**Oskar Stefański**[1]
Uniwersytet Mikołaja Kopernika w Toruniu

https://doi.org/10.29316/9788368103373_13

# CYBERZAGROŻENIA A PROCES TRANSFORMACJI ENERGETYCZNEJ. W JAKI SPOSÓB NOWE ZAGROŻENIA MOGĄ SPOWALNIAĆ PROCES TRANSFORMACJI ENERGETYCZNEJ PAŃSTWA NA PRZYKŁADZIE POLSKI?

## CYBER THREATS AND THE ENERGY TRANSITION. HOW MIGHT NEW THREATS SLOW DOWN A COUNTRY'S ENERGY TRANSITION, TAKING POLAND AS AN EXAMPLE?

**Streszczenie**

Cyberzagrożenia i transformacja energetyczna to zagadnienia ze sobą powiązane. Ponieważ systemy energetyczne są coraz częściej uzależnione od cyfryzacji, wiąże się to zarówno z korzyściami, jak i z zagrożeniami. Korzyściami mogą być szybsze dostawy i większa automatyzacja. Z kolei zagrożenia to przykładowo potencjalne cyberzagrożenia takie jak cyberataki, a także wiele innych zjawisk, którymi mogą być wyłudzenia danych i oszustwa finansowe. W Polsce od wielu lat zachodzą zarówno

[1] https://orcid.org/0009-0005-5419-0342, e-mail: oskar.stefanski@doktorant.umk.pl

proces cyfryzacji, jak i transformacji energetycznej. Celem pracy jest zbadanie tego, w jaki sposób cyberzagrożenia mogą negatywnie wpływać na transformację energetyczną państwa na przykładzie Polski. W Polsce od 2014 roku liczba zgłoszonych cyberzagrożeń w sektorze energetycznym stale rośnie w liczbach bezwzględnych, a sektor energetyczny jest wśród pięciu najczęściej obsługiwanych sektorów przez zespół CERT Polska. Najpoważniejszymi incydentami, które dotyczą polskiej transformacji energetycznej, są różne cyberataki. Najczęściej doprowadzają one do wykradzenia danych poufnych od firm energetycznych i instytucji zajmujących się energetyką. Są także inne skutki takich działań, jak utrata częściowej kontroli nad elektrowniami i stronami internetowymi firm energetycznych. Bezpośrednio powoduje to mniejszy dostęp społeczeństwa do energii elektrycznej, a także zmniejsza zaufanie Polaków do firm energetycznych. W trakcie badania przedstawione zostały w formie tabel i opisów incydenty w liczbie nominalnej, a także w formie opisowej najpoważniejsze przypadki cyberzagrożeń dotykających polskiej transformacji energetycznej i całego sektora energetycznego.

**Słowa kluczowe:** transformacja energetyczna, cyberzagrożenia, Polska, cyberataki, CERT Polska

**Abstract**

Cyber threats and the energy transition are intertwined. Since energy systems are increasingly dependent on digitalisation, this brings both numerous negative and positive consequences. Benefits include faster deliveries and greater automation. Threats include potential cyberattacks and other cyber threats, such as data theft and financial fraud. Poland has been undergoing both digitalisation and energy transition for many years. This study examines how cyber threats can negatively impact the country's energy transition, using Poland as an example. In Poland, the number of reported cyberthreats in the energy sector has been steadily increasing in absolute numbers since 2014, and the energy sector is among the five most frequently serviced sectors by CERT Polska. The most serious incidents affecting the Polish energy transition are various cyberattacks. These incidents most often result in the theft of confidential data from energy companies and institutions involved in the energy sector. Other consequences include the loss of partial control over power plants and energy company websites. This directly reduces public access to electricity and diminishes Poles' trust in energy companies. The study presented a nominal number of incidents in tables and descriptions, along with descriptive reports on the most serious cyber threats affecting the Polish energy transition and the entire energy sector.

**Keywords:** energy transition, cyber threats, Poland, cyberattacks, CERT Polska

## Wstęp

Transformacja energetyczna to proces trwały, przez który przechodzą wszystkie państwa świata. Powszechnie transformację energetyczną określa się jako przejście z systemu energetycznego opartego na paliwach kopalnych, takich jak węgiel, ropa czy gaz ziemny, do systemu opartego na odnawialnych źródłach energii, takich jak bioenergetyka, energetyka słoneczna, wiatrowa, wodna czy wykorzystywanie wodoru (Harichandan i in., 2022). Z tego względu, że paliwa kopalne są potencjalnie skończonym źródłem energii, prędzej czy później na skutek wyczerpania zasobów, wszystkie państwa i jednostki będą zmuszone do przeprowadzenia transformacji energetycznej. Jednakże surowce te mogą być wykorzystywane w procesie przejściowym. Celem transformacji jest neutralność klimatyczna, a od tych surowców należy odchodzić stopniowo, uwzględniając potrzeby swojego społeczeństwa i systemu energetycznego. Ważna jest także perspektywa wykorzystywania nowych technologii mogących sprawiać, że konwencjonalne źródła energii staną się „czystsze". Z tego względu poszczególne typy energetyki konwencjonalnej mogą być wykorzystywane w fazie przejściowej (Pepłowska, 2025).

Kluczowe w badaniach nad transformacją energetyczną jest stwierdzenie tego, jaki obszar terytorialno-prawny ona dotyka. W literaturze przedmiotu wyznacza się dwa główne typy transformacji energetycznej. Są to transformacja energetyczna w ujęciu państwowym i transformacja energetyczna w ujęciu lokalnym (Solomon, Krishna, 2011). Transformacja w ujęciu lokalnym dotyczy, jak nazwa wskazuje, terytorium mniejszego niż państwo. Niezależnie od tego, czy to jednostka administracyjna, czy chociażby firma. Z tego względu istotne jest zaznaczenie, że badanie dotyczy transformacji energetycznej państwa, a w tym przykładzie Rzeczpospolitej Polskiej. Istotne dla tematu są też pojęcia takie jak zielona transformacja energetyczna czy czysta transformacja energetyczna ze względu na ich powszechne występowanie w literaturze. Są to procesy bliźniacze transformacji energetycznej i nie różnią się od niej (Carley, Konisky, 2020; Muhire i in., 2024).

Istotna z perspektywy badania nad transformacją energetyczną jest kwestia udziału energetyki jądrowej w transformacji energetycznej. Jest to kwestia indywidualna dla poszczególnych państw, niektóre, takie jak Niemcy, wykluczają udział energetyki jądrowej w ich miksie energetycznym

(Kędzierski, 2024). Z kolei inne, takie jak Szwecja, zakładają ważną rolę energetyki jądrowej w transformacji energetycznej (Regeringen, 2024). Ważne jest to, że w doktrynie uznaje się często istotną rolę energetyki jądrowej w transformacji energetycznej niezależnie od państwa (Blecking, 2023; Wang, Guo, Li, Jiang, 2023; Muhire i in., 2024). Przez to należy uznać, że wśród źródeł energii wykorzystywanych w ramach transformacji energetycznej, jednym z docelowych jest energetyka jądrowa. Polski proces transformacji energetycznej opiera się głównie na przejściu z energetyki opartej na węgiel i w mniejszym stopniu na inne paliwa kopalne na system energetyczny oparty na czyste źródła energii. W wciąż obowiązującym dokumencie „Polityka energetyczna Polski do 2040 roku" z 2021 roku i aktualizowanym w 2022 roku po rosyjskiej agresji na Ukrainę zakłada się, że polska energetyka opierać się będzie docelowo na miksie energetyki odnawialnej z energetyką jądrową. Głównym celem polskiej transformacji energetycznej jest neutralność klimatyczna, czyli emitowanie równej bądź mniejszej ilości gazów cieplarnianych niż ich wchłanianie. Co ważne, system energetyki Polski ma opierać się w dużym stopniu na cyfryzacji (Ministerstwo Klimatu i Środowiska, 2021).

Pojęciami kluczowymi dla transformacji energetycznej są czynniki napędzające (ang. drivers) i spowalniające (nazywane często barierami). Kluczowe dla badania będą bariery, czyli czynniki spowalniające transformację energetyczną. Bariery hamują proces transformacji energetycznej, a aby go przyspieszyć i usprawnić, należy pokonać barierę (Pereira, Silva, Ferreira, 2025). Bariery są powiązane z czynnikami napędzającymi; brak takowego czynnika może stanowić barierę (Muhire i in., 2024). Przez to istnieją między nimi wysokie zależności, często również bariery i czynniki napędzające się wykluczają. W literaturze przyjmuje się, że czynniki i bariery mają charakter polityczno-prawny, ekonomiczny, społeczny, środowiskowy i technologiczny (Muhire i in., 2024; Aparisi-Cerdá, Ribó-Pérez, García-Melón, D'Este, Poveda-Bautista, 2024). Ze względu na wyznaczenie takich kategorii łatwiej określać, co i w jaki sposób napędza bądź spowalnia transformację energetyczną. Dzięki temu łatwiej jest dokonać określenia sukcesów i problemów tego procesu w danym miejscu.

Nowe technologie niosą transformacji energetycznej wiele szans, takich jak wytwarzanie energii w sposób czystszy, tańszy i efektywniejszy,

ale także stwarzają potencjalne zagrożenia i bariery. Ze względu na aspekt technologiczny cyberbezpieczeństwo jest kluczowe dla transformacji energetycznej. Przez to zagadnienia związane z cyberbezpieczeństwem stanowią fundament do tego, aby w procesie transformacji energetycznej nie zaistniały bariery, które będą hamować ten proces. Zdaniem publicystów Światowego Forum Ekonomicznego cyberzagrożenia będą coraz istotniejszym problemem dla infrastruktury energetycznej, w tym dla całego procesu transformacji energetycznej. Cyberodporność powinna zatem stać się jednym z fundamentów (Ukyab, Simonovich, 2025). Cyberzagrożenia spowalniają proces transformacji energetycznej, stąd mogą być nazwane barierami, co powinno ułatwić badanie danego zjawiska.

Badania nad powiązaniem cyberzagrożeń z barierami i wyzwaniami w transformacji energetycznej są powszechne w dyskursie naukowym zajmującym się transformacją energetyczną. Spośród przykładowych pozycji można wymienić publikację badaczy z World Energy Council „Cyber challenges to the energy transition", którzy uznali, że cyberzagrożenia są jednymi z najmniej spodziewanych zagrożeń, a także jednymi z bardziej istotnych dla sektora energetycznego państwa. Uwzględniają w tym rolę cyberbezpieczeństwa w bezpieczeństwie energetycznym państwa i przeprowadzaniu transformacji energetycznej. Uznają także, że cyberzagrożenia są istotne w spowalnianiu transformacji energetycznej. Dodatkowo wymieniają różne incydenty związane z cyberzagrożeniami, które wpłynęły negatywnie na transformację energetyczną. Spośród nich wymieniają przykładowo cyberataki na elektrownie jądrowe i wodne w Korei Południowej z 2015 roku, cyberataki w Unii Europejskiej na infrastrukturę energetyczną z 2015 roku, a także zaburzenia w sieci połączeń energetycznych w ramach cyfryzowanego systemu energetycznego w Urugwaju i Argentynie w 2019 roku (Nottingham, Young, 2019).

W Korei Południowej atak ten doprowadził do zakłócenia dostaw energii i usług opartych na energii elektrycznej. W Unii Europejskiej hakerzy dostali się do zabezpieczeń poszczególnych elektrowni i mogli w każdym momencie wyłączyć elektrownie i przerwać dostęp energii w wybranych państwach. Z kolei w Urugwaju i Argentynie awaria sprawiła, że przestały jeździć pociągi i metro, a także zabrakło w niektórych miejscach dostępu do wody. Przedstawione cyberzagrożenia miały miejsce od 2014 roku, gdyż

od tego roku na świecie cyberzagrożenia dotykają coraz częściej procesu transformacji energetycznej. Celowo wybrane zostały różne skutki cyberzagrożeń, w tym cyberataków, aby pokazać mnogość skutków, które wystąpiły w tych państwach (Nottingham, Young, 2019).

Zdaniem Raphaela Röttingera postępująca cyfryzacja i transformacja energetyczna są ze sobą powiązane, przez co cyfryzacja niesie ze sobą wiele potencjalnych zagrożeń, w tym przede wszystkim cyberataki na infrastrukturę energetyczną. Pomimo postępującej cyfryzacji i automatyzacji systemów energetycznych w ramach transformacji, wciąż będzie wysoka zależność od czynnika ludzkiego, co sprawia, że potencjalne błędy i cyberzagrożenia ze strony hakerów będą tak samo bądź bardziej dotkliwe (Röttinger, 2024). Inni badacze są również podobnego zdania, że postępująca cyfryzacja niesie ze sobą coraz większe zagrożenia dla transformacji energetycznej i ma potencjał spowalniający, w momencie, gdy transformacja energetyczna napotka cyberzagrożenia (np. Awad, Bayoumi, 2025; Abraham, Houmd, Erdodi, 2025; Deryugina, 2023).

Z tego względu powiązanie tematyki cyberzagrożeń z transformacją energetyczną jest bardzo kluczowe, w szczególności w obliczu konfliktu cybernetycznego Polski z Rosją i Białorusią. Istotne jest zbadanie tego, jak cyberzagrożenia mogą oddziaływać na transformację energetyczną Polski na podstawie dotychczasowych doświadczeń.

## Metodologia

Z uwagi na wciąż wzrastające ryzyko wystąpienia cyberzagrożeń, które mogą razić system energetyczny Polski, istotne jest zweryfikowanie tego, w jaki sposób mogą one wpływać na spowalnianie procesu transformacji energetycznej. Badanie opierać się będzie na dotychczasowych przykładach takich działań i różnych incydentach z tym związanych, które miały miejsce na terenie Polski o dotyczyły szeroko pojętego systemu energetycznego. Dlatego postawiony został cel badawczy, który dotyczy zbadania tego, w jaki sposób cyberzagrożenia mogą negatywnie wpływać na transformację energetyczną państwa na przykładzie Polski. Z tego względu postawiony zostanie problem badawczy P: W jaki sposób cyberzagrożenia mogą negatywnie wpływać na proces transformacji energetycznej państwa na przykładzie takich działań wobec Polski? Z racji dotychczasowych doświadczeń na

podstawie państw, które zostały dotknięte przez cyberzagrożenia, takich jak Stany Zjednoczone, Korea Południowa, Argentyna i Urugwaj, można postawić hipotezę badawczą odpowiadającą na postawiony problem. H: Cyberzagrożenia mogą być czynnikiem spowalniającym (barierą) transformację energetyczną państwa poprzez zakłócenie dostaw energii, kontrolowanie elektrowni przez hakerów, doprowadzenie do zaburzeń w funkcjonowaniu infrastruktury transportowej państwa i dostępu do podstawowych potrzeb mieszkańców. Hipoteza zostanie zweryfikowana pozytywnie, częściowo pozytywnie bądź całkowicie negatywnie w ramach wniosków końcowych badania.

Kluczowe są też podstawowe założenia badawcze przyjęte w ramach badania, które dotyczą podstawowych pojęć wykorzystywanych w pracy. Jednym z nich jest transformacja energetyczna. Zgodnie z przedstawionym teoretycznym podejściem do zagadnienia transformacji energetycznej państwa w ramach wstępu, na potrzeby badania przyjęte zostanie, że jest to przejście z systemu energetycznego opartego na paliwach kopalnych na czyste źródła energii takie jak OZE, atom czy wodór. Jednakże istotny jest cały proces transformacji energetycznej, hipotetyczne zagrożenia względem chociażby elektrowni węglowych mogą spowalniać odchodzenie od ich eksploatacji. Może to mieć miejsce chociażby poprzez potrzebę reinwestycji w to źródło energii ze względu na brak alternatyw, a także przez inne powody. W Polsce przez znaczne uzależnienie od elektrowni węglowych i innych źródeł konwencjonalnych należy uwzględnić ich rolę przejściową. Zgodnie z tym polem badawczym jest cała transformacja energetyczna Polski, w tym zarówno konwencjonalne źródła energii jako źródła przejściowe, jak i niekonwencjonalne źródła energii jako źródła docelowe. Stąd istotne będzie także dalsze sprecyzowanie pola badawczego, konkretnie w zakresie stwierdzeń takich jak cyberprzestrzeń i cyberzagrożenia.

Kwestia definicyjna cyberprzestrzeni jest prosta przez to, że w Polsce jest regulowana np. w ustawie o stanie wyjątkowym. Według tejże ustawy cyberprzestrzeń to „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami" (Ustawa z 21.06.2002 r. o stanie

wyjątkowym Dz. U. z 2017 r. poz. 1928, s. 2). Natomiast cyberzagrożenia to zagrożenia, które występują w cyberprzestrzeni. Co za tym idzie, przyjętym polem badawczym jest cyberprzestrzeń dotycząca występujących w niej cyberzagrożeń, które oddziałują na transformację energetyczną w Polsce. Stąd przedmiotem badań są cyberzagrożenia wpływające na polską transformację energetyczną i dotykające czystych źródeł energii. Strona internetowa rządu Rzeczypospolitej Polskiej wymienia przykładowe cyberzagrożenia: wirusy, robaki, spyware i wiele innych (Gov.pl, b.d.).

Podstawową metodą badawczą jest studium przypadku, jakim jest transformacja energetyczna Polski. Kluczowe w badaniu będą także cyberzagrożenia w relacji z transformacją energetyczną. Ponadto zastosowana zostanie krytyczna analiza źródeł, w tym przypadku analiza źródeł pierwotnych i wtórnych. Będą nimi źródła będą głównie dokumenty NASK (w tym szczególnie CERT Polska, dalej nazywane CERT) i dokumenty prasowe informujące o danych cyberzagrożeniach dotykających transformacji energetycznej w Polsce. Przypadki zostaną przedstawione również w formie tabeli prezentującej dane cyberzagrożenia.

Przyjętym okresem badawczym będą lata 2014-2025 ze względu na to, że od 2014 roku na świecie występuje coraz więcej cyberzagrożeń dotykających procesu transformacji energetycznej, a także wzmożoną aktywność Rosjan w cyberprzestrzeni powodującą cyberzagrożenia w Europie. Stąd jest to o tyle istotny okres, że obejmuje także czas po inwazji rosyjskiej na Ukrainę z 22 lutego 2022 roku.

## Cyberzagrożenia w transformacji energetycznej Polski

Pierwszym przypadkiem cyberzagrożeń, w postaci cyberataku, który należy wymienić, jest działalność Dragonfly/Energetic Bear, która na szeroką skalę rozpoczęła się w 2014 roku i trwa do dzisiaj. Grupa Dragonfly zaatakowała wiele państw Zachodu, w tym Polskę, celując głównie w infrastrukturę energetyczną bez szczególnego różnicowania, jaki to jest typ energetyki. Grupa wysyłała zainfekowane maile na konta Gmail z załącznikiem w formacie pdf, a także zmieniała strony internetowe firm energetycznych, które następnie przekierowywały użytkowników na inne strony. Innym sposobem było użycie pakietów oprogramowania ICS. Przez to hakerzy infekowali strony internetowe firm energetycznych tzw. trojanem, a system nie

wykrywał niebezpieczeństwa związanego z potencjalnym oprogramowaniem szkodliwym dla użytkowników. Dzięki temu wykradali dane od użytkowników, a także firm i poufne informacje takie jak hasła. Hakerzy próbowali dostać się do systemu zabezpieczeń firm energetycznych, a także całej infrastruktury energetycznej. Prawdopodobnie głównym celem grupy było zdobycie informacji na temat badań geologicznych i geograficznych, planów eksploatacji złóż i planów inwestycji firm energetycznych. Dotknięty został zarówno sektor energetyki konwencjonalnej, jak i niekonwencjonalnej. Doniesienia prasowe informowały wówczas, że atak mógł być inspirowany z Rosji. Głównym skutkiem tych ataków był wyciek danych dotyczących polityki energetycznej wybranych firm. Co najistotniejsze, był to atak szpiegowski, a nie sabotażowy, jednakże sprawił, że hakerzy dostali się do ściśle tajnych danych dotyczących polskiego sektora energetycznego (Rzeczpospolita, 2014; CERT, 2015; Malko, Wojciechowski, 2015).

W 2014 roku upubliczniono także do informacji publicznej raport z ataku grupy SandWorm na sieć energetyczną w Polsce. Co istotne, główna część ataku grupy dotyczyła w większości Ukrainy, lecz także częściowo Polski, a w znacznie mniejszym stopniu innych państw NATO. Natomiast, co kluczowe, cały atak polegał na zainfekowaniu systemów energetycznych i systemów firm energetycznych w obu krajach oprogramowaniem BlackEnergy. Ataki były bardzo precyzyjne, gdyż wysyłano specjalnie tworzone zainfekowane pliki pakietu Microsoft Office i wysyłano je pracownikom przedsiębiorstw i sektora publicznego. Następnie dzięki temu skradziono dane poufne na masową skalę. Otwarcie pliku sprawiało, że był on potem pobierany i dalej instalowany na komputerze, a następnie w sposób zdalny pobierał i przesyłał poufne dane hakerom. Zdaniem CERT udało się zidentyfikować 28 unikalnych adresów IP w Polsce, które w większości dotknęły sektora energetycznego, zarówno w sferze prywatnej, jak i publicznej. Podobnie jak w przypadku działalności Dragonfly nie różnicowano sektora na ten zajmujący się energetyką konwencjonalną i niekonwencjonalną, tylko atakowano cały sektor energetyczny zasilający infrastrukturę krytyczną. Jest to także kolejny przypadek, który prawdopodobnie wiąże się z działalnością Rosji w cyberprzestrzeni (CERT, 2015). Dodatkowo należy zaznaczyć, że ta sama grupa i to samo oprogramowanie doprowadziły w grudniu 2015 roku do blackoutu na Ukrainie (CERT, 2016; Gapiński, 2016).

Kolejne większe opisywane incydenty miały miejsce po 2022 roku. W czerwcu 2022 roku Elbląskie Przedsiębiorstwo Energetyki Cieplnej (EPEC) zgłosiło, że stało się ofiarą cyberataku. Sieć informatyczna firmy została zainfekowana groźnym Ramsonware Ragnar Locker. Zainfekowanie sieci szkodliwym oprogramowaniem sprawiło, że wyciekło aż 8 GB danych osobowych klientów i pracowników firmy, w tym takich danych jak numery PESEL. Hakerzy dostali się także do danych wewnętrznych finansowych firmy. Twórcy złośliwego oprogramowania upublikowali nawet dane, które zostały przez nich skradzione. Celem hakerów była właśnie kradzież danych osobowych i finansowych firmy, a nie atak bezpośredni na systemy energetyczne. Nie zmienia to faktu, że jest to incydent poważny, przez który firma zajmująca się energetyką ciepłowniczą, kluczową w procesie transformacji energetycznej, straciła zaufanie i nie była w stanie kontrolować swoje serwery. Co warto odnotować, to incydent jedynie o charakterze lokalnym, a nie ogólnokrajowym bądź regionalnym (EPEC, 2022; Stankiewicz, 2022; Nowosad, 2022; Szczęsny, 2022).

Następnym poważnym incydentem jest proceder związany z fałszywymi sklepami z węglem, który był bezpośrednim skutkiem zaprzestania handlu surowcami energetycznymi z Rosją. Braki w dostawach węgla, na skutek rosyjskiej agresji na Ukrainę z 2022 roku sprawiły, że polskie społeczeństwo uzależnione od ogrzewania węglowego było zmuszone szukać surowca w innych miejscach niż dotychczas. CERT zwraca uwagę na to, że dotyczyło to wszelkiej maści cyberzagrożeń, nie tylko cyberataków, jak w poprzednich przypadkach. W tym czasie, gdy na polskim rynku brakowało węgla, dochodziło do licznych prób wykradania haseł przez zhackowane linki do fałszywego zakupu, a także wyłudzano dane osobowe osób kupujących. Fałszywe sklepy, często podające się za rzeczywiste (przypadek sklepu podszywającego się pod Polską Grupę Górniczą), oferowały możliwość kupna jedynie poprzez przelewy, co już budziło podejrzenia. CERT przedstawia, że w grudniu 2022 roku działało aż 12 takich fałszywych sklepów internetowych, które oszukiwały swoich nabywców (CERT, 2023). Co istotne, proceder ten powrócił w 2023 i 2024 roku wraz z rozpoczęciem sezonu grzewczego w październiku 2023 i 2024 roku (CERT, 2024; CERT, 2025). Jest to o tyle istotne, że ludzie często tracili swoje fundusze przez wywindowane ceny surowców, a także przez fałszywe oferty sprzedaży węgla. Ostatecznie

doprowadziło to do licznych nadużyć i strat finansowych gospodarstw, które mogłyby utracone fundusze wydać na wymianę pieca w swoim domu i eksploatację czystej energii bądź usprawienie działania swojego pieca.

W 2023 roku doszło do cyberataków powiązanych z grupą ATP28, które dotknęły sektory energetyczne wielu państw, w tym Polski. Grupa wykorzystywała błędy w Microsoft Outlook i przez to była w stanie dostać się do danych osobowych użytkowników. Ponadto wykradała w ten sposób hasła do zabezpieczeń. Hakerzy wykradli w ten sposób hasła pracowników sektora transportu, sektora zbrojeniowego, a także, co najważniejsze, pracowników sektora energetycznego (CERT, 2024).

Ostatni warty odnotowania incydent miał miejsce w lipcu i sierpniu 2025 roku. Rosyjscy hakerzy wówczas zaatakowali Polską elektrownię wodną i wodociąg, a także próbowali nieudanie zaatakować bioreaktor. W przypadku bioreaktora manipulowano temperaturami pomieszczeń niektórych budynków w Nowym Mieście Lubawskim. W przypadku elektrowni wodnej także manipulowano temperaturami. W lipcu Rosjanie nie byli w stanie całkowicie przejąć kontroli nad hydroelektrownią, jednakże w sierpniu udało im się dostać do systemu zabezpieczeń. Zmieniono wówczas parametry temperatur, a także ilość wody w elektrowni. Sprawiło to, że Rosjanie byli w stanie częściowo kontrolować elektrownię wodną (Klimczuk, 2025a; Klimczuk, 2025b).

Poza wymienionymi dużymi incydentami, do CERT zgłaszane były też mniejsze incydenty. Od 2018 CERT udostępnia liczbę incydentów obłużonych przez CERT w danych sektorach gospodarki państwa, a także ich procentowy udział względem innych sektorów. Incydenty to zgłoszenia do CERT różnej maści cyberzagrożeń, w tym chociażby cyberataków czy manipulacji (Tabela 1).

**Tabela 1**. Incydenty związane z cyberzagrożeniami w sektorze energetycznym w Polsce w latach 2018-2024 obsłużone przez CERT

| Rok | Łączna ilość incydentów | Incydenty w sektorze Energetyki | Procent względem ogółu incydentów |
|---|---|---|---|
| 2018 | 3739 | 20 | 0,53% |
| 2019 | 6484 | 28 | 0,40% |
| 2020 | 10420 | 101 | 0,97% |
| 2021 | 29483 | 4084 | 13,85% |

| Rok | Łączna ilość incydentów | Incydenty w sektorze Energetyki | Procent względem ogółu incydentów |
|---|---|---|---|
| 2022 | 39683 | 4320 | 10,89% |
| 2023 | 80278 | 9196 | 11,46% |
| 2024 | 103449 | 5216 | 4,50% |

Źródło: opracowanie własne na podstawie raportów CERT, 2019-2025.

Ilość ogółu incydentów związanych z cyberzagrożeniami w Polsce rośnie w znacznym tempie. Istotne jest to, że ich liczba w sektorze energetycznym także do 2023 roku była w trendzie wzrostowym. Przed 2021 rokiem ich liczba stanowiła łącznie mniej niż jeden procent ogółu incydentów. Znaczny wzrost incydentów w sektorze energetycznym nastąpił w 2021 roku, gdyż w ujęciu nominalnym był on prawie czterdziestokrotny. W ujęciu procentowym wzrost z mniej niż 1% do prawie 14% względem ogółu incydentów jest także bardzo zauważalny. Do 2023 roku liczba incydentów w sektorze osiągnęła swoje maksimum nominalne wynoszące 9196 incydentów, aczkolwiek w ujęciu procentowym do ogółu wynosiła 11,46%. W 2024 roku nastąpił spadek liczby incydentów w sektorze energetycznym w ujęciu zarówno nominalnym, jak i procentowym, przy jednoczesnym wzroście ogólnej liczby incydentów związanych z cyberzagrożeniami. Pomimo takiego spadku wciąż sektor energetyczny znajdował się wówczas wśród pięciu sektorów, które są dotykane najwięcej incydentów o tym charakterze, i jest to niezmienne od 2021 roku (CERT, 2025).

## Wnioski

Cyberzagrożenia dotykające sektora energetyki i transformację energetyczną w Polsce od 2021 roku są wśród pięciu (względem innych branż gospodarki) najczęściej raportowanych cyberzagrożeń, a ich liczba nominalnie stale rośnie. Spośród najważniejszych od 2014 roku przypadków cyberzagrożeń dotykających sektora energetycznego i polskiej transformacji energetycznej, zdecydowana większość to cyberataki (Tabela 2). Doniesienia prasowe uznają, że znaczna część z nich była powiązana z Rosją. Cyberataki miały głównie na celu kradzież danych osobowych i danych finansowych atakowanych jednostek, a także zaburzenie działalności firm i elektrowni, które były wówczas atakowane przez hakerów. Istotny jest także długotrwały incydent związany z fałszywymi sklepami z węglem. Doprowadził on

wiele gospodarstw domowych do utraty funduszy na rzecz fałszywych ofert sprzedaży węgla. Do 2025 roku incydenty nie dotykały bezpośrednio poszczególnych elektrowni, a jedynie firm energetycznych bądź konsumentów. Jednakże proceder z 2025, w którym, zdaniem prasy, Rosjanie kontrolowali jedną z polskich elektrowni wodnych, wydaje się najistotniejszy. Sprawia on, że w przyszłości przez braki w zabezpieczeniach i wzmożoną aktywność hakerów łatwiej będzie im przejmować kontrolę nad działalnością poszczególnych elektrowni bądź reaktorów. Istotne jest to, że taki proceder potencjalnie może doprowadzić nawet do blackoutu na mniejszą bądź większą skalę, co pokazuje przypadek Ukrainy w momencie, w którym państwo nie kontroluje swojej jednostki odpowiadającej za produkcję energetyczną.

**Tabela 2**. Główne incydenty w transformacji energetycznej związane z cyberzagrożeniami od 2014 roku

| Incydent | Typ cyberzagrożenia | Rok/lata trwania |
|---|---|---|
| Ataki Dragonfly/Energetic Bear | Cyberatak | 2014 |
| Ataki Sandworm | Cyberatak | 2014 |
| Atak na EPEC | Cyberatak | 2022 |
| Fałszywe sklepy z węglem | Phishing | 2022-2024 |
| Atak ATP28 | Cyberatak | 2023 |
| Atak na elektrownię wodną | Cyberatak | 2025 |

Źródło: opracowanie własne na podstawie incydentów opisanych w badaniu.

Odpowiadając na problem badawczy P: W jaki sposób cyberzagrożenia mogą negatywnie wpływać na proces transformacji energetycznej państwa na przykładzie takich działań wobec Polski? Należy stwierdzić, że mogą to robić poprzez zmniejszanie zaufania społecznego wobec firm na podstawie dotychczasowych ataków hakerskich a także fałszywych aukcji związanych ze sprzedażą węgla. Potencjalnie mogą także doprowadzać do manipulacji na rynku, wykradać dane osobowe, a także manipulować elektrowniami i przyjmować nad nimi chociażby część kontroli, mając możliwość także wyłączenia elektrowni bądź reaktora. Dodatkowo takie zagrożenia mogą doprowadzić do tego, że potencjalne plany firm energetycznych zostaną ukradzione przez hakerów, co także może spowolnić proces transformacji energetycznej na podstawie wydarzeń z 2014 roku. Weryfikując hipotezę

badawczą H: Cyberzagrożenia mogą być czynnikiem spowalniającym (barierą) transformację energetyczną państwa poprzez zakłócenie dostaw energii, kontrolowanie elektrowni przez hakerów, co może doprowadzić do zaburzeń w funkcjonowaniu infrastruktury transportowej państwa i dostępu do podstawowych potrzeb mieszkańców. Należy stwierdzić, że w Polsce zakłócenia dostaw energii mogą mieć rzeczywiste miejsce; kontrolowanie elektrowni przez hakerów również na podstawie incydentu z 2025 roku. Jednakże incydenty w Polsce nie doprowadziły do zaburzeń w funkcjonowaniu infrastruktury transportowej państwa i dostępu do podstawowych potrzeb mieszkańców. Hipotezę należy zatem zweryfikować częściowo pozytywnie. Co warto także dodać: cyberzagrożenia mogą spowalniać transformację także przez zmniejszanie zaufania społecznego państwa, wyłudzenia finansowe i wykradanie danych inwestycyjnych firm zajmujących się energetyką i transformacją energetyczną. Kluczowe jest także to, że liczba groźnych i poważnych ataków stale rośnie, a incydent z 2025 roku pokazał, że istnieje ryzyko bezpośredniego ataku na elektrownie.

## Literatura


1. Abraham, D., Houmb, S. H., Erdodi, L. (2025). Cyber-Attacks on Energy Infrastructure-A Literature Overview and Perspectives on the Current Situation. *Applied Sciences*, *15*(17), 1-19. https://doi.org/10.3390/app15179233
2. Aparisi-Cerdá, I., Ribó-Pérez, D., García-Melón, M., D'Este, P., Poveda-Bautista, R. (2024). Drivers and barriers to the adoption of decentralised renewable energy technologies: A multi-criteria decision analysis. *Energy*, *305*, 1-13. https://doi.org/10.1016/j.energy.2024.132264
3. Awad, H., Bayoumi, E. H. E. (2025). Next-Generation Smart Inverters: Bridging AI, Cybersecurity, and Policy Gaps for Sustainable Energy Transition. *Technologies*, *13*(4), 1-31.
4. Blecking J. (2023). The Nuclear Option: Green Energy Goals in the European Energy Transition, *Wisconsin International Law Journal*, *41*(1), 1-32. https://doi.org/10.3390/technologies13040136
5. Carley, S., Konisky, D. M. (2020). The justice and equity implications of the clean energy transition. *Nature Energy*, *5*, 569-577. https://doi.org/10.1038/s41560-020-0641-6

6. CERT. (2015). *CERT Polska Raport 2014*. Warszawa: NASK.
7. CERT. (2016). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2015*. Warszawa: NASK.
8. CERT. (2017). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2016*. Warszawa: NASK.
9. CERT. (2018). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2017*. Warszawa: NASK.
10. CERT. (2019). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2018*. Warszawa: NASK.
11. CERT. (2020). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2019*. Warszawa: NASK.
12. CERT. (2021). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2020*. Warszawa: NASK.
13. CERT. (2022). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2021*. Warszawa: NASK.
14. CERT. (2023). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2022*. Warszawa: NASK.
15. CERT. (2024). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2023*. Warszawa: NASK.
16. CERT. (2025). *Raport roczny z działalności CERT Polska. Krajobraz Bezpieczeństwa Polskiego Internetu 2025*. Warszawa: NASK.
17. Derugina, T. (2023). *The green transition, energy security and energy independence*. W: Ch. Gollier, D. Rohner (red.), *Peace not Pollution-How Going Green Can Tackle Both Climate Change and Toxic Politics* (185-191). Paryż: CEPR.
18. Duszczyk, M. (2014). *Cyberatak na polskie firmy energetyczne*. Pobrane z: https://energia.rp.pl/energetyka/art4985261-cyberatak-na-polskie-firmy-energetyczne? (dostęp: 12.02.2026).
19. Elbląskie Przedsiębiorstwo Energetyki Cieplnej. (2022). *Cyberatak: EPEC powiadamia UODO*. Pobrane z: https://epec.pl/aktualnosci/cyberatak-na-epec-spolka-powiadamia-urzad-ochrony-danych-osobowych (dostęp: 12.02.2026).
20. Gapiński, K. (2016). *Blackout w zachodniej Ukrainie – cyber atak o wymiarze międzynarodowym*. Pobrane z: https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym (dostęp: 12.02.2026).

21. Gov.pl (b.d.). *Rodzaje cyberzagrożeń – zagrożenia techniczne*. Pobrane z: https://www.gov.pl/web/baza-wiedzy/zagr-techniczne (dostęp: 12.02.2026).
22. Harichandan, S. i in. (2022). Energy transition research: A bibliometric mapping of current findings and direction for future research. *Cleaner Production Letters*, 3(100026), 1-17. https://doi.org/10.1016/j.clpl.2022.100026
23. Kędzierski, M., (2024). *Klucz do przyszłości Energiewende: wsparcie budowy nowych elektrowni*. Pobrane z: https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2024-02-12/klucz-do-przyszlosci-energiewende-wsparcie-budowy-nowych (dostęp: 12.02.2026).
24. Klimczuk, O. (2025a). R*osjanie zaatakowali polską elektrownię i wodociąg*. Pobrane z: https://cyberdefence24.pl/cyberbezpieczenstwo/rosjanie-zaatakowali-polska-elektrownie-i-wodociag (dostęp: 12.02.2026).
25. Klimczuk, O. (2025b). *Polska elektrownia ponownie zaatakowana przez Rosję*. Pobrane z: https://cyberdefence24.pl/cyberbezpieczenstwo/polska-elektrownia-wodna-zaatakowana-po-raz-drugi (dostęp: 12.02.2026).
26. Malko, J. Wojciechowski, H. (2015). Sektor energetyczny i cyberbezpieczeństwo. *Nowa Energia*, *1*, 10-15.
27. Ministerstwo Klimatu i Środowiska. (2021). *Polityka Energetyczna Polski do 2040 r.* Warszawa: Ministerstwo Klimatu i Środowiska.
28. Muhire, F., Turyareeba, D., Adaramola, M. S., Nantongo, M., Atukunda, R., Olyanga, A. M. (2024). Drivers of green energy transition: A review. *Green Energy and Resources*, *2(4)*, 1-17. https://doi.org/10.1016/j.gerr.2024.100105
29. Nottingham, L., Young, M. (2019). *Cyber challenges to the energy transition*. Pobrane z: https://www.worldenergy.org/publications/entry/cyber-challenges-to-the-energy-transition (dostęp: 12.02.2026).
30. Nowosad, M. (2022). *Sieć ciepłownicza w Elblągu zaatakowana przez hakerów. Przepadła część danych klientów*. Pobrane z: https://radiogdansk.pl/wiadomosci/region/elblag/2022/06/30/siec-cieplownicza-w-elblagu-zaatakowana-przez-hakerow-przepadla-czesc-danych-klientow (dostęp: 12.02.2026).

31. Pepłowska, M. (2025). Climate neutrality in Poland: the role of the coal sector in achieving the 2050 goal. *Polityka Energetyczna – Energy Policy Journal*, *28*(1), 113-126. https://doi.org/ 10.33223/epj/202307
32. Pereira, S., Silva, C., Ferreira, L. M. (2025). Barriers to energy transition: Comparing developing with developed countries. *Energy for Sustainable Development*, *87*, 1-17. https://doi.org/10.1016/j.esd.2025.101753
33. Regeringen. (2024). *Energipolitikens långsiktiga inriktning*, Sztokholm: Rząd Królestwa Szwecji.
34. Röttinger, R. (2024). Cyberattacks on renewable energies: "how hackers are threatening the energy transition and which technologies can protect us". *European Journal of Engineering and Technology, 12*(1), 42-49.
35. Solomon, B., Krishna, D. (2011). The coming sustainable energy transition: History, strategies, and outlook. *Energy Policy*, *39*(11), 7422-7431. https://doi.org/10.1016/j.enpol.2011.09.009
36. Stankiewicz, M. (2014). *Cyberatak na Elbląskie Przedsiębiorstwo Energetyki Cieplnej*. Pobrane z: https://radioolsztyn.pl/cyberatak-na-elblaskie-przedsiebiorstwo-energetyki-cieplnej/01644460 (dostęp: 12.02.2026)
37. Szczęsny, J. (2022). *Koszmarny wyciek danych z polskiej instytucji. Kłamano odnośnie okoliczności*. Pobrane z: https://antyweb.pl/epec-atak-hakerski (dostęp: 12.02.2026).
38. Ukyab, K. T., Simonovich, L. (2025). *Powering cyber resilience in the energy sector*. Pobrane z: https://www.weforum.org/stories/2025/05/powering-cyber-resilience-energy-sector (dostęp: 12.02.2026).
39. Ustawa z 21.06.2002 r. o stanie wyjątkowym (Dz. U. z 2017 r. poz. 1928).
40. Wang, Q., Guo, J., Li, R., Jiang, X. (2023). Exploring the role of nuclear energy in the energy transition: A comparative perspective of the effects of coal, oil, natural gas, renewable energy, and nuclear power on economic growth and carbon emissions. *Environmental Research*, *221.* https://doi.org/10.1016/j.envres.2023.115290