TEORIA „CZARNEGO ŁABĘDZIA" A PRZEWIDYWANIE KRYZYSÓW I KATASTROF

DOI: 10.33141/po.2021.4.03

Przegląd Organizacji, Nr 4(975), 2021, s. 23-31

www.przegladorganizacji.pl

Jerzy Kisielnicki

Wprowadzenie

Termin „Czarny Łabędź" jest alegorią dla określenia niespodziewanych niebezpieczeństw. Celem artykułu jest zarówno prezentacja podstaw teorii „Czarnego Łabędzia", jak i analiza rozwiązań oraz skutków wybranych problemów dotyczących pojawiania się kryzysów i katastrof w kontekście projektu budowy takiego systemu informatycznego, który będzie ukierunkowany na ich monitorowanie. Zajęto się takimi kryzysami i katastrofami, które pojawiają się niezwykle rzadko i niespodziewanie. Znajdują się one bowiem na samym końcu rozkładu prawdopodobieństwa ich zaistnienia[1]. Teoria „Czarnego Łabędzia" próbuje opisać problematykę tych zagrożeń współczesnej cywilizacji, które wywierają olbrzymi wpływ na badany obiekt i jego otoczenie. Pomaga to, jak pisze jej twórca N.N. Taleb (2014; 2015; 2019), lepiej zrozumieć przełomowe momenty w historii świata.

W artykule postawiono tezę, że informacyjno-komunikacyjna technologia, czyli ICT (*Information Communication Technology*), jest zarówno sprawcą kryzysów i katastrof, jak i może być pomocna w budowie skutecznego i efektywnego narzędzia do monitorowania zagrożeń. Wynika to z faktu, że wraz z postępem cywilizacyjnym i rozwojem informatycznej infrastruktury zarządzania Polska jest od niej coraz bardziej uzależniona i w konsekwencji narażona na zagrożenia zawarte w teorii „Czarnego Łabędzia".

Badania, które są elementem uzasadnienia postawionej tezy, dotyczą zarówno identyfikowania skutków wystąpienia „Czarnego Łabędzia", jak i prezentacji przesłanek zasadności decyzji o konieczności budowy systemu przewidywania oraz monitorowania kryzysów i katastrof. Założono, że każdy sukces związany z postępem w technice i technologii w zakresie ICT wymaga analizy możliwości wystąpienia negatywnych skutków. Takie dyskusje o efektach i niebezpieczeństwach dotyczą między innymi problematyki związanej z zastosowaniem systemów informatycznych stosujących sztuczną inteligencję (Bostrom, 2016[2]; Ertel, 2017; Ishiguro, 2021[3]). Dlatego skoncentrowano się na poszukiwaniu tych zagadnień, co do których nasza obecna wiedza nie jest jeszcze sprecyzowana. Ważniejsze od tego, co wiemy, jest to, o czym nie wiemy.

Aby zrealizować tak sformułowaną tezę, zastosowano następującą procedurę badawczą:

Etap pierwszy – przedstawiono problematykę przewidywania kryzysów i katastrof jako temat istotny w zarządzaniu organizacją. W tym etapie badań przeprowadzono zarówno analizę literaturową, jak i charakterystykę własnych prac nad projektowaniem i eksploatacją systemów informatycznych wspomagających zarządzanie (Kisielnicki, 2017; Kisielnicki, Gałązka-Sobótka, 2012; Olszak, Kisielnicki, 2018; Kisielnicki, Sobolewska, 2019; Kisielnicki, Zadrożny, 2021).

Etap drugi – scharakteryzowano następujące zagadnienia: (1) działania i skutki cyberwojny i cyberterroryzmu jako przykłady wystąpienia „Czarnego Łabędzia", (2) procesy transformacji informacyjnej i jej reperkusje w związku z budową systemu zabezpieczenia przed „Czarnym Łabędziem".

Etap trzeci – to określenie najważniejszych konkluzji, które płyną z przeprowadzonej analizy oraz przedstawienie propozycji dalszych kierunków prac projektowo-badawczych w tym zakresie.

Podczas pisania niniejszego tekstu stosowano takie metody badawcze, jak: krytyczna analiza literatury przedmiotu, metoda dedukcji oraz doświadczenia i wyniki badań płynące z realizacji wspominanych wcześniej projektów dotyczących informatycznego wspomagania zarządzania.

O teorii „Czarnego Łabędzia" jako narzędziu opisu pojawiania się kryzysów i katastrof

Teoria „Czarnego Łabędzia" została zaprezentowana w literaturze przez Nassima Nicholasa Taleba (2014), profesora Nowojorskiego Uniwersytetu. Została ona rozwinięta w następnych jego pracach (Taleb, 2015; 2019). Według N.N. Taleba, „Czarny Łabędź" jest to zdarzenie, którego praktycznie nie można było przewidzieć. Wystąpienie takiego zdarzenia charakteryzuje się bardzo małym prawdopodobieństwem, bardzo bliskim zeru. Natomiast gdy już wystąpi, to jego zaistnienie ma bardzo duże negatywne konsekwencje ekonomiczne, jak też społeczne. W większości modeli prognostycznych powstających w zespołach ekonometryków lub przedstawicieli nauk systemowych taka sytuacja nie jest uwzględniana.

Można przyjąć, że teoria zaistnienia „Czarnego Łabędzia" dotyczy analizy istoty zmienności i kalkulowania ryzyka w takich sytuacjach, kiedy stosując tradycyjne algorytmiczne modele, nie można przewidywać przyszłości. N.N. Taleb twierdzi, że na „Czarne Łabędzie" można

się przygotować. Jest to twierdzenie słuszne, ale wymaga odpowiedniej infrastruktury i kwalifikacji do posługiwania się takimi narzędziami, które pozwalają twórcom i użytkownikom na monitorowanie tych specyficznych zagrożeń. N.N. Taleb (2014) podkreśla, że „Czarnym Łabędziem" są nie tylko katastrofy w rodzaju ataku terrorystów na USA 11 września 2001 r. (którego bezpośrednim następstwem były m.in. wojny w Iraku i Afganistanie) czy krachu giełdowego, który nastąpił w 2008 r. po upadku banku Lehman Brothers. Jest nim także Internet i jego rozwój. Jest to zgodne z poglądem, że nieopanowany sukces jest również zwiastunem przyszłych katastrof.

Społeczeństwo poddawane jest różnym działaniom i nie zawsze potrafi reagować na niebezpieczeństwa „Czarnego Łabędzia". Powszechną praktyką jest to, że decydenci nie lubią przyznawać się do błędów i takie niespodziewane działania zrzucają na niezależne od ich decyzji czynniki losowe. Koncentrują się oni na analizie przeszłości po to, aby uzasadnić stanowisko, że przesłanek do katastrofy nie było. Czasem też przeprowadzają analizę, która ma za zadanie znalezienie przyczyn popełniania błędów. W konsekwencji tworzone są modele postępowania na przyszłość. W tego typu modelach uwzględniane są minione wydarzenia. A ponieważ sytuacja, która doprowadziła do katastrofy, najczęściej się nie powtórzy, to takie modele mają wartość teoretyczną a nie praktyczną.

Budując modele zabezpieczające przed działaniem „Czarnego Łabędzia", powinno się brać pod uwagę to, że:

- wiele sytuacji nie można przewidzieć i w konsekwencji nie można się w naszych działaniach opierać na doświadczeniach przeszłości,
- świat, w którym żyjemy, nie zawsze jest nam znany i nie zawsze zachodzące w nim sytuacje są dla nas zrozumiałe i skwantyfikowane,
- w wielu państwach buduje się tego typu modele i dlatego istotna jest współpraca międzynarodowa w tym zakresie.

Budując prognozy, trzeba analizować różne, nawet nieprawdopodobne scenariusze. Tradycyjnie na zabezpieczenie przed ewentualnymi przyszłymi kryzysami i katastrofami wydatkuje się niekiedy nawet znaczne środki finansowe. Jednak nie ma pewności, czy ponoszone nakłady były zasadne. Dlatego też proponuje się takie rozwiązanie, jakim jest budowa dedykowanego systemu informatycznego, który będzie pomocny przy ocenie niebezpieczeństwa pojawienia się „Czarnego Łabędzia". Obecnie prowadzone są prace nad architekturą systemu informatycznego i opisu zbiorów użytych do identyfikacji charakterystycznych zbiorów danych. Elementami dedykowanego systemu do monitorowania przyszłych kryzysów i katastrof są między innymi: hurtownie danych, bazy wiedzy, modele symulacyjne zawierające rekomendowane procedury do prognozowania niespodziewanych sytuacji kryzysowych, sztuczna inteligencja. Tego typu systemy pozwalają na weryfikacje dziesiątków różnych, wydających się teoretycznie niemożliwych, sytuacji. Scenariusze, które uzyska się, stosując modele symulacyjne, mają na celu podjęcie czynności profilaktycznych. Cel przeprowadzonych symulacji i analiza każdej możliwej decyzji to droga do zapobieżenia wystąpienia „Czarnego Łabędzia". Systemy o rekomendowanej charakterystyce pozwalają na przygotowanie się i zminimalizowanie strat w sytuacji, kiedy jednak zaistnieje katastrofa lub kryzysowa sytuacja.

Wstępna charakterystyka danych niezbędnych do analizy zachodzących relacji, które istnieją w systemie, wykazuje, że obok deterministycznych i stochastycznych danych powinno używać się do zarządzania danymi teorii zbiorów rozmytych (Zimmermann, 2011). Złożoność problematyki i charakterystyka występujących zależności pozwala na sprawdzenie zastosowania w budowie modeli zbiorów rozmytych, np. typu 2 (Rutkowski, 2005; Mittal i in., 2020). Zbiory te znalazły szerokie zastosowanie m.in. w dziedzinie inteligentnego sterowania, rozpoznawania wzorców i klasyfikacji. W sytuacji kiedy nasza informacja o prawdopodobieństwie zaistnienia sytuacji jest niepewna, jak również miara jej zaistnienia jest też niepewna, zastosowanie zbiorów rozmytych typu 2 pozwala na uzyskanie informacji użytecznej do dalszej analizy. Do zastosowania w analizie informacji zbiorów rozmytych typu 2 interesujące są w tym zakresie prace A. Niewiadomskiego (2019).

Charakterystyczną cechą pojawiania się w świecie realnym kryzysów i katastrof jest to, że dane o przeszłości nie wskazują symptomów ich zaistnienia. Jednak kiedy one już zaistnieją, wywiera to drastyczny wpływ na rzeczywistość. Na nieprzewidywane wystąpienie „Czarnego Łabędzia" poszukuje się pseudoobiektywnego wytłumaczenia jego zaistnienia. Analiza przyczyn tego, iż nie przygotowaliśmy się na pojawienie się kryzysów i katastrof jest następująca:

a) złudzenie zrozumiałości, wydaje się, że wiemy, co się dzieje na świecie, ale jest on bardziej złożony i nie jesteśmy w stanie uświadomić sobie kwestii zaistnienia czekających nas niespodziewanych negatywnych zdarzeń;
b) zniekształcenie retrospektywne, ponieważ potrafimy ocenić negatywne zdarzenia dopiero po fakcie;
c) przecenianie rekomendacji i prognoz autorytetów i ekspertów związanych najczęściej z określoną orientacją polityczną lub interesami organizacji, które narzucają swój nie zawsze obiektywny punkt widzenia.

Jak pisze N.N. Taleb (2014), „Czarne Łabędzie" biorą się z faktu, iż nie rozumiemy prawdopodobieństwa zajścia niespodziewanych zdarzeń. Niemal wszystko na świecie da się wyjaśnić przez odwołanie do niewielkiej liczby takich „Czarnych Łabędzi", które związane są z: określonymi ideami i religią, wydarzeniami historycznymi, a nawet rozmaitymi elementami naszego życia osobistego. Z upływem czasu, na skutek rozwoju techniki i technologii, wpływ „Czarnych Łabędzi" na rzeczywistość nieustannie rośnie.

Obecnie prowadzone są przez nas prace dotyczące budowy kokpitu menedżerskiego jako jednego z podstawowych elementów całego systemu. Zadaniem kokpitu jest wspomaganie systemu monitorującego prawdopodobieństwa możliwości wystąpienia kryzysów i katastrof. Szczególna uwaga w realizacji projektu związana jest z koniecznością identyfikacji i analizy słabych sygnałów zaistnienia „Czarnego Łabędzia". Oddzielne prace dotyczą

badań nad bazami danych i wiedzy, które będą zasilały kokpit menedżerski. W ramach badań z tego zakresu szczególną uwagę poświęca się roli sytemu filtrowania informacji w kanałach komunikacyjnych. Funkcjonowanie filtrów w kanałach komunikacyjnych zasilających systemy monitorowania często osłabiają jego skuteczność i efektywność, co wiążą się również z tym, że:

a) skupiamy się na z góry wybranych segmentach rzeczywistości widzialnej, a uzyskane w ten sposób wnioski rozciągamy na to, co niewidoczne;
b) przyjmujemy te teorie, które zaspokajają nasze wizje i wzorce;
c) zachowujemy się tak, jak gdyby „Czarne Łabędzie" nie istniały albo jeżeli istniały, to nas one nie dotyczą:
d) analiza przeszłości ukrywa przed nami „Czarne Łabędzie" i wprowadza nas w błąd co do prawdopodobieństwa zaistnienia takich niespodziewanych negatywnych zdarzeń;
e) upraszczamy złożoność rzeczywistości i skupiamy się na kilku jasno zdefiniowanych sytuacjach, mimo iż realna sytuacja jest coraz to bardziej złożona.

Uważamy, iż prezentowana w artykule teoria N.N. Taleba jest użyteczna do wyjaśnienia mechanizmów pojawiania się niespodziewanych kryzysów i katastrof, czyli „Czarnego Łabędzia". W konsekwencji może zostać wykorzystana w budowie systemu wczesnego ostrzegania, jak też prognozowania i monitorowania omawianych zjawisk.

Cyberwojna i cyberterroryzm jako przykłady wystąpienia „Czarnego Łabędzia"

Jeżeli społeczeństwo jest świadome możliwości, jakie daje zastosowanie ICT, i umie je zastosować dla wzbogacenia się i wspomagania procesów podejmowania decyzji, to na pewno będzie szczęśliwsze (w potocznym słowa tego rozumieniu). Jednak współczesna cywilizacja, która często bywa nazywana cywilizacją informacyjną, to nie tylko pozytywy, to także nowe zagrożenia. Amerykański admirał J. Ryan stwierdził nawet, że: „Ataki informacyjne są największą innowacją w dziedzinie prowadzenia wojen od czasu wymyślenia prochu" (Bartoszek, 2012). „Czarny Łabędź" niespodziewanie i przy niewielkich nakładach finansowych zdolny jest w znacznym stopniu sparaliżować kluczową infrastrukturę lub gospodarkę państwa przeciwnika. Niespodziewany atak najczęściej nie ma jakichkolwiek wcześniejszych symptomów zaistnienia. Jest to klasyczne pojawienie się „Czarnego Łabędzia". Jego działania są w dużym stopniu asymetryczne, co pozwala na prowadzenie wrogich działań przez państwa „słabsze" przeciwko „silniejszym".

Pojawienie się: cyberwojny, cyberterroryzmu, cyberszpiegostwa zwiększa ryzyko nawet nieumyślnej wojny nuklearnej w konwencjonalnym konflikcie (Acton, 2020). W teorii cyberszpiegostwo i cyberataki mogą pozwolić na zwiększenie zdolności jednego państwa do osłabiania i odstraszania innego państwa (Colarik, Janczewski, 2011; Clarke, Knake, 2012, Straub, 2019). Bez względu na to, jak skuteczne mogą okazać się takie operacje w praktyce, strach przed nimi może generować eskalację presji „użyj-to-zanim-to-stracisz". Ponadto zagrożenia cybernetyczne mogą stworzyć następujące jakościowo nowe mechanizmy, za pomocą których państwo uzbrojone w broń jądrową może błędnie stwierdzić, że jego odstraszająca broń nuklearna jest atakowana:

Po pierwsze, cyberszpiegostwo można pomylić z cyberatakiem.

Po drugie, złośliwe oprogramowanie mogło przypadkowo rozprzestrzenić się z systemów obsługujących operacje niejądrowe do systemów związanych z energią jądrową.

Po trzecie, operacja przeprowadzona przez osobę trzecią może zostać niewłaściwie przypisana przez jedno państwo w dwustronnej konfrontacji ze swoim przeciwnikiem.

Jak pisze Y.N. Harari (2018), wojna cybernetyczna (według autora artykułu, jest to postać „Czarnego Łabędzia"), może zdestabilizować świat. Daje ona bowiem nawet małym państwom oraz tworom innym niż państwa możliwość skutecznej walki z supermocarstwami. Takie państwa jak Korea Północna czy Iran mogą użyć bomb logicznych[4] do: odcięcia prądu w Kalifornii, wysadzenia rafinerii w Teksasie, zderzenia pociągów w Michigan. Jak dalej pisze Y.N. Harari, te trzy problemy stanowią egzystencjalne wyzwania dla naszego gatunku. Są to: wojna nuklearna, załamanie ekologiczne i zakłócenia technologiczne. Obecnie powinniśmy się na nich skupić. Wojna nuklearna i zapaść ekologiczna są już znanymi zagrożeniami, natomiast mniej znane zagrożenia stanowią zakłócenia spowodowane przez technologię. Jednym z nich jest cyberwojna.

Pod pojęciem cyberwojny ujmuje się konflikt w skali międzypaństwowej lub globalnej, który będzie prowadzony przede wszystkim z udziałem ICT. Rozumie się pod tym, że zarówno cyberwojna, jak i cyberterroryzm są elementami „Czarnego Łabędzia", polegającymi na użyciu systemów informatycznych w celu przeprowadzania ataków na systemy informacyjne oraz informatyczne przeciwnika.

Działanie „Czarnego Łabędzia" w cyberprzestrzeni jest inne niż w przestrzeni tradycyjnej. Jest to konsekwencją faktu, że wojnę cybernetyczną od tzw. klasycznych wojen odróżnia środowisko pola walki. Tu nie ma ściśle określonego terenu w znaczeniu fizycznym, ale wirtualna przestrzeń, np. chmury komputerowe, sieci teleinformatyczne. W takiej wojnie strona atakująca zdolna byłaby sparaliżować kluczową infrastrukturę zarządzania, a w konsekwencji gospodarkę państwa przeciwnika. Możena tylko przypuszczać, iż najbardziej prawdopodobny scenariusz to wojna hybrydowa. W wojnie tej obok działań klasycznych udział będą miały też działania określane terminem cyberwojny i cyberkonfliktu. Relacje między tymi elementami będą różne, ale na pewno działania te będą się wspomagały. „Czysta" cyberwojna oznacza to, że tylko technologia informatyczna byłaby stosowana przez obie strony konfliktu.

Przestrzeń kosmiczna oraz Internet (rozumiane jako cyfrowa przestrzeń) to kolejne fronty działań militarnych w czymś, co można określić mianem zbliżającej się

III wojny światowej. Według raportu zamieszczonego w Super Biznesie (marzec 2021 roku), wiele zbrojnych konfliktów mogłoby się przerodzić w III wojnę światową, co dla mieszkańców Europy czy USA w dobie pandemii koronawirusa to tylko science fiction. Jednak dla władz i dla wojska wojna jest zawsze realnym zagrożeniem, dlatego armie świata zbroją się jak mogą. Wydatki na wojskowość są takie, jakby III wojna światowa czaiła się tuż za rogiem. Na wojsko wydano miliardy dolarów więcej niż w poprzednim dziesięcioleciu.

E. Snowden (Fondren, 2017) ujawnił jako jeden z pierwszych fakty o sposobie, w jaki Amerykanie przygotowują się do ewentualnej cyberwojny. I tak „Czarny Łabędź" pod postacią określonej organizacji nie będzie brał cyfrowych jeńców, ale będzie niszczył: komputery, routery i inny elektroniczny sprzęt przeciwnika. W razie konieczności zaatakowane zostaną: elektrownie, oczyszczalnie wody, lotniska. Wiemy również z materiałów, które zostały ujawnione przez E. Snowdena, że cały czas „Czarny Łabędź" wyposażony w narzędzia informatyczne zbiera informacje o praktycznie każdym obywatelu kuli ziemskiej, nie wyłączając inwigilacji szefów rządów zaprzyjaźnionych państw. Mamy do czynienia ze śledzeniem każdego kroku (znają hasła, loginy) inwigilowanej osoby. Te rozwiązania nie są niczym nowym, ale według informacji E. Snowdena, amerykańska Agencja Bezpieczeństwa Narodowego NSA i podobnego typu organizacje, specjalizują się w takich działaniach. Zgodnie z upublicznionymi przez niego materiałami, NSA jest przekonana, że „III wojna światowa rozpocznie się w Internecie". W przygotowaniach do nowego rodzaju wojny pojawiają się różnego typu nowe rozwiązania, np. zdobywanie nowych informacji z użyciem samolotów bezzałogowych (dronów). Drony są przecież sterowane z użyciem ICT.

„Czarny Łabędź" może używać narzędzia w postaci zastosowania informatycznego systemu takiego jak przykładowo Systemu Pegasus (Deelman i in., 2019). System ten został opracowany przez firmę NSO Group[5]. Potrafi on bez wiedzy użytkownika: odczytywać dane ze smartfonów, nagrywać rozmowy czy wręcz podglądać obraz z kamery. Specjaliści wykryli ślady działania systemu m.in. w Polsce. System Pegasus określa się jako narzędzie do wykrywania, zwalczania i przeciwdziałania terroryzmowi. Przedstawiciele NSO zapewniają, że ich program może przyczynić się też do rozbijania karteli narkotykowych czy odnajdywania porywanych dzieci.

Problematyka cyberwojny i cyberkonfliktów jest analizowana zarówno przez władze polityczne, jak i wojskowe (Sommerville, 2008; Straub, 2019).

„Czarny Łabędź" ma do wyboru wiele narzędzi do niespodziewanego ataku. Ma w arsenale tysiące różnego rodzaju oprogramowań, a w tym tzw. wirusy i robaki. Może też użyć mechanizmu Distributed Denial of Service (DDoS), który został zastosowany w ataku na Estonię[6]. Groźba ataku DDoS bywa czasami używana do szantażowania firm, np. serwisów aukcyjnych, firm brokerskich i podobnych, gdzie przerwa w działaniu systemu transakcyjnego przekłada się na bezpośrednie straty finansowe firmy i jej klientów. W takich przypadkach osoby stojące za atakiem żądają okupu za odstąpienie od ataku lub jego przerwanie. Szantaż taki jest przestępstwem. Należy zwrócić uwagę na fakt, ze szczególnie niebezpieczne są jednak ataki „Czarnego Łabędzia" w postaci nawet pojedynczej osoby z wewnątrz organizacji. Osoba taka może przeprowadzić atak „Czarnego Łabędzia", aby się zemścić na instytucji, dla której pracuje lub pracowała, na rozkaz swoich mocodawców. Dla „Czarnego Łabędzia" posiadanie takiej osoby w szeregach przeciwnika jest warte więcej niż brygada wojsk pancernych. Jej działalność zwiększa znacznie zdolność do strategicznego uderzenia cybernetycznego.

Liczba ataków „Czarnego Łabędzia" na systemy komputerowe obsługujące sieci infrastruktury w USA wzrosła od 2009 r. niemal 17-krotnie – poinformowała NSA, która po raz pierwszy opublikowała dane na ten temat (Forbes, 2012). Szczególnie wrażliwe na atak „Czarnego Łabędzia" są państwa o rozwiniętych systemach informacyjnych. Ich rozwój spowodował to, że cechują się one dużym stopniem zależności od systemów informatycznych szczególnie klasy MIS – Management Information Systems (Kisielnicki, 2016). „Im bardziej określone państwo jest uzależnione od swoich infrastruktur informacyjnych, w tym większym stopniu infrastruktury te stają się środkami ciężkości wartymi atakowania i obrony", jak stwierdza G.R. Ratrray (2006, s. 16). Departament Obrony USA już w 1999 roku uznał, że „naród będący obiektem ataku na sieci komputerowe, finansowanego przez inne państwo może legalnie odpłacić się tym samym, a w szczególnych przypadkach usprawiedliwiona może być obrona własna przy użyciu tradycyjnych środków wojskowych". G.R. Ratrray (2006) postuluje, aby w prawie międzynarodowym uregulować kwestię cyberwojny i uznać ją za akt agresji usprawiedliwiający użycie do obrony wszelkich dostępnych środków nawet nuklearnych.

Zmienia się świat, a wraz z nim zmienia się działanie największej plagi XXI wieku, jaką jest terroryzm. To nie brodaty anarchista z bombą, ale wykształcona siedząca przy komputerze osoba potrafi, nawet nie wiedząc o tym, stosować zasady teorii „Czarnego Łabędzia", wywołując panikę i przerażenie świata.

Szef amerykańskiej Agencji Bezpieczeństwa Narodowego jest zaniepokojony rosnącą liczbą zagranicznych cybernetycznych ataków wymierzonych w „krytyczną infrastrukturę" oraz brakiem dostatecznego przygotowania Stanów Zjednoczonych na takie działania. Stopień przygotowania kraju ocenił na „około 3" w skali od 1 do 10 (Janczewski, 2015). Uważa się, że również Polska wielokrotnie była obiektem cyberataków. W połowie września 2009 roku ABW udaremniła zorganizowany atak na kilka polskich serwerów rządowych, który pochodził prawdopodobnie ze Wschodu. Sprawa była na tyle poważna, że powołano Rządowy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego. Ustawa o krajowym systemie cyberbezpieczeństwa ustanowiła trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego: CSIRT NASK, CSIRT GOV oraz CSIRT MON. Każdy z CSIRT odpowiedzialny jest za koordynację incydentów zgłaszanych przez przyporządkowane zgodnie z ustawą podmioty. Międzynarodową organizacją zajmującą się cy-

berbezpieczeństwem, do której należy Polska, jest CERT (*Computer Emergency Response Team*). Zadaniem CERT jest całodobowe nadzorowanie ruchu internetowego i podejmowanie natychmiastowych akcji w razie pojawienia się zagrożeń. jest nadzór nad systemem wczesnego ostrzegania o incydentach sieciowych ARAKIS-GOV. Dodatkowo CERT prowadzi rutynową akcję monitorowania bezpieczeństwa rządowych witryn internetowych (materiały Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego, 2019).

W związku z planowanym podpisaniem przez Polskę porozumienia ACTA 21 stycznia 2012 r. około godziny 19:00 rozpoczął się szereg ataków „Czarnego Łabędzia" na strony polskich instytucji parlamentarnych i rządowych. Do ataku przyznała się grupa Anonymous[7]. To, czy pierwsze problemy (przestała działać strona Sejmu) były wynikiem DDoS, nie jest do końca jasne. W TVP Info i w prasie codziennej pojawiły się też opinie, że była to zwykła usterka techniczna, niezwiązana z działalnością hakerów. Po ich wystąpieniu w sieci zaczęły krążyć niepotwierdzone informacje, co mogło wywołać efekt ataku DDoS w sposób naturalny (duża liczba internautów sprawdzających, czy strona rzeczywiście nie działa). Rzecznik rządu podał, że przyczyną późniejszych problemów mogło być duże zainteresowanie treścią porozumienia, które zostało zamieszczone na serwerach ministerstwa w pliku pdf o wielkości ponad 20 MB, zawierającym zeskanowany oryginał dokumentu. Później jednak przestały działać witryny innych ministerstw i instytucji rządowych, czego najbardziej prawdopodobną przyczyną jest właśnie atak DDoS. Przemawia za tym również fakt, że wkrótce po tym, jak rzecznik rządu zaprzeczył doniesieniom na temat ataku hakerskiego, przestała działać jego strona www.

Rewolucja informacyjna i jej reperkusje dla budowy systemu zabezpieczenia przed „Czarnym Łabędziem"

W tworzonym obecnie nowym informacyjnym społeczeństwie na plan pierwszy wysuwa się właśnie informacja. Człowiek staje się wolnym, ponieważ posiada informacje i wiedzę, które to zasoby pozwalają mu na decydowanie o swoim losie. Rewolucja informacyjna, w którą wchodzi rozwinięty świat, stwarza niezwykłe szanse dla jednostki i społeczeństwa. Wynika to z faktu, iż zwiększając znacząco możliwości przekazu informacji, stwarza się całkowicie nowe warunki dla komunikowania się i współdziałania. Obdarzony ogromną wyobraźnią futurolog A. Toffler już w roku 1998 pisał o konieczności rozwiązania różnorodnych problemów, takich jak elektroniczna autostrada, powstanie monopoli informacyjnych, totalna wojna informacyjna. Świat w różny sposób ulega transformacji, staje się coraz bardziej złożony i ulega coraz bardziej wpływowi rewolucji informacyjnej (Harari, 2018).

Polska jako członek Unii Europejskiej powinna dążyć do zacieśnienia współpracy gospodarczej, kulturalnej, turystycznej z krajami starej Unii Europejskiej. Zapobieżenie atakowi „Czarnego Łabędzia" to posianie szerokiego spektrum informacji, które będzie wykorzystane w systemie wczesnego ostrzegania. Realizacja tego postulatu powoduje konieczność jak najszybszego przystąpienia do budowy wspólnej przestrzeni informacyjnej Europy z różnych obszarów działalności. Przestrzeń informacyjna obejmuje między innymi bazy: danych, wiedzy, modeli, obrazów, dźwięku, wraz z odpowiednim oprogramowaniem, jak też środki techniczne, które umożliwiają użytkownikom korzystanie z posiadanych zasobów w sposób bezpieczny i zgodny z przeznaczeniem. Dla osiągnięcia tych celów trzeba wydatkować odpowiednie kwoty na zabezpieczenie określonych modeli prognostycznych.

Jak wielkie powinny być te kwoty? Na pewno powinny one proporcjonalnie odpowiadać kwotom wydatkowym w tych krajach, których poziom życia pragniemy osiągnąć. Oczywiście nakłady na współczesną infrastrukturę zarządzania pokrywane są w większości przez prywatnych przedsiębiorców. Od państwa zależy, czy dla tego celu zostaną stworzone odpowiednie warunki makroekonomiczne. Wydaje się, iż polityka gospodarcza nie zawsze jest skoordynowana z działaniami zarówno Unii Europejskiej, jak i naszych bezpośrednich sąsiadów. Przeprowadzone badania pod kierunkiem W. Cellarego (2002) wykazały, że Polska jest w grupie krajów o najniższym poziomie informatycznej infrastruktury. Mimo upływu lat sytuacja ta się nie poprawiła.

Według Global Information Technology (The Global Competitiveness Index 2019 Rankings), Polska w roku 2019 była na 37 pozycji, zaraz za takimi państwami Unii, jak: Estonia, Republika Czeska i Słowenia. Z analizy zamieszczonych w opracowaniach danych statystycznych European Information Technology Observatory (bitcom Research, 2020) wynika, że mimo iż dynamika wydatków na ICT w Polsce jest wysoka, to jednak bezwzględna ich wysokość jest o wiele niższa niż w rozwiniętych krajach Unii Europejskiej. Polska należy w Europie do krajów najbardziej opóźnionych w zakresie wydatków na infrastrukturę zarządzania.

Były premier J. Hausner (2020b) stawia w swoim raporcie następującą diagnozę: „Pozbawione inteligencji informacyjnej państwo nie podoła poprawieniu kompetencji cyfrowych obywateli. Mamy bardzo wielu młodych, uzdolnionych Polaków, wykazujących się niezwykłymi predyspozycjami w gospodarce i w technologiach cyfrowych, a jednocześnie nasze państwo jest jednym z najsłabszych pod względem wykorzystywania tych technologii".

Efekty negatywne takiej sytuacji i nasze opóźnienia w zakresie infrastruktury zarządzania to między innymi trudności w obronie przed atakiem „Czarnego Łabędzia" . Problematyka ta jest przedmiotem obrad między innymi w Information Society Forum (ISF)[8]. Według prac Komisji Europejskiej korzystającej z opinii ISF, wydatki na ICT są niezbędne do realizacji Europejskiej Drogi do Społeczeństwa Informacyjnego. Europejska droga to stawianie na silny rynek, nieustanną innowacyjność oraz wolny przepływ informacji i wiedzy.

Dla Polski możliwości, jakie niesie ze sobą realizacja wniosków Komisji Europejskiej, to duża szansa dla obrony przed niespodziewanymi atakami „Czarnego Łabędzia".

Europejska droga to również szansa wzrostu konkurencyjności tak małych, jak i dużych organizacji na rynku globalnym. Atak „Czarnego Łabędzia" na pewno będzie hamować rozwój przedsiębiorczości i integrację krajów Unii Europejskiej. Dlatego też należy budować takie narzędzia, którą pozwolą na powstrzymanie działania w tym zakresie „Czarnego Łabędzia".

Jednak czy organizacje globalne nie będą łatwiej wystawione na atak „Czarnego Łabędzia"? Na całym świecie poszczególne organizacje dążą w stronę globalizacji rozumianej jako ekspansja na rynki zagraniczne. Problematyka ta jest tym bardziej aktualna, że, niezależnie od tego, czy poszczególne osoby chcą globalizacji czy też są jej przeciwne, jest to naturalna droga rozwoju niemal wszystkich działów i gałęzi gospodarki narodowej.

Ostatnio praktykę wykorzystania koncepcji „Czarnego Łabędzia" w intersujący sposób doprecyzowała polska filozofka K. Lewestam (2020). Zwróciła ona uwagę, iż nieprofesjonalne zastosowanie perspektywy wynikającej ze wspomnianej idei N.N. Taleba może prowadzić także do lenistwa umysłowego, polegającego na przyjęciu przez analityków wygodnej, ale zarazem niebezpiecznej tezy, iż wszystko jest nieprzewidywalne. Tymczasem, by móc dobrze przygotować się na działanie „Czarnego Łabędzia" (a więc na czynnik rzeczywiście nieprzewidywalny), trzeba w budowanych modelach precyzyjnie uwzględnić wszystkie zmienne, dające się przewidzieć. K. Lewestam (2020) nazywa ich oddziaływanie metaforycznie „efektem hipopotama", który jest często dziś lekceważony. Dopiero złożony model ujmujący probabilistycznie mieszankę poznanych trendów i obszarów nieprzewidywalności może stanowić efektywne narzędzie do budowy systemów informatycznych, które zwiększają szanse społeczeństw na efektywne stawienie czoła „Czarnym Łabędziom"[9].

Podsumowanie

Czarny Łabędź" niesie różnego rodzaju cyberniebezpieczeństwa (wojna, terroryzm). Problematyka jest bardzo silnie związana z ICT i budową społeczeństwa informacyjnego. Problematyka cybernieubezpieczeń łączy się z kluczowymi zagrożeniami bezpieczeństwa państwa i jego obywateli. Analizując piramidę potrzeb Maslowa, krytykowaną, a zarazem oddającą usługi intelektualne jako narzędzie dobrze tłumaczące strukturę potrzeb człowieka, widać, że dla ludzi zaraz po zaspokojeniu potrzeb fizjologicznych najważniejsze jest zaspokojenie potrzeb bezpieczeństwa.

Odpowiedź na podstawowe pytanie: Czy musimy się obawiać globalnego „Czarnego Łabędzia"? stanowi kwestę trudną i odpowiedzialną. Przypomnijmy, że w tym artykule zajmujemy się „Czarnym Łabędziem" w kontekście ICT. Nie zajmujemy się pandemią. Jest to ciekawy, ale oddzielny problem. W XXI w. na świecie miały miejsce dwie epidemie w wyniku przełamania bariery człowiek-koronawirus: MERS oraz SARS. Obecnie trwająca pandemia SARS-CoV-2, wywołująca chorobę COVID-19 jest trzecią i pierwszą o zasięgu globalnym z tak raptownym rozprzestrzenieniem. Nie mamy jednak danych, aby za jej rozpowszechnienie obarczyć ICT. Jednak w walce z nią ICT, a zwłaszcza złożone systemy modelowania matematycznego i zastosowanie narzędzi symulacyjnych, są bardzo użyteczne.

Pomimo wielu zaniepokojonych głosów pochodzących z różnych źródeł prawdopodobieństwo poważnego konfliktu światowego z wykorzystaniem ICT jest w chwili obecnej bardzo niskie. Czy tak jest? Analiza czynników, które należy brać pod uwagę w analizie prawdopodobieństwa zaistnienia „Czarnego Łabędzia" i wybuchu cyberwojny, pokazuje, że czynnikami, które:

- zwiększają prawdopodobieństwo takiej wojny są:

1. Uzależnienie państw od informacji. Informacje dotyczą wszystkich aspektów naszego życia. W tych państwach, które mają wysoki stopień rozwoju, mieszkańcy nie mogą żyć bez ICT. W konsekwencji atak na infrastrukturę informacyjną zarządzania może skutecznie sparaliżować kraj.
2. Cyberwojna jest konfliktem, w którym strona atakująca może nie ponieść strat materialnych (to nie jest wojna nuklearna). Cyberataki są zazwyczaj o wiele mniej kosztowne niż tradycyjne działania wojskowe. ICT rozwija się bardzo szybko i praktycznie wszystkie duże organizacje są z nim związane.
3. Zawsze znajdą się takie siły, które zechcą, nie patrząc na koszty, wygrać konflikt.

- zmniejszają prawdopodobieństwo takiej sytuacji, są:

1. Konflikty zbrojne w przeszłości były prowadzone na podstawie niewystarczającej informacji na temat planów wroga. Obecnie wszystkie główne mocarstwa mają dość szczegółowe informacje o swoich przeciwnikach. W konsekwencji zaskakujący atak jest bardzo trudny do przeprowadzenia.
2. W ciągu ostatnich dziesięcioleci handel międzynarodowy rośnie w zawrotnym tempie. Pomimo znacznych różnic ideologicznych mocarstwa uczestniczą w międzynarodowym handlu. Oznacza to, że konflikt z takim państwem, które jest dostawcą kluczowych elementów do gospodarki, nie znajduje się na liście priorytetów politycznych potęg światowych.

Na świecie jesteśmy świadkami wielu lokalnych „Czarnych Łabędzi". Konflikty takie, za które odpowiedzialnością obarczamy „Czarnego Łabędzia", są zazwyczaj w krajach mniej rozwiniętych. Jednak i one mogą być źródłem zagrożeń. Do uruchomienia „Czarnego Łabędzia" nie są wymagane duże środki. Cyberwojna nie wymaga tysięcy okrętów, samolotów i rakiet.

Należy zgodzić się z wnioskami zawartymi w raporcie J. Hausnera (2020a), że w Polsce brak jest państwowego ośrodka myśli strategicznej, którego działanie opierałoby się na uznaniu, że w coraz bardziej zróżnicowanym i coraz lepiej wykształconym społeczeństwie wiedza potrzebna do skutecznego rządzenia jest rozproszona pomiędzy wiele podmiotów. Panujący w Polsce chaos organizacyjny i informacyjny na pewno ułatwi działanie „Czarnego Łabędzia". Dlatego wniosek z przeprowadzonych badań to zarówno podjęcie prac projektowych

nad stworzeniem narzędzia informatycznego do monitorowania trudno przewidywalnych zagrożeń polskiej gospodarki i polskiego społeczeństwa państwa, jak i zaproponowanie związanych z nim rozwiązań organizacyjnych na przykład w proponowanym przez J. Hausnera państwowym ośrodku myśli strategicznej.

Budowa społeczeństwa informacyjnego jest faktem. Polska musi wejść do tego „pociągu", jeżeli ma ambicje bycia liczącym się krajem w Unii Europejskiej. Innych dróg nie ma dla stania się państwem nowoczesnym. Musimy zdawać sobie jednak sprawę z konieczności poniesienia znacznych nakładów na realizację polityki „Bezpieczna Polska". Polska w zakresie dysponowania nowoczesną infrastrukturą zarządzania nie należy do liderów, ale bez niej będziemy na pewno podatni na ataki „Czarnego Łabędzia". Wraz z naszym uzależnieniem się od ICT będą pojawiać się nowe zagrożenia, a jednym z najbardziej istotnych jest cyberterroryzm w różnych postaciach. Przeznaczając coraz to większe środki na tworzenie społeczeństwa informacyjnego, winniśmy również pamiętać o przeznaczeniu części dysponowanych środków na takie narzędzia, które wspomagają działania zabezpieczające Polskę przed destrukcyjnym działaniem „Czarnego Łabędzia".

Artykuł należy potraktować jako istotny element prac nad założeniami do realizacji projektu systemu informatycznego wspomagającego przewidywanie kryzysów i katastrof. W tym etapie prac przedstawiono podstawy teoretyczne i uzasadnienie konieczności budowy tego typu systemu. Złożoność tematyki i jej waga wymaga dalszych prac badawczo-projektowych nad opracowaniem pełnych założeń do realizacji projektu systemu komputerowego.

Na liście propozycji tematów badawczych znajdują się następujące zagadnienia, które można potraktować jako zadania potrzebne do realizacji projektu systemu informatycznego wspomagającego przewidywanie kryzysów i katastrof:

1. Określenie zakresu projektu systemu, w tym opracowanie modelu organizacyjnego i biznesowego. Można bowiem rozpocząć od projektu systemu dla: branży czy regionu a następnie przejść do terytorium państwa, a nawet do Europy. W zakresie modelu biznesowego można adaptować model Osterwaldera i Pigneura stosowanego między innymi w projekcie SINTO (System Informacji Naukowej, Technicznej i Organizacyjnej, patrz Kisielnicki, Hajkiewicz-Górecka, 2012).
2. Określenie zbiorów potrzebnych informacji i zaprojektowanie procedur ich przechowywania i aktualizacji oraz projekty kokpitów menedżerskich niezbędnych do zarządzaniem tego typu projektami. (Modele takie są między innymi zaproponowane przez J. Kisielnickiego (2016; 2017).
3. Określenie czynników krytycznych wpływających na prace projektowe. W tym zakresie metodyka wyznaczenia i analizy czynników jest zaprezentowana w monografiach J. Kisielnickiego (2017) oraz J. Kisielnickiego i O. Sobolewskiej (2018).
4. Ocena rozwiązań sprzętowo-programowych, czyli odpowiedź na pytanie, jakie rozwiązanie wybrać do budowy systemu, czy obecnie stosowaną technologię SMAC (*Social*, *Mobile*, *Analytics*, *Cloud*), czy też oczekiwać na korzyści z wyłaniającej się technologii DARQ (*Distributed ledger*, *Artificial Intelligence*, *extended Reality*, *Quantum*) – Kisielnicki, Zadrożny (2021).
5. Jakie powinno być powiązanie systemu informatycznego wspomagającego przewidywanie kryzysów i katastrof z innymi tego typu globalnymi systemami opracowanymi w innych państwach. Wymaga to adaptacji istniejących platform albo zaprojektowania specjalnej platformy interoperacyjnej, która będzie wykorzystała takie narzędzia w proponowanym systemie informatycznym, jak: sztuczna inteligencja, analiza historyczna, analiza strumieni danych, wykrywanie anomalii, modele zbiorów rozmytych, modele predykcyjne itp. Wydaje się, że obiecujące jest w tym zakresie zastosowanie platformy Watson IBM (2021). Jest to otwarta, wielochmurowa platforma, która wykorzystuje najnowsze innowacje w dziedzinie uczenia maszynowego i pozwala na zautomatyzowanie cyklu eksploatacji sztucznej inteligencji. W tym względzie potrzebne będą rozwiązania związane ze standaryzacją poszczególnych zadań projektowych, w tym dobór metodyki projektowania. Obecne doświadczenie rekomenduje zastosowanie podejścia zwinnego – agilowego (Jørgensen 2018).

Zaprojektowanie systemu informatycznego wspomagającego przewidywanie kryzysów i katastrof jest zadaniem realnym. Wymaga jednak kontynuacji rozwoju przedstawionych prac badawczych nad opracowaniem systemu prognozująco-monitorującego najwcześniejszych stadiów pojawienia się niebezpieczeństw, które określa się jako działania „Czarnego Łabędzia".

prof. dr hab. inż. Jerzy Kisielnicki
Uniwersytet Warszawski
Wydział Zarządzania
ORCID: 0000 0002 2451 7202
e-mail: jkisielnicki@wz.uw.edu.pl

Przypisy

[1] Artykuł powstał na bazie referatu plenarnego wygłoszonego na V Konferencji Informatyka w Zarządzaniu IwZ'2020 organizowanej przez Uniwersytet Ekonomiczny w Katowicach w grudniu 2020 roku.

[2] N. Bostrom (2016, s. 174) sugeruje, że nawet uzyskanie maksymalnej kontroli nad superinteligencją nie gwarantuje, że nie uzna ona ludzi za „przeszkodę", którą należy usunąć.

[3] Książka laureata literackiej Nagrody Nobla to opowieść o sztucznej inteligencji i ludzkich uczuciach jego wytworu.

[4] Bomby logiczne" to złośliwe oprogramowanie zainstalowane w okresie pokoju i uruchamiane zdalnie.

[5] NSO Group to izraelska firma zajmująca się produkcją szpiegowskiego oprogramowania.

6) DDoS (ang. Distributed Denial of Service – rozproszona odmowa usługi) – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów.

7) Anonymous – globalna, zdecentralizowana grupa aktywistów, która stosuje ICT jako narzędzie do sprzeciwiania się ograniczaniu wolności obywatelskich, korupcji, konsumpcjonizmowi, cenzurze.

8) Forum to powołane w 1995 roku jako niezależne ciało doradcze Komisji Europejskiej, którego zadaniem jest wyciąganie wniosków i formułowanie zaleceń dla wszystkich instytucji Unii Europejskiej.

9) K. Lewestam (2020) odwołuje się w swoim tekście do problematyki pandemii, która na łamach niniejszego artykułu została pominieta. Stwierdzić jednak należy, iż uwagi cytowanej autorki są godne rozważenia także na szerszym, bardziej ogólnym poziomie niż tylko kwestia pandemii.

Bibliografia

[1] Acton J. (2020), *Cyber Warfare & Inadvertent Escalation*, „Dædalus, the Journal of the American Academy of Arts & Sciences", Vol. 149, No. 2, pp. 133–149.

[2] Bartoszek B. (2012), http://www.mojeopinie.pl/cyber-wojna_wojna_xxi_wieku, 3,1215862210, data dostępu: 16.11.2020 r.

[3] bitcom Research (2020), *11 Tech Trends for 2021 and Beyond*, https://www.bitkom-research.de/de/market_report/11-tech-trends-2021-and-beyond, access date: 15.12.2020.

[4] Bostrom N. (2016), *Superinteligencja: scenariusze, strategie, zagrożenia*, Wydawnictwo Helion, Gliwice.

[5] Cellary W. (2002) *Polska w drodze do globalnego społeczeństwa informacyjnego*, Raport UNDP, Warszawa.

[6] Clarke R.A., Knake R. (2012), *Cyber War: The Next Threat to National Security and What to Do about It,* HarperCollins Publishers, New York.

[7] Colarik A., Janczewski L. (2011), *Developing a Grand Strategy for Cyber War*, Proceedings of the 7th International Conference on Information Assurance and Security, IAS2011, Melaka, Malaysia.

[8] Deelman E., Vahi K., Rynge M., Mayani R., Ferreira da Silva R., Papadimitriou G., Livny M. (2019), *The Evolution of the Pegasus Workflow Management Software,* „Computing in Science & Engineering", Vol. 21, No. 4, pp. 22–36.

[9] Ertel W. (2017), *Introduction to Artificial Intelligence*, Springer International Publishing, Cham.

[10] Fondren E. (2017), *Snowden*, „American Journalism", Vol. 34, No. 3, pp. 381–383.

[11] Forbes (2012), *Coraz więcej cyberataków na infrastrukturę w USA*, www.forbes.pl/artykuly/sekcje/Wydarzenia/coraz-wiecej-cyberatakow-na-infrastrukture-w-usa, 29113,1, data dostępu: 10.05.2017 r.

[12] Ishiguro K. (2021), *Klara i słońce*, Wyd. Albatros, Warszawa.

[13] Janczewski L. (2015), *3rd World War: Cyber War?* [w:] W. Chmielarz, J. Kisielnicki, T. Parys (red.), *Informatyka 2 przyszłości. 30 lat informatyki na Wydziale Zarządzania UW*, Wyd. WZ UW, Warszawa.

[14] Jørgensen M. (2018), *Do Agile Methods Work for Large Software Projects?* Proceedings of the 19th International Conference on Agile Software Development, Porto, Portugal.

[15] Hausner J. (2020a), *Państwo i My. Osiem grzechów głównych Rzeczpospolitej – 5 lat później,* Raport na Open Eyes Economy Summit, https://www.gazetaprawna.pl/wiadomosci/artykuly/1496411,panstwo-i-my-osiem-grzechow-glownych-rzeczypospolitej-5-lat-pozniej-raport.html, data dostępu: 20.03.2021 r.

[16] Hausner J. (2020b), *Prof. Jerzy Hausner o ośmiu głównych grzechach RP: „Patologia coraz głębsza, ale jest alternatywa"*, https://krakow.wyborcza.pl/krakow/7,44425,26515857,prof-jerzy-hausner-wymienia-osiem-glownych-grzechow-rp-patologia.html, data dostępu: 16.11.2020 r.

[17] Harari Y.N. (2018), *Sapiens. Od zwierząt do bogów*, Wydawnictwo Literackie, Kraków.

[18] Kisielnicki J., Gałązka-Sobotka M. (2012), *Rozwiązania organizacyjne zapewniające trwałość systemu informacji naukowo-technicznej*, Elipsa, Warszawa.

[19] Kisielnicki J., Hajkiewicz-Górecka M. (2012), *Model biznesowy i model finansowy dla platformy SYNAT*, Elipsa, Warszawa.

[20] Kisielnicki J. (2016), *Zarządzanie i informatyka*, Placet, Warszawa.

[21] Kisielnicki J. (2017), *Zarządzanie projektami badawczo-rozwojowymi*, Wyd. 2, Nieoczywiste, Warszawa.

[22] Kisielnicki J., Sobolewska O. (2018), *Knowledge Management and Innovation in Network Organizations: Emerging Research and Opportunities*, IGI Global, Hershey.

[23] Kisielnicki J., Zadrożny J. (2021), *DARQ Technologies as a Digital Transformation Strategy in Terms/Conditions of Global Crises*, „Problemy Zarządzania", Nr 4 (w druku).

[24] Lewestam K. (2020), *To nie efekt motyla, ale efekt hipopotama. Wiele rzeczy można było przewidzieć*, Forsal.pl/gospodarka/polityka/artykuly/8050602,to-nie-efekt-motyla-efekt-hipopotama-pandemie-mozna-bylo-przewidziec-opinia.html, data dostępu: 20.12.2020 r.

[25] Mittal K., Kunwar A., Vaisla S., Castillo O., Kacprzyk J. (2020), *A Comprehensive Review on Type 2 Fuzzy Logic Applications: Past, Present and Future*, „Engineering Applications of Artificial Intelligence", Vol. 95, art. 103916.

[26] Niewiadomski A. (2019), *Zbiory rozmyte typu 2. Zastosowania w reprezentowaniu informacji*, Wyd. EXIT, Warszawa.

[27] Olszak C., Kisielnicki J. (2018), *A Conceptual Framework of Information Systems for Organizational Creativity Support. Lessons from Empirical Investigations*, „Information Systems Management", Vol. 35, No. 1, pp. 29–48.

[28] *Raport o niebezpieczeństwach*, Super Biznes (2021), https://superbiz.se.pl/wiadomosci/iii-wojna-swiatowa-trwaja-zbrojenia-chiny-przemowily-co-z-polska-a-a-QAtg-mc5R-2RmT.html, data dostępu: 18.03.2021 r.

[29] Rutkowski L. (2005), *Metody i techniki sztucznej inteligencji – Inteligencja obliczeniowa*, Wydawnictwo Naukowe PWN, Warszawa.

[30] Ratrray G.R. (2006), *Wojna strategiczna w cyberprzestrzeni*, WNT, Warszawa.
[31] Schwab K. (2019), *The Global Competitiveness Index 2019 Rankings*, http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf, access date: 16.11.2020.
[32] Sommerville D. (2008), *The Complete Illustrated History of World War Two: An Authoritative Account of the Deadliest Conflict in Human History with Analysis of Decisive Encounters and Landmark Engagements*, Lorenz Books, Leicester.
[33] Straub J. (2019), *Mutual Assured Destruction in Information, Influence and Cyber Warfare: Comparing, Contrasting and Combining Relevant Scenarios*, „Technology in Society", Vol. 59, art. 101177.
[34] Taleb N.N. (2014), *Czarny Łabędź. O skutkach nieprzewidzianych zdarzeń*, Media, Warszawa.
[35] Taleb N.N. (2015), *Antykruchość*, Publishing Kurhaus, Warszawa.
[36] Taleb N.N. (2019), *Na własne ryzyko. Ukryte asymetrie w codziennym życiu*, Wyd. Zysk i S-ka, Poznań.
[37] Toffler A. (1998), *Szok przyszłości*, Wyd. Zysk i S-ka, Poznań.
[38] Watson IBM (2021), https://www.ibm.com/pl-pl/watson, access date: 20.03.2021.
[39] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) (2019), https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt, data dostępu: 16.11.2020 r.
[40] Zimmermann H.J. (2011), *Fuzzy Set Theory and its Application*, Springer Science & Business Media, New York.

The „Black Swan" Theory and Predicting Crises and Catastrophes

Summary

The main objective of this paper is to present the black swan theory to analyse contemporary threats related to the cybersecurity domain. The aim of conducted works is to develop design assumptions justifying the need to obtain effective tools for monitoring crises and disasters. Their characteristic is that they appear unexpectedly and very rarely, therefore they are situated at the very end of the tail of the probability distribution. The main thesis of the work stands that ICT is not only the perpetrator of crises and disasters but can also help to build an effective and efficient tool for analysing threats. The progress of civilization and development of ICT in Poland brings the country more and more exposed to the threats described in the black swan theory. The conclusion of the research is the statement that shows and explains the need for building an early warning system to prevent the Black Swan phenomenon.

Keywords

ICT, Black Swans, system monitoring, crises and disasters, cyberwar, cyberspace