DOI: https://doi.org/10.34862/rbm.2020.1.13

Izabela Oleksiewicz
Politechnika Rzeszowska
oleiza@prz.edu.pl
https://orcid.org/0000-0002-1622-7467

Cyberbezpieczeństwo i sztuczna inteligencja w sektorze energetycznym UE

Streszczenie: Ogromne ilości danych, jakie przechodzą przez sektor energetyczny, stwarzają potrzebę wdrażania nowych technologii i rozwiązań z zastosowaniem technik i algorytmów sztucznej inteligencji (AI). Tematyka z tym związana ma utorować drogę do analizy problemu badawczego, jakim jest wpływ sztucznej inteligencji na zwiększenie odporności sieci energetycznych i zmniejszenie prawdopodobieństwa występowania przerw w dostawach energii spowodowanych atakami w cyberprzestrzeni. Oczekuje się więc, że sztuczna inteligencja będzie jednym ze środków rozwoju bezpieczeństwa, ekonomii i niezawodności energetyki. W artykule wskazano lukę prawną, która dotyczy obecnej sztucznej inteligencji, sektora energii i polityki cyberterroryzmu. Postawiono tezę, że połączenie platformy w ramach sztucznej inteligencji i badań nad energią daje szansę na to, że platforma energetyczna lub rynek oparty na sztucznej inteligencji mogą być potencjalnym rozwiązaniem dla systemów energetycznych nowej generacji we włączeniu ogromnych rozproszonych zasobów odnawialnych, a taką możliwość stwarza dyrektywa NIS. Wraz z postępującym rozwojem narzędzi sztucznej inteligencji wzrasta wrażliwość całej struktury na ryzyko ataków cybernetycznych. Ponieważ istnieje uzasadniona obawa, że AI zostanie wykorzystana do niepożądanych celów, konieczne jest zabezpieczenie systemów z nią związanych.

Słowa kluczowe: sztuczna inteligencja, polityka energetyczna, cyberbezpieczeństwo, Unia Europejska

Cybersecurity and Artificial Intelligence in the EU Energy Sector

Summary: The huge amounts of data that pass through the energy sector create the need to implement new technologies and solutions using artificial intelligence techniques and algorithms. The subject matter related to this is to pave the way for the analysis of the fundamental research problem, which is the impact of artificial intelligence on increasing the resilience of energy networks and reducing the likelihood of interruptions in energy supplies caused by attacks in cyberspace. In general, artificial intelligence is expected to be one of the means to develop energy, security, economics, and reliability. The key to this article is to show the existing legal gap that applies to current Artificial Intelligence (AI), the energy sector, and cyberterrorism policy. This article has put forward the thesis that combining the platform under Artificial Intelligence and Energy

Research gives a chance that an energy platform or market based on artificial intelligence can be a potential solution for new generation energy systems to include huge distributed renewable resources, and this possibility is provided by the NIS directive. With the progressive development of artificial intelligence tools, the sensitivity of the entire structure to the risks of cyberattacks is increasing. Hence, there is a need to secure systems associated with it, as there is a reasonable fear that it will be used for undesirable purposes.

Keywords: artificial intelligence, energy policy, cybersecurity, European Union

Wstęp

Z pojęciem sztucznej inteligencji (AI – *Artificial Intelligence*) ściśle są związane zagadnienia dotyczące cyberbezpieczeństwa, które w sektorze energii zaczęło odgrywać istotną rolę. Wraz z postępującym rozwojem narzędzi sztucznej inteligencji rośnie wrażliwość całej struktury na ryzyko ataków cybernetycznych. Pojawia się zatem potrzeba zabezpieczeń systemów z nią związanych, wynikająca z uzasadnionej obawy, że zostanie wykorzystana do niepożądanych celów. Zastosowanie metod sztucznej inteligencji daje wiele możliwości, jednocześnie może powodować wzrost ataków w cyberprzestrzeni. W związku z tym zwiększa się popyt na coraz to nowsze metody i narzędzia wspierające cyberbezpieczeństwo.

Ogromne ilości danych, jakie przechodzą przez sektor energetyczny, stwarzają potrzebę wdrażania nowych technologii i rozwiązań z wykorzystaniem technik i algorytmów sztucznej inteligencji. Tematyka z tym związana ma wskazać drogę do analizy zasadniczego problemu badawczego, jakim jest wpływ sztucznej inteligencji na zwiększenie odporności sieci energetycznych i zmniejszenie prawdopodobieństwa występowania przerw w dostawach energii spowodowanych skokami i brakami energii. Kluczem jest więc ukazanie różnic między sztuczną inteligencją a sztuczną świadomością, zwłaszcza w obliczu faktu, że sztuczna inteligencja stanowi obecnie jedno z wyzwań bezpieczeństwa społecznego.

Inną istotną kwestią w tym obszarze jest obecny status prawny sztucznej inteligencji w Unii Europejskiej.W tym ujęciu niezmiernie ważna jest świadomość istniejących wyzwań oraz problemów polityki klimatycznej, jakie wiążą się z kształtowaniem europejskiej polityki energetycznej. Sektor energetyczny i polityka klimatyczna stanowią integralny element strategii rozwoju Unii Europejskiej oraz harmonizacji prawa europejskiego. Odpowiednie planowanie, zarządzanie i efektywne wdrażanie projektowanych instrumentów, w tym tych związanych ze sztuczną inteligencją, stanowią warunek konieczny do osiągnięcia sukcesu projektu integracyjnego oraz zapewnienia bezpieczeństwa dostaw energii, a także realizacji wcześniejszych założeń do 2030 r.

Stan badań nad problemem

Europa musi się zmierzyć z wieloma zagrożeniami. Do najważniejszych należy zaliczyć: konflikty regionalne, bioterroryzm, cyberterroryzm, przestępczość zorganizowaną, politykę środowiskową i klimatyczną, kryzysy ekonomiczne. Przedmiotem badawczym niniejszego artykułu jest ukazanie znaczenia sztucznej inteligencji w rozwoju polityki energetycznej UE. W ramach tego zagadnienia omówienia wymagają również zagrożenia wynikające z zależności polityki ochrony cyberprzestrzeni od poziomu integracji państw członkowskich, a w szczególności od nowych zagrożeń i wyzwań związanych z bezpieczeństwem cybernetycznym.

W tym celu założono, że ewolucja sztucznej inteligencji w UE rozwija się w różnych dziedzinach życia. Rozwój AI powoduje jednak wiele problemów społecznych i etycznych, np. relacje między użytkownikami a robotami społecznie interaktywnymi mogą prowadzić do zależności psychologicznych, które prawdopodobnie zostaną wykorzystane przez firmy tworzące te roboty. Niezbędne są więc badania dotyczące etyki i praw robotów w różnych środowiskach kulturowych, ponieważ podobne problemy pojawiające się w różnych kulturach mogą przynieść różne wyniki (Mamak, 2017, s. 156; Scheutz, 2012; Malle i in., 2015, s. 117–120). Nick Bostrom wskazuje, że poziom sztucznej inteligencji systematycznie wzrasta i zmierza w kierunku, który wykracza nawet poza ludzki poziom (Bostrom, 2014, s. 76).

Pozwoliło to na przeprowadzenie wstępnego badania, jakim było porównanie i zestawienie wyników wcześniejszych badań (Quan, Sanderson, 2018, s. 22–23). Podstawę źródłową przeprowadzonej analizy stanowiły dokumenty Unii Europejskiej regulujące problematykę polityki energetycznej, sztucznej inteligencji (B2G, 2020, s. 31–37) i ochrony cyberbezpieczeństwa (NIS, 2019). Powstało na ten temat wiele raportów międzynarodowych, np. materiałów statystycznych, artykułów naukowych i opracowań, np. Unii Europejskiej, Międzynarodowej Agencji Energii Odnawialnej (IRENA, 2019), EECSP (2017), IEEE (*Institute of Electrical and Electronics Engineers*).

Połączenie badań nad energią i sztuczną inteligencją sugeruje, że rynek oparty na sztucznej inteligencji może być potencjalnym rozwiązaniem dla systemów energetycznych nowej generacji w celu włączenia ogromnych rozproszonych zasobów odnawialnych. Wyniki umożliwiły uzyskanie końcowej odpowiedzi na pytanie, czy obecnie obowiązująca *Biała Księga w sprawie sztucznej inteligencji*.

Europejskie podejście do doskonałości i zaufania (Komisja Europejska, 2020a) i *Skoordynowany plan w sprawie sztucznej inteligencji* (Komisja Europejska, 2018) zawierają właściwe rozwiązania oraz w jakim stopniu wymagają modyfikacji, aby stworzyć większą wartość dla systemu branży energetycznej i rynku.

W strategii dotyczącej sztucznej inteligencji dla Europy Komisja zaproponowała współpracę z państwami członkowskimi nad skoordynowanym planem w zakresie sztucznej inteligencji do końca 2018 r. Miało to na celu maksymalizowanie wpływu inwestycji na poziomie UE i szczeblu krajowym, zachęcenie do synergii i współpracy w UE, wymianę najlepszych praktyk i wspólne określenie dalszych działań, tak aby zapewnić UE możliwość konkurowania na całym świecie. Propozycja skoordynowanego planu opartego na deklaracji współpracy w zakresie sztucznej inteligencji ogłoszona w kwietniu 2018 r. została podpisana przez wszystkie państwa członkowskie i Norwegię. Następnie została zatwierdzona przez Radę Europejską w czerwcu 2018 r. Państwa członkowskie (jako część grupy ds. cyfryzacji europejskiego przemysłu i AI), Norwegia, Szwajcaria oraz Komisja przygotowały plan na kilku spotkaniach między czerwcem a listopadem 2018 r. Wymiana poglądów odbyła się również podczas posiedzeń Rady ds. Konkurencyjności pod przewodnictwem Austrii, w trakcie jej prezydencji w UE. Podczas tych spotkań państwa członkowskie i Komisja określiły wiele wspólnych działań, które mają prowadzić do zwiększenia inwestycji, gromadzenia danych – surowca dla sztucznej inteligencji, wspierania talentów i zapewniania zaufania, opartych na strategii europejskiej. Za priorytetowe uznano obszary zainteresowania publicznego, takie jak opieka zdrowotna, transport i mobilność, bezpieczeństwo, ochrona i energia, a także ważne sektory gospodarki, takie jak produkcja i usługi finansowe. Rezultatem tych wspólnych prac był *Skoordynowany plan w sprawie sztucznej inteligencji* (Komisja Europejska, 2018). Poszczególne działania zostały rozpoczęte w latach 2019–2020. Kolejnym potwierdzaniem działań było przyjęcie *Białej Księgi* w *sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania* (Komisja Europejska, 2020a).

Sztuczna inteligencja łącząca różnorodne pola technologiczne musiała być zmieniana i dostosowywana przez wiele sektorów światowego przemysłu i gospodarek, a przy tym jest postrzegana jako front innowacji i technologii wspomagającej (Campbell, 1986, s. 5–7). Sztuczna inteligencja obejmuje obszerny zbiór technik obliczeniowych do wydobywania spostrzeżeń z różnych źródeł danych, w tym tak zwanych „małych danych" generowanych przez sam algorytm,

które pomagają w podejmowaniu decyzji (Teece, 2018, s. 1370–1372) i tworzą przydatne informacje. Sztuczną inteligencję uważa się za technologię ogólnego zastosowania, która może mieć znaczące implikacje technologiczne, społeczne, gospodarcze i polityczne[1]. AI radykalnie przekształci sektor energetyczny. General Electric szacuje, że AI może zwiększyć produkcję farmy wiatrowej nawet o 20%. Jednocześnie, jak twierdzą Nagy i Hajrizi (2018, s. 308–310), transformacja AI w przemyśle energetycznym będzie bezpośrednio wpływać na międzynarodową stabilność energetyczną i dobrobyt gospodarczy. Przykładowo, zastosowanie sztucznych sieci neuronowych ma ogromne znaczenie dla przedsiębiorstw energetycznych w celu poprawy ich wydajności, jakości i bezpieczeństwa produkcji oraz stabilności energii elektrycznej. Z kolei Centrum Danych Google wykorzystało sztuczną inteligencję DeepMind, aby skutecznie osiągnąć 40% oszczędności energii na działanie centrum danych (Yao, 2018). Jednak wraz ze wzrostem przyswajania technologii sztucznej inteligencji i wskaźników penetracji w sektorze energetycznym obecnie prowadzone badania nad sztuczną inteligencją i związane z energią są nadal niedostateczne dla naukowego zastosowania. Badanie Quana i Sandersona (2018) wprowadza holistyczne ramy do analizy systemów i platform AI, w tym podstawowych technologii AI, platform AI i aplikacji AI. Oparte na tych ramach badania nad AI i energią były w dużej mierze skoncentrowane na podstawowych technologiach AI, np. technologia AI szybko przeniknęła do aplikacji technicznych w systemach przemysłowych. Technicznie, w dziedzinie energetyki i elektrotechniki, techniki AI (takie jak systemy ekspertowe, sieci neuronowe i logika rozmyta) zostały wykorzystane do rozwiązania problemów technicznych (Bose, 2017, s. 2268–2270), w tym m.in. do prognozowania energii (Johannesen, Kolhe, Goodwin, 2019, s. 555–560) i cen na rynku energii (Lu, Hong, Yu, 2019), do inteligentnego wykrywania awarii sieci, zarządzania popytem, zarządzania energią budynku, zarządzania reagowaniem na zapotrzebowanie inteligentnego domu (Xu, Ahokanga, Louis i Pongracz, 2019, s. 2148) i zapewnienia bezpieczeństwa danych inteligentnych sieci dzięki AI i łańcuchowi blokowemu (Salah, Rehman, Nizamuddin i Al-Fuqaha, 2019). W ramach procesu transformacji energii największy potencjał w zastosowaniu AI będą mieć odnawialne źródła energii, zarządzanie i optymalizacja systemów

[1] W 2016 roku w Europie w sztuczną inteligencję zainwestowano około 3,2 mld EUR, w porównaniu z około 12,1 mld EUR w Ameryce Północnej i 6,5 mld EUR w Azji (Komisja Europejska, 2020).

energii odnawialnej (Macedo, Galo, de Almeida i de Lima, 2015, s. 130; Mocanu, Nguyen, Gibescu i Kling, 2016, s. 93).

Sztuczna inteligencja a sektor energetyczny UE

Według niektórych uczonych do połowy tego wieku sztuczna inteligencja będzie poza ludzkim zrozumieniem i kontrolą (Barfield, 2015). Jeśli tak się stanie, ludzkość napotka bezprecedensowe problemy prawne, a antropocentryczny punkt widzenia dzisiejszych systemów prawnych nie pozwala ludzkości rozwiązać tych problemów (Pagallo, 2013, s. 47–66). To antropocentryczne podejście postrzega nasz gatunek w centrum wszechświata (Leach, 2015, s. 159–162). Jednak zgodnie z przewidywaniami Raya Kurzweila sztuczna inteligencja do połowy wieku będzie miliard razy bardziej zdolna niż inteligencja ludzka (Hansell, Grassie, 2011, s. 34–40). Jeśli tak się stanie, Ziemia wkroczy w nową erę ewolucji biologicznej. Dzisiaj ludzkość ma zamiar stworzyć nowe gatunki nieorganiczne, które prawdopodobnie zdominują świat. Te bardziej inteligentne formy życia pewnego dnia mogą wymagać takich samych praw, jakie ma człowiek. To nieuchronnie doprowadzi do pojawienia się złożonych problemów prawnych dla ludzkości (Acemoglu, Restrepo, 2018). Można zatem stwierdzić, że przyszły status prawny sztucznej inteligencji jest dość niepewny (Turing, 1950). Mimo że roboty obecnie są uważane za własność, w niektórych krajach przeprowadzono wiele badań dotyczących praw robotów (Turkle, 2011, s. 97–101). Pod tym względem istnieją różne podejścia. Niektórzy badacze sugerują, że przyszłe świadome roboty mogą mieć ten sam status co niewolnicy w czasach starożytnych (Kakoudaki, 2014, s. 65–72). Zgodnie z tym poglądem zasady starożytnego rzymskiego prawa dotyczącego niewolnictwa są proponowane jako ramy prawne, aby zapewnić robotom odpowiedzialność prawną. Wdrażanie praw niewolników dla robotów jest podejściem antropocentrycznym, jednak traktowanie mądrzejszego i wyższego stworzenia jako niewolnika nie byłoby zrównoważonym zachowaniem ludzkości. Na dłuższą metę można powiedzieć, że rozwiązania oparte na równości okażą się bardziej rozsądne, a problemem dla ludzkości byłoby umieszczenie przyszłych relacji człowiek–robot na właściwej podstawie prawnej.

Według badań Quana i Sandersona sztuczna inteligencja w sektorze energii jest głównie ukierunkowana na techniki i rozwiązania do projektowania, optymalizacji i zarządzania działaniami różnych domen. W badaniach energii i odnawialnych jej źródeł przegląd literatury pokazuje, że sztuczną inteligencję

badano w takich obszarach, jak energia słoneczna, wiatrowa, geotermalna i wodna (Bilalovic, Patel, Zhang, 2017, s. 297–300). Znaczna liczba badań koncentrowała się na prognozowaniu zapotrzebowania na energię (Ahmad, Chen, Shah, 2019, s. 242–250). Przykładowo, modele predykcyjne można podzielić na następujące typy (Ahmad, Chen, 2018, s. 410–417): zorientowane fizycznie, zorientowane na dane, hybrydowe i wielkoskalowe. W dziedzinie prognozowania energii sztuczna sieć neuronowa jest dobrze znana z dokładnego prognozowania fenotypu energii. Znaczącym problemem jest jednak jego dokładność, gdy skala jest zmniejszana (np. na poziomie sąsiedztwa lub gospodarstwa domowego), chociaż możliwe jest precyzyjne prognozowanie obciążenia na poziomie zagregowanym (np. na poziomie państwa). Wyniki badania A. Ahmadi i A. Afrouzi (2012, s. 1672–1680) sugerują, że sieć AI jest rozwinięta aż w 40% z algorytmu sztucznej sieci neuronowej energii (Kumar i in., 2017, s. 297–299).

Zastosowania AI w energii słonecznej zostały przeanalizowane w literaturze (Dounis, 2010, s. 287–288). Aplikacje często wymagają użycia sztucznych sieci neuronowych do modelowania słonecznego zarówno w podejściu pojedynczym, jak i hybrydowym (Brancucci Martinez-Anido i in., 2016, s. 198–200). Przykładowo, zastosowanie uczenia maszynowego może poprawić dokładność prognozowania energii słonecznej od 30% do 50% wzrostu (Gawer, 2014, s. 1242–1245) w porównaniu z konwencjonalnymi modelami prognozowania. W przypadku energetyki wiatrowej badania empiryczne i próby przeprowadzone przez przemysł w takich obiektach jak GE pokazują, że dzięki wykorzystaniu czujników Internetu Rzeczy, sieci danych i zaawansowanej analityki można zoptymalizować turbiny wiatrowe, tak aby osiągały nawet 20% szczytowej wydajności w wytwarzaniu energii przez sztuczną sieć neuronową (Evans, Gawer, 2016, s. 265).

Polityka cyberbezpieczeństwa Unii Europejskiej a sektor energetyczny

Polityka cyberbezpieczeństwa definiuje sposoby korzystania z kont użytkowników i danych przechowywanych w systemie, zapewniające właściwą ochronę informacji instytucji. W każdej organizacji istnieją informacje chronione, np. dane osobowe, informacje finansowe oraz informacje jawne (marketingowe itp.). Przedmiotem polityki bezpieczeństwa Unii Europejskiej jest więc również informacja znajdująca się w systemie teleinformatycznym. Używając pojęcia polityki cyberbezpieczeństwa, ustala się zbiór praw, reguł i wskazówek

praktycznych. Określają one takie kwestie, jak zasoby teleinformatyczne, w tym informacje wrażliwe, które są zarządzane, chronione i dystrybuowane w UE, jak również pomiędzy państwami członkowskim i samej UE w ich systemach teleinformatycznych (Oleksiewicz, 2019, s. 23–26).

Należy zauważyć, że polityka cyberbezpieczeństwa jest reakcją powstałą na zaistniałe zagrożenie, jakim jest cyberterroryzm. Należy także stwierdzić, że polityka cyberbezpieczeństwa Unii Europejskiej jest nie tylko odpowiedzią na działania prowadzone na poziomie regionalnym i państwowym, ale także wynikiem tych działań. Przyczyną jej powstania był również brak odpowiednich mechanizmów i regulacji w tym zakresie. W związku z tym mamy do czynienia z tzw. procesem instytucjonalizacji. Zagrożenia związane z cyberprzestrzenią stały się jednym z głównych tematów polityki wielu państw, organizacji międzynarodowych, w tym również Unii Europejskiej, ponieważ cyberprzestrzeń staje się coraz ważniejszym wymiarem systemu międzynarodowego, a UE dostosowuje swoją strategię w tym obszarze[2].

Rosnące zagrożenia cybernetyczne i postrzeganie niepewności cybernetycznej powodowały wzrost nieufności wśród obywateli, potencjalnie powstrzymując europejską gospodarkę w miarę jej cyfryzacji. Komisja Europejska, uznając, że bezpieczeństwo cybernetyczne stanowi kluczowy element strategii rynku, wskazała na potrzebę ochrony sieci energetycznych, infrastruktury krytycznej UE i skutecznego reagowania na zagrożenia cybernetyczne oraz na potrzebę korzystania z istniejących krajowych i unijnych strategii regulacji w zakresie bezpieczeństwa cybernetycznego (Wróblewska-Łysik, 2016, s. 67–70). Podstawą reformy miały być działania przewidziane w strategii cyberbezpieczeństwa oraz główny filar strategii – dyrektywa o bezpieczeństwie sieci i informacji (Dyrektywa NIS – *Network and Information Systems Directive,* 2016). Dyrektywa NIS dotycząca bezpieczeństwa sieci i informacji stworzyła ogólnounijny system cyberbezpieczeństwa, który ma na celu m.in. zapewnienie niezakłóconego

[2] Komisja Europejska była pionierem tego podejścia w 2013 roku, podkreślając, że „te same przepisy i normy, które obowiązują w innych obszarach naszego codziennego życia, obowiązują również w dziedzinie domen internetowych" (European Commission and High Representative of the EU for Foreign Affairs and Security Policy, 2013), jak również Parlament Europejski i Rada (Dyrektywa Parlamentu Europejskiego i Rady, 2013). Ramy polityki UE w zakresie cyberobrony (Rada Unii Europejskiej, 2014) dostosowują UE do tej nowej rzeczywistości. CSDP nie jest wyjątkiem. W przypadku misji w ramach WPBiO operacjonalizację cyber należy traktować jako zadanie trójstronne. Bezpieczeństwo cybernetyczne ujęte jest również w Globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej, która została wydana w grudniu 2016 r. przez European External Action Service (EEAS, 2016).

świadczenia kluczowych usług oraz obsługi incydentów przez osiągnięcie właściwego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług. Należy jednak podkreślić, że jej podstawą prawną jest art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, odnoszący się do wspólnego rynku.

Globalna strategia UE na rzecz polityki zagranicznej i bezpieczeństwa, która została przyjęta przez Radę Europejską 28 czerwca 2016 r. (EEAS, 2016), określa wspólne interesy UE i państw członkowskich. Opiera się na takich celach, jak bezpieczeństwo obywateli i terytorium, dobrobyt, demokracja i ład światowy, które mają doprowadzić do stworzenia wiarygodnej, reaktywnej i spójnej Unii Europejskiej. Oparta jest na zasadach takich jak: jendość, współdziałanie z innymi, odpowiedzialność, pogłębianie partnerstw zewnętrznych[3].

Strategią jednolitego rynku cyfrowego dla Europy (Komisja Europejska, 2015) powtórzyła strategię bezpieczeństwa cybernetycznego UE z 2013 r. Celem unijnej strategii bezpieczeństwa cybernetycznego było ustanowienie wspólnych minimalnych wymagań dotyczących bezpieczeństwa sieci i informacji między państwami członkowskimi, ustanowienie skoordynowanych mechanizmów zapobiegania, wykrywania, łagodzenia i reagowania oraz poprawa gotowości i zaangażowania sektora energetycznego i prywatnego (Biscop, 2019, s. 1–3).

Obecny szybki rozwój usług komunikacyjnych związany z przesyłaniem olbrzymiej ilości danych stawia wiele wyzwań przed podmiotami odpowiedzialnymi za ich przesyłanie, przechowywanie i przetwarzanie. Dodatkowo automatyzacja sieci energetycznych i budowa tzw. sieci inteligentnych powoduje również wzrost ilości gromadzonych danych. Ta szeroko rozumiana informatyzacja działalności związanej z dostarczaniem energii elektrycznej sprawia, że jest ona narażona na cyberataki. Konieczne jest zatem rozwijanie

[3] Strategia z 2016 r. identyfikuje pięć priorytetów: 1) bezpieczeństwo samej UE, które ma polegać na intensyfikacji działań w zakresie obronności, bezpieczeństwa cybernetycznego, zwalczania terroryzmu oraz w zakresie energii i strategicznej komunikacji; 2) sąsiedztwo – ten priorytet dotyczy odporności państw i społeczeństw leżących na wschód i południe od UE; pojęcie „odporność" zdefiniowano jako zdolność państw i społeczeństw do reformowania się, a tym samym do zwalczania różnorakich kryzysów; 3) zintegrowane podejście do sytuacji konfliktowych (wojna i kryzys) – ten obszar wiąże się z bezzwłocznym reagowaniem na tego typu sytacje, zapobieganiem im oraz inwestowaniem w stabilizację; 4) wspieranie stabilnych porządków regionalnych opartych na współpracy na całym świecie (regiony jako kluczowa przestrzeń ładu); 5) skuteczne globalne rządzenie w XXI w. Ten ostatni priorytet dotyczy działania na rzecz globalnego ładu, opartego na prawie międzynarodowym i zapewniającego poszanowanie praw człowieka, zrównoważony rozwój oraz trwały dostęp do globalnych wspólnych dóbr.

narzędzi, które pozwolą maksymalnie zabezpieczyć zarówno prowadzenie działalności dystrybucyjnej, jak i samych odbiorców energii[4] .

Dyrektywa NIS (2016) zobowiązała wszystkie państwa członkowskie UE do zagwarantowania minimalnego poziomu zdolności krajowych w dziedzinie cyberbezpieczeństwa przez ustanowienie organów właściwych oraz pojedynczego punktu kontaktowego do spraw cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcie krajowych strategii w zakresie cyberbezpieczeństwa. Dyrektywa formułuje obowiązki służące zapewnieniu cyberbezpieczeństwa systemów informacyjnych w sektorach usług, mających kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej, a więc przede wszystkim w energetyce[5]. Wprowadza pojęcie operatora usługi kluczowej, czyli podmiotu świadczącego z wykorzystaniem systemów informacyjnych usługę kluczową, w przypadku której incydenty bezpieczeństwa teleinformatycznego mogłyby mieć istotny wpływ na jej świadczenie[6]. Dyrektywa NIS określiła obowiązki dla operatorów usług kluczowych dotyczące wdrożenia efektywnego systemu zarządzania bezpieczeństwem, obejmującego m.in. zarządzanie ryzykiem, procedury i mechanizmy zgłaszania i postępowania z incydentami czy organizację struktur na poziomie operatora. W załączniku do ustawy znajdują się natomiast wszystkie potencjalne kategorie podmiotów w poszczególnych sektorach gospodarki i działalności państwa, z których mogą

[4] W 2016 r. CERT Polska działający w NASK – Państwowym Instytucie Badawczym obsłużył 1926 incydentów, tj. o 32% więcej niż w 2015 r. Do najczęściej zgłaszanych należą następujące kategorie incydentów: oszustwa komputerowe (55,5%), obraźliwe i nielegalne treści (12,31%), złośliwe oprogramowanie (10,96%), próby włamań (5,66%), gromadzenie informacji (3,37%), włamania (2,8%), dostępność zasobów (2,34%), atak na bezpieczeństwo informacji (2,34%), inne (4,72%). Przykładowo, *phishing* (podszywanie się pod znane marki celem wyłudzenia wrażliwych danych) był zgłaszany do CERT Polska 722 584 razy, a otrzymanych zgłoszeń dotyczących unikatowych adresów IP, które są narażone na ataki oraz wyciek informacji, było 1,8 mln. CERT firmy Orange w 2017 r. miesięcznie rejestrował nawet 10 mld zdarzeń systemowych (o ponad 1 mld więcej niż rok wcześniej). Zarejestrowanych anomalii w 2017 r. było prawie 148 tys. średnio każdego miesiąca, wśród których tysiąc z nich było sklasyfikowanych jako incydenty i wymagało udzielenia wsparcia.W 2017 r. CERT Orange Polska obsłużył 12 029 incydentów (17 199 incydentów w 2016 r.).

[5] Infrastruktura cyfrowa obejmuje punkty wymiany ruchu internetowego, dostawców usług systemu nazw domen, rejestrów nazw domen najwyższego poziomu.

[6] Obecnie w Polsce kwestie zabezpieczania systemów teleinformatycznych są regulowane sektorowo lub wycinkowo, według zadań różnych podmiotów. Istnieją regulacje dotyczące zapewnienia systemu zarządzania bezpieczeństwem informacji w podmiotach publicznych, np. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2017, poz. 2247).

być wyłaniani w drodze decyzji administracyjnej operatorzy kluczowych usług[7].

Operatorzy usług kluczowych, dostawcy usług cyfrowych, podmioty publiczne, podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz niewymienione wprost w ustawie, ale też istniejące zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawcy sieci i usług łączności elektronicznej, dostawcy technologii i usług w zakresie bezpieczeństwa oraz inne podmioty (także publiczne) mają prawo do przetwarzania danych osobowych w zakresie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych przez te sieci i systemy przez organy publiczne. W rozumieniu ogólnego rozporządzenia o ochronie danych (2016)[8] jest to prawnie uzasadniony interes administratora, którego sprawa dotyczy.

Rozporządzenie wskazuje, że może to obejmować zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów, przerywanie ataków typu „odmowa usługi", a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej[9]. W tym miejscu należy podkreślić, że przetwarzanie danych osobowych w zakresie związanym z bezpieczeństwem narodowym nie podlega regulacjom rozporządzenia 2016/679 ze względu na motyw 16 i art. 2 ust. 2 lit. a rozporządzenia.

Obowiązki o charakterze administracyjnym, regulacyjnym i kontrolnym zostały przypisane właściwym ministrom do wymienionych w dyrektywie

[7] W kwestii udostępniania informacji ustawa wprowadza zasadę, że informacje o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o poziomie ryzyka wystąpienia incydentu ze względu na bezpieczeństwo państwa, a także mając na uwadze ochronę tajemnic prawnie chronionych operatorów usług kluczowych i dostawców usług cyfrowych, są wyłączone z reżimu ustawy o dostępie do informacji publicznej. W celu zapobiegania incydentom albo zapewnienia obsługi trwającego incydentu CSIRT mogą, po konsultacji ze zgłaszającym operatorem usługi kluczowej, opublikować na stronie podmiotowej BIP odpowiednio ministra obrony narodowej, NASK – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje o poszczególnych incydentach poważnych (art. 37 ust. 3 ustawy o krajowym systemie cyberbezpieczeństwa…, 2018).

[8] W związku z wejściem w życie w maju 2016 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, 2016) ustawodawca uwzględnił zawarte w tym rozporządzeniu wymogi względem podmiotów objętych krajowym systemem cyberbezpieczeństwa, w tym zwłaszcza dotyczące przetwarzania danych przez CSIRT i sektorowe zespoły cyberbezpieczeństwa w związku ze wsparciem i koordynacją obsługi incydentu. Minister właściwy do spraw informatyzacji, dyrektor Rządowego Centrum Bezpieczeństwa, pełnomocnik, o którym mowa w art. 60 ustawy, oraz organy właściwe będą mogły przetwarzać dane w związku z realizowaniem funkcji regulacyjnych i kontrolnych w węższym niż CSIRT zakresie.

[9] Motyw 49 rozporządzenia 2016/679.

2016/1148 sektorów, czyli np. sektora energii (art. 41 ustawy o krajowym systemie cyberbezpieczeństwa). W art. 42 został wskazany katalog zadań, które będą realizować organy właściwe. Zadania te obejmują prowadzenie analiz, wydawanie decyzji administracyjnych pod kątem uznania przez operatora usług kluczowych, wygaśnięcia decyzji o uznaniu przez operatora usług kluczowych, monitorowanie stosowania przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych we właściwych im sektorach.

Organy właściwe mogą wezwać operatora usługi kluczowej lub dostawcę usługi cyfrowej na wniosek właściwego CSIRT do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego. To uprawnienie jest szczególnie ważne w kontekście organu właściwego dla dostawcy usług cyfrowych, który, współpracując z odpowiednikami w innych państwach członkowskich, może się zwracać o podejmowanie działań wobec dostawców naruszających przepisy ustawy i rozporządzenia wykonawczego 2018/151.

Artykuł 42 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa wprowadza mechanizm, który pozwoli organowi właściwemu dla dostawców usług cyfrowych zwrócić się do swojego odpowiednika w innym właściwym państwie członkowskim UE o podjęcie analogicznych działań, jakie ustawa przypisuje polskiemu organowi, czyli przeprowadzanie kontroli, zobowiązywanie do usunięcia nieprawidłowości ustalonych w wyniku kontroli oraz nakładanie kar pieniężnych. Tego rodzaju zwrócenie się do organu innego państwa członkowskiego UE będzie możliwe, jeżeli dostawca usługi cyfrowej nie posiada siedziby zarządu na terytorium RP bądź nie wyznaczył przedstawiciela na jej terytorium, ale jego systemy informacyjne znajdują się na terytorium RP. Zawarcie takiego rozwiązania w ustawie jest konieczne, ponieważ część dostawców usług cyfrowych nie posiada w Polsce siedziby ani przedstawiciela, ale wiele osób przebywających na terytorium Polski jest usługobiorcami usług świadczonych przez takich dostawców (Tomaszewski, 2018, s. 135–137).

Ustawodawca wprowadza w art. 43 dla organów właściwych przepisy uprawniające do żądania przekazania informacji od podmiotów działających w sektorach i podsektorach wymienionych w załączniku nr 1 do ustawy i świadczących usługi zależne od systemów informacyjnych. Uzyskanie tych informacji w trybie poza kontrolą pozwoliłoby organowi właściwemu na należytą ocenę ryzyka niespełniania wymogów ustawowych przez poszczególnych

operatorów kluczowych, bez nakładania dodatkowych, nadmiernych obowiązków na operatora usług kluczowych, wynikających z konieczności czynnego uczestnictwa w prowadzonej kontroli. Zgodnie z przyjętymi rozwiązaniami wystąpienie o udzielnie informacji oraz brak udzielenia informacji przez podmiot lub operatora usługi kluczowej nie wpływa na możliwość wszczęcia postępowania administracyjnego albo postępowania kontrolnego.

Wnioski

Sztuczna inteligencja jest strategiczną technologią, która przynosi wiele korzyści obywatelom, przedsiębiorstwom i całemu społeczeństwu, pod warunkiem że jest ukierunkowana na człowieka, zrównoważona i przestrzega podstawowych praworaz wartości. AI oferuje istotne korzyści związane z efektywnością i wydajnością, które mogą wzmocnić konkurencyjność przemysłu europejskiego. Może się również przyczynić do znalezienia rozwiązań niektórych najpilniejszych wyzwań społecznych, w tym związanych z przeciwdziałaniem zmianie klimatu i degradacją środowiska, wyzwań związanych ze zrównoważonym rozwojem i zmianami demograficznymi oraz ochroną demokracji, a także – w razie potrzeby i w sposób proporcjonalny – przyczynić się do walki z przestępczością. Aby Europa mogła w pełni wykorzystać możliwości oferowane przez AI, musi rozwijać i wzmacniać niezbędne zdolności przemysłowe i technologiczne. Jak określono w *Europejskiej strategii w zakresie danych* (Komisja Europejska, 2020b) towarzyszącej *Białej księdze* (Komisja Europejska, 2020a), wymaga to również środków, które pozwolą UE stać się globalnym centrum danych.

Obecna literatura i badania pokazują również lukę i brak badań, które integrują systemy ICT, systemy zasilania energii, a także badań rynku energii (Ramos, Liu, 2011, s. 5). Bardziej autonomiczna, zoptymalizowana i elastyczna konstrukcja systemu energetycznego może być obsługiwana przez technologię AI, która jest wspierana przez postęp w zakresie dużych zbiorów danych, technologii IoT, a także technologii obliczeniowej. Liczne badania pokazują, że AI może poprawić efektywność operacyjną, niezawodność i inteligentne możliwości systemu energetycznego. Ogólnie rzecz biorąc, oczekuje się, że sztuczna inteligencja będzie jednym ze środków rozwoju bezpieczeństwa, ekonomii i niezawodności energetyki.

Dzięki wdrażaniu w życie różnych modeli platform stworzonych na podstawie dyrektywy NIS i przepisów prawa krajowego badanie wskazuje, że obecna

AI koncentruje się na wąskich jej zastosowaniach w sektorze energetycznym. W artykule zwrócono uwagę na możliwość tworzenia platformy AI, która może włączać, koordynować i zarządzać różnymi aplikacjami sztucznej inteligencji, tak aby stworzyć większą wartość dla złożonego systemu branży energetycznej i rynku. Połączenie platformy w ramach sztucznej inteligencji i badań nad energią sugeruje, że platforma energetyczna lub rynek oparty na AI może być potencjalnym rozwiązaniem dla systemów energetycznych nowej generacji w celu włączenia ogromnych rozproszonych zasobów odnawialnych. Takie firmy jak Google, Amazon czy Airbnb udowodniły, że sztuczna inteligencja ma zdolność do zarządzania oraz automatyzacji cyfrowego systemu i platformy, które mogą wykraczać poza ludzkie ograniczenia, np. obsługując dziesiątki tysięcy zapytań badawczych na sekundę bez utraty jakości.

Bibliografia

Acemoglu, D., Restrepo, P. (2018). *Artificial Intelligence, Automation and Work*. (NBER Working Paper 24196). Cambridge: The National Bureau of Economic Research.: https://doi.org/10.3386/w24196.

Ahmad, T., Chen, H. (2018). Utility Companies Strategy for Short-term Energy Demand for Ecasting Using Machine Learning Based Models. *Sustainable Cities and Society*, *39*, 401–417. DOI: https://doi.org/10.1016/j.scs.2018.03.002.

Ahmad, T., Chen, H., Shah, W. (2019). Effective Bulk Energy Consumption Control and Management for Power Utilities Using Artificial Intelligence Techniques under Conventional and Renewable Energy Resources. *International Journal of Electrical Power & Energy Systems*, *109*, 242–258. DOI: https://doi.org/10.1016/j.ijepes.2019.02.023.

Ahmadi, A., Afrouzi, M. (2012). An Empirical Analysis on the Adoption of Electronic Banking in the Financial Institutes Using Structural, Behavioral and Contextual Factors. *Management Science Letters*, *2*(5), 1669–1682. DOI: https://doi.org/10.5267/j.msl.2012.04.022

AI Watch (2020, 29 kwietnia). *AI Watch. Monitor the Development, Uptake and Impact of Artificial Intelligence for Europe.* European Commission. Dostęp: https://ec.europa.eu/knowledge4policy/ai-watch_en [29.04.2020].

Barfield, W. (2015). *Cyber-Humans. Our Future with Machines*. Cham: Copernicus Books/Springer.

Bilalovic, J., Patel, A., Zhang, H. (2017). Renewable Energy. Present Research and Future Scope of Artificial Intelligence. *Renewable and Sustainable Energy Reviews*, *77*, 297–317. DOI: https://doi.org/10.1016/j.rser.2017.04.018.

Biscop, S. (2019). *The EU Global Strategy 2020* (Security Policy Brief No.108). Brussels: EGMONT – Royal Institute for International Relations. Dostęp: http://www.egmontinstitute.be/content/uploads/2019/03/SPB108.pdf?type=pdf [15.04.2020].

Bose, B.K. (2017). Artificial Intelligence Techniques in Smart Grid and Renewable Energy Systems – Some Example Applications. *Proceedings of the IEEE*, *105*(11), 2262–2273. DOI: https://doi.org/10.1109/JPROC.2017.2756596.

Bostrom, N. (2014). *Superintelligence. Paths, Dangers, Strategies*. Oxford: Oxford University Press.

Brancucci Martinez-Anido, C., Botor, B., Florita, A.R., Draxl, A., Lu, S., Hamann, H.F., Hodge, B. (2016).The Value of Day–ahead Solar Power Forecasting Improvement. *Solar Energy*, *129*, 192–203. DOI: https://doi.org/10.1016/j.solener.2016.01.049.

[B2G] High-Level Expert Group on Business-to-Government Data Sharing (2020). *Towards a European Strategy on Business-to-government Data Sharing for the Public Interest. Final Report.* European Commission. Luxembourg: Publications Office of the European Union. Dostęp: https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf [10.04.2020].

Campbell, J.A. (1986). On Artificial Intelligence. *Artificial Intelligence Review*, *1*(1), 3–9. DOI: https://doi.org/10.1007/BF01988524.

Dounis, A. (2010). Artificial Intelligence for Energy Conservation in Buildings. *Advances in Building Energy Research*, *4*(1), 267-299. DOI: https://doi.org/10.3763/aber.2009.0408.

Dyrektywa NIS (2016). Dyrektywa Parlamentu Europejskiego i Rady UE nr 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. Unii Europejskiej L 194/1 z 19.07.2016). Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=EN [10.04.2020].

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. Unii Europejskiej L 218/8 z 14.08.2013). Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32013L0040&from=pl [10.04.2020].

[EEAS] European External Action Service (2016). *Wspólna wizja, wspólne działanie: Silniejsza Europa. Globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej.* Dostęp: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_pl_.pdf [13.04.2020].

EECSP (2017). *Cyber Security in the Energy Sector. Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector* (EECSP Report). Energy Expert Cyber Security Platform. Dostęp: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf [15.04.2020].

EU Member States sign up to cooperate on Artificial Intelligence (2018, 27 July). DG Connect. European Commission. Dostęp: https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence [28.04.2020].

European Commission and High Representative of the EU for Foreign Affairs and Security Policy (2013, 7 luty). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (JOIN (2013) 1 final). Dostęp: http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [20.04.2020].

Evans, P., Gawer, A. (2016). *The Rise of the Platform Enterprise: a Global Survey* (The Emerging Platform Economy Series No. 1). New York: The Center for Global Enterprise. Dostęp: https://www.issuelab.org/resources/23830/23830.pdf [28.04.2020].

Gawer, A. (2014). Bridging Differing Perspectives on Technological Platforms: Toward an Integrative Framework. *Research Policy*, *43*(7), 1239–1249. DOI: https://doi.org/10.1016/j.respol.2014.03.006

Hansell, G., Grassie, W. (2011). *Transhumanism and Its Critics*. Philadelphia: Metanexus Institute.

IRENA (2019). Artificial Intelligence and Big Data Innovation Landscape Brief. Abu Dhabi: International Renewable Energy Agency. Dostęp: https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Sep/IRENA_AI_Big_Data_2019.pdf?la=en&hash=9A003F48B639B810237FEEAF61D47C74F8D8F07F [10.04.2020].

Johannesen, N.J., Kolhe, M., Goodwin M. (2019). Relative Evaluation of Regression Tools for Urban Area Electrical Energy Demand Forecasting. *Journal of Cleaner Production*, *218*, 555–564. DOI: https://doi.org/10.1016/j.jclepro.2019.01.108.

Kakoudaki, D. (2014). *Anatomy of a Robot: Literature, Cinema, and the Cultural Work of Artificial*. New Brunswick & London: Rutgers University Press.

Komisja Europejska (2020a, 19 luty). *Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania* (COM (2020) 65 final). Dostęp: https://op.europa.eu/pl/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1/language-pl/format-PDF [15.04.2020].

Komisja Europejska (2020b, 19 luty). *Europejska strategia w zakresie danych.* Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów (COM (2020) 66 final). Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0066&from=EN [15.04.2020].

Komisja Europejska (2018, 7 grudnia). *Skoordynowany plan w sprawie sztucznej inteligencji.* Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów (COM (2018) 795 final). Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52018DC0795 [10.04.2020].

Komisja Europejska (2015, 6 maja). *Strategia jednolitego rynku cyfrowego dla Europy.* Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów (SWD (2015) 100 final). Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52015DC0192&from=EN [10.04.2020].

Kumar, B.R.S., Varalakshmi, N., Lokeshwari, S.S., Rohit, K., Manjunath, R., Sahana, D.N. (2017). Eco-friendly IOT based waste segregation and management. W: *2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT,* Mysuru, 2017, s. 297-299). DOI 10.1109/ICEECCOT.2017.8284686.

Leach, R. (2015). *Political Ideology in Britain* (3rd ed.). London: Macmillan International Higher Education.

Lu, R., Hong, S.H., Yu, M. (2019). *Demand Response for Home Energy Management Using Reinforcement Learning and Artificial Neural Network*. *IEEE Transactions on Smart Grid*, *10*(6), 6629–6639. DOI: https://doi.org/10.1109/TSG.2019.2909266.

Macedo, M.N.Q., Galo, J.J.M., de Almeida, L.A.L., de Lima, A.C. (2015). Demand Side Management Using Artificial Neural Networks in a Smart Grid Environment. *Renewable and Sustainable Energy Reviews*, 41, 128-133. DOI: https://doi.org/10.1016/j.rser.2014.08.035.

Malle, B., Scheutz, M., Arnold, T., Voiklis, J., Cusimano, C. (2015). *Sacrifice One for the Good of Many? People Apply Different Moral Norms to Human and Robot Agents*. HRI ,15: Proceedings of the Tenth Annual ACM (IEEE International Conference on Human-Robot Interaction (pp. 117–124). DOI: https://doi.org/10.1145/2696454.2696458.

Mamak, K. (2017). *Prawo karne przyszłości*. Warszawa: Wolters Kluwer.

Mocanu, E., Nguyen, P., Gibescu, M., Kling, W. (2016). Deep Learning for Estimating Building Energy Consumption. *Sustainable Energy, Grids and Networks*, *6*, 91–99. DOI: https://doi.org/10.1016/j.segan.2016.02.005.

Nagy, K., Hajrizi, E. (2018). Beyond the Age of Oil and Gas. How Artificial Intelligence Is Transforming the Energy Portfolio of the Societies. *IFAC PapersOnLine*, *51*(30), 308–310. DOI: https://doi.org/10.1016/j.ifacol.2018.11.307.

NIS (2019). *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks – Report* (2019). NIS Operation Group. Brussels: European Union. Dostęp: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 [15.04.2020].

Oleksiewicz, I. (2019). *Zarys polityki cyberbezpieczeństwa Unii Europejskiej. Casus Polski i RFN*. Warszawa: Dom Wydawniczy Elipsa.

Pagallo, U. (2013). *The Laws of Robots: Crimes, Contracts, and Torts*. Dodrecht: Springer.

Quan, X.I., Sanderson, J. (2018). Understanding the Artificial Intelligence Business Ecosystem. *IEEE Engineering Management Review*, *46*(4), 22–25, DOI: https://doi.org/10.1109/EMR.2018.2882430.

Rada Unii Europejskiej (2014, 18 listopada). *Ramy polityki UE w zakresie cyberobrony* (15585/14). Dostęp: http://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/pl/pdf [10.04.2020].

Ramos, C., Liu, C.C. (2011). AI in Power Systems and Energy Markets. *IEEE Intelligent Systems*, *26*(2), 5–8. DOI: https://doi.org/10.1109/MIS.2011.26.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. Unii Europejskiej L 119/1 z 4.05.2016). Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=PL [10.04.2020].

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2017, poz. 2247).

Rozporządzenie wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. Unii Europejskiej L 26/48 z 31.01.2018). Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018R0151&from=EN [15.04.2020].

Salah, K., Rehman, M.H.U., Nizamuddin N., Al-Fuqaha, A. (2019). Blockchain for AI: Review and Open Research Challenges. *IEEE Access*, *7*, 10127–10149. DOI: https://doi.org/10.1109/ACCESS.2018.2890507.

Scheutz, M. (2012). The Inherent Dangers of Unidirectional Emotional Bonds between Humans and Social Robots. W: P. Lin, K. Abney, G.A. Bekey (Eds.). *Robot ethics: the ethical and social implications of robotics* (s. 205-221). Cambridge: The MIT Press.

Teece, D.J. (2018). Profiting from Innovation in the Digital Cconomy: Enabling Technologies, Standards, and Licensing Models in the Wireless World. *Research Policy*, *47*(8), 1367–1387. DOI: https://doi.org/10.1016/j.respol.2017.01.015.

Tomaszewski, K. (2018). Polityka energetyczna Unii Europejskiej w kontekście problematyki bezpieczeństwa gospodarczego. *Przegląd Politologiczny*, 1, 132–146. DOI: https://doi.org/10.14746/pp.2018.23.1.9.

Traktat o Funkcjonowaniu Unii Europejskiej (Dz. Urz. Unii Europejskiej C 326/47 z 26.10.2012). Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:12012E/TXT&from=GA [29.04.2020].

Turing, A.M. (1950). Computing Machinery and Intelligence. *Mind – A Quarterly Review of Psychology and Philosophy*, *59*(236), 433–460. Dostęp: http://phil415.pbworks.com/f/TuringComputing.pdf [10.04.2020].

Turkle, S. (2011). *Alone Together. Why We Expect More from Technology and Less from Eachother*. New York: Basic Books.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018, poz. 1560 ze zm.).

Wróblewska-Łysik, M. (2016). *Europejska Strategia Globalna a możliwości współpracy Unii Europejskiej z NATO po szczycie w Warszawie*. Bezpieczeństwo Narodowe, 37-40, 67-83. Dostęp: https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Wroblewska.pdf [15.04.2020].

Xu, Y., Ahokangas, P., Louis, J.L., Pongracz E. (2019). Electricity Market Empowered by Artificial Intelligence. A Platform Approach. *Energies*, *12*(21), 4128. DOI: https://doi.org/10.3390/en12214128.

Yao, W. (2018). Analysis on the Application of the Artificial Intelligence Neural Network on the New Energy Micro Grid. *Proceedings of the 2017 4th International Conference on Machinery, Materials and Computer* (MACMC 2017). DOI: https://doi.org/10.2991/macmc-17.2018.144.