

ЗАПЛАХИТЕ ПРЕД ЕНЕРГОПРЕНОСНИТЕ СИСТЕМИ КАТО ИНСТРУМЕНТ В МОДЕРНОТО СЪРЕВНОВАНИЕ НА ВЕЛИКИТЕ СИЛИ В КОНТЕКСТА НА КИБЕРПРОСТРАНСТВОТО

ас. Димитър Събев Димитров

Висше военноморско училище „Н. Й. Вапцаров“ – Варна

E-mail: ds.dimitrov@naval-acad.bg

Резюме: Статията разглежда заплахите пред енергопреносните системи като елемент от модерното стратегическо съревнование в киберпространството. Фокусът е поставен не върху отделни видове зловреден софтуер, а върху механизмите, чрез които достъпът до електроенергийна инфраструктура може да създава разузнавателни, принудителни и оперативни предимства. Анализирани са предварителното позициониране в мрежите, компрометирането на идентичности и отдалечен достъп, манипулирането на данни за състоянието на мрежата, веригите на доставки, нарушенията на наличността и зависимостите между енергетика, комуникации, транспорт и военна логистика.

Ключови думи: енергопреносни системи, критична инфраструктура, стратегическо съревнование, кибероперации, предварително позициониране, оперативна устойчивост.

THREATS TO POWER TRANSMISSION SYSTEMS AS AN INSTRUMENT IN MODERN GREAT-POWER COMPETITION IN CYBERSPACE

Assist. Dimitar S. Dimitrov

Nikola Vaptsarov Naval Academy – Varna

E-mail: ds.dimitrov@naval-acad.bg

Abstract: This article examines threats to power transmission systems as an element of modern strategic competition in cyberspace. The focus is placed not on individual types of malware, but on the mechanisms through which access to electrical energy infrastructure can generate intelligence, coercive, and operational advantages. The analysis covers pre-positioning within networks, identity compromise and remote access, manipulation of grid-state data, supply-chain risks, disruptions to availability, and the interdependencies among energy, communications, transport, and military logistics.

Keywords: power transmission systems, critical infrastructure, strategic competition, cyber operations, pre-positioning, operational resilience.

1. ВЪВЕДЕНИЕ

Електроенергийната инфраструктура е едновременно техническа система и стратегическа предпоставка за функционирането на съвременната държава. Енергопреносните мрежи поддържат не само производството и потреблението на електроенергия, а комуникации, транспорт, здравеопазване, цифрови услуги, държавно управление и отбранителни дейности. Именно тази системна зависимост превръща киберриска за електропреноса в проблем, който надхвърля границите на отделния оператор. При нарушение на управлението или продължително отпадане на електрозахранването последствията могат да се разпространяват между сектори и да ограничат способността на публичните институции и въоръжените сили да изпълняват основни функции (NATO, 2026).

В модерното съревнование между велики сили киберпространството предоставя възможност за продължително взаимодействие под прага на открития въоръжен конфликт. Киберкампаниите могат да съчетават разузнаване, придобиване на достъп, поддържане на скрити позиции и подготовка на опции за бъдещо въздействие, без всяка отделна операция да има незабавен разрушителен резултат (Harknett and Smeets, 2022). По тази причина стратегическата оценка на заплахите към енергопреносните системи не следва да започва едва при прекъсването на електроснабдяването. Значение имат и дейностите, които дават на противника знания за архитектурата, резервните механизми, зависимостите, процедурите и точките, в които локален цифров достъп може да бъде преобразуван в непропорционално голям ефект (Nikolov, 2026).

Статията има обзорец характер и изследва как киберзаплахи към енергопреносната инфраструктура могат да се използват като инструмент на стратегическо позициониране, принуда и ограничаване на свободата на действие. Публичните източници не предоставят симетрична видимост върху кибероперациите на всички велики сили, част от държавните способности остават класифицирани и публичните атрибуции отразяват преди всичко гледната точка на институциите, които ги публикуват. Поради това разглежданите случаи се използват като примери за модели на поведение, а не като класация или изчерпателно описание на национални кибердоктрини.

2. ЕНЕРГОПРЕНОСНИТЕ СИСТЕМИ КАТО СТРАТЕГИЧЕСКА ЗАВИСИМОСТ

Енергопреносната система представлява кибер-физическа среда, в която центрове за управление, SCADA и енергийни мениджмънт системи, подстанции, защитни релета, интелигентни електронни устройства, RTU, PLC и комуникационна инфраструктура участват в наблюдението и управлението на физическия поток на електроенергия. Цифровизацията увеличава наблюдаемостта и автоматизацията, но същевременно свързва технологичните процеси с корпоративни мрежи, външни доставчици, дистанционна поддръжка и широк набор от софтуерни и комуникационни зависимости. Така атакуемата повърхност не се ограничава до отделна подстанция или контролер, а включва цяла екосистема от идентичности, услуги, устройства и доверени връзки (Stouffer et al., 2023; Zografopoulos et al., 2021).

Стратегическата стойност на електропреноса произтича от неговата функция на инфраструктура, която поддържа други инфраструктури. Авария в комуникациите може да затрудни управлението на електрическата мрежа, но и обратното – загубата на електрозахранване може да засегне телекомуникационни възли, транспортни системи, логистични центрове и центрове за управление. НАТО включва устойчивото енергоснабдяване сред базовите изисквания за съюзна устойчивост и го свързва с поддръжката на военни планове, Host Nation Support, междусекторните зависимости и способността за бързо възстановяване след стратегически шок (NATO, 2026). В този смисъл кибероперация срещу енергопреносна система може да бъде насочена не само към самата електроенергийна услуга, а към вторичните функции, които зависят от нея.

Особеностите на ОТ допълнително увеличават стойността на предварителното разузнаване. Дългите жизнени цикли, необходимостта от висока наличност, ограничените прозорци за обновяване и наличието на наследени протоколи създават среда, в която промяната трябва да бъде внимателно контролирана. NIST подчертава, че мерките за защита на ОТ трябва да бъдат съобразени с изискванията за надеждност, производителност и безопасност на физическия процес (Stouffer et al., 2023). За нападателя това означава, че познаването на работния режим, конфигурацията и реакциите на оператора може да бъде също толкова важно, колкото самото техническо проникване.

3. КАТЕГОРИИ КИБЕРЗАПЛАХИ КЪМ ЕНЕРГОПРЕНОСНАТА ИНФРАСТРУКТУРА

Първата категория е компрометирането на идентичности, устройства за отдалечен достъп и доверени административни канали. Реални кампании срещу енергийни организации показват използване на валидни акаунти, VPN, RDP, интернет-достъпни устройства и инфраструктура на трети страни като вход към вътрешни мрежи (CISA, FBI and DOE, 2022). Този тип достъп има стратегическа стойност, когато може да бъде запазен продължително и да позволи наблюдение на мрежовата архитектура, процедурите и взаимоотношенията между ИТ и ОТ. В такъв сценарий компрометирането не е краен резултат, а средство за натрупване на знания и за създаване на опция за действие при бъдеща криза.

Втората категория засяга целостта на оперативните данни. Електропреносните системи зависят от телеметрия, измервания и state estimation, чрез които операторът формира картина за текущото състояние на мрежата. Внимателно конструирани false data injection атаки могат теоретично да манипулират оценката на състоянието, без непременно да бъдат уловени от традиционни механизми за откриване на лоши измервания (Abudin et al., 2024). От стратегическа гледна точка атаката срещу целостта може да бъде по-трудна за разпознаване от директното спиране на система: тя цели да промени решенията на оператора, да затрудни ситуационната осведоменост или да създаде неправилна оценка на риска.

Третата категория обхваща нарушенията на наличността – DDoS, ransomware, destructive действия и прекъсване на поддържащи ИТ услуги. ENISA отчита, че в европейския енергиен сектор DDoS и ransomware остават сред най-често наблюдаваните заплахи, а нарастващата зависимост от ICT увеличава експозицията на целия сектор (ENISA, 2025). Дори когато атаката не достига до ОТ, загубата на корпоративни услуги, идентичности, комуникации или системи за планиране може да принуди оператора да премине към ограничен режим на работа. Следователно стратегическият ефект може да се постигне и чрез нарушаване на организационната способност за управление и възстановяване, а не само чрез пряка команда към физическо устройство (Nikolov and Nikolov, 2024).

Четвъртата категория е рискът от веригата на доставки и доверените доставчици. Електропреносните оператори използват специализиран хардуер, firmware, инженерни инструменти, облачни услуги, телекомуникации и външна поддръжка. Компрометирането на доставчик или на общ компонент може да създаде мащабируем

вход към повече от една организация. Тази логика е особено важна в съревнование между държави, защото превръща зависимостите от технологии и услуги в част от стратегическия риск. Директивата на ЕС за устойчивостта на критичните субекти изисква оценка на рисковете и мерки за предотвратяване, защита, реагиране и възстановяване, а европейският мрежов код за киберсигурността на трансграничните електроенергийни потоци поставя акцент върху общи минимални изисквания, мониторинг, докладване и управление на кризи (European Parliament and Council, 2022; European Commission, 2024).

4. ОТ ТЕХНИЧЕСКИ ДОСТЪП ДО СТРАТЕГИЧЕСКО ПРЕИМУЩЕСТВО

Наличието на технически достъп до енергийна организация не е равнозначно на способност за контрол върху електропреносната мрежа. Между двете има съществена разлика, която включва познаване на топологията, правата на отделните акаунти, връзките към подстанциите, процедурите за превключване, резервните канали и механизмите за възстановяване (Николов, 2025). Въпреки това именно продължителният достъп създава условия тази разлика постепенно да бъде преодоляна. Съвместното предупреждение на CISA, NSA, FBI и международни партньори за Volt Turphoon оценява, че наблюдаваното поведение на свързани с КНР участници е насочено към предварително позициониране в мрежи на критична инфраструктура с възможност за последващо придвижване към ОТ и нарушаване на функции при бъдеща криза или конфликт (CISA et al., 2024). Тази оценка е показателна за стратегическата логика на достъпа като резервна опция, а не само като средство за класически кибершпионаж.

Подобна логика се наблюдава и в публични оценки за руски държавно подкрепяни операции срещу енергийния сектор. CISA, FBI и DOE описват многогодишни кампании, при които са придобивани отдалечен достъп, идентификационни данни и информация за enterprise и ICS среди, включително чрез доверена инфраструктура и услуги за отдалечено администриране (CISA, FBI and DOE, 2022). Различните случаи не трябва да бъдат механично приравнявани, но показват общ принцип: в стратегическото съревнование стойността на проникването може да бъде отложена във времето. Достъпът може да се използва за разузнаване днес, за

сигнализиране на способност утре или за оперативно въздействие при промяна на политическата и военната обстановка.

Енергопреносната инфраструктура предоставя и специфична възможност за непряк натиск. Не е необходимо да бъде предизвикан национален blackout, за да възникне стратегически ефект. Ограничено, но добре избрано нарушение може да засегне логистичен възел, комуникационна инфраструктура, индустриален район или обект с значение за военна мобилност. При взаимосвързани мрежи локалното действие може да изисква преразпределение на ресурси, активиране на резерви и промяна на оперативни планове. Точно затова устойчивостта на енергоснабдяването е включена в съюзното гражданско планиране за поддръжка на военни операции и Host Nation Support (NATO, 2026).

5. СЪРЕВНОВАНИЕ ПОД ПРАГА НА ВЪОРЪЖЕН КОНФЛИКТ

Киберпространството позволява действия с неясна граница между шпионаж, подготовка на средата, саботаж и сигнализация. Тази двусмисленост е особено съществена при критична инфраструктура. Компрометиран акаунт или устройство може да служи за наблюдение, но същият достъп може да бъде използван и за по-нататъшно проникване. Затова намерението невинаги може да бъде изведено само от техническия артефакт. Harknett и Smeets подчертават, че стратегическите резултати от киберкампаниите често са кумулативни и се формират чрез последователни взаимодействия във времето (Harknett and Smeets, 2022). За енергопреносните системи това означава, че защитата трябва да следи не само за финалния разрушителен акт, а за процеса на изграждане на позиция.

Предварителното позициониране има и принудителен потенциал. Ако в период на политическо напрежение една държава счита, че критичните ѝ мрежи могат да бъдат нарушени, тя може да бъде принудена да отдели допълнителни ресурси за защита, да промени планове или да приеме по-висока несигурност при вземане на решения. В този смисъл киберспособността може да влияе върху поведението дори без да бъде активирана. Това обаче не означава, че всяко проникване е акт на принуда. Стратегическият ефект зависи от контекста, достоверността на способността, възприемането от противника и способността на защитника да запази основните функции.

Допълнителен фактор е проблемът с атрибуцията и ескалацията (Kamdzhlov and Nikolov, 2026). Техническите индикатори могат да показват инфраструктура, инструменти или сходни техники, но политическата атрибуция изисква по-широк набор от разузнавателни и дипломатически данни. Същевременно физическите последици от кибероперация срещу енергийна система могат да бъдат по-бързи от процеса на уверено определяне на извършителя. Това създава риск от погрешна оценка на намерението и усложнява пропорционалния отговор. Поради това защитата на енергопреносните системи е едновременно технически и стратегически проблем: тя трябва да намалява вероятността за успешен ефект и същевременно да осигурява достоверна информация за вземане на решения.

6. ЗАКЛЮЧЕНИЕ

Заплахите пред енергопреносните системи имат стратегическо значение, защото електроенергията е предпоставка за функционирането на множество други критични услуги и за способността на държавата да действа в условия на криза. В киберпространството тази зависимост може да бъде използвана не само чрез непосредствено прекъсване, но и чрез продължително разузнаване, предварително позициониране, манипулиране на информация, експлоатация на доверени връзки и създаване на несигурност относно надеждността на инфраструктурата. Така техническият достъп се превръща в потенциален стратегическо преимущество.

В съревнованието между велики сили най-опасният сценарий не е непременно най-видимият. По-значима може да бъде способността противникът да запази достъп, да разбере зависимостите и да разполага с готови опции за действие в момент, когато електроснабдяването е необходимо за гражданската устойчивост, военната мобилност и политическото управление. Следователно ефективната защита на енергопреносните системи трябва да се оценява не само по броя предотвратени прониквания, а по способността да се ограничи стратегическата ползност на компрометирането: чрез сегментация, контрол на доверените връзки, надеждна ситуационна осведоменост, бързо възстановяване и координация между оператори, държавни институции и съюзни партньори.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

ANDREEV, E., D. DIMITROV. 2021. Challenges Related to the Cyber Security of Nuclear Programs and Power Plants. – In: Радиационната безопасност в съвременния свят. Sofia: Rakovski National Defence College, pp. 128 – 135. DOI: 10.34660/INF.2021.32.95.012.

Chagovec, A.; Bakardjieva, T.; Ivanova, A.; Sapundzhi, F.; Spasova, V.; Ivanova, A. AI-Driven Threat Detection and Automated Incident Response for Securing Cloud Workloads. Appl. Sci. 2026, 16, 6454. <https://doi.org/10.3390/app16136454>

CISA, FBI, DOE. 2022. Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector. Cybersecurity Advisory AA22-083A, 24 March 2022. Available from: <https://www.cisa.gov/ncas/alerts/aa22-083a>. [viewed 03.10.2026].

CISA, NSA, FBI et al. 2024. PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Joint Cybersecurity Advisory AA24-038A, 7 February 2024. Available from: https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf. [viewed 03.10.2026].

ENISA. 2025. ENISA NIS360 2024. European Union Agency for Cybersecurity, February 2025. Available from: https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf. [viewed 02.10.2026].

EUROPEAN COMMISSION. 2024. Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj. [viewed 04.10.2026].

EUROPEAN PARLIAMENT AND COUNCIL. 2022. Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities. Official Journal of the European Union, L 333, pp. 164 – 198. Available from: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>. [viewed 03.10.2026].

HARKNETT, R. J., M. SMEETS. 2022. Cyber campaigns and strategic outcomes. – In: Journal of Strategic Studies. Vol. 45, No. 4, pp. 534 – 567. DOI: 10.1080/01402390.2020.1732354.

KAMDZHALOV, S., D. NIKOLOV. CYBER THREAT INTELLIGENCE BASED SCOPING OF RED TEAM EXERCISES. – In: SysTechDev. 2026, vol. 3, pp. 115 – 119. DOI: 10.68302/std2026.vol3.210.

ABUDIN, M. J., S. THOKCHOM, R. T. NAAYAGI, G. PANDA. 2024. Detecting False Data Injection Attacks Using Machine Learning-Based Approaches for Smart Grid Networks. – In: Applied Sciences. Vol. 14, No. 11, Article 4764. DOI: 10.3390/app14114764.

NATO. 2022. NATO 2022 Strategic Concept. Brussels: North Atlantic Treaty Organization. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf. [viewed 06.10.2026].

NATO. 2026. 2026 Resilience Baseline Requirements. North Atlantic Treaty Organization, 15 September 2026. Available from: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/09/15/2026-resilience-baseline-requirements>. [viewed 05.10.2026].

NIKOLOV, B., D. NIKOLOV. A Scenario-based Approach to Cybersecurity Training for Seafarers. – In: 24th International Association of Maritime Universities (IAMU) Conference. Massachusetts Maritime Academy, USA, 2024, pp. 385 – 390. ISSN 2706-6762.

NIKOLOV, D. DCSYNC ATTACK FROM AN ADVERSARY POINT OF VIEW. – In: SysTechDev. 2026, vol. 3, pp. 219 – 222. DOI: 10.68302/std2026.vol3.213.

STOUFFER, K., M. PEASE, C. TANG, T. ZIMMERMAN, V. PILLITTERI, S. LIGHTMAN, A. HAHN, S. SARAVIA, A. SHERULE, M. THOMPSON. 2023. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-82r3.

ZOGRAFOPOULOS, I., J. OSPINA, X. LIU, C. KONSTANTINOOU. 2021. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. – In: IEEE Access. Vol. 9, pp. 29775 – 29818. DOI: 10.1109/ACCESS.2021.3058403.

НИКОЛОВ, Д. Анализ на планирането и изпълнението на киберупражнения. – В: Девета международна научна конференция Радиационната безопасност в съвременния свят. 2025, с. 146 – 158. ISSN 2738-7607. COBISS.BG-ID 48925192.