KWARTALNIK NAUK O PRZEDSIĘBIORSTWIE

3/2024

mgr Arkadiusz Zalewski
Szkoła Główna Handlowa
w Warszawie
e-mail:
az110844@doktorant.sgh.waw.pl
ORCID: 0000-0001-5321-2013

Nowy paradygmat zarządzania kapitałem intelektualnym w przedsiębiorstwach produkcyjnych State Owned Enterprises (SOE) w turbulentnych czasach

The new paradigm of intellectual capital management in State Owned Manufacturing Enterprises (SOE) during turbulent times

Słowa kluczowe:
zarządzanie kapitałem intelektualnym, State Owned Enterprises (SOE), bezpieczeństwo energetyczne, wojna hybrydowa, odporność na ataki, Balanced Scorecard (BSC), Orlen-PGNiG

Streszczenie: W obliczu rosnących zagrożeń hybrydowych, takich jak wojna hybrydowa i manipulacje cenami surowców, przedsiębiorstwa State Owned Enterprises (SOE) stają przed wyzwaniem zapewnienia bezpieczeństwa energetycznego kraju i ochrony swoich interesów. W artykule autor wskazuje na nowy paradygmat zarządzania kapitałem intelektualnym w SOE, oparty na filozofii odporności na ataki. Na przykładzie spółki Orlen-PGNiG, która jest kluczowym graczem na polskim rynku energetycznym, analizuje możliwości uwzględnienia w zarządzaniu kapitałem intelektualnym, perspektywy BSC, która realizuje odporność przedsiębiorstwa na tego typu zagrożenia.
Nowy paradygmat opiera się na trzech filarach. Kompleksowe podejście do bezpieczeństwa: obejmuje analizę ryzyka, monitorowanie sytuacji geopolitycznej, opracowanie strategii obronnej, wzmocnienie infrastruktury cybernetycznej, edukację pracowników i współpracę z instytucjami państwowymi. Długoterminowa perspektywa: uwzględnia ciągłe monitorowanie sytuacji, inwestycje w badania i rozwój, utworzenie zespołu ds. bezpieczeństwa, wdrożenie planów awaryjnych i współpracę z partnerami biznesowymi.

Zastosowanie Balanced Scorecard (BSC): pozwala na pomiar i monitorowanie postępów w zakresie celów związanych z bezpieczeństwem, odpornością i zrównoważonym rozwojem. Wdrażając te zalecenia SOE mogą stać się bardziej odporne na wyzwania turbulentnych czasów i budować długoterminową wartość dla swoich interesariuszy.

Keywords:
intellectual capital management, State-Owned Enterprises (SOE), energy security, hybrid warfare, attack resilience, Balanced Scorecard (BSC), ORLEN-PGNiG

Abstract: A New Paradigm for Intellectual Capital Management in State-Owned Enterprises (SOE) in Turbulent Times In the face of growing hybrid threats, such as hybrid warfare and commodity price manipulation, State-Owned Enterprises (SOEs) face the challenge of ensuring the country's energy security and protecting their interests. In this paper, we propose a new paradigm for intellectual capital management in SOEs, based on the philosophy of attack resilience. Using the example of ORLEN-PGNiG, a key player in the Polish energy market, we analyze the impact of hybrid warfare on hydrocarbon prices and propose intellectual capital management strategies that increase the company's resilience to such threats.
The new paradigm is based on three pillars:
Comprehensive approach to security: Includes risk analysis, geopolitical monitoring, defense strategy development, cyber infrastructure strengthening, employee education, and cooperation with government agencies.
Long-term perspective: Encompasses continuous monitoring of the situation, investments in research and development, the creation of a security team, the implementation of contingency plans, and cooperation with business partners.
Application of the Balanced Scorecard (BSC): Allows for the measurement and monitoring of progress towards security, resilience, and sustainable development goals.
By implementing these recommendations, SOEs can become more resilient to the challenges of turbulent times and build long-term value for their stakeholders.

JEL:
C1, G32, G34

Wprowadzenie

Peter Drucker, uznawany za jednego z najwybitniejszych teoretyków zarządzania, zauważył, że „Żyjemy w jednej z tych wielkich epok historycznych, które zdarzają się raz na 200 lub 300 lat, kiedy ludzie przestają rozumieć świat, a przeszłość nie jest wystarczająca, by wyjaśnić przyszłość" [Drucker, 1993].

Słowa te są wyjątkowo trafne w kontekście współczesnych wyzwań, przed którymi stają przedsiębiorstwa, zwłaszcza będące w portfelu inwestycyjnym Ministerstwa

Aktywów Państwowych. Jesteśmy świadkami dynamicznych zmian geopolitycznych, ekonomicznych i technologicznych, które wymagają nowego podejścia do zarządzania i planowania strategicznego. Tradycyjne metody zarządzania, które sprawdzały się w stabilnych czasach, okazują się bowiem niewystarczające w obliczu obecnych zagrożeń i konkurencji, która często przychodzi spoza branży w sytuacji, kiedy technologia umożliwia uzyskiwanie przewagi konkurencyjnej a naturalne staje się rozszerzanie łańcuchów wartości przez przedsiębiorstwa w obszarach nie tylko pokrewnych, ale i całkowicie nowych.

Współczesna gospodarka, zwłaszcza w kontekście sektora wydobywczego surowców energetycznych, jest coraz bardziej uzależniona od działań spółek Skarbu Państwa. Przedsiębiorstwa, w których Skarb Państwa jest większościowym bądź dominującym akcjonariuszem, pełnią kluczową rolę w zapewnieniu bezpieczeństwa energetycznego kraju oraz stabilności gospodarczej. Tym samym definiując pojęcie State Owned Enterprises (SOE), należy zwrócić uwagę na specyficzną pozycję podmiotów działających w interesie państwa, zarówno pod względem strategicznym, jak i ekonomicznym. Motywy, jakie mogą kierować ich działaniami, obejmują nie tylko osiągnięcie zysku, ale również zapewnienie ciągłości dostaw surowców energetycznych, ochronę infrastruktury krytycznej oraz promowanie interesów narodowych w kontekście napięć geopolitycznych zwłaszcza w dobie obecnych wydarzeń na Ukrainie, czy odnawianych konfliktów na Bliskim Wschodzie.

Coraz częściej w ekonomii uważa się, że maksymalizacja zysków dla udziałowców nie powinna być głównym celem przedsiębiorstw, biorąc pod uwagę złożoność otoczenia, w którym działają, oraz różnorodne interakcje z interesariuszami. Nowe podejście wywodzące się ze zrównoważonego rozwoju oparte na dyrektywie CSRD, a dotyczące raportowania ESG, polegające na maksymalizacji pozytywnego wpływu przedsiębiorstw na wszystkich interesariuszy, przyczynia się do transformacji strategii biznesowych przedsiębiorstw z różnych sektorów, zwłaszcza tych, które generują negatywne skutki społeczne i środowiskowe, jak przedsiębiorstwa energetyczne czy ciepłownicze [Nesterak, Kołodziej-Hajdo, Kowalski, 2023, s. 1]. W innym aspekcie decyzje inwestycyjne motywowane są również polityką energetyczną i długoterminową strategią bezpieczeństwa narodowego, w tym uniezależnieniem się od dostaw zewnętrznych, zwłaszcza w sytuacjach międzynarodowych konfliktów lub napięć geopolitycznych.

Głównym celem artykułu jest przedstawienie nowego paradygmatu zarządzania przedsiębiorstwem wraz z propozycją narzędzi w wymiarze strategicznym i operacyjnym, które powinny być wdrażane dualnie, odpowiadają bowiem na wyzwania współczesnych, niestabilnych czasów. Osiągnięto to poprzez analizę przykładów konkretnych działań, inwestycji oraz strategii spółek State Owned Enterprises, na przykładzie GK Orlen-PGNiG, w kontekście ich działań w poszukiwaniu i wydobyciu węglowodorów, jak również propozycję wskaźników i inicjatyw, a także ich zastosowanie w wymiarze

strategicznym BSC (Balanced Scorecard) i w operacyjnym koncepcja VUCA (Volatility, Uncertainty, Complexity, Ambiguity). Wdrożenie powyższych rozwiązań pozwala na pomiar i monitorowanie postępów w zakresie celów związanych z bezpieczeństwem, odpornością oraz zrównoważonym rozwojem, a także pokazuje, jak można skutecznie zarządzać kapitałem intelektualnym w warunkach zwiększonego ryzyka związanego z konfliktami i napięciami geopolitycznymi.

W ramach analizy literatury zastosowano podejście systematyczne, które obejmowało przeszukiwanie baz danych naukowych. Kryteria doboru obejmowały publikacje z ostatnich dziesięciu lat, napisane w języku angielskim i polskim. Przeprowadzono krytyczną ocenę jakości wybranych prac, skupiając się na metodyce, wynikach i wnioskach. Dodatkowo dokonano porównania i syntezy głównych tematów oraz trendów występujących w literaturze, co pozwoliło na identyfikację luk badawczych i potencjalnych obszarów do dalszych badań. Temat analizy jest stosunkowo nowy, z tego też powodu trudno było znaleźć literaturę bezpośrednio dotyczącą tego zagadnienia. Jednak, poprzez szerokie podejście do analizy, uwzględniono pokrewne tematy i teorie, które mogą mieć zastosowanie w kontekście badanego problemu.

Przykłady inwestycji politycznych – bezpieczeństwo energetyczne kraju

Analizując działania Grupy Kapitałowej Orlen oraz Polskiego Górnictwa Naftowego i Gazownictwa (PGNiG) w kontekście ich działań w poszukiwaniu i wydobyciu węglowodorów można wskazać na kluczowe inwestycje ukierunkowane na realizację powyższych celów. W przypadku PGNiG i magazynów gazu można przywołać przykład decyzji rozbudowy infrastruktury magazynów gazu – Terminal LNG w Świnoujściu, jak i Projekt Baltic Pipe. W obliczu zwiększonej niepewności geopolitycznej, spółki te mogły dokonywać zmian w strukturze zakupów gazu, dążąc do większej dywersyfikacji dostawców oraz źródeł surowca. W wyniku transakcji zakupu Kufpec Norway, PGNiG Upstream Norway z Grupy Orlen (PUN) przejął kontrolę nad udziałami w 5 produkujących złożach: Gina Krog, Sleipner Vest, Sleipner Ost, Gungne i Utgard. Pozwoliło to zwiększyć ilość surowca wydobywanego w Norwegii o 1 mld m^3 – do 4 mld m^3 rocznie. Docelowo produkcja węglowodorów na Norweskim Szelfie Kontynentalnym ma wynieść ponad 6 mld m^3 gazu rocznie w 2030 r. Wydobywany surowiec jest przesyłany do Polski gazociągiem Baltic Pipe, w którym Grupa Orlen ma zarezerwowaną przepustowość umożliwiającą transport nieco ponad 8 mld m^3 gazu rocznie. Skierowanie do Baltic Pipe dodatkowych wolumenów uzyskanych w wyniku nabycia Kufpec Norway oznacza, że w ujęciu średniorocznym wydobycie PGNiG Upstream Norway może stanowić ok. połowy gazu sprowadzanego przez Orlen z Norwegii przy

wykorzystaniu maksymalnej zarezerwowanej przepustowości gazociągu Baltic Pipe [Lipczyński, 2024, s. 1].

Powyższe działania są związane z dywersyfikacją dostaw, które w dużej mierze niwelują ryzyko związane z ewentualnymi zakłóceniami na rynku, co może mieć kluczowe znaczenie dla zapewnienia stabilności dostaw surowca. Dzięki temu GK Orlen może zmniejszyć swoją zależność od importu i dużej zmienności cen związanych z ostatnimi kryzysami wywołanymi pandemią COVID i obecnymi – z wojną w Ukrainie, zapewniając tym samym ciągłość dostaw i bezpieczeństwo energetyczne Polski. Odnotowany w ostatnich latach znaczący rozdźwięk pomiędzy ceną ropy a cenami paliw pozwalający na generowanie wysokiej marży rafineryjnej jest związany z wygaszaniem rafinerii w Europie wynikającej z polityki klimatycznej i skokowym popycie na paliwa wynikającym z konfliktu na wschodniej granicy Polski, a ostatnimi czasy również na Bliskim Wschodzie.

W kontekście tych zmian, zarządzanie rezerwami strategicznymi gazu oraz strategie dywersyfikacji dostaw stają się kluczowymi elementami strategii spółek Skarbu Państwa, mającymi na celu zarówno zapewnienie stabilności dostaw surowców energetycznych, jak i minimalizację ryzyka związanego z zewnętrznymi czynnikami, takimi jak sytuacja geopolityczna czy wymogi regulacyjne. Dążenie do zdywersyfikowania źródeł dostaw gazu do Polski poprzez import gazu skroplonego (LNG) wiąże się z budową Terminalu LNG w Świnoujściu, otwartym w 2015 r. Powyższa inwestycja umożliwia import gazu z różnych źródeł, w tym z USA czy krajów Bliskiego Wschodu. Jest to kluczowy krok w redukcji zależności od jednego głównego dostawcy gazu, co zwiększa bezpieczeństwo energetyczne Polski. Wspomniany Projekt Baltic Pipe to inwestycja mająca na celu połączenie polskiego systemu gazociągów z systemami duńskimi i norweskimi, umożliwiając dostęp do norweskiego gazu ziemnego poprzez duńskie góry. Gazociąg ma przyczynić się do dalszej dywersyfikacji źródeł dostaw gazu do Polski, a także umożliwić odcięcie się od dostaw gazu z Rosji. Obie te inwestycje są rezultatem decyzji podejmowanych na poziomie państwowym, które mają na celu zwiększenie niezależności energetycznej Polski. Chociaż mogą one być kosztowne i wymagające inwestycji, ich strategiczne znaczenie dla bezpieczeństwa energetycznego i suwerenności państwa jest niepodważalne. W obliczu zwiększonych zagrożeń wynikających z napięć geopolitycznych, zarówno w Ukrainie, jak i na Bliskim Wschodzie, przedsiębiorstwa (SOE) muszą podejmować strategiczne decyzje w zakresie zarządzania infrastrukturą krytyczną, taką jak w przypadku GK Orlen instalacje wydobywcze i rurociągi transportujące surowce. Wzrastające napięcia geopolityczne spowodowały rosnącą potrzebę utrzymania rezerw strategicznych gazu w celu zabezpieczenia dostaw w przypadku ewentualnych zakłóceń na rynku, a także na wypadek konfliktu, w którym może uczestniczyć Polska. Decyzje dotyczące wielkości i struktury tych rezerw musiały być dostosowane do zmieniającej się sytuacji politycznej oraz ekonomicznej. Unia Europejska wprowadziła szereg

regulacji dotyczących utrzymania rezerw strategicznych gazu w celu zwiększenia bezpieczeństwa energetycznego regionu. GK Orlen-PGNiG, musiała dostosować się do tych wymogów, co skutkowało zmianami w ich strategiach zakupowych oraz dywersyfikacji dostaw. Tym samym przedsiębiorstwa (SOE) są zobligowane przez rząd do inwestowania w rozbudowę infrastruktury magazynów gazu w celu zwiększenia zdolności jego przechowywania. Inwestycje w magazyny gazu wpływają również na stabilizację cen energii, zwłaszcza w przypadku zmiennych cen gazu na rynkach międzynarodowych, kiedy rząd może preferować posiadanie zapasów gazu w celu złagodzenia jego skoków cenowych. W kontekście zrównoważonego rozwoju i zwiększenia bezpieczeństwa energetycznego, warto zwrócić uwagę również na rozwój biometanowni oraz zastosowanie wodoru. Biometanownie mogą przyczynić się do dywersyfikacji źródeł energii, redukcji emisji gazów cieplarnianych oraz zwiększenia niezależności energetycznej kraju, a zastosowanie wodoru jako nośnika energii ma potencjał zrewolucjonizowania sektora energetycznego, zwłaszcza w kontekście dekarbonizacji. Biometan, produkowany z odpadów rolniczych i przemysłowych, może być używany jako paliwo w sektorze transportowym oraz źródło energii w elektrociepłowniach, wodór, z kolei jako paliwo przyszłości, może być wykorzystywany w sektorze przemysłowym, transportowym i energetycznym. W Polsce istnieje duży potencjał rozwoju biometanowni, zwłaszcza na terenach wiejskich, gdzie dostępność surowców organicznych jest wysoka. Dodatkowo dzięki posiadaniu znaczących zasobów węgla i rozwijaniu technologii sekwestracji CO_2, Polska może stać się liderem w produkcji wodoru na skalę europejską.

Powyższe czynniki wpływają na decyzje inwestycyjne (SOE), prowadząc do podejmowania działań, które mogą być bardziej związane z interesami strategicznymi państwa niż działaniem obliczonym na poprawę wyników ekonomiczno-finansowych. Tym samym kapitał intelektualny w takich przedsiębiorstwach ma nieco inny konstrukt niż w przypadku przedsiębiorstw niewchodzących w aktywa państwowe. Kultura organizacji jest czymś pomiędzy ministerstwem a korporacją, co jest związane z przenikaniem się procesów decyzyjnych na styku przedsiębiorstwa i państwa. Wydaje się oczywiste, że strategiczne zarządzanie spółkami wchodzącymi w portfel aktywów państwa polskiego w czasach niestabilnych wymaga elastyczności i zdolności do szybkiego podejmowania decyzji, niekoniecznie obliczonej na generowanie dodatniego wskaźnika EBIDA. Zarządy tych spółek muszą być w stanie odpowiednio zareagować na zmieniające się warunki na rynku oraz na ewentualne zagrożenia wynikające z napięć geopolitycznych, będąc zobligowane do utrzymania ciągłości dostaw przy określonej cenie. W tym kontekście podejmowane przez nie działania muszą być ukierunkowane na minimalizację ryzyka i zapewnienie stabilności funkcjonowania, nawet w warunkach skrajnej niepewności podyktowanej włączeniem działań militarnych jako determinanty wpływu polityczno-ekonomicznego.

Nowy paradygmat zarzadzania kapitałem intelektualnym – perspektywa odporności

Wartość dodana dla gospodarki narodowej wnoszona przez przedsiębiorstwa SOE wymaga wdrażania przez nie nowych strategii zarządzania, które uwzględniają zarówno aspekty bezpieczeństwa, jak i budowania wartości ekonomiczno-finansowej. W obliczu zmieniających się warunków geopolitycznych i gospodarczych, SOE muszą być gotowe do dynamicznej adaptacji i podejmowania skutecznych działań, aby zapewnić im trwałość i rozwój w turbulentnych czasach. W kontekście nowego paradygmatu zarządzania kapitałem intelektualnym w przedsiębiorstwach aktywów państwowych w turbulentnych czasach, perspektywa strategiczna stabilności i bezpieczeństwa zarządzania staje się kluczowa.

Rozwój gospodarczy krajów ściśle związany jest z dostępem do energii. Analizując ten aspekt przez pryzmat danych liczbowych, obserwujemy, że w latach 2010–2020 globalne zapotrzebowanie na energię elektryczną wzrosło z 64,4 tys. PJ (petajoule) do 82,0 tys. PJ, co oznacza wzrost o 27,3% w ciągu dekady. W Polsce także zauważalny był ten trend wzrostowy. Zużycie energii elektrycznej w Polsce w 2010 r. wyniosło 427 PJ, natomiast w 2020 r. sięgnęło 494 PJ, co stanowi wzrost o 15,7% [Nesterak, Kołodziej-Hajdo, Kowalski, 2023, s. 3].

Jedną z form transparentnego działania na styku interes państwowy a przedsiębiorstwo może być wprowadzenie nowych regulacji, takich jak utworzenie Rady ds. Bezpieczeństwa Strategicznego. Jest to też odpowiedź na rosnące wyzwania związane z napięciami geopolitycznymi, co generuje niepewność na rynku surowców energetycznych. Jak już wspomniano, dla przedsiębiorstw SOE, które operują w sektorze wydobywczym i energetycznym, priorytetem staje się nie tylko osiągnięcie zysku, ale również zapewnienie ciągłości dostaw surowców oraz ochrona infrastruktury krytycznej. Przedsiębiorstwa energetyczne, prowadząc swoją działalność gospodarczą, muszą zapewnić ciągłość dostaw energii, co wymaga nadzoru ze strony rządów. Podlegają one również różnorodnym regulacjom na poziomie krajowym i międzynarodowym. Sektor energetyczny odgrywa istotną rolę w gospodarce, ponieważ z jednej strony jest odpowiedzialny za zapewnienie bezpieczeństwa energetycznego, a z drugiej strony może przyczynić się do zjawiska ubóstwa energetycznego, gdy wzrost cen energii bezpośrednio wpływa na dostępność energii dla konsumentów [Neacsa, Panait, Muresan, 2020].

W obliczu zmieniających się warunków geopolitycznych i wzrastającej niepewności na rynku, zarządzanie stabilnością oraz skuteczne reagowanie na potencjalne zagrożenia stają się kluczowymi wyzwaniami dla zarządu SOE. Nowe przepisy, takie jak projekt noweli ustawy o zasadach zarządzania mieniem państwowym, podkreślają konieczność zabezpieczenia stabilności zarządzania strategicznymi spółkami państwowymi. Wprowadzenie Rady ds. Bezpieczeństwa Strategicznego ma na celu zapewnienie niezależnej

oceny decyzji dotyczących odwołania członków organów zarządzających oraz utrzymanie spójności strategii długofalowych. Z jednej strony przedsiębiorstwa działające w sektorze energetyki i górnictwa odgrywają kluczową rolę w gospodarce każdego kraju; z drugiej strony, aktualne warunki działalności tych firm stawiają przed menedżerami szereg wyzwań decyzyjnych, z którymi muszą się zmierzyć. Wprowadzenie efektywnego systemu controllingowego do tych przedsiębiorstw może stanowić rozwiązanie, wspierające menedżerów w podejmowaniu trafnych decyzji. To z kolei wymusza na naukowcach prowadzenie dogłębnych badań w celu zidentyfikowania obecnych i przyszłych kierunków rozwoju controllingowych praktyk w firmach sektora energetycznego [Irrek, 2003]. Jednocześnie nowy paradygmat zarządzania kapitałem intelektualnym w SOE musi uwzględniać także aspekty innowacyjności i adaptacyjności. W warunkach zmieniającego się środowiska biznesowego, przedsiębiorstwa te muszą być gotowe do szybkiej adaptacji do nowych warunków oraz inwestować w rozwój technologiczny i kadrowy, aby zachować konkurencyjność na rynku globalnym.

Wdrożenie nowego narzędzia zarządzania kapitałem intelektualnym w SOE w turbulentnych czasach wymaga skupienia się na kilku kluczowych obszarach działania. Po pierwsze, konieczne jest pogłębienie analizy ryzyka oraz identyfikacja potencjalnych zagrożeń wynikających z napięć geopolitycznych, zmian regulacyjnych oraz dynamicznie zmieniającego się otoczenia biznesowego. Działania te mogą obejmować opracowanie scenariuszy zarządzania kryzysowego oraz wzmocnienie infrastruktury technologicznej w celu zabezpieczenia przed np. atakami cybernetycznymi. Po drugie, przedsiębiorstwa SOE muszą inwestować w rozwój konstruktów kapitału intelektualnego pozwalających na skuteczne realizacje kryzysowych scenariuszy tak, aby budować odporność na wrogie działania zarówno na rynku makro, jak i w samym przedsiębiorstwie. Wprowadzenie elastycznych struktur organizacyjnych oraz zachęcanie do współpracy i wymiany wiedzy pomiędzy różnymi działami może przyczynić się do zwiększenia adaptacyjności i kreatywności pracowników w sytuacjach zmiany. Po trzecie, przedsiębiorstwa SOE powinny rozwijać partnerstwa strategiczne z innymi przedsiębiorstwami oraz instytucjami wojskowymi, co umożliwi wymianę know-how oraz wspólne opracowywanie innowacyjnych rozwiązań zarzadzania kryzysowego budującego odporność organizacji na działania będące elementem wojny hybrydowej.

Doktryna wojny hybrydowej a odporność spółek Skarbu Państwa

Doktryna wojny hybrydowej to strategia militarna, która wykorzystuje różnorodne środki, w tym militarną, polityczną, ekonomiczną, informacyjną oraz cybernetyczną, aby osiągnąć cele polityczne poprzez wpływanie na społeczeństwo, gospodarkę i instytucje państwowe. W ramach tej doktryny gospodarka staje się jednym z kluczowych

elementów oddziaływania, a ataki na sektor gospodarczy mogą być wykorzystywane do osłabienia państwa i destabilizacji jego funkcjonowania[1].

W kontekście Polski Ministerstwo Obrony Narodowej monitoruje i analizuje odporność państwa oraz gospodarki na ataki z zewnątrz. Jednak, ze względu na złożoność zagadnienia i konieczność interdyscyplinarnej analizy, również inne resorty, takie jak Ministerstwo Spraw Wewnętrznych i Administracji czy Ministerstwo Cyfryzacji, mogą być zaangażowane w ten proces. Pytanie, kto dokładnie w Ministerstwie Obrony Narodowej zajmuje się badaniem odporności państwa i gospodarki na ataki z zewnątrz, może prowadzić do zrozumienia struktury i działań podejmowanych w celu zapewnienia bezpieczeństwa narodowego.

Jeśli chodzi o działania osłabiania państwa w obszarze społecznym, zgodnie z tezami zawartymi w książce Tomasza Schumana, możemy rozważać, czy istnieją podobne mechanizmy działające w Polsce. Oczywiście, należy zachować zdrową ostrożność w tej ocenie, aby unikać nadinterpretacji i spekulacji. Niemniej jednak badanie wpływu różnych czynników na społeczeństwo oraz analiza potencjalnych działań wywrotowych czy manipulacyjnych stanowi ważny element pracy nad bezpieczeństwem narodowym. W kontekście ustawy o obronności oraz długoterminowej strategii bezpieczeństwa narodowego ich celem jest zapewnienie skutecznej ochrony państwa niezależnie od aktualnej sytuacji politycznej czy zmian w rządzie. Te dokumenty mają na celu stworzenie ram strategicznych i operacyjnych, które umożliwią skuteczną odpowiedź na różnorodne zagrożenia, w tym także te wynikające z działań hybrydowych czy wywrotowych.

W kontekście działań hybrydowych i ochrony przed nimi ważne jest, aby przedsiębiorstwa SOE rozwijały skuteczne mechanizmy zarządzania kryzysowego w ramach perspektywy odporności, w tym strategie cyberbezpieczeństwa, monitorowanie zagrożeń informacyjnych oraz zapewnienie ochrony systemów krytycznej infrastruktury na ataki cybernetyczne i inne. Ponadto konieczne jest wzmocnienie zdolności obronnych oraz współpracy międzynarodowej w zakresie zwalczania zagrożeń hybrydowych. W trosce o stabilność gospodarki w przypadku konfrontacji hybrydowej, przedsiębiorstwa SOE powinny działać w sposób strategiczny i elastyczny. Może to obejmować inwestycje w nowe technologie, zwiększenie dywersyfikacji dostaw surowców oraz rozwój zdolności produkcyjnych w kluczowych sektorach. Zasadne staje się też wsparcie

[1] Wikipedia definiuje termin „wojny hybrydowej" jako strategię wojenną łączącą działania konwencjonalne, nieregularne, cybernetyczne, terroryzm i przestępczość, w tym samym czasie i na tym samym polu bitwy, z zamiarem osiągnięcia celów politycznych. Wojna taka często jest prowadzona bez oficjalnego wypowiedzenia. Jej charakter ma pozwolić agresorowi na całkowite lub częściowe uniknięcie za nią odpowiedzialności. Zagrożenie hybrydowe jest definiowane jako działanie jakiegokolwiek adwersarza używającego wyżej wymienionych kombinacji działań. Działania w ramach wojny hybrydowej są prowadzone na różnorodnych płaszczyznach: militarnej, politycznej, gospodarczej, społeczno-kulturowej, historycznej, psychologicznej oraz informacyjnej (dezinformacja i propaganda).

innowacyjnych projektów oraz programy badawczo-rozwojowe, które mogą umocnić potencjał odporności poprzez wzmocnienie istotnych dla realizacji powyższego celu konstruktów kapitału intelektualnego, zarówno kompetencji i adekwatnych postaw, jak i systemów zabezpieczających i wczesnego ostrzegania. Z tego powodu przedsiębiorstwa muszą opracować i wdrożyć rozwiązania diagnozujące objawy kryzysów, czyli systemy wczesnego ostrzegania. Są to narzędzia optymalizacji ryzyka wykorzystywane w ramach metod zarządzania ryzykiem ilościowym. Wraz z podejściem strategicznym, tego typu narzędzia odgrywają coraz istotniejszą rolę w środowisku niestabilności gospodarczej i niepewności. Konieczność przewidywania zagrożeń jest niekwestionowana – wyzwanie polega na wyborze odpowiednich metod, które minimalizują ryzyko błędnych prognoz. Jednak termin „ostrzeżenie", powszechnie używany, może być mylący. Akt ostrzeżenia może bowiem wskazywać zarówno na próbę wykrycia zagrożeń, jak i na identyfikację możliwości. Stąd też termin „identyfikacja" wydaje się być bardziej odpowiedni w tym kontekście [Kaczmarek, 2012, s. 3].

W perspektywie długoterminowej, niezależnie od zmian politycznych, kluczowe jest kontynuowanie strategii bezpieczeństwa narodowego i ciągłe doskonalenie mechanizmów odporności na ataki. Odpowiednia alokacja zasobów finansowych i niefinansowych na cele obronne oraz rozwój zdolności obronnych, w tym obronności cyberprzestrzeni, są niezbędne dla zapewnienia bezpieczeństwa przedsiębiorstw SOE, państwa i jego obywateli. W kontekście współpracy międzynarodowej na szczeblu ministerstw Polska powinna aktywnie uczestniczyć w międzynarodowych forach (takich jak NATO i Unia Europejska) oraz współpracować z partnerami strategicznymi w zakresie zwalczania zagrożeń hybrydowych. Współdziałanie z innymi krajami w zakresie wymiany informacji, wspólnych ćwiczeń obronnych oraz wspierania i rozwoju zdolności obronnych jest kluczowe dla skutecznego przeciwdziałania zagrożeniom hybrydowym obliczonym na osłabienie przedsiębiorstw, których zadaniem jest budowa bezpieczeństwa energetycznego kraju.

Warto również podkreślić rolę społeczeństwa obywatelskiego w zabezpieczaniu państwa przed zagrożeniami hybrydowymi. Edukacja społeczeństwa w zakresie cyberbezpieczeństwa, promowanie krytycznego myślenia oraz budowanie świadomości na temat zagrożeń hybrydowych są kluczowe dla budowania odporności społecznej na działania wywrotowe czy manipulacyjne. Skuteczne przeciwdziałanie zagrożeniom hybrydowym wymaga koordynacji działań na wielu płaszczyznach, włącznie z wymiarem politycznym, ekonomicznym, społecznym i militarnym. Współpraca wszystkich sektorów kluczowych obszarów gospodarki mających aktywa infrastruktury krytycznej, społeczeństwa oraz skoordynowane działania państwa są kluczowe dla zapewnienia bezpieczeństwa i stabilności w obliczu zagrożeń hybrydowych.

Narzędzia zarządzania strategicznego kapitałem intelektualnym

Przedsiębiorstwa działające w warunkach zagrożeń hybrydowych powinny być wyposażone w narzędzia, które umożliwią im skuteczne zarządzanie ryzykiem i budowanie odporności na potencjalne konflikty oraz wrogie działania [Shanks, Johnston, 2014]. Zastosowanie BSC (Balanced Scorecard) pozwala przedsiębiorstwom na kompleksowe podejście do zarządzania, uwzględniając nie tylko cele finansowe, ale także aspekty związane z bezpieczeństwem, odpornością na kryzysy i zrównoważonym rozwojem [Kaplan, Norton, 2000]. W odpowiedzi na te wyzwania, przydatna może okazać się też koncepcja VUCA (Volatility, Uncertainty, Complexity, Ambiguity) przeniesiona z kontekstu wojskowego do zarządzania przedsiębiorstwami. VUCA jest akronimem opisującym zmienność, niepewność, złożoność i niejednoznaczność środowiska, w którym organizacje muszą funkcjonować. Koncepcja ta wywodzi się z amerykańskiej armii i po raz pierwszy została wprowadzona przez U.S. Army War College na przełomie lat 80. i 90. XX wieku, opisując nową dynamikę i wyzwania, z jakimi muszą mierzyć się wojskowi w erze po zimnej wojnie. Później koncepcja VUCA została przyjęta również w świecie biznesu i zarządzania, gdzie jest używana do opisywania skomplikowanych i szybko zmieniających się warunków rynkowych oraz przygotowania liderów i organizacji na te wyzwania.

Przykładowe narzędzia i determinanty, którymi powinny kierować się zarządy przedsiębiorstwa, mogą mieć wymiar strategiczny opierający się na stworzeniu dodatkowej perspektywy BSC, a także operacyjny oparty na filozofii VUCA i jej wskaźniki w zarządzaniu przedsiębiorstwem.

Poniżej przedstawiono zestawienie powyższych dwóch proponowanych podejść, które mogą a może nawet powinny być stosowane dualnie.

Warstwa operacyjna uwzględniająca założenia koncepcji VUCA

V–Volatility (**zmienność**) rozumiana jako szybkość zachodzących zmian w otoczeniu.
Przykładowe wskaźniki: częstotliwość i intensywność zmian w rynkach surowcowych, fluktuacje cen, zmiany regulacji.
Przykłady działań zaradczych: rozwój elastycznych strategii zakupowych, dywersyfikacja źródeł zaopatrzenia, szybka adaptacja do zmian.
U – Uncertainty (**niepewność**) rozumiana jako brak przewidywalności i trudności w prognozowaniu przyszłości.
Przykładowe wskaźniki: liczba nieprzewidywalnych wydarzeń geopolitycznych, brak stabilności regulacyjnej, niepewność rynkowa.
Przykłady działań zaradczych: monitorowanie sytuacji geopolitycznej, rozwój scenariuszy kryzysowych, inwestycje w analizy i prognozy rynkowe.

C – Complexity (**złożoność**) rozumiana jako wiele wzajemnie powiązanych części i zmiennych.
Przykładowe wskaźniki: liczba partnerów biznesowych, skomplikowane łańcuchy dostaw, wielość regulacji do spełnienia.
Przykłady działań zaradczych: integracja różnych aspektów działalności w strategii, rozwój kompetencji analitycznych, wprowadzenie zaawansowanych systemów zarządzania.
A – Ambiguity (**niejednoznaczność**) rozumiana jako niejasność i wieloznaczność informacji.
Przykładowe wskaźniki: brak jasnych wytycznych, sprzeczne sygnały rynkowe, trudności w interpretacji danych.
Przykłady działań zaradczych: inwestycje w technologie i systemy analizy danych, rozwój zdolności adaptacyjnych, szkolenia dla pracowników z zakresu interpretacji i analizy informacji.

Warstwa strategiczna uwzgledniająca cele i wskaźniki KPI w ramach BSC

1. Zwiększenie odporności na ataki cybernetyczne
   KPI: Czas wykrycia incydentu cybernetycznego (mierzony w godzinach)
2. Poprawa świadomości pracowników w zakresie cyberbezpieczeństwa
   KPI: Procent przeszkolonych pracowników w zakresie bezpieczeństwa IT
3. Zapewnienie ciągłości działania w przypadku ataku hybrydowego
   KPI: Czas przywrócenia normalnego funkcjonowania po ataku (mierzony w godzinach)
4. Zwiększenie współpracy z instytucjami państwowymi w zakresie bezpieczeństwa
   KPI: Liczba udziałów w ćwiczeniach obronnych z instytucjami państwowymi

Działania pozwalające na podniesienie potencjału kapitału intelektualnego przedsiębiorstwa w obszarze budowania odporności powinny rozpocząć się od powołania dedykowanego zespołu odpowiedzialnego za monitorowanie, ocenę i reakcję na zagrożenia. Do zadań zespołu powinno należeć:

A. Stałe monitorowanie sytuacji: Prowadzenie stałego monitoringu sytuacji geopolitycznej i biznesowej oraz nowych zagrożeń.
B. Inwestycje w badania i rozwój: Kontynuowanie inwestycji w technologie bezpieczeństwa.
C. Plany awaryjne: Opracowanie i regularna aktualizacja planów awaryjnych i procedur reagowania na kryzysy.
D. Współpraca z partnerami biznesowymi: Budowanie relacji partnerskich z innymi firmami i instytucjami państwowymi w celu wymiany informacji, doświadczeń i wspólnego działania na rzecz bezpieczeństwa [Roth, 2016, s. 512–534], obejmu-

jąca wymianę najlepszych praktyk w zakresie cyberbezpieczeństwa, wspólne szkolenia i ćwiczenia oraz wspólne opracowywanie planów awaryjnych.

Jak w każdej strategii, tak i w tej, kluczowe staje się posiadanie adekwatnego potencjału kapitału intelektualnego pozwalającego na realizację celów strategii budowania odporności przedsiębiorstwa. Tym samym w ramach podnoszenia poziomu kapitału intelektualnego można zaproponować następujące działania:

- Analiza ryzyka: Przeprowadzanie kompleksowej analizy ryzyka, uwzględniającej zagrożenia hybrydowe, takie jak ataki cybernetyczne, dezinformacja i destabilizacja ekonomiczna.
- Monitorowanie sytuacji geopolitycznej: Regularne śledzenie sytuacji politycznej i geopolitycznej, aby dostosować strategię działania do bieżących zagrożeń.
- Strategia obronna: Opracowanie strategii obronnej, obejmującej aspekty cyberbezpieczeństwa i ochrony przed innymi zagrożeniami hybrydowymi.
- Wzmocnienie infrastruktury cybernetycznej: Inwestycje w IT i zabezpieczenia, które zapewnią odporność na ataki cybernetyczne.
- Edukacja pracowników: Szkolenia z zakresu cyberbezpieczeństwa i świadomości zagrożeń hybrydowych.
- Współpraca z instytucjami państwowymi: Nawiązanie współpracy z instytucjami odpowiedzialnymi za bezpieczeństwo narodowe i udział w programach wzmacniających zdolności obronne.

Poprzez ustanowienie takich celów i wskaźników KPI, przedsiębiorstwo będzie mogło monitorować skuteczność swoich działań w zakresie budowania odporności na zagrożenia hybrydowe i szybko reagować w przypadku wystąpienia incydentów. Kluczowym elementem w zarządzaniu przedsiębiorstwem w warunkach zagrożeń hybrydowych jest ciągłe dostosowywanie strategii i działań do zmieniającego się środowiska oraz rozwijanie zdolności obronnych. Przedsiębiorstwa powinny również rozwijać swoje relacje z instytucjami państwowymi oraz innymi podmiotami, aby zwiększyć swoją odporność na potencjalne zagrożenia. Monitorowanie tych wskaźników KPI pozwoli przedsiębiorstwu na bieżąco oceniać skuteczność swoich działań w zakresie budowania odporności na zagrożenia hybrydowe oraz szybko reagować na zmieniające się warunki. Zastosowanie BSC pozwoli przedsiębiorstwom na kompleksowe podejście do zarządzania, uwzględniając nie tylko cele finansowe, ale także aspekty związane z bezpieczeństwem, odpornością na kryzysy i zrównoważonym rozwojem. Dzięki temu przedsiębiorstwa będą bardziej przygotowane na sytuacje kryzysowe oraz lepiej zintegrowane z potrzebami społeczności lokalnych i wymaganiami dotyczącymi ochrony środowiska.

Podsumowanie

Świat zmienia się w sposób, który Peter Drucker przewidział, wymagając od nas nowego spojrzenia na zarządzanie w wymiarze strategicznym (BSC) i operacyjnym (koncepcja VUCA). Adaptacja tych metod jest kluczowa dla zwiększenia odporności i konkurencyjności przedsiębiorstw w dzisiejszych turbulentnych czasach i oferuje cenne ramy analityczne i narzędzia do zarządzania w zmiennym, niepewnym, złożonym i niejednoznacznym środowisku.

Wnioski z przeprowadzonej analizy wskazują na konieczność dalszego rozwoju strategii zarządzania przedsiębiorstwami SOE w obliczu zagrożeń wojny hybrydowej w kontekście zmieniających się warunków geopolitycznych. Kluczowe jest podejmowanie działań mających na celu zwiększenie odporności infrastruktury krytycznej na ewentualne zagrożenia oraz dywersyfikacja źródeł dostaw surowców i zapewnienie ciągłości procesów wydobycia produkcji węglowodorów w przypadku przedsiębiorstw GK Orlen. Ponadto konieczne jest wzmacnianie współpracy międzynarodowej oraz podejmowanie inicjatyw mających na celu promowanie produkcji surowców na terenie Europy, co mogłoby zmniejszyć zależność od importu i zwiększyć bezpieczeństwo energetyczne regionu.

Pytanie, czy możliwe wypracowanie takiego modelu biznesu, który pozwoli na funkcjonowanie z dodatnim wynikiem ekonomiczno-finansowym przy spełnieniu tych warunków brzegowych, jest istotne. W czasach kryzysu i zagrożeń wojennych, ruchy militarne i napięcia polityczno-wojenne mogą wpłynąć na stabilność działania przedsiębiorstw. Czy zatem te założenia, budowane w stabilnym otoczeniu rynkowym, mogą być skuteczne w tak turbulentnych czasach? Odpowiedź nie jest jednoznaczna. Zarządzanie przedsiębiorstwem w czasach konfliktu i zagrożeń wojennych wymaga elastyczności, szybkiego reagowania na zmiany i zdolności adaptacji do nowych warunków. Może to być trudne, jeśli założenia modelu biznesowego są oparte na stabilności i przewidywalności rynku. Jednak, przy odpowiednim przygotowaniu, przedsiębiorstwa mogą próbować dostosować się do zmieniających się warunków poprzez elastyczne strategie biznesowe, inwestycje w bezpieczeństwo infrastruktury oraz uwzględnienie kwestii ESG w swoich działaniach. Kluczowe jest również zaangażowanie wysoko wykwalifikowanych menedżerów, którzy potrafią szybko analizować sytuację i podejmować trafne decyzje w czasach niepewności i kryzysu. W kontekście dzisiejszych geopolitycznych napięć i potencjalnych zagrożeń wojennych, zarządzanie przedsiębiorstwem staje się bardziej złożone niż kiedykolwiek wcześniej.

W obliczu potencjalnych zagrożeń wojennych, ochrona infrastruktury kluczowej dla funkcjonowania państwa staje się priorytetem. Przedsiębiorstwa działające w sektorach strategicznych, takich jak energetyka czy telekomunikacja, muszą być przygotowane na różne scenariusze konfliktu i działań wrogich, w tym cyberataków czy sabotażu.

Bibliografia

Drucker P.F. [1993], *Post-Capitalist Society*, Harper Business.

Irrek W. [2023], *Controlling der Energiedienstleistungsunternehmen*, Josef Eul Verlag GmbH, Lohmar, Germany.

Kaczmarek J. [2012], *The Identification and Measurement of Financial Threat Vs. The Cases of Insolvency in the Period of Poland's Economic Transformation*, „The Business & Management Review", vol. 2(2).

Kaplan R.S., Norton D.P. [2000], *The balanced scorecard: Translating strategy into action*, Harvard Business Press.

Lipczyński T. [2024], *Grupa Orlen zwiększyła ilość gazu przesyłanego do Polski z Norwegii o ponad 30 proc.*, Forsal.pl, 9 kwietnia, https://forsal.pl/biznes/energetyka/artykuly/9482392, grupa-orlen-zwiekszyla-ilosc-gazu-przesylanego-do-polski-z-norwegii-o.html (data dostęp: 9.04.2024).

Neacsa A., Panait M., Muresan J.D. [2020], *M.C. Energy poverty in European Union: Assessment difficulties, effects on the quality of life, mitigation measures. some evidences from Romania*, Voica.

Nesterak J., Kołodziej-Hajdo M., Kowalski J.M. [2023], *Controlling in the Process of Development of the Energy and Heating Sector Based on Research of Enterprises Operating in Poland*, „Energies", vol. 16(2).

Roth G. [2016], *Hybrid warfare and the role of the state*, „Journal of Strategic Studies", vol. 39(3).

Shanks K., Johnston R. [2014], *Cybersecurity for state-owned enterprises: A practical guide*, Springer.