیدهای سایبری بالقوه و تأثیرگذاری بر رفتار متجاوزان بالقوه تمرکز دارد. در سال ۲۰۱۸ نیز لایحه‌ای به نام فعالیت‌های سایبری مخرب را تصویب کرد و نگرانی خود را از افزایش توانایی و تمایل کشورهای دیگر و بازیگران غیردولتی برای پیگیری هدف‌های خود به‌وسیلهٔ انجام فعالیت‌های مخرب سایبری ابراز کرد. کمیسیون اروپا اقدام‌های جدیدی نیز برای مقابله با حمله‌های سایبری به کار گرفته است، از جمله به اشتراک‌گذاری اطلاعات و نفوذ سیستم و تست اعتماد سیستم (Ivan, 2019: 5). با وجود این، تأخیر در به‌روزرسانی سیستم‌ها همچنان اتحادیه را آسیب‌پذیر نگه داشته است. این‌گونه واکنش‌های اتحادیهٔ اروپا در قالب تقویت پروتکل‌ها و همکاری‌ها، نمونه‌ای از رفتار دولت‌ها در چارچوب نوواقع‌گرایی تدافعی است که بر حفظ امنیت و بقا در نظام آنارشیک بین‌المللی تأکید دارد. از این دیدگاه، دولت‌ها با به‌کارگرفتن تدبیرهای دفاعی و موازنه‌سازی امنیتی تلاش می‌کنند تهدیدها را کاهش دهند و از آسیب‌پذیری‌های خود بکاهند، بدون اینکه به‌ضرورت به‌دنبال افزایش بیش از حد قدرت باشند.

تحلیل این مطالعات موردی نشان می‌دهد که حمله‌های سایبری روسیه، چه به‌صورت مستقل و چه در ترکیب با اقدام‌های ترکیبی، برای امنیت انرژی اتحادیهٔ اروپا تهدیدی جدی به شمار می‌روند. واکنش‌های اتحادیه، از جمله تقویت سیاست‌های سایبری، همکاری با ناتو و اجرای برنامه‌هایی مانند توانمندسازی انرژی اتحادیهٔ اروپا، نشان‌دهندهٔ رویکردی تدافعی است که با نوواقع‌گرایی تدافعی هم‌خوانی دارد. ولی چالش‌هایی مانند نبود هماهنگی سریع، وابستگی به سیستم‌های قدیمی و دشواری شناسایی عاملان حمله‌ها، کارایی این اقدام‌ها را محدود کرده است.

1. EU Cyber Diplomacy Toolbox

تحلیل راهبردهای اتحادیهٔ اروپا در برابر تهدیدهای سایبری روسیه

در این بخش با تکیه بر یافته‌های مطالعات موردی و چارچوب نوواقع‌گرایی تدافعی، به ارزیابی راهبردهای امنیتی اتحادیهٔ اروپا، ارائهٔ راهکارهای سیاستی و ترسیم چشم‌انداز آیندهٔ امنیت انرژی می‌پردازیم. همان‌گونه که در بخش روش پژوهش بیان کردیم، تحلیل کیفی این نوشتار بر الگوهای حمله‌های سایبری روسیه و پاسخ‌های اتحادیهٔ اروپا متمرکز است. این بررسی نه‌تنها کارایی رویکرد تدافعی اتحادیه را در برابر تهدیدهای سایبری روشن می‌کند، بلکه پیشنهادهایی عملی برای افزایش تاب‌آوری در برابر چالش‌های ژئوپلیتیکی و فناورانه ارائه می‌دهد.

ارزیابی راهبردهای امنیتی اتحادیهٔ اروپا در چارچوب نوواقع‌گرایی تدافعی

نوواقع‌گرایی تدافعی، به‌عنوان چارچوب نظری این نوشتار، بر این اصل استوار است که در نظام بین‌المللی آنارشیک، دولت‌ها برای حفظ امنیت و بقای خود به اقدام‌های تدافعی و بازدارنده متکی می‌شوند. واکنش‌های اتحادیهٔ اروپا به تهدیدهای سایبری روسیه علیه امنیت انرژی، از جمله تقویت سیاست‌های امنیت سایبری، گسترش همکاری با ناتو و کاربست تحریم‌های اقتصادی، با این چارچوب هم‌راستاست. این اقدام‌ها نشان‌دهندهٔ تلاش اتحادیه برای ایجاد توازن قدرت و کاهش آسیب‌پذیری‌ها بدون تحریک مستقیم تنش‌های نظامی است، رویکردی که با تأکید نوواقع‌گرایی تدافعی بر بازدارندگی و پرهیز از رویارویی تهاجمی سازگار است.

تحریم‌های اتحادیه اروپا علیه بخش انرژی روسیه، که پس از تهاجم این کشور به اوکراین در سال ۲۰۲۲ اعمال شد، نمونه‌ای بارز از این رویکرد تدافعی است. این تحریم‌ها با هدف محدود کردن درآمدهای انرژی روسیه و کاهش وابستگی اروپا به منابع روسی طراحی شدند. بر اساس پژوهش‌ها، این تحریم‌ها منجر به تغییرهای ساختاری در زنجیره تأمین انرژی جهانی شده‌اند، از جمله کاهش صادرات انرژی روسیه به اروپا و افزایش تنوع‌بخشی به منابع انرژی اتحادیه اروپا از راه واردات از کشورهایی مانند نروژ، ایالات متحد و خاورمیانه (نیکنامی، ۱۴۰۳: ۲۴). این تغییرها نه تنها بر اقتصاد روسیه تأثیر گذاشته، بلکه نشان‌دهنده تلاش اتحادیه اروپا برای افزایش انعطاف‌پذیری و امنیت انرژی در بلندمدت است.

تحلیل مطالعات موردی، مانند حملهٔ نات‌پتیا در سال ۲۰۱۷ و خراب‌کاری خط لولهٔ نورد استریم در سال ۲۰۲۲ نشان می‌دهد که این راهبرد تدافعی با چالش‌هایی روبه‌رو است. نخست، سرشت ناهم‌تراز حمله‌های سایبری که بیشتر، گروه‌های هکری وابسته به دولت انجام می‌دهند، شناسایی عاملان و پاسخ‌گویی مستقیم را دشوار می‌کند (Pawlak, 2018: 7). دوم، وابستگی

متقابل زیرساخت‌های انرژی در اتحادیهٔ اروپا، برخلاف فرض استقلال واحدهای سیاسی در نوواقع‌گرایی، به این معناست که اختلال در یک کشور می‌تواند کل منطقه را در تأثیر قرار دهد. این محدودیت‌ها کارایی اقدام‌های دفاعی سنتی را کاهش می‌دهد و نیاز به هماهنگی فراتر از سطح ملی را برجسته می‌کند. همچنین ناهماهنگی در اجرای سیاست‌ها میان کشورهای عضو، مانند تأخیر برخی اعضا در پیاده‌سازی دستورکارهای امنیت شبکه و اطلاعات[1]، انسجام دفاعی اتحادیه را تضعیف کرده است (Vasiliu, 2019: 14). در این راستا، اتحادیه اروپا برای تبدیل شدن به یک بازیگر منسجم در زمینه امنیت سایبری با چالش‌هایی از جمله تعدد بازیگران، نهادها و مؤسسه‌ها و احتمال تضاد منافع میان آنها روبه‌رو است. با وجود این، اتحادیه اروپا با انتشار راهبردها، دستورعمل‌ها و مقررات تلاش کرده است تا این تعدد خللی در رویکرد یکپارچه آن ایجاد نکند. با این حال، تنها انتشار این اسناد کافی نیست و وجود شفافیت، مشارکت و پاسخ‌گویی نیز برای موفقیت ضروری است (Rohami, 2022: 25). در مجموع، اگرچه رویکرد دفاعی اتحادیهٔ اروپا با اصول نوواقع‌گرایی هم‌خوانی دارد، موفقیت آن به رفع این شکاف‌ها و سازگاری با پویایی‌های فضای سایبری وابسته است.

افزایش تاب‌آوری امنیت انرژی اتحادیهٔ اروپا

یافته‌های این نوشتار نشان می‌دهند که تهدیدهای سایبری روسیه علیه امنیت انرژی اتحادیهٔ اروپا، به‌ویژه پس از تهاجم به اوکراین در سال ۲۰۲۲، پیچیدگی و شدت بیشتری یافته‌است. برای مقابله با این تهدیدها و تقویت تاب‌آوری، تقویت هماهنگی میان کشورهای عضو ضروری است، زیرا ناهماهنگی سیاستی یکی از موانع اصلی در اجرای مؤثر اقدام‌های امنیت سایبری به شمار می‌رود. در این زمینه، اتحادیهٔ اروپا باید برای استانداردسازی پروتکل‌های امنیتی زیرساخت‌های انرژی، چارچوبی الزام‌آور تدوین کند. سرمایه‌گذاری در نوسازی زیرساخت‌ها اهمیت فراوانی دارد، زیرا وابستگی به سیستم‌های قدیمی کنترل صنعتی، همان‌گونه که در حمله به شبکه‌های برق اروپای شرقی دیده شد، آسیب‌پذیری‌ها را تشدید کرده است و تخصیص بودجه برای جایگزینی این سیستم‌ها با فناوری‌های مقاوم در برابر حمله‌های سایبری ضروری است.

همچنین تعمیق همکاری‌های بین‌المللی به‌دلیل سرشت فراملی تهدیدهای سایبری اهمیت دارد.

1. NIS Directive

برگزاری رزمایش‌های مشترک سایبری و ایجاد سازوکارهای اشتراک‌گذاری سریع اطلاعات می‌تواند بازدارندگی را تقویت کند. توسعهٔ قابلیت‌های مبتنی بر فناوری نیز از دیگر راهکارها است. استفاده از هوش مصنوعی برای تشخیص زودهنگام تهدیدها و بهره‌گیری از فناوری بلاک‌چین برای ایمن‌سازی ارتباطات زیرساختی می‌تواند پاسخ‌گویی اتحادیه را بهبود بخشد. افزایش شفافیت و پاسخ‌گویی به‌وسیلهٔ ایجاد پایگاه دادهٔ مشترک تهدیدهای سایبری، به رفع ضعف‌های ناشی از نبود اشتراک‌گذاری اطلاعات میان بخش دولتی و خصوصی کمک می‌کند.

نتیجه

در این نوشتار تأثیر تهدیدهای سایبری روسیه بر امنیت انرژی اتحادیهٔ اروپا و واکنش‌های این اتحادیه را بررسی و از چارچوب نوواقع‌گرایی تدافعی به‌عنوان راهنمای نظری استفاده کردیم. با اتکا به رویکرد کیفی، داده‌ها را با مرور نظام‌مند ادبیات و تحلیل مطالعات موردی هدفمند گردآوری کردیم تا ابعاد عملی و نظری این تهدیدها و پاسخ‌های اتحادیه را ارزیابی کنیم. یافته‌های پژوهش نشان داد که حمله‌های سایبری، به‌ویژه پس از تهاجم روسیه به اوکراین در سال ۲۰۲۲، بخشی از راهبرد جنگ ترکیبی این کشور برای بی‌ثبات‌سازی اروپا هستند. این تهدیدها نه‌تنها زیرساخت‌های حیاتی انرژی را هدف قرار داده‌اند، بلکه با بهره‌گیری از پیچیدگی‌های فناورانه و سرشت ناهم‌تراز خود، مشکل امنیتی را تشدید کرده‌اند که با افزایش اقدام‌های تدافعی اتحادیهٔ اروپا ممکن است از سوی روسیه تهدید براورد شود.

یافته‌ها نشان می‌دهد که رویکرد تدافعی اتحادیهٔ اروپا، شامل تقویت سیاست‌های امنیت سایبری، گسترش همکاری‌های بین‌المللی، و کاربست تحریم‌های اقتصادی، با اصول نوواقع‌گرایی تدافعی، مانند بازدارندگی و حفظ توازن قدرت، هم‌خوانی دارد. با وجود این، چالش‌هایی مانند ناهماهنگی میان کشورهای عضو، وابستگی به سیستم‌های قدیمی و دشواری شناسایی عاملان حمله‌ها که در مواردی مانند خراب‌کاری نورد استریم مشهود بود، کارایی این اقدام‌ها را محدود کرده است. این محدودیت‌ها ناکافی‌بودن رویکردهای سنتی در برابر تهدیدهای نوین سایبری را نشان می‌دهد و بر ضرورت سازگاری اقدام‌ها تأکید دارد. ازاین‌رو، پیشنهاد می‌کنیم که اتحادیهٔ اروپا چارچوب‌های الزام‌آوری برای هماهنگی سیاستی میان اعضا تدوین کند، در نوسازی زیرساخت‌ها با فناوری‌های مقاوم در برابر حمله‌های سایبری سرمایه‌گذاری کند و همکاری با شریک‌های بین‌المللی را با رزمایش‌های مشترک و اشتراک‌گذاری اطلاعات تقویت کند. سرانجام در این نوشتار به این نتیجه رسیدیم که امنیت انرژی، به‌عنوان پایهٔ ثبات اقتصادی و سیاسی اتحادیهٔ اروپا، نیازمند بازنگری فوری

در سیاست‌های دفاعی سایبری و سازگاری سریع با تهدیدهای نوپدید است. تداوم وضعیت کنونی می‌تواند آسیب‌پذیری اتحادیهٔ اروپا را در برابر حمله‌های ترکیبی در حال گسترش تشدید کند.

منابع

فارسی

کتانچی، الناز و بابک پورقهرمانی (۱۳۹۸) «سیاست‌های نمادین کنوانسیون جرایم سایبری شورای اروپا»، **فصلنامه مطالعات بین‌المللی**، دوره ۱۶، شماره ۶۲، صص. ۳۱-۴۷، (doi: 10.22034/isj.2019.99238).

فرشاسعید، پرویز و محمود جلالی و مهناز گودرزی (۱۴۰۱)، «ضرورت تقویت امنیت سایبری در بخش انرژی توسط دولت‌ها»، **مطالعات حقوق انرژی**، دوره ۸، شماره ۱، صص. ۱۷۳-۱۹۳، (doi: 10.22059/jrels.2022.316656.4).

نیکنامی، رکسانا (۱۴۰۳)، «تحریم های انرژی اتحادیه اروپا علیه فدراسیون روسیه و تأثیر آن بر نظام تجاری آنها (۲۰۲۲-۲۰۲۴)»، **مطالعات اوراسیای مرکزی**، دوره ۱۷، شماره ۱، صص. ۳۶۳-۳۹۰، (doi: 10.22059/jcep.2024.379436.45023).

رهامی، روح الله و امیرحسین اژدری (۱۴۰۱)، «امنیت سایبری اتحادیه اروپا: تهدیدها، فرصت ها و اقدامات (از آغاز تا ۲۰۲۱)»، **فصلنامه تحقیقات حقوقی**، دوره ۲۵، شماره ۱، ۲۵ (ویژه نامه حقوق و فناوری)، صص. ۲۷۳-۳۰۲، (doi: 10.52547/jlr.2023.228106.226).

صابری، سارا و مهتاب کوهی‌زاده، جوزف سرکیس و لجیا شن (۲۰۱۸)، «فناوری بلاکچین و روابط آن با مدیریت زنجیره تأمین پایدار»، **مجله بین المللی تحقیقات تولید**، دوره ۵۷، شماره ۳، صص. ۱-۱۹، (doi:10.1080/00207543.2018.1533261).

قنبری، سمیه و حسین‌خانی (۲۰۱۹) «بازدارندگی سایبری روسیه از دیدگاه اروپایی»، **فصلنامه مطالعات آسیای مرکزی و قفقاز**، دوره ۲۶، شماره ۱، صص. ۱۱۷-۱۵۶، قابل دسترسی: http://ca.ipisjournals.ir/article_242984.html.

English

Aljohani, Tawfiq (2022), "Cyberattacks on Energy Infrastructures: Modern War Weapons", **IEEE Technology and Society Magazine**, (doi: 10.48550/arXiv.2208.14225).

Arslan, Ahmet (2023), "Neorealist Analysis of Security Dilemma in Cyberspace; A Quantitative Study", **APSA Preprints**, (doi: 10.33774/apsa-2023-wvw2z-v9).

Bélaïd, Fateh and Aisha Sarihi (2023), "Balancing Climate Mitigation and Energy

Security Goals amid Converging Global Energy Crises: The Role of Green Investments", **Renewable Energy**, Vol. 205, No. 2023, pp. 534-54, (doi: 10.1016/j.renenenene.2023.01.083).

Blank, Stephen (2024), **The Russian Military in Contemporary Perspective**, translated by Elaheh Koolaee and Seyyedeh Motahereh Hosseini, Tehran: University of Tehran Press, [in Persian].

Bouramdane, Ayat-Allah (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**, Vol. 3, No. 2, pp. 662-705, (doi:.org/ 10.3390/jcp3040031).

Buinevich, Mikhail and Grigory Moiseenko (2023), "Combining of Heterogeneous Destructive Impact on the Information System and Countering Attacks (on Example by Insider Activity and DdoS-Attack)", **Telecom IT**, (doi:.org/10.31854/2307-1303-2023-11-3-27-36).

Wüest, Candid (2014), "Targeted Attacks against the Energy Sector", **Symantec Corporation**, Available at: https://icscsi.org/library/Documents/Cyber_Events/Symantec%20-%20Targeted%20Attacks%20Against%20the%20Energy%20Sector.pdf (Accessed on: 13/11/2024).

Cao, Yang, Wei Wei, Jianhui Wang, Shengwei Mei, Miadreza Shafie-khah and Catalão (2020), "Capacity Planning of Energy Hub in Multi-Carrier Energy Networks: A Data-Driven Robust Stochastic Programming Approach", **IEEE Transactions on Sustainable Energy**, Vol. 11, No. 1, pp. 3-14, (doi: 10.1109/TSTE.2018.2878230).

Chaikin, Marc (2023), "Problems and Prospects of Implementing Assessment of the Level of Maturity of Cyber Security Processes of Critical Infrastructure Objects of the Energy Sector of Ukraine in Accordance with the NIST Cybersecurity Framework", **Èlektronnoe Modelirovanie**, (doi: 10.15407/emodel.45.05.08).

European Union Agency for Cybersecurity (ENISA), (2018), "EU Policy on Cyber Defence: Strengthening Europe's Cyber Resilience", **ENISA Publications**, Available at: https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf (Accessed on: 10/11/2024).

Fedotenko, Kateryna (2023), "Cyber Warfare as Part of Information Warfare of Russia against Ukraine since the Beginning of the 2022 Russian Invasion", **Věda a Perspektivy**, (doi: 10.52058/2695-1592-2023-8(27)-351-357), [in Russian].

Hartvig, Áron Dénest Kiss-Dobronyi, Kotek, Takácsné Tóth, Iaonic Gutzianasand

Zareczky and András Zsombor (2024), "The Economic and Energy Security Implications of the Russian Energy Weapon", **Energy**, (doi: 10.1016/j.energy.2024.130972).

Ivan, Paul (2019), "Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox", **EPC Discussion Paper**, Available at: http://aei.pitt.edu/id/eprint/9707, (Accessed on: 18/03/2025).

Kavocs, Eduard (2016), "Ukraine Power Grid Attacks Part of a 2-Year Campaign", Available at: https://www.securityweek.com/ukraine-power-grid-attacks-part-2-year-campaign, (Accessed on: 12/2/2025)

Krzykowski, Michał (2021), "Legal Aspects of Cybersecurity in the Energy Sector—Current State and Latest Proposals of Legislative Changes by the EU", **Energies**, Vol. 14, No. 23, pp. 1-14,
(doi: 10.3390/en14237836).

Limnell, jarno (2018), "Cyber Threats and Energy Security in the European Union: Strategic Implications and Policy Responses", **Journal of Cyber Policy**, Vol. 3, No. 2, pp. 187–202. Available at: https://www.jstor.org/stable/pdf/resrep21140.10.pdf (Accessed on: 18/03/2025).

Lin, Faqin, Xuecao Li, Ningyuan Jia, Fan Feng, Hai Huang, Jianxi Huang, Shenggen Fan, Philippe Ciais and Xiao-Peng Song (2023), "The Impact of Russia-Ukraine Conflict on Global Food Security", **Global Food Security**, Vol. 36, No. 2, pp. 17-25, (doi: 10.1016/j.gfs.2022.100661).

Maliki, Musa (2022), "The Ideology Critique of Mearsheimer's Theory of Offensive Neorealism: The Case of Russia-Ukraine War and Its Ideologization in Indonesia", **Journal of Global Strategic Studies**, (doi: 10.36859/jgss. V2i2.1212).

Molchanov, Matevosova (2020), "Energy Security in the Age of Digitalization", **Courier of Kutafin Moscow State Law University** (MSAL), Vol. 3, No. 67, pp. 86-95, (doi: 10.17803/2311-5998.2020.67.3.086-095).

Nawrocki, Tomasz and Jonek-Kowalska (2023), "Efficiency of Polish Energy Companies in the Context of EU Climate Policy", **Energies**, (doi: 10.3390/en16020826).

Pawlak, Patryk (2018), "Energy Security and Cyber Warfare: The Role of State and Non-State Actors in EU Cyber Resilience", **European Journal of Security Studies**, Vol. 6, No. 1, pp. 45–67, Available at: https://www.jstor.org/stable/pdf/resrep21140.14.pdf, (Accessed on: 18/03/2025).

Pishchik, Victor and Petr V. Alekseev (2024), "Current Cybersecurity Issues in Russia: Global and National Aspects", **Теория и Практика Общественного**

Развития, Vol. 24, No. 10, pp. 112–121, (doi:10.24158/tipor.2024.10.15), [in Russian].

Schmitz-Berndt, Sandra and Pier Giorgio Chiara (2022), "One Step Ahead: Mapping the Italian and German Cybersecurity Laws Against the Proposal for a NIS2 Directive", Vol. 3, No. 2, pp. 1-23, **International Cybersecurity Law Review**, https://link.springer.com/article/10.1365/s43439-022-00058-7, (Accessed on: 25/01/2025).

Shestak, Viktor and Alyona Tsyplakova (2023), "Countering Cyberattacks on the Energy Sector in the Russian Federation and the USA", **BRICS Law Journal**, (doi: 10.21684/2412-2343-2023-10-4-35-52).

Sun, Nan, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo and Yonghang Tai (2023), "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives", **IEEE Communications Surveys and Tutorials**, (doi:10.1109/COMST.2023.3273282).

Taliaferro, Jeffrey (2000), "Security Seeking under Anarchy: Defensive Realism Revisited", **International Security**, Vol. 25, No. 3, pp. 128-151, (doi: 10.1162/016228800560635).

Tichy, Lukáš and Zbyněk Dubsky (2024), "Cybersecurity in the European Energy Sector: Challenges and Policy Developments", **Energy Policy Review**, Vol. 55, No. 1, pp. 92–108, (doi: 10.1016/j.exis.2023.101392).

Tin, Derrick, Dennis G. Barten, Fredrik Granholm, Pavlo Kovtonyuk, Frederick M. Burkle and Gregory R. Ciottone (2023), "Hybrid Warfare and Counter-Terrorism Medicine", **European Journal of Trauma and Emergency Surgery**, Available at: https://link.springer.com/article/10.1007/s00068-023-02230-y, (Accessed on: 10/02/2025).

Vasiliu, Tomas (2019), "Cybersecurity Strategies for Critical Infrastructure Protection in the European Union", **International Journal of Security Studies**, Vol. 12, No. 3, pp. 211–228, Available at: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/12412/Vasileiou_18012.pdf?sequence=2&isAllowed=y, (Accessed on: 14/02/2024).

Long Vu, Thanh, Sayak Mukherjee, Renke Huang and Qiuhua Hung (2021), "Barrier Function-Based Safe Reinforcement Learning for Emergency Control of Power Systems", **60th IEEE Conference on Decision and Control** (CDC), pp. 3652-3657, IEEE,
(doi: 10.1109/CDC45484.2021.9683573).

Waltz, Kenneth (1979), "Theory of International Politics", **Addison-Wesley Publishing**, Available at: https://dl1.cuni.cz/pluginfile.php/486328/mod_resource/content/0/Kenneth%20N.%20Waltz%20Theory%20of%20International%20Politics%20Addison-

Wesley%20series%20in%20political%20science%20%20%20%201979.pdf, (Accessed on: 15/11/2024).

Watney, Murdoch (2022), "Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: A Legal Perspective", **European Conference on Cyber Warfare and Security**, Vol. 21, No. 1, pp. 319-327, (doi:10.34190/eccws.21.1.196).

Wójtowicz, Anna (2024), "EU Energy Security after Russia's Invasion of Ukraine– Substance, Strategy and Lobbying", **Studia Europejskie**, Vol. 28, No. 2, pp. 157-171, (doi: 10.33067/SE.2.2024.8).

Wright, Rob (2017), "Industroyer malware a turning point for ICS security", Available at: https://www.techtarget.com/searchsecurity/news/450423487/Industroyer-malware-a-turning-point-for-ICS-security, (Accessed on: 8/2/2025).

Yakoviyk, Ivan and Maksym Tsvelikh (2023), "Energy Security of the European Union in the Context of Russian Aggression against Ukraine", **Problems of Legality**, Vol. 23, No. 160, pp. 170–191, (doi:10.21564/2414-990x. 160.274518).