Instytut Kościuszki

CYBERSEC
Europejskie Forum Cyberbezpieczeństwa

PARTNER RAPORTU

Microsoft

PATRONAT

RCB
Rządowe Centrum Bezpieczeństwa

# SYSTEMOWA ODPORNOŚĆ PAŃSTWA W CYFROWEJ ERZE

IZABELA ALBRYCHT, ŁUKASZ GAWRON, MACIEJ GÓRA,
DR MICHAŁ HAMPEL, MICHAŁ KRAWCZYK,
SŁAWOMIR ŁAZAREK, DR KRZYSZTOF MALESA,
DR INŻ. WITOLD SKOMRA.
REDAKCJA: IZABELA ALBRYCHT

INSTYTUT KOŚCIUSZKI

CYBERSEC
EUROPEJSKIE FORUM CYBERBEZPIECZEŃSTWA

Microsoft
PARTNER RAPORTU

RCB
Rządowe Centrum Bezpieczeństwa
PATRONAT

# SYSTEMOWA ODPORNOŚĆ PAŃSTWA W CYFROWEJ ERZE

IZABELA ALBRYCHT, ŁUKASZ GAWRON,
MACIEJ GÓRA, DR MICHAŁ HAMPEL, MICHAŁ KRAWCZYK,
SŁAWOMIR ŁAZAREK, DR KRZYSZTOF MALESA,
DR INŻ. WITOLD SKOMRA.
REDAKCJA: IZABELA ALBRYCHT

**AUTORZY:**

**Izabela Albrycht**
Wstęp

**dr Krzysztof Malesa**
Słowo wstępu Partnera raportu

**Izabela Albrycht**
Odporność państwa

**Michał Krawczyk**
Odporność społeczna

**Izabela Albrycht, Łukasz Gawron, Maciej Góra, dr Michał Hampel, Sławomir Łazarek**
Siedem podstawowych wymogów NATO dotyczących odporności

**dr inż. Witold Skomra**
Droga do odporności państwa

**Redakcja:** Izabela Albrycht

**Korekta:** Adam Ladziński

**Skład i oprawa graficzna:** Wiktoria Konieczniak

**PARTNERZY**

CYBERSEC
EUROPEJSKIE FORUM CYBERBEZPIECZEŃSTWA

Microsoft

**PATRONAT**

RCB
Rządowe Centrum Bezpieczeństwa

Niniejszy raport stanowi publikację Instytutu Kościuszki. Jednocześnie poglądy wyrażone w ramach publikacji stanowią oceny poszczególnych autorów i nie powinny być utożsamiane ze stanowiskiem Instytutu Kościuszki i partnerów publikacji. Publikacja stanowi wkład w debatę publiczną. Poszczególni autorzy są odpowiedzialni wyłącznie za swoje opinie i ich stanowisko nie może być utożsamiane ze stanowiskami innych autorów tego raportu.

INSTYTUT KOŚCIUSZKI

Opublikowane przez:
Instytut Kościuszki
ul. Feldmana 4/9-10,
31-130 Kraków, Polska
Telefon: 12 632 97 24
www.ik.org.pl
instytut@ik.org.pl

© Instytut Kościuszki
Kraków, 2022

# WSTĘP

## Izabela Albrycht

Historia ludzkości przeplatana jest cyklicznie powtarzającymi się wojnami, katastrofami i kataklizmami. Niektóre z nich są nieuniknione, ale część jest rezultatem decyzji zaniedbania lub ignorowania pesymistycznych scenariuszy. Wynika to często z powodów psychologicznych, z właściwości ludzkiej natury – chcemy żyć i zachowywać się tak jakby nic złowieszczego nie mogło się wydarzyć i negatywnie wpłynąć na nasz byt. Prawdopodobieństwo i nieuniknioność tego typu zdarzeń nie tylko nie zniknie, ale należy założyć, że znacznie wzrośnie. Obecna i kolejne dekady XXI wieku charakteryzować się będą wyjątkowo skomplikowanym krajobrazem nakładających się na siebie zagrożeń – militarnych, ekonomicznych, środowiskowych, społecznych – oraz dalszym rozwojem relatywnie nowych domen, generujących nie tylko cywilizacyjny postęp, ale także nowe wyzwania dla bezpieczeństwa – cyberprzestrzeni i kosmosu. Dlatego na decydentów spada odpowiedzialność, aby tym katastrofom zapobiec lub się na nie odpowiednio przygotować. Wielki powrót strategicznej rywalizacji państw, wszechogarniająca transformacja cyfrowa, zagrożenia pandemiczne, zmiany klimatyczne, czy rozrywanie łańcuchów dostaw, skutkują pojawieniem się wielowymiarowych i zmultiplikowanych wyzwań, zarówno poniżej, jak i powyżej progu wojny, które wymagają strategicznego podejścia do budowania systemowej odporności. Rządy i instytucje państwa muszą tworzyć strategie odpornościowe i realizować je w jeszcze bardziej skoordynowany sposób, angażując we współpracę liczne podmioty, oraz stymulować tworzenie niezbędnych zasobów i rozwiązań. Budowanie systemowej odporności (czy inaczej: odporności państwa) wymaga zaangażowania całego społeczeństwa, administracji i gospodarki oraz stworzenia ram współpracy w wielu wymiarach: cywilnym, militarnym, krajowym, międzynarodowym, politycznym, organizacyjnym czy technologicznym. W czasach dynamicznej transformacji cyfrowej ostatni element – technologiczny – jest szczególnie istotny, gdyż może pomóc osiągnąć założony cel, choć równocześnie może być źródłem nieznanych zagrożeń, wymaga zatem odpowiednich działań zapobiegawczych.

**Na początku trzeciej dekady XXI w. budowanie odporności uznane zostało za strategiczne podejście do wzmacniania bezpieczeństwa**, na co wskazują działania podejmowane zarówno przez NATO, jak i Unię Europejską oraz poszczególne kraje. Zmierzają one do budowy odporności i w warstwie fizycznej, i cyfrowej. **Odporność państwa** coraz częściej jest wzmacniana dzięki zastosowaniu technologii cyfrowych, które pozwalają skutecznie reagować na sytuacje kryzysowe (tzw. **odporność cyfrowa**) oraz poprzez budowanie **cyberodporności**, która jest odpowiedzią na zagrożenia płynące z cyberprzestrzeni. Istotny element odporności stanowi **odporność społeczna**, która również jest jednym z istotnych wymiarów bezpieczeństwa, i także w jej przypadku można mówić o dwóch aspektach. Pierwszy to odporność na dezinformacje, która towarzyszy cyberatakom i cyberzagrożeniom, w tym hybrydowym, drugi to rozwijanie i doskonalenie kompetencji w sferze współużytkowania cyberprzestrzeni, które wymagają wbudowania w nasze „cyfrowe DNA" wiedzy z zakresu korzystania z cyfrowych technologii oraz higieny cyfrowej, ale także rozwijania cyfrowych kompetencji przyszłości, pozwalających budować konkurencyjną pozycję państwa w cyfrowej gospodarce oraz jego bezpieczeństwo w dłuższym okresie. Innymi słowy odporność wpływać będzie na pozycję geopolityczną i geoekonomiczną państw.

Dlatego przed wszystkimi państwami stoją w tym wymiarze poważne wyzwania. W Polsce istotne wsparcie polityczne dla wzmacniania odporności „państwa i społeczeństwa na współczesne zagrożenia"[1] przynosi Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, która została zatwierdzona w dniu 12 maja 2020 r. przez Prezydenta RP. Wskazuje ona równocześnie na potrzebę „rozwoju odporności" jak i „zdolności obronnych Polski", jako na dwa elementy większej całości systemu bezpieczeństwa. Jednocześnie wskazując, że „kompleksowa odporność państwa na zagrożenia niemilitarne i militarne", obejmujące także hybrydowe, wymaga zaangażowania wielu podmiotów, w tym „instytucji państwowych i samorządowych, podmiotów systemu edukacji i szkolnictwa wyższego, społeczności lokalnych, podmiotów gospodarczych, organizacji pozarządowych oraz obywateli."[2]. Strategia podkreśla również konieczność budowy odporności na cyberzagrożenia, w tym skuteczne im zapobieganie, zwalczanie oraz reagowanie na nie, poprzez zwiększenie poziomu „odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej"[3].

Wymienione wymiary i warstwy odporności systemowej wzajemnie się przenikają i warunkują, dlatego warto poddać je wspólnej analizie, a w zakresie wysiłków na rzecz wzmacniania odporności państwa rozwinąć jedyne słuszne podejście jakim jest podejście *whole of sociaty* – obejmujące całe społeczeństwo.

# SŁOWO WSTĘPU PARTNERA RAPORTU

**dr Krzysztof Malesa**

Budowanie odporności jest długotrwałym procesem wymagającym dużych wysiłków i nakładów, ale niestety jest też chyba jedynym niemilitarnym sposobem na odparcie działań hybrydowych, które dziś stanowią stały element geopolitycznego krajobrazu północno-wschodniej flanki NATO. Znaczenie odporności dobitnie określa artykuł trzeci Traktatu Północnoatlantyckiego, rozwinięty w deklarację wzmacniania odporności przyjętą w 2016 r. na warszawskim szczycie NATO i ponowioną na szczycie w Brukseli w roku 2021 r. Odporność – pozostająca w odpowiedzialności państwa członkowskiego – jest kluczowym elementem umożliwiającym realizację sojuszniczej polityki odstraszania i mechanizmu obrony kolektywnej.

Budowanie odporności państwa członkowskiego nie ogranicza się do zbrojeń. Wręcz przeciwnie, to w znacznej mierze domena administracji cywilnej: zadanie przekrojowe i ponadresortowe, wymagające koordynacji z poziomu Rady Ministrów. To też zadanie w znacznym stopniu angażujące podmioty prywatne, a szczególnie operatorów infrastruktury krytycznej.

Współpraca w tym obszarze z sektorem prywatnym, często reprezentującym duże międzynarodowe korporacje, wymaga od administracji zrozumienia specyfiki biznesu i osiągnięcia określonego poziomu dojrzałości technologicznej. Wzmacnianie odporności w dzisiejszych czasach musi być bowiem wspierane przez technologię cyfrową.

Opisane w raporcie doświadczenia świadczą o tym, że w każdym z siedmiu obszarów odporności zdefiniowanych przez NATO jest miejsce dla technologii chmury obliczeniowej, uczenia maszynowego czy AI inteligencji (SI). Zawarte w tekście *case studies* dowodzą, jak bardzo te rozwiązania mogą wesprzeć nasze wysiłki na rzecz wzmacniania odporności, ale też pokazują właściwe miejsce technologii w procesie zarządzania: powinna ona być wsparciem dla przemyślanych rozwiązań organizacyjnych realizowanych przez przeszkolonych, świadomych ludzi. Te rozwiązania organizacyjne powinny w dzisiejszych niespokojnych czasach być efektem śmiałych i progresywnych decyzji, również decyzji politycznych, z którymi nie należy zwlekać. Wzmocnijmy odporność Polski, póki jest na to czas.



# 1. ODPORNOŚĆ PAŃSTWA

**Izabela Albrycht**

## 1.1 Perspektywa NATO

Budowanie systemowej odporności jest jednym z priorytetów wszystkich państw Sojuszu Północnoatlantyckiego, wynikającym z art. 3 Traktatu Północnoatlantyckiego[4], a potwierdzonym zobowiązaniem do wzmacniania odporności przyjętym w 2016 r. podczas szczytu NATO w Warszawie. Odporność przede wszystkim jest obowiązkiem indywidualnym każdego sojusznika, który musi być wystarczająco silny i zdolny do przystosowania się i radzenia sobie z całym spektrum kryzysów, w obliczu których staje sojusz. Suma odporności sojuszników jest wspólną odpornością NATO, z kolei brak odporności jednego sojusznika jest słabością całego sojuszu. Odporny kraj jest mniej atrakcyjny jako cel i tym samym przyczynia się do ogólnego, kolektywnego bezpieczeństwa sojuszu. Zbiorowa odporność, także dzięki cywilnej gotowości państw sojuszniczych, jest zatem kluczowym celem polityki i działań NATO.

Coraz częstsze podkreślanie znaczenia odporności wynika ze zmiany charakteru zagrożeń w nowym geopolitycznym układzie sił, które w wielu aspektach przyjmują postać nie tylko militarną, ale coraz częściej także hybrydową, terrorystyczną bądź cyber. Gotowość cywilna, czyli „wspieranie sojuszniczych sił zbrojnych przy pomocy zasobów cywilnych i cywilnej infrastruktury zarówno w czasie pokoju, w kryzysie, jak i w czasie wojny”[5], pełni trzy podstawowe funkcje: zapewnienie ciągłości rządu i ciągłości kluczowych usług dla ludności oraz cywilnego wsparcia operacji wojskowych. Na szczycie NATO w Warszawie te trzy kluczowe funkcje zostały rozwinięte w siedem bazowych wymogów dotyczących odporności, omówionych szczegółowo w rozdziale 3. Ogólnie, polityką NATO dotyczącą odporności i gotowości cywilnej kieruje Komitet ds. Odporności (Resilience Committee), który podlega bezpośrednio Radzie Północnoatlantyckiej, głównemu organowi decyzyjnemu NATO, co charakteryzuje znaczenie tego elementu współpracy sojuszników[6].

Na szczycie w Brukseli w czerwcu 2021 r., po raz kolejny podkreślono istotność odporności, a konkretniej jej zwiększenia. W deklaracji zaznaczono,

**Definicja „odporności” NATO**

**Odporność to zdolność społeczeństwa do stawiania oporu oraz łatwego i szybkiego powrotu do funkcjonowania, po poważnym wstrząsie, takim jak klęska żywiołowa lub atak zbrojny. Odporność jest połączeniem gotowości cywilnej i wojskowych zdolności, za których budowę odpowiada każde państwo członkowskie NATO[7].**

że mimo iż odporność pozostaje obowiązkiem poszczególnych krajów, to konieczne jest przyjęcie bardziej zintegrowanego i lepiej skoordynowanego podejścia w ramach NATO, zgodne ze zobowiązaniem traktatowym, po to aby zmniejszyć podatność na zagrożenia i zapewnić sojuszniczym siłom zbrojnym możliwość skutecznego działania w warunkach pokoju, kryzysu i konfliktu. Postanowiono, że sojusznicy opracują propozycję ustanowienia, oceny, przeglądu i monitorowania celów w zakresie odporności (tzw. resilience objectives) jako drogowskazu do działań na szczeblu krajowym w zakresie narodowych celów odporności i planów ich wdrażania[8]. Podkreślono, że do każdego z członków Sojuszu należeć będzie określenie, jak ustanawiać i realizować krajowe cele w zakresie odporności oraz ich plany wdrażania, tak aby były one zgodne z kompetencjami, strukturami, procesami i obowiązkami krajowymi, oraz w niektórych przypadkach również z unijnymi[9]. W deklaracji podkreślony został także dodatkowy element testujący odporność NATO – pandemia COVID-19.

Szczyt NATO w Madrycie w 2022 r. oraz wydana na nim Deklaracja potwierdziły dotychczasowe znaczenie odporności jako obowiązku państw sojuszniczych, ale jednocześnie wspólnego zobowiązania sojuszników, która powinna być dalej wzmacniana poprzez realizację celów opracowanych na szczeblu krajowym i planów wdrożeniowych stworzonych wspólnie w ramach sojuszu. NATO zobowiązało się przyspieszyć adaptację do wyzwań bezpieczeństwa we wszystkich obszarach, zagrożeń militarnych i niemilitarnych, zwiększając odporność na zagrożenia cybernetyczne i hybrydowe oraz wzmacniając interoperacyjność[10]. Podobnie rolę odporności i jej znaczenie dla kolektywnej obrony i bezpieczeństwa definiuje nowa przyjęta na madryckim szczycie Koncepcja Strategiczna Sojuszu, podkreślając, że jej zapewnienie ma kluczowe znaczenie dla wszystkich podstawowych zadań sojuszu, zwłaszcza że jest ona regularnie testowana przez strategicznych rywali i konieczna w świetle rosyjskiej agresywnej polityki. Stanowi ona także podstawę wysiłków na rzecz ochrony sojuszników, społeczeństwa i wspólnych wartości[11]. Warto zaznaczyć, że wzmocnienie odporności występuje w dokumencie w korelacji z koniecznością wzmocnienia technologicznej przewagi Sojuszu[12]. NATO podkreśla również potrzebę współpracy w zakresie wzmacniania odporności z Unią Europejską, jako dziedziny wspólnego zainteresowania, ale także zwraca uwagę na potrzebę współpracy między podmiotami cywilnymi i wojskowymi. Istotnym novum jest podkreślenie, że także zmiany klimatyczne i ich wpływ na bezpieczeństwo przynoszą ryzyka dla odporności i gotowości cywilnej. Uwypukla to opublikowana w czasie szczytu w Madrycie Ocena wpływu zmian klimatu na bezpieczeństwo, która stwierdza, że „imperatywem NATO i sojuszników będzie kontynuacja wzmacniania odporności krajowej i międzynarodowej, biorąc pod uwagę wpływ zmian klimatu”[13].

## 1.2 Perspektywa Unii Europejskiej

Komisja Europejska zwróciła uwagę na strategiczne znaczenie odporności w 2020 r. w Strategic Foresight Report,



**Definicja „odporności” Komisji Europejskiej**

**Zdolność nie tylko stawiania czoła wyzwaniom i radzenia sobie z nimi, ale także realizacji przemian w sposób zrównoważony, sprawiedliwy i demokratyczny.**

uznając, że jej wzmocnienie musi być nowym kompasem w procesie decyzyjnym dotyczącym polityk unijnych[14] dla przywódców UE, i wynikać z połączenia umiejętności strategicznego prognozowania oraz tworzenia adekwatnej odpowiedzi politycznej na dające się przewidzieć zmiany i wyzwania oraz zdarzenia nieprzewidywalne. Budowanie odporności to ciągłe rozwijanie przez państwa zdolności mogących pomóc odnieść się do podatności systemu i utrzymać ciągłość funkcjonowania państwa oraz realizacji celów polityk publicznych w obliczu wyzwań związanych z transformacją społeczną i ekonomiczną. Odporność rozumiana jako odpowiedź na wyzwania i kryzysy musi być realizowana w sposób zrównoważony, sprawiedliwy i demokratyczny, a jednocześnie przyjąć szeroką, multidyscyplinarną perspektywę, czyli „360-stopniowe podejście”[15].

W listopadzie 2021 r. KE przedstawiła stworzone we współpracy z krajami członkowskimi panele oceny odporności (ang. *resilience dashboards*), aby stworzyć narzędzie do całościowej oceny odporności UE i krajów członkowskich, Mierzą one ich mocne i słabe strony w każdym z czterech wymiarów: społeczno-ekonomicznym, zielonym, cyfrowym i geopolitycznym. Jednym z instrumentów wzmacniania odporności jest stworzenie dedykowanego funduszu pomocowego Recovery and Resilience Facility (RRF), w ramach programu NextGenerationEU, mającego na celu pobudzenie reform i inwestycji służących dalszej transformacji gospodarek i społeczeństwa. Postępy we wzmacnianiu odporności dzięki RFF także będą monitorowane w ramach paneli oceny odporności. Minimum 20% wydatków w ramach Krajowych Planów Odbudowy powinno zostać przeznaczone na wspieranie transformacji cyfrowej[16]. Zdaniem Komisji Europejskiej cyfrowe rozwiązania mogą wzmocnić nie tylko odbudowę gospodarek osłabionych wskutek pandemii COVID-19[17], ale także odporność społeczno-gospodarczą krajów unijnych na ewentualne kolejne sytuacje kryzysowe i wstrząsy. Dlatego projekty realizowane z RFF będą również skoncentrowane na inicjatywach cyfrowych. Z analizy planów RRF poszczególnych krajów członkowskich wynika, że wiele z nich zamierza zainwestować w rozwój i budowę sieci szerokopasmowych, cyfryzację administracji publicznej z naciskiem na interoperacyjność i zasadę *once-only*, dalszą cyfryzację przedsiębiorstw, zmierzającą do poprawy procesów produkcyjnych, a także w rozwój umiejętności cyfrowych i transformację systemów edukacji, tak aby sprostały wyzwaniom przyszłości[18]. Droga do osiągnięcia odporności wiedzie także przez inwestycje nakierowane na rozwój zaawansowanych technologii cyfrowych, w tym SI czy *blockchain*[19].

## 1.3 Cyberodporność

W procesach przemian wynikających z przyspieszonej transformacji cyfrowej i gwałtownych zmian geopolitycznych istotne miejsce zajmuje cyberbezpieczeństwo i cyberobrona. Po latach zyskiwania na znaczeniu, wraz z wybuchem wojny na Ukrainie zostało definitywnie zaklasyfikowane do strategicznych wyzwań dla państwa i uznane za element bezpieczeństwa narodowego. Już na początku pandemii COVID-19 obserwowaliśmy istotny wzrost cyberataków, gdyż wraz z pierwszymi lockdownami skokowo wzrosła liczba osób, które musiały rozpocząć zdalną pracę i edukację. Setki milionów osób na całym świecie z dnia na dzień przeszły z firmowych systemów bezpieczeństwa do najczęściej słabo zabezpieczonych sieci czy urządzeń prywatnych i zaczęły z nich korzystać w celach służbowych. Jednocześnie szereg firm i instytucji przeszło proces przyspieszonej transformacji cyfrowej, wdrażając systemy do zarządzania projektami czy usługi chmurowe. Zgodnie z raportem Deloitte[20], już rok od wybuchu pandemii zwiększyła się dynamicznie liczba smartfonów i komputerów podłączonych do internetowej infrastruktury, która pozwala miliardom osób pozostawać ze sobą w kontakcie, korzystać z usług służby zdrowia, robić zakupy. Wzrosło także zainteresowanie urządzeniami do rozrywki czy sportu, takimi jak konsole do gry, urządzenia do streamingu multimediów, inteligentne telewizory i zegarki. W związku z wypełnieniem cyberprzestrzeni większą ilością komponentów cyfrowych rozszerzyła się również „powierzchnia", którą dotknąć mogą cyberataki i wzrosło wyzwanie cyberodporności.

**Cyberodporność należy rozumieć jako osiągniętą przez daną organizację umiejętność zarządzania cyberatakiem oraz jego skutkami w sposób, który utrzyma jej zdolności operacyjne. Obejmuje takie elementy jak bezpieczeństwo informacyjne, infrastrukturę IT i OT, procesy biznesowe i kontynuację działalności[21].**

Cyberodporność jest także istotna w aspekcie bezpieczeństwa i obronności, gdyż działania ofensywne w cyberprzestrzeni stały się kluczowym komponentem współczesnych wojen, co dobitnie udowodniła wojna Rosji przeciwko Ukrainie. A ponieważ cyberwojna obejmuje operacje przeprowadzane w sieci, ale także z użyciem sieci i z infrastrukturą fizyczną jako celem, to cyberodporność odnosi się nie tylko do sieci i systemów teleinformatycznych, ale również do bezpieczeństwa przeważającej liczby obiektów fizycznych. Dlatego w zglobalizowanym, ale także bardziej konfrontacyjnym i skomplikowanym świecie odporność pozostanie nieustannym problemem państw unijnych i natowskich, wymagającym ciągłych dostosowań w miarę pojawiania się nowych zagrożeń i niedostatecznych zabezpieczeń, ale także współpracy i skoordynowanych działań wynikających z natury cyfrowych wyzwań, które charakteryzuje transgraniczność. Celem cyberodporności stało się nie tylko zapewnianie ciągłości operacyjnej w świecie cyfrowym, ale także przygotowanie się państw, instytucji, firm, organizacji na trudne do przewidzenia i nietypowe zdarzenia i zagrożenia płynące z cyberprzestrzeni, w tym w czasach kryzysu.

W tych uwarunkowaniach wzmacnianie przez kraje cyberbezpieczeństwa wiedzie przez budowę cyberodporności, która wydaje się słowem kluczem AD 2022. Wymaga ona podjęcia wysiłku wspólnego przygotowania się do cyfrowych zagrożeń, odpowiedniego i skutecznego reagowania na nie i radzenia sobie z ich skutkami.

Odporna na cyberzagrożenia struktura może dostosować się do znanych i nieznanych zagrożeń, wyzwań i ryzyk, czyli cyberoperacji i incydentów, z którymi mamy do czynienia aktualnie, a także tych, które z uwagi na ustawiczną ewolucję technologii pojawią się w kolejnych latach. Zatem budowanie cyberodporności jest i pozostanie długoterminowym procesem, który w zależności od uwarunkowań – wynikających ze zmiennej natury cyberprzestrzeni i cyberzagrożeń – będzie modyfikowany odpowiednio do wyzwań i potrzeb. Wraz ze wzrostem nasycenia cyberprzestrzeni kolejnymi technologiami i miliardami połączonych z siecią urządzeń celem pozostaje wypełnienie jej jak największą liczbą bezpiecznych komponentów, a także zbudowanie zdolności organizacyjnych. Należy uznać, że cyberodporność powinna być właściwością całego cyfrowego ekosystemu, tj. wdrożoną w ramach wszystkich sektorów i z uwzględnieniem całego łańcucha powiązanych ze sobą elementów (sieć, software, hardware, aplikacje) i wymiarów (administracja, przemysł, samorządy, inne). Dlatego podejmowane były próby zawarcia globalnych zobowiązań w zakresie pokojowego użytkowania cyberprzestrzeni, ale w aktualnych okolicznościach geopolitycznych wydają się niemożliwe do osiągnięcia. Stąd w pierwszej kolejności konieczne jest polityczne wsparcie dla regulacji wzmacniających dalsze budowanie cyberbezpieczeństwa, wpływających na biznes i funkcjonowanie firm w UE i obszarze transatlantyckim. Te dążenia widać wyraźnie po stronie unijnej wraz z przyspieszeniem prac nad kolejną odsłoną dyrektywy w sprawie bezpieczeństwa sieci i informacji (NIS2) czy spodziewanym w trzecim kwartale 2022 r. projektem aktu dot. cyberodporności (Cybersecurity Resilience Act). 13 maja 2022 r. Rada i Parlament Europejski porozumiały się w sprawie przyspieszenia prac nad przepisami „o wysokim wspólnym poziomie cyberbezpieczeństwa w całej UE", których zadaniem jest dalsze zwiększenie odporności i zdolności reagowania sektora publicznego i prywatnego, a także UE jako całości"[22]. Porozumienie obejmuje proces decyzyjny w zakresie wspomnianej dyrektywy NIS2, ale także dyrektywy (Directive on the Resilience of Critical Entities, CER) o odporności podmiotów krytycznych w zakresie fizycznego jej wzmocnienia. Funkcjonowanie tych podmiotów może być zaburzone przez klęski żywiołowe, terroryzm lub ataki hybrydowe, podczas gdy zależą od nich usługi publiczne i rynek wewnętrzny. W procesie legislacyjnym jest także unijne rozporządze-

nie w sprawie operacyjnej odporności cyfrowej (DORA), które ma zwiększyć bezpieczeństwo informatyczne sektora finansowego – banków, ubezpieczycieli, firm inwestycyjnych – poprzez utrzymanie odporności operacyjnej. W wymiarze cyfrowym odporność w najszerszym zakresie ma z kolei pomóc budować akt dot. cyberodporności, którego celem będzie nasycenie „europejskiej" cyberprzestrzeni bezpieczniejszymi rozwiązaniami i sprzętem, mniej podatnymi na ataki, sabotaż czy celowe działania. Komisja zaproponuje zatem „wprowadzenie wspólnych przepisów dotyczących cyberbezpieczeństwa dla producentów i sprzedawców materialnych i niematerialnych produktów cyfrowych i usług pomocniczych"[23].

Polityczny impuls do wzmacniania odporności na cyberzagrożenia został wysłany w strategii cyberbezpieczeństwa UE (EU Cybersecurity Strategy) z 2020 r., gdzie cyberodporność została uznana za jeden z głównych obszarów zainteresowania i kluczowy cel działania. Dokument stwierdza, że dzięki realizacji strategii wzmocniona zostanie zbiorowa odporność Europy na cyberzagrożenia, a wszyscy obywatele i przedsiębiorstwa będą mogły w pełni korzystać z godnych zaufania i niezawodnych usług oraz narzędzi cyfrowych[24].

To podejście widoczne jest także na poziomie krajów członkowskich. Przykładowo, w Polsce dokumentem, który formułuje krajowe ambicje w zakresie podniesienia poziomu odporności na cyberzagrożenia jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024. Strategia określa działania, których celem jest zwiększenie odporności na cyberzagrożenia systemów informacyjnych, operatorów usług kluczowych i infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej[25].

W konsekwencji takiej polityki nakierowanej na wzmocnienie cyberodporności należy się spodziewać, że kraje unijne przeprowadzą dogłębną analizę całego ekosystemu informatycznego pod kątem bezpieczeństwa – stosu technologicznego, czyli tego, co się na niego składa w wymiarze sprzętowym, oprogramowania, ale też usługodawców i zasobów ludzkich, a zatem w całym łańcuchu dostaw i zgodnie z polityką *„know your supplier"*. Takie działania powinny zostać podjęte na poziomie firm, ale także państw i organizacji międzynarodowych. Dla budowania cyberodporności UE, i szerzej obszaru transatlantyckiego, konieczne jest także wspólne rozwijanie standardów, certyfikacja produktów i usług pod kątem cyberbezpieczeństwa oraz wsparcie dla inicjatyw mających na celu zwiększenie bezpieczeństwa oprogramowania. Należy także znacznie zwiększyć wysiłki w zakresie budowy mocnej pozycji krajowych sektorów cyberbezpieczeństwa w globalnych łańcuchach wartości i dostaw produktów i usług dla bezpieczeństwa sieci i systemów teleinformatycznych, w tym w ramach tych nowych i przełomowych technologii (ang. *emerging and disruptive technologies*), które wpływają na rozwój cybertechnologii, innowacyjność gospodarki i zdolności obronne. Komisja Europejska także w tym obszarze stara się wpłynąć na rynek, między innymi przedstawiając propozycję wspólnych działań, których podjęcia przez kraje członkowskie chciałaby w najbliższych latach – została ona opisana w konsultowanej aktualnie tzw. mapie drogowej (The roadmap on critical technologies for security and defence)[26]. Należy zauważyć, że proces rozwijania technologii poprzez innowacje także wymaga oceny pod względem cyberodporności i cyberbezpieczeństwa, co jest inwestycją w bezpieczeństwo krajów i gospodarek w dłuższym okresie.

W wymiarze operacyjnym niezbędna jest bardziej proaktywna polityka bezpieczeństwa zmierzająca do wzmocnienia współpracy publiczno-prywatnej i nie tylko większego, ale także zinstytucjonalizowanego zaangażowania firm w budowanie systemu cyberbezpieczeństwa zarówno w ramach UE, jak i NATO. Chodzi nie tylko o realizację takich inicjatyw jak amerykańska Shields Up, która ma zmobilizować firmy i pomóc im zwiększać swój poziom cyberzabezpieczeń, ale także o otwartość, jeśli chodzi o nawiązanie realnego partnerstwa publiczno-prywatnego obejmującego w pierwszej kolejności *cyber threat intelligence sharing, threat hunting*, lepszą koordynację sektorową w zakresie *information sharing*, pogłębienie tej współpracy i nadanie jej charakteru stałego, na przykład poprzez stworzenie sieci sektorowych CERT-ów, współpracę w budowaniu SOC-ów czyli Security Operation Centers, czy realizację bug bounties. Przykładami istniejących partnerstw są na przykład Government Security Program Microsoftu czy stworzony przez polski rząd Program Współpracy w Cyberbezpieczeństwie (PWCyber). Z kolei na szczycie NATO w Madrycie zadecydowano o stworzeniu „wirtualnych zdolności do szybkiego reagowania w cyberprzestrzeni" bazujących na zasobach krajowych sojuszników i do dalszego pogłębiania współpracy z sektorem prywatnym.

# 2. ODPORNOŚĆ SPOŁECZNA

**Michał Krawczyk**

## 2.1 Oporność społeczna na dezinformację

Dezinformacja jest elementem współczesnych wojen, konfliktów i rywalizacji, stąd odporność społeczna jest ważnym elementem bezpieczeństwa państwa. Pandemia COVID-19 oraz rosyjska inwazja na Ukrainę zwielokrotniły zagrożenia płynące z przestrzeni informacyjnej. Chociaż dezinformacja to narzędzie prowadzenia polityki i działań militarnych od wielu dekad, ostatnie lata potwierdziły wzrastający problem zaburzeń informacyjnych, szczególnie tych związanych z cyfrowymi przestrzeniami informacyjnymi. Konsekwencją jest szereg wyzwań związanych z przeciwdziałaniem dezinformacji oraz komunikacją strategiczną. W odpowiedzi na nie powstało wiele nowych rozwiązań oraz inicjatyw prezentowanych przez rządy, społeczeństwo obywatelskie, ekspertów, naukowców i organizacje komercyjne. Działania te obejmują nowe rozwiązania w obszarze komunikacji strategicznej, np. w kontekście sposobów informowania o szczepionkach, oraz inicjatywy legislacyjne i technologiczne na rzecz zwalczania dezinformacji. Spora część z tych inicjatyw ma charakter *ad hoc* i skupia się na przeciwdziałaniu jednemu typowi zagrożenia lub ogranicza do specyficznego obszaru, zdefiniowanego przez grupę docelową dezinformacji, typ dezinformacji lub platformę, za pomocą której jest rozprzestrzeniana. Co istotne, problem dezinformacji wykracza poza ramy rywalizacji i konfliktów międzynarodowych. Może bowiem oddziaływać na życie zwykłych ludzi, co pokazuje przede wszystkim przykład pandemii COVID-19 i związanej z nią infodemii, czyli niespotykanej fali fałszywych wiadomości. W takim kontekście dezinformacja może bezpośrednio wpływać na zdrowie ludzi, a w skrajnych przypadkach stanowić nawet zagrożenie dla życia. Dlatego tak istotne jest zaangażowanie oraz interwencja instytucji publicznych i międzynarodowych, ale nie tylko.

**Proces ten należy rozumieć jako oparte na współpracy, kompleksowe działania na rzecz zrozumienia problemu dezinformacji, przeciwdziałania mu, ograniczania negatywnych skutków oraz edukacji, skierowane do całego społeczeństwa i wypracowane przez instytucje publiczne, społeczeństwo obywatelskie, środowisko akademickie oraz sektor prywatny.**

Poziom skomplikowania oraz rozległość problematyki dezinformacji i powiązanych z nią zagrożeń sprawia, że jej zapobieganie musi obejmować bardzo szeroki zakres działań, prowadzonych przez różne instytucje i organizacje. Dlatego kluczowym zagadnieniem w tym kontekście jest budowanie społecznej odporności na dezinformację. Odporność społeczna, aby była skuteczna, musi zaistnieć równocześnie na poziomie państwa i społeczeństwa. Kwestię tę dostrzegły rządy poszczególnych państw oraz m.in. NATO i UE, które swoimi działaniami podkreśliły istotność tego problemu oraz chęć przeciwdziałania. W tzw. „raporcie mędrców" NATO możemy przeczytać: „obywatele państw NATO oczekują ochrony przed nowymi zagrożeniami, w tym cyfrowymi i dezinformacyjnymi, oraz spodziewają się, że ich rządy przy wsparciu Sojuszu rozwiną narzędzia atrybucji i odstraszania. Odporność systemowa musi być elementem i państw, i społeczeństw"[27].

## 2.2 Działania Unii Europejskiej na rzecz odporności społecznej

Kluczowym aktorem w kontekście zwalczania dezinformacji wydaje się być UE, której oddziaływanie, płynące z pozycji na arenie międzynarodowej oraz siły gospodarczej, pozwala na szeroki wpływ na sektor prywatny oraz publiczny. Każdy z najważniejszych organów UE, tj. Parlament Europejski, Komisja Europejska, Rada Europejska i Rada Unii Europejskiej uczestniczy w tym procesie, kierując swoje działania do państw członkowskich, sektorów prywatnego i trzeciego oraz obywateli UE. Poza nimi aktywną rolę pełni również Wysoki Przedstawiciel ds. Polityki Zagranicznej i Polityki Bezpieczeństwa wraz z podlegającym mu Centrum Analiz Wywiadowczych UE (EU Intelligence and Situation Centre, INTCEN) oraz działające w jego ramach komórki zajmujące się komunikacją strategiczną, szczególnie grupa zadaniowa East StratCom. Swoją rolę odgrywają również unijne podmioty zajmujące się zagrożeniami hybrydowymi, czyli Centrum Doskonalenia ds. przeciwdziałania zagrożeniom hybrydowym (Hybrid Center of Excellence) oraz komórka UE ds. syntezy informacji o zagrożeniach hybrydowych (Hybrid Fusion Cell).

Ważną rolę w unijnym podejściu do zwalczania dezinformacji pełni kooperacja z sektorem prywatnym oraz próby jego regulowania. UE rozpoznała częściową odpowiedzialność firm technologicznych za zjawisko dezinformacji, zauważając, że to podmioty prywatne odpowiadają za działanie platform społecznościowych, na których kampanie dezinformacyjne są tworzone i rozprzestrzeniane, a ich funkcjonowanie oparte na algorytmach umożliwia szerzenie fałszywych wiadomości na taką skalę. Unia otwarcie wezwała przedstawicieli sektora prywatnego do zwiększenia wysiłków na rzecz zwalczania dezinformacji. Ważnym elementem tych działań jest wprowadzony w 2018 r. Kodeks Postępowania UE w zakresie dezinformacji (The EU Code of Practice on Disinformation)[28]. Porusza on pięć obszarów kompetencyjnych na rzecz zwiększenia transparentności i odpowiedzialności środowiska mediów online. Wśród nich znalazły się: zwiększenie przejrzystości reklam online i kontroli nad reklamodawcami; zwiększenie przejrzystości reklam politycznych; zintensyfikowanie wewnętrznych działań platform w obszarze zwalczania dezinformacji; promowanie rzetelnych źródeł informacji oraz intensyfikacja współpracy ze społecznością ekspercką. Był to pierwszy akt samoregulacyjny tego typu, który został dobrowolnie przyjęty przez największych gigantów technologicznych. Jednak od samego początku środowisko eksperckie oraz sama UE dostrzegały potrzebę rewizji Kodeksu i wprowa-

dzenie do niego bardziej restrykcyjnych zasad. Stało się to w czerwcu 2022 r., kiedy opublikowana została jego druga wersja[29]. Nowa wersja jest bardziej szczegółowa (zawiera 44 zobowiązania, wersja z 2018 r. zawierała ich 21) i według Komisji Europejskiej oparta na doświadczeniach kilku ostatnich lat. Główne obszary poruszane przez Kodeks to: demonetyzacja dezinformacji, przejrzystość reklam politycznych, ograniczenie technik manipulacyjnych (aktywne zwalczanie fałszywych kont, botów, *deep fake* itp.); ochrona użytkowników (rozwijanie narzędzi do identyfikacji i raportowania nieprawdziwych treści); stworzenie ogólnoeuropejskiej sieci *fact-checking* oraz umożliwienie dostępu do danych badaczom. Implementacja Kodeksu, która zawiodła w kontekście dokumentu z 2018 r., będzie nadzorowana i monitorowana przez zapowiedziane nowe centrum transparentności (ang. *transparency center*) oraz stałą grupę zadaniową.

Komisja Europejska przedstawiła i doprowadziła równocześnie do zatwierdzenia Digital Services Act (DSA) – propozycji legislacyjnej aktu o usługach cyfrowych, regulującego ich dostawców[30]. DSA przede wszystkim udostępnia szereg narzędzi, które mogą zostać użyte do zwalczania dezinformacji, szczególnie poprzez nałożenie odpowiedzialności za dezinformację na platformy. Te ostatnie będą musiały działać w bardziej przejrzysty sposób oraz co najważniejsze, za niespełnianie wytycznych będą mogły zostać pociągnięte do odpowiedzialności. DSA obejmie również wprowadzenie możliwości odwołania użytkownika od decyzji platformy oraz wgląd w uzasadnienie danych postępowań moderacyjnych[31]. Po przyjęciu finalnego brzmienia DSA przez Parlament Europejski akt będzie musiał jeszcze zostać ratyfikowany przez parlamenty krajowe państw członkowskich.

UE wspiera również aktywnie działania sektora pozarządowego, głównie za pomocą instrumentów finansowych, w tym zobowiązała się do szczególnego wspierania organizacji *fact-checking* oraz promowania umiejętności korzystania z mediów (ang. *media literacy*) i jakościowego dziennikarstwa[32]. W tym kontekście w 2018 r. powstało międzynarodowe obserwatorium dezinformacji i analizy platform społecznościowych SOMA[33]. W jej ramach powstały trzy centra badawcze oraz rozwijana i promowana jest sieć organizacji trudniących się analizą mediów społecznościowych.

Kolejnym przykładem współpracy UE z trzecim sektorem jest sieć Europejskie Obserwatorium Mediów Społecznościowych (European Digital Media Observatory, EDMO)[34]. UE w jej ramach i w oparciu o struktury Europejskiego Instytutu Uniwersyteckiego (European University Institute) we Florencji stworzyła ogólnoeuropejskie centrum, któremu podlegają regionalne ośrodki (tworzone przez podmioty z różnych krajów unijnych). EDMO umożliwia i ułatwia współpracę specjalistów od *fact-checking*, ekspertów z obszaru *media literacy* oraz naukowców w celu zrozumienia i analizy dezinformacji.

Powyższe aktywności UE na rzecz budowy systemowej i społecznej odporności na dezinformację obejmują wszystkie najważniejsze elementy oddziaływania.



## CASE STUDY – UKRAINA

Rosyjska inwazja na Ukrainę nie ograniczyła się jedynie do działań kinetycznych w domenie militarnej, ale objęła również wrogie aktywności w cyberprzestrzeni oraz domenie informacyjnej. Rosyjskie działania propagandowe i dezinformacyjne stanowią ważną część sztuki wojennej Moskwy, a nieprawdziwe i zmanipulowane informacje są używane jako narzędzia do prowadzenia działań poniżej progu wojny zarówno przeciwko Ukrainie, jak i w ujęciu globalnym. Ukraina jest celem wojny informacyjnej od co najmniej dekady i bazując na tym doświadczeniu, rozwijała w ciągu ostatnich lat system odporności na dezinformację, szczególnie w obszarze współpracy sektora publicznego ze społeczeństwem obywatelskim.

Ukraińskie działania w kontekście zwalczania rosyjskiej dezinformacji opierają się na kilku priorytetowych obszarach: walka ze wszystkimi przejawami działań hybrydowych (cyberataki, dezinformacja rozprzestrzeniana w mediach, manipulacje polityków, propaganda kościoła prawosławnego itp.); podejście strategiczne skupiające się nie tylko na obalaniu rosyjskich kłamstw, ale również na ustanawianiu własnego przekazu; promowanie jedności poprzez współpracę rządu ze społeczeństwem obywatelskim. Takie podejście do problemu dezinformacji współgra z pojęciem budowania społecznej odporności na dezinformację, szczególnie poprzez fakt skupienia się strony ukraińskiej na współpracy sektora publicznego ze społeczeństwem obywatelskim oraz chęć zwalczania wszystkich przejawów dezinformacji.

Już od pierwszego dnia rosyjskiej inwazji ukraiński opór objął również świat cyfrowy oraz przestrzeń informacyjną. Pojawił się szereg rozwiązań technologicznych, wprowadzanych przez rząd, sektor prywatny oraz pozarządowy, budujących społeczną odporność na dezinformację. W ramach wspólnych działań Ministerstwa Kultury i Polityki Informacyjnej oraz Ministerstwa Transformacji Cyfrowej powstała Armia Internetowa, zrzeszająca ok. 500 000 ochotników (deweloperów, twórców, marketingowców, copywriterów), którzy skupiają swoje siły m.in. na zwalczaniu rosyjskiej propagandy w sieci[35]. Poprzez zaangażowanie ochotników spośród społeczeństwa ukraińskiego, rośnie powszechna świadomość na temat kłamstw i taktyk wykorzystywanych przez Kreml. Wspomniane już wcześniej proaktywne podejście do prowadzenia wojny informacyjnej z Rosją również przejawia się w wykorzystaniu technologii cyfrowych. SI jest wykorzystywana w ramach aplikacji Diia do wyszukiwania profili społecznościowych poległych rosyjskich żołnierzy na podstawie ich zdjęć[36]. Następnie odnalezione profile są używane do powiadomienia rodziny poległego o jego śmierci, co powoduje propagandowy efekt w rosyjskim społeczeństwie. Komunikacja strategiczna odgrywa bardzo ważną rolę w opisywanych działaniach Ukrainy – rzetelne informowanie całego społeczeństwa jest wspomagane przez aplikacje Diia TV oraz Diia Radio, które są źródłem

oficjalnych i zaufanych wiadomości, dostępnych za ich pomocą nawet w wypadku braku telewizji lub sygnału radiowego[37]. Możliwość dotarcia z rzetelnymi informacjami nawet do okupowanych terenów stanowi bardzo istotny element odporności na dezinformację. Służy do tego również chatbot o nazwie „Mariupol now status"[38], działający na platformie Telegram. Za jego pomocą mieszkańcy okupowanego miasta otrzymują aktualne informacje na temat sytuacji w mieście i jego poszczególnych częściach. Za pomocą bota mieszkańcy mogą również dowiedzieć się o stanie swoich bliskich, od których zostali odłączeni.

Jak pokazują powyższe przykłady, w rzeczywistości wojennej kluczową rolę odgrywa sprawna komunikacja strategiczna oraz zdolność do szybkiego informowania obywateli. Pomaga w tym technologia oraz kooperacja rządu z pozostałymi sektorami. Tylko posiadając rzetelne informacje, obywatel może być odporny na dezinformację i propagandę. W kontekście wojny informacyjnej równie ważne jest kreowanie własnych narracji, opartych na prawdzie, do czego również służy technologia oraz współpraca, np. z ochotnikami z Armii Internetowej i proaktywne działanie wobec społeczeństwa rosyjskiego. Tylko taka mieszanka jest w stanie zapewnić społeczną odporność na dezinformację oraz pozwolić na dotarcie z prawdziwym obrazem wojny do mieszkańców pozostałych części świata.

## 2.3 Rozwiązania technologiczne

Budowa społecznej odporności może zostać wsparta i potencjalnie przyspieszona przez działania zewnętrzne, w tym rozwiązania technologiczne. Ważnym elementem budowania społecznej odporności jest ***fact-checking*** – na jego istotność zwracają uwagę UE oraz firmy technologiczne. Jednak ogromne ilości treści oraz danych, publikowanych w każdej chwili na samych platformach społecznościowych, sprawiają, że efektywna analiza dużej części z nich jest niemożliwa. Naprzeciwko temu problemowi wychodzą organizacje rozwijające rozwiązania technologiczne pozwalające na **automatyzację części elementów procesu *fact-checking*.** Automatyzacja jest stosowana na większości z etapów: od prób wprowadzania „*fact-checking* na żywo" oferowanego przez PolitiFact[39], który analizuje filmy wideo zawierające wypowiedzi polityków i sprawdza na bieżąco podawane przez nich informacje poprzez automatyczne porównanie ich z bazą „*fact-checków*" i wyświetlenie na ekranie sprawdzonej informacji; przez wykorzystanie SI i uczenia maszynowego do automatyzacji analizy informacji pojawiających się w serwisach informacyjnych i wyłapywania tych potencjalnie fałszywych[40]; aż po wyszukiwania w sieci pojawiających się powtórzeń informacji, które zostały już sprawdzone[41]. Technologie rozwijane na rzecz automatyzacji *fact-checking* mogą stanowić ważny element rozszerzania zasięgu tych działań i przyczynić się tym samym do rozwijania społecznej odporności



na dezinformację. Nowe rozwiązania powinny zostać oparte na SI i odpowiadać na najważniejsze wyzwania stojące przed specjalistami od *fact-checking* oraz stanowić wsparcie dla codziennych czynności przez nich wykonywanych. Można do nich zaliczyć:

- wyszukiwanie wypowiedzi lub twierdzeń wartych sprawdzenia;
- wykrywanie już wcześniej sprawdzonych informacji;
- pozyskiwanie i gromadzenie dowodów;
- automatyczny *fact-checking*.

Rozwiązania takie powinny również obejmować języki inne niż angielski, aby w ten sposób zwiększać potencjał *fact-checking* w wymiarze globalnym. Kluczowym w tym kontekście wydaje się również rozwój oprogramowania *open-source*, dostępnego dla wszystkich chętnych specjalistów od *fact-checking*, oferującego narzędzia niewymagające wiedzy technicznej, a zapewniające efektywne rezultaty oraz pracę w czasie rzeczywistym. Oczywiście automatyzacja *fact-checking* rodzi szereg zagrożeń oraz ryzyk, które muszą zostać wzięte pod uwagę. Wynikać one mogą ze stronniczości systemu, braku wyczulenia na kontekst badanych treści oraz różnorodności narzędzi, za pomocą których rozprzestrzeniana jest dezinformacja, takich jak tekst, wideo, obrazy, wypowiedzi ustne itp. Wszystkie muszą znaleźć odbicie w opracowywanych systemach.

Nowoczesna przestrzeń informacyjna coraz bardziej opiera się na technologiach cyfrowych i działaniach platform społecznościowych, które bazują na SI, przetwarzaniu *big data* oraz algorytmizacji procesów. Również mechanizmy dezinformacyjne są coraz bardziej wyrafinowane i bazują na **najnowszych technologiach, w tym SI**. Dlatego odpowiedź na te zagrożenia także powinna uwzględniać zaawansowane rozwiązania, które pozwolą na budowę bezpiecznego i opartego na zaufaniu środowiska. Technologie SI należy ująć w projektowaniu narzędzi i serwisów ekosystemu medialnego, pozwalając na szerszy dostęp do rzetelnych informacji, ułatwiając ich tworzenie i dystrybucję oraz przeciwdziałając zaawansowanym mechanizmom dezinformacji. To ostatnie zadanie może w szczególny sposób ułatwić stworzenie narzędzi opartych o SI do analizy ilościowej, zautomatyzowanej analizy sieciowej oraz zdolnych rozpoznawać treści zmanipulowane oraz typu *deep fake*. Równie istotnym zadaniem jest ujęcie technologii SI w procesie tworzenia narzędzi skierowanych do obywateli, mających na celu ułatwienie poruszania się w przestrzeni informacyjnej, identyfikacji i rozpoznawania dezinformacji oraz jej zwalczania. Rozwiązania takie powinny obejmować zautomatyzowaną analizę i śledzenie treści, porównywanie różnych źródeł informacji oraz analizę uwzględniającą kontekst badanych treści. Technologia SI może również odegrać kluczową rolę w zwalczaniu tzw. propagandy obliczeniowej (ang. *computational propaganda*), opartej na działaniu botów, trolli oraz innych zautomatyzowanych sposobów na manipulację dyskusji odbywających się na platformach społecznościowych. Przeciwdziałanie jej skupia się na wykrywaniu nieautentycznego ruchu w sieci, dlatego rozwiązania technologiczne mogą być bardziej efek-

tywne niż w przypadku prób automatyzacji oceny prawdziwości informacji. Należy natomiast zaznaczyć, że na obecnym poziomie rozwoju technologia SI służy do uzupełnienia oraz zwiększenia efektywności działań ludzi, którzy nadal są koniecznym elementem w procesie analizy dezinformacji.

Automatyczna analiza treści, szczególnie w kontekście dezinformacji, jest utrudniona ze względu na specyfikę poszczególnych języków, kontekst informacji, pojęcia ironii, sarkazmu czy satyry i potrzebę wzięcia ich wszystkich pod uwagę podczas analizy rzetelności danej informacji. Próby automatyzacji takich działań wykorzystują technologię **przetwarzania języka** naturalnego (ang. *natural language processing, NLP*). Jest to dziedzina zajmująca się automatyzacją analizy, rozumienia i tłumaczenia języka naturalnego przez systemy komputerowe, łącząca zagadnienia SI oraz językoznawstwa[42]. Przetwarzanie języka naturalnego jest już wykorzystywane do analizy *fake news* i do prób automatyzacji wykrywania fałszywych informacji oraz manipulacji. Najczęściej rozwiązania takie są oparte o analizę wzorców słownictwa, porównywanie ich oraz statystyczne badanie korelacji pomiędzy artykułami prasowymi[43]. Ich zastosowanie ma jednak spore ograniczenia, szczególnie w kontekście bardziej wyszukanych sposobów manipulacji, opierających się na używaniu półprawd, ironii itp. Dlatego potrzeba środków i możliwości rozwoju międzysektorowych projektów wykorzystania przetwarzania języka naturalnego w kontekście zwalczania dezinformacji.

Dezinformacja jest w wielu przypadkach napędzana przez **algorytmy**, które jednak mogą również posłużyć do ograniczania zasięgu nieprawdziwych i zmanipulowanych informacji. Wiele firm technologicznych podjęło działania w tym kontekście, redukując liczbę *fake news* pojawiających się na tablicach użytkowników[44]. Ponadto platformy oraz dostawcy technologii oferują rozszerzenia do przeglądarek oraz *widgety*, które ułatwiają dostęp do zweryfikowanych treści dla zwykłych użytkowników.

Wiele ryzyk związanych z dezinformacją w sieci może zostać ograniczonych za pomocą technologii ***blockchain***. System ten używa zdecentralizowanego, współużytkowanego i niezmienialnego rejestru, który ułatwia śledzenie informacji, pozwala na jej weryfikację przez każdego użytkownika i prawie całkowicie uniemożliwia zmanipulowanie informacji, która już raz została stworzona. Jego potencjał może zostać wykorzystany w zwalczaniu różnych typów dezinformacji, np. *deep fakes* oraz w budowaniu przejrzystości cyklu życia cyfrowych treści. Zastosowanie może znaleźć w śledzeniu i weryfikacji źródeł oraz samych treści, np. poprzez stworzenie rejestru rzetelnych obrazów, zdjęć, informacji oraz metadanych, które są publikowane przez danego wydawcę. Publiczny rejestr utrudniłby możliwość ich manipulacji przez aktorów dezinformujących. *Blockchain* może również posłużyć do certyfikacji i identyfikacji procesu *fact-checking*. Technologia ta oferuje pewne potencjalne rozwiązania, które mogą być elementem budowania społecznej i systemowej odporności na dezinformację.



Budowanie zdolności rozpoznawania *fake news* i podnoszenie świadomości o dezinformacji wymaga opracowania efektywnych sposobów dotarcia do osób w wieku szkolnym. Pomóc może w tym tzw. **grywalizacja**, czyli wykorzystanie gier oraz pochodzących z nich mechanizmów do edukacji. Stosowanie jej pozwala na utrzymanie wysokiego zaangażowania, budowanie nawyków i kształtowanie pożądanych zachowań oraz kreowanie pozytywnego środowiska do nauki. W kontekście dezinformacji temat ten jest stale eksplorowany, powstają nowe gry oraz komiksy i kreskówki pomagające najmłodszym oswoić się z tym zagadnieniem, a jak wskazują badania naukowe, taki sposób nauczania rzeczywiście przynosi najlepsze skutki[45]. Gry takie jak Get Bad News, w której gracze wcielają się w rolę twórców *fake news*, aby poznać mechanizmy stojące za nimi[46], *Fake News: The Game*, w której gracze mają za zadanie odróżnić prawdziwe wiadomości od fałszywych[47], czy *Fake It To Make It*, pokazujące jak osoby rozprzestrzeniające dezinformację na niej zarabiają[48], to tylko mała część z dostępnych obecnie gier podejmujących problematykę dezinformacji. Rozwój interesujących i merytorycznych gier wymaga jednak nakładów finansowych, dostępu do technologii oraz wiedzy eksperckiej.

## 2.4 Inne obszary budowania odporności społecznej

Poza elementami technologicznymi warto podkreślić potrzebę inwestycji oraz wsparcia innych obszarów budowania odporności społecznej. Wśród najważniejszych należy wymienić:

- Rozwój edukacji medialnej i nauki o krytycznym myśleniu oraz wprowadzenie jej do programów nauczania na każdym etapie edukacji publicznej.
- Prowadzenie kampanii społecznych podkreślających wagę problemu i prezentujących mechanizmy stojące za dezinformacją.
- Promowanie współpracy międzysektorowej i uwzględnienie społeczeństwa obywatelskiego oraz organizacji pozarządowych w procesie edukacji i szkoleń z obszaru dezinformacji.
- Stosowanie tzw. *pre-bunking*, czyli promowania rzetelnych i sprawdzonych informacji w kontrze do popularyzujących się *fake news*. W taki sposób użytkownik staje się odporny na manipulacje i fałszywe wiadomości, na które może natknąć się później. Jest to swego rodzaju „szczepienie" na dezinformację i jest promowane w kontrze do żmudnego i mało wydajnego *fact-checking*.
- Finansowanie międzysektorowych badań nad dezinformacją i sposobami jej przeciwdziałania. Proces ten powinien obejmować ekspertów, badaczy, naukowców, sektor publiczny oraz prywatny. Badania nad dezinformacją wymagają zastanowienia się nad różnymi czynnikami: technologicznymi, psychologicznymi, społecznymi, ekonomicznymi itp. Dlatego kluczowe jest rozwijanie badań obejmujących wszystkie z nich.
- Rozwijanie nowych technologii z uję-ciem tzw. *human-based approach*, uwzględniającym prawa człowieka, inkluzywność oraz bezpieczeństwo użytkownika już na etapie ich produkcji.

Budowa społecznej odporności na dezinformację jest jedynym sposobem na efektywną walkę z dezinformacją oraz powiązanymi z nią zagrożeniami. Musi ona obejmować zarówno edukację, działania legislacyjne, regulacje rynku prywatnego, inicjatywy biznesowe, rozwój nowych technologii oraz działania organizacji pozarządowych i eksperckich. Rozumie to UE, która w ostatnich latach rozwinęła działania w każdym z tych obszarów i podjęła kooperację z wymienionymi wyżej sektorami oraz państwami członkowskimi. Jednym z kluczowych elementów budowania społecznej odporności jest wykorzystanie nowych technologii do rozwoju rozwiązań i wdrożeń przydatnych w różnych jej obszarach: edukacji, *fact-checking*, korzystania z platform oraz zarządzania nimi. We wszystkich z nich ten proces już się rozpoczął, istnieje wiele inicjatyw związanych z użyciem najnowszych technologii w tym kontekście i wprowadzających w życie wymienione w tym rozdziale ich sposoby zastosowania. Jest to jednak dopiero początek procesu budowy odporności społecznej, która wymaga dalszego rozwoju, finansowania oraz badań, nie tylko w obszarze nowych technologii. Warto zaznaczyć, że nie jest możliwe pełne oparcie walki z dezinformacją na rozwiązaniach technologicznych. Te mogą być jedynie uzupełnieniem działań człowieka oraz wspierać poszczególne elementy szerokiego podejścia do problemu, jaki prezentuje społeczna odporność na dezinformację.



# 3. SIEDEM PODSTAWOWYCH WYMOGÓW NATO DOTYCZĄCYCH ODPORNOŚCI

**Izabela Albrycht, Łukasz Gawron, Maciej Góra, dr Michał Hampel, Sławomir Łazarek**

Ponieważ najbliższa dekada będzie czasem, w którym bezpieczeństwo stanie się nadrzędnym priorytetem rządów, mającym wpływ na kształt pozostałych polityk publicznych, to przede wszystkim warto przyjrzeć się celom odporności wyznaczonym przez NATO na szczycie w Warszawie. Szefowie państw i rządów zobowiązali się do wzmacniania odporności[49], w szczególności poprzez działania na rzecz spełnienia przez poszczególne państwa członkowskie **siedmiu bazowych wymogów dotyczących odporności** (7 Baseline Requirements).

Komitet Planowania Cywilnego NATO (CEPC) opracował zestaw kryteriów

**Siedem bazowych wymogów NATO dotyczących odporności***

**1. Ciągłość działania administracji i kluczowych procesów państwa** (zdolność do utrzymania procesu decyzyjnego państwa w czasie narastającego kryzysu, w tym polityczno-militarnego).

**2. Zaopatrzenie w energię** np.: plany awaryjne i zapasowe źródła energii (wewnętrzne/krajowe oraz zewnętrzne/zagraniczne).

**3. Zdolność do reagowania na masowe niekontrolowane migracje** np.: zdolność do dekonfliktacji przemieszczeń uchodźców z przemieszczeniami sił zbrojnych.

**4. Zaopatrzenie w wodę i żywność** np.: zapewnienie zasobom żywnościowym ochrony przed zakłóceniami i sabotażem.

**5. Zdolność do reagowania na zdarzenia z dużą liczbą ofiar** np.: zapewnienie wydolności cywilnego systemu służby zdrowia w przypadku dużych ilości poszkodowanych, łącznie z zapasami środków zaopatrzenia medycznego.

**6. Zapewnienie cywilnej łączności** np.: zapewnienie ciągłości pracy systemów łączności i telekomunikacyjnych w sytuacjach kryzysowych, łącznie z adekwatnym stanem środków zapasowych.

**7. System transportu** np.: zapewnienie swobody przemieszczania się sił zbrojnych (w tym VJTF czyli tzw. szpica), odporne na zakłócenia systemy informatyczne wspierające funkcjonowanie sytemu transportowego państwa.

* https://www.nato.int/cps/en/natohq/topics_132722.htm [online: 30.06.2022].

ewaluacji[50] dla każdego z siedmiu wymogów, aby ujednolicić metodologię oceny stanu realizacji wytycznych sojuszniczych i ogólnej odporności krajów członkowskich. Grupy robocze NATO CEPC wspierają państwa członkowskie, opracowując te wytyczne. Celem raportu będzie dokonanie analizy zastosowania technologii cyfrowych na rzecz wzmocnienia odporności w siedmiu obszarach i na tej podstawie wypracowanie rekomendacji wskazujących na możliwości wykorzystania zdobyczy cyfryzacji do budowania odporności.

### 3.1 Ciągłość działania administracji i kluczowych procesów państwa

Izabela Albrycht, Maciej Góra

Na liście siedmiu bazowych wymagań, które zobowiązały się spełnić państwa NATO, na pierwszym miejscu znajduje się **„ciągłość działania administracji i kluczowych procesów państwa".**

Ciągłość sprawowania władzy jest skoordynowanym wysiłkiem w ramach władzy wykonawczej, ustawodawczej i sądowniczej, mającym na celu zapewnienie zarządzania i realizacji podstawowych funkcji państwa, kontynuowanych przed, w trakcie i po wystąpieniu sytuacji kryzysowej[51]. Zagadnienie zapewnienia ciągłości władzy państwowej oraz administracji jest pojęciem szerokim oraz wielowymiarowym. W Stanach Zjednoczonych podstawą ciągłości działania państwa, tworzoną przez zapewnienie ciągłości operacji (ang. *continuity of operations*), ciągłości sprawowania władzy (ang. *continuity of government*) oraz ciągłości trwania konstytucyjnego rządu (ang. *continuity of constitutional government*), są narodowe funkcje kluczowe (ang. *national essential functions*), obejmujące osiem zagadnień: zachowanie konstytucyjnego rządu, zapewnienie widocznego przywództwa, obrona kraju, utrzymanie stosunków międzynarodowych, obrona ojczyzny, reagowanie kryzysowe oraz odbudowa, utrzymanie stabilnej gospodarki oraz zapewnienie funkcjonowania krytycznych usług rządowych[52]. Plany warunkujące wypełnianie zadań z obszaru zadań działalności statutowej w administracji publicznej w czasach kryzysu powinny być tworzone, ćwiczone oraz rewidowane na poziomie nie tylko centralnym, lecz również samorządowym oraz lokalnym i odznaczać się elastycznością oraz skalowalnością, pozwalającymi odpowiedzieć na zagrożenia o różnej formie i zasięgu oraz w różnych miejscach oddziaływania. Podstawą tworzenia takich planów jest identyfikacja, analiza i ewaluacja ryzyka oraz oceny odporności na nie **w wymiarze logistycznym, finansowym, kadrowym, informacyjnym, czasowym i jakościowo-efektywnościowym**[53].

Aby sprostać wielowymiarowości procesu budowy odporności, jednym z najważniejszych narzędzi pomagających tworzyć plany zarządzania kryzysowego są modele oraz symulacje, kreujące scenariusze rozwoju danych sytuacji zagrożeń i pozwalające je testować. W rozumieniu tym modele są abstrakcyjnymi opisami obiektów z uwzględnieniem ich cech charakterystycznych, zaś symulacje to obliczenia ich wartości oraz wizualizacji wyników przy użyciu komputera[54]. Połączenie modelowania oraz symulacji pozwala na zmniejszenie zapotrzebowania na ręczną analizę, pozwalając przeprowadzać różne scenariusze sytuacji o zmiennych parametrach i w efekcie, po ich analizie, przygotować odpowiednie plany działań. Modelowanie i metodologia statystyczna są szeroko stosowane przez władze państwowe na całym świecie w celu wspierania decyzji operacyjnych i politycznych rządu podejmowanych w złożonych środowiskach[55], takich jak finanse, energetyka, logistyka i transport. Ważnym przypadkiem wykorzystania tych technologii w zakresie zachowania ciągłości władzy jest modelowanie biologiczne, z zakresu wirusologii i przenoszenia się chorób, które zyskało na znaczeniu w czasie epidemii SARS-CoV-2 i służyło wielu państwom do kreowania polityk publicznych w dobie kryzysu pandemicznego. Elementami składowymi modelowania i symulacji, które pozwalają na tworzenie odpowiednich scenariuszy, są technologie takie jak Internet Rzeczy (ang. *Internet of Things*), ekstrapolowane z nich big data oraz odpowiedzialne za ich przetworzenie algorytmy SI.

W odniesieniu do czynników warunkujących planowanie i odpowiedź na kryzys jasna staje się centralna rola zarządzania (rozumianego jako proces decyzyjny, w tym przypadku przebiegający pod presją czasu) w sytuacjach wymagających przywrócenia ciągłości działania administracji państwowej. Z kolei w procesie zarządzania kluczową rolę odgrywają zasoby informacyjne oraz możliwości ich gromadzenia, przetwarzania oraz odtworzenia, które należy uznać za strategiczny atrybut systemów bezpieczeństwa oraz część składową systemów infrastruktury krytycznej[56]. Dane te powinny być odpowiednio chronione przed nieuprawnionym dostępem, kradzieżą, modyfikacją oraz zniszczeniem. Dlatego też w polskim Narodowym Programie Ochrony Infrastruktury Krytycznej za system zapewniający ciągłość działania administracji publicznej (podobnie jak system łączności oraz system sieci teleinformatycznych) odpowiedzialny jest minister właściwy do spraw informatyzacji[57]. Kluczowym czynnikiem zachowania integralności danych jest więc cyberbezpieczeństwo i najnowsze rozwiązania w tym zakresie.

Jednocześnie zasoby państwa w postaci cyfrowej, zwłaszcza te, od których zależy funkcjonowanie kluczowych obszarów państwa (bezpieczeństwo wewnętrze i zewnętrzne, finanse publiczne, ubezpieczenia społeczne, opieka zdrowotna, łączność, energetyka), należy chronić także przed fizycznymi zagrożeniami. Ten wymiar odporności jako zabezpieczenia ciągłości cyfrowej państwa stał się krytycznym elementem bezpieczeństwa i suwerenności państwa, zwłaszcza w świetle ataku zbrojonego Rosji na Ukrainę i zagrożenia jego dalszą eskalacją teraz lub w przyszłości. Dominujący, militarny wymiar konfliktu, przypomniał decydentom, że odporność musi także uwzględniać aspekt fizycznego zabezpieczenia danych i elementów infrastruktury cyfrowej. Dlatego coraz więcej krajów zadaje sobie pytanie, jak zabezpieczyć centra danych przechowujące cyfrowe rejestry państwowe oraz kluczowe dane cyfrowe o istotnym znaczeniu dla gospodarki i administracji na wypadek zagrożeń militarnych, takich np. jak-

**CASE STUDY**

Jak ważną rolę w zachowaniu ciągłości administracji publicznej odgrywa chmura, dowiodły wydarzenia w Ukrainie mające miejsce pod koniec lutego 2022 r., przytoczone w raporcie Microsoft *Defending Ukraine: Early Lessons from the Cyber War*. Przed wojną ukraińskie Prawo Ochrony Danych zabraniało władzom państwowym gromadzenia oraz przetwarzania danych w chmurach pozarządowych, co oznaczało, że infrastruktura cyfrowa państwa gromadzona była na serwerach umieszczonych w budynkach rządowych. Dostrzegając ich podatność na działania zarówno kinetyczne, jak i cybernetyczne, na tydzień przed pełnoskalową eskalacją konfliktu ukraiński parlament przegłosował poprawkę pozwalającą na migrację danych do chmury publicznej. W ciągu 10 tygodni przeniesiono krytyczne dane oraz procesy ponad 20 ministerstw oraz 100 agencji państwowych i firm państwowych. Uchroniło je to przed zniszczeniem, gdyż jednym z wczesnych celów ataków rakietowych oraz cybernetycznych (z użyciem *malware* typu *wiper*, a więc mającego destrukcyjne cele) Rosjan były właśnie rządowe centra danych Ukrainy[58]. Jak twierdzi Heorhij Dubyńskyj, Wiceminister Transformacji Cyfrowej Ukrainy, od początku wojny przeniesiono ponad 150 rejestrów państwowych do chmury[59]. Ukraina podpisała także umowę z Wielką Brytanią o współpracy pomiędzy Archiwum Państwowym Służby Ukrainy a Archiwum Państwowym Zjednoczonego Królestwo w sprawie tymczasowego przeniesienia przechowywania danych w chmurze oraz cyfrowych kopii zapasowych archiwów państwowych państwa ukraińskiego na wypadek ich ewentualnej utraty[60].

atak rakietowy albo inne zdarzenia ze skutkami fizycznymi. Należy przy tym założyć, że zagrożenie bezpieczeństwa i integralności danych zlokalizowanych fizycznie wyłącznie na terenie krajów znajdujących się w bliskim sąsiedztwie Ukrainy utrzyma się co najmniej tak długo, jak długo Federacja Rosyjska realizować będzie imperialistyczną i rewizjonistyczną linię geopolityczną. Za równie ważne niebezpieczeństwo należy także uznać katastrofy naturalne wynikające z postępujących zmian klimatu. W tym kontekście na uwagę zasługuje **idea „ambasady danych”**. Jest to bezpieczny ośrodek przechowywania kluczowych danych państwowych, w tym kopii kluczowych rejestrów państwowych na wypadek uszkodzenia lub utraty danych przetwarzanych w kraju. Takie ambasady i zgromadzone w nich dane oraz infrastruktura, w której byłyby one przechowywane, powinny podlegać jurysdykcji swoich krajów, być objęte tymi samymi gwarancjami prawnymi, co dane i serwery w krajach rodzimych, i być zlokalizowane poza potencjalnym teatrem działań wojennych[61]. Specjalnie zabezpieczone centrum danych, zintegrowane z chmurą rządową, zlokalizowane na podstawie ratyfikowanej umowy międzynarodowej w Luksemburgu posiada już Estonia. Są w nim przechowywane zaszyfrowane kopie zapasowe danych cyfrowych państwa na wypadek ataku – cyfrowego i fizycznego.

Innym sposobem gromadzenia, przetwarzania i odtwarzania danych, który może w znaczący sposób wpłynąć na budowanie odporności państw – rozumianej zarówno klasycznie, jak i w kontekście budowania cyberodporności – w zakresie ciągłości działania administracji państwowej podczas kryzysu, jest ewakuacja (odmiejscowienie) rejestrów państwowych do chmury obliczeniowej. Według definicji amerykańskiego Krajowego Instytutu Norm i Technologii (National Institute of Standards and Technology), chmury obliczeniowe to model umożliwiający wszechobecny, wygodny, sieciowy dostęp na żądanie do współdzielonej puli konfigurowalnych zasobów obliczeniowych, które są dostępne w sieci[62]. Rozwiązanie takie pozwala na rezygnację z inwestycji w określone aktywa fizyczne, takie jak serwery, oraz elastyczny dostęp do usług technologicznych, co ma kluczowe znaczenie w wypadku wystąpienia zagrożeń mogących potencjalnie przerwać ciągłość działania administracji państwowej.

Innym ważnym elementem składowym budowania cyberodporności jest tzw. *panic button*, czyli przycisk alarmowy. Rozwiązanie takie powinno być stosowane w sytuacjach zagrożenia bądź niemożności pełnienia funkcji przez urzędników państwowych i spełniać kilka funkcji: alarmować odpowiednie osoby oraz służby o kryzysowej sytuacji i namierzać pozycję poszkodowanego, uruchamiać proces zapewnienia ciągłości funkcjonowania administracji państwowej poprzez wdrożenie w życie planów reagowania kryzysowego, a także rozpocząć procedurę szyfrowania i przenoszenia danych znajdujących się w posiadaniu osoby korzystającej z tej usługi. Przyciski powinny funkcjonować w ramach sieci internetowych, korzystając z systemów ochrony przesyłu danych takich jak szyfrowanie *end-to-end,* oraz niezależnie od nich, np. poprzez fale radiowe. Przyciski alarmowe powinny zostać zintegrowane z aplikacjami wspomagającymi proces decyzyjny w przypadku wystąpienia sytuacji kryzysowych.

Jednym z podstawowych zabezpieczeń przed utratą ciągłości działania administracji państwowej jest również przygotowanie alternatywnych lokalizacji funkcjonowania komórek państwowych. Zabezpieczenie takie pozwala na natychmiastowe wznowienie działań w wypadku zaistnienia katastrofy[63]. Lokalizacje te powinny być zarówno fizyczne, wyposażone w sprzęt pozwalający na realizację statutowych działań (agregaty prądotwórcze, sprzęt teleinformatyczny, dostęp do Internetu itp.), jak również wirtualne, pozwalające na zdalną koordynację działań z dowolnego miejsca. Te ostatnie powinny też być silnie zabezpieczone przed potencjalnymi naruszeniami integralności.

## 3.2 Zaopatrzenie w energię

Łukasz Gawron

Usługi zapewniające dostęp społeczeństwa do stabilnych źródeł energii należą do najbardziej wrażliwych części infrastruktury krytycznej. Dzisiejsza gospodarka opiera się na stabilnych dostawach

energii elektrycznej, gazu czy ropy naftowej i jakiekolwiek zakłócenie dostaw może spowodować katastrofalne skutki dla społeczeństwa, gospodarki i bezpieczeństwa państwa. Zapewnienie bezpieczeństwa instalacjom dystrybuującym lub przetwarzającym kluczowe zasoby energetyczne jest zatem priorytetem. W dobie cyfryzacji oprócz kwestii związanych z bezpieczeństwem fizycznym i odpowiednim zabezpieczeniem infrastruktury przed katastrofami naturalnymi, zamachami terrorystycznymi czy działaniami wojennymi coraz bardziej istotna staje się kwestia bezpieczeństwa teleinformatycznego.

Wyraz troski o odpowiednie zabezpieczenie infrastruktury energetycznej widać na przykładzie przyjętych na poziomie unijnym regulacji. Dyrektywa NIS wyznacza środki mające na celu osiągnięcie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych wśród Operatorów Usług Kluczowych. Każde przedsiębiorstwo zidentyfikowane jako Operator Usługi Kluczowej przez dane państwo musi wdrożyć odpowiednio wysoki poziom cyberbezpieczeństwa w organizacji, aby zapobiegać incydentom, w odpowiedni sposób na nie reagować oraz przede wszystkim zachować ciągłość działania i odbudować ich funkcjonowanie[64]. W polskim prawodawstwie większość dużych przedsiębiorstw zajmujących się zaopatrzeniem w energię należy do katalogu Operatorów Usług Kluczowych i ustawa o Krajowym Systemie Cyberbezpieczeństwa z 2018 r. (jako implementacja Dyrektywy NIS) nakłada na nich stosowne obowiązki w obszarze wzmacniania zdolności cyberbezpieczeństwa[65]. Ponadto Ustawa o zrządzaniu kryzysowym z 2007 r. identyfikuje systemy zaopatrzenia w energię, surowce energetyczne i paliwa, jako część infrastruktury krytycznej[66]. Powyższe przykłady pokazują, że działania za poziomie unijnym i poszczególnych państw członkowskich z jednej strony przykładają szczególną wagę do ochrony zaopatrzenia w energię, z drugiej zaś coraz częściej wymuszają na nich położenie większego nacisku na bezpieczeństwo teleinformatyczne. W kontekście budowania cyberodporności organizacji zajmujących się zaopatrzeniem w energię możemy wyróżnić dwie płaszczyzny: technologiczną oraz organizacyjną.

Sfera technologiczna odnosi się do kwestii wdrażania odpowiednich rozwiązań cyberbezpieczeństwa, podnoszących ogólną odporność systemów teleinformatycznych w organizacji. Może odnosić się to zarówno do fizycznego sprzętu (*hardware*), jak i oprogramowania (*software*). Należy jednak zaznaczyć, że przedsiębiorstwa energetyczne oprócz korzystania z klasycznie rozumianej infrastruktury IT w dużej mierze opierają się na systemach automatyki przemysłowej (OT). Warstwy IT i OT działają komplementarnie, więc istotnym zagadnieniem, o którym nie można zapomnieć, jest monitorowanie bezpieczeństwa na styku systemów IT (czyli warstwy biznesowej) z OT (warstwy przemysłowej)[67].

Rozwiązania budujące cyberodporność w sektorze energetycznym nie będą znacząco różniły się od innych rozwiązań stosowanych w przedsiębiorstwach innego sektora. Spośród nich można wyróżnić pewne tematy, które w szczególnym stopniu należy wdrożyć, aby uwzględnić cyberbezpieczeństwo,



**CASE STUDY**

Systemy klasy IDS (Intrusion Detection System) są rozwiązaniami przeznaczonymi do monitoringu sieci IT oraz mogą z powodzeniem spełniać swoją rolę w OT. Nowoczesne sondy wyróżniają się zastosowaniem dedykowanych modeli predykcyjno-analitycznych, które dostosowują się do każdej konfiguracji sieci z wykorzystaniem metod *machine learning* i SI, dzięki czemu jest w stanie poprawnie wykryć anomalie i zagrożenia w sieci. Narzędzie to jest w stanie monitorować, wykrywać, inwentaryzować i raportować o nawet najbardziej zaawansowanych atakach przepuszczanych na przedsiębiorstwa[68]. Narzędzia tego typu mogą mieć zastosowanie w szczególności w przedsiębiorstwach, które swoją działalność opierają na systemach automatyki przemysłowej. Do tego katalogu zalicza się duża część infrastruktury krytycznej, w szczególności transportu, energetyki czy zaopatrzenia w wodę pitną.

np. bezpieczeństwo i monitorowanie infrastruktury sieciowej, ochrona urządzeń końcowych, segmentacja sieci i szyfrowanie, bezpieczeństwo dostępu zdalnego czy bezpieczeństwo stacji roboczych. W szczególnym stopniu natomiast należy zadbać o bezpieczeństwo instalacji OT, które ze względu na swoją specyfikę wymagają zastosowania innego podejścia do kwestii bezpieczeństwa, a co za tym idzie innych technologii wzmacniających odporność.

Szczególną kwestią zyskującą w ostatnim czasie na znaczeniu jest bezpieczeństwo na styku sieci IT i OT. Oczywiste jest, że IT i OT działają inaczej oraz mają różne cele i ryzyka. Ponieważ jednak systemy cyfrowe będą łączyć się z systemami przemysłowymi, to jednocześnie będą narażone na więcej cyberzagrożeń. Eksperci branżowi przewidują, że IT-OT będzie w dalszym ciągu zbliżać się do siebie. Oznacza to, że administratorzy OT powinni dołożyć wszelkich starań, aby zrozumieć środowisko IT i odwrotnie[69]. Nowe technologie mogą wspierać oba te środowiska, a jednym z innowacyjnych rozwiązań w tym zakresie są sondy monitorujące zagrożenia w sieci przemysłowej.

Budowania cyberodporności nie można jednak oprzeć tylko na kwestiach technologicznych. W kontekście budowania odporności sektora energii, jak i w każdym innym sektorze, istotnym aspektem są kwestie bezpieczeństwa organizacyjnego. Przez bezpieczeństwo organizacyjne rozumie się konkretne polityki bezpieczeństwa informacji, organizacje zarządzania systemem cyberbezpieczeństwa, metodyki szacowania ryzyka, procesy czy niskopoziomowe budowanie kultury cyberbezpieczeństwa w organizacji. Nawet najlepsze i najnowocześniejsze technologie nie będą w stanie powstrzymać ataku i umocnić organizacji, jeśli nie będą odpowiednio zarządzane, a ludzie odpowiedzialni za bezpieczeństwo nie zostaną odpowiednio przeszkoleni i nie będą mieli odpowiednio przypisanych ról. Dlatego bez-

pieczeństwo technologiczne zawsze powinno iść w parze z wdrożeniami organizacyjnymi, a pracowników odpowiedzialnych za ten obszar trzeba regularnie szkolić. Pomocne w budowaniu odporności organizacyjnej mogą być międzynarodowe standardy i ramy, jak:

- ISO27001 – zawiera wymagania dla systemu zarządzania bezpieczeństwem informacji (SZBI); korzystanie z niego umożliwia organizacjom wszelkiego rodzaju zarządzanie bezpieczeństwem aktywów, takich jak dane pracowników, dane powierzone przez strony trzecie czy własność intelektualna[70].
- NIST 800-82 – zawiera wskazówki dotyczące bezpieczeństwa systemów przemysłowych (ang. Industrial Control Systems, ICS)[71].
- ISO 22301 – opisuje strukturę i wymagania dotyczące wdrażania i utrzymywania systemu zarządzania ciągłością działania[72].

Kwestia zaopatrzenia w energię musi cechować się jeszcze jedną istotną i kluczową właściwością, mianowicie ciągłością działania i odbudową po jej zakłóceniu. W tym kontekście priorytetowe z punktu widzenia dostawców energii jest stworzenie planu ciągłości działania obejmującego m.in. opracowanie procedur wraz ze zdefiniowaniem zakresu odpowiedzialności, opracowanie procedur odtworzenia procesów kluczowych, identyfikacji kluczowych systemów informatycznych, a także stworzenie odpowiednich procedur komunikacji[73]. Szczególnie pomocną technologią w kontekście zachowania ciągłości działania i odbudowy po katastrofie są rozwiązania chmurowe. Odzyskiwanie ciągłości działania po awarii w chmurze to połączenie strategii adaptacji chmury i usług przeznaczonych do tworzenia kopii zapasowych danych, aplikacji i innych zasobów w chmurze publicznej lub usługodawcach dedykowanych. W przypadku wystąpienia katastrofy dane, aplikacje i inne zasoby, których ona dotyczy, można przywrócić do lokalnego centrum danych – lub dostawcy chmury – i wznowić normalne działanie w przedsiębiorstwie[75].

**CASE STUDY**

*Cloud disaster recovery* (CDR) to usługa, która pozwala na przetwarzanie, przechowywanie i odzyskiwanie danych systemowych na zdalnej platformie opartej na chmurze. Odzyskiwanie danych w oparciu o chmurę obliczeniową ma kilka istotnych przewag nad klasycznym odzyskiwaniem danych *on premise*:

- Nie trzeba kupować fizycznego sprzętu i oprogramowania do obsługi krytycznych operacji.
- CDR jest łatwo skalowalny w zależności od potrzeb.
- Jest efektywniejszy cenowo.
- Odzyskiwanie po awarii w chmurze obliczeniowej można przeprowadzić w ciągu kilku minut z dowolnego miejsca – potrzebne jest jedynie urządzenie podłączone do Internetu.
- Kopie zapasowe można przechowywać w wielu centrach danych rozsianych po całym świecie.
- Wszelkie problemy lub błędy mogą być szybko zidentyfikowane i usunięte przez dostawcę chmury[74].

## 3.3 Zdolność do reagowania na masowe niekontrolowane migracje

Łukasz Gawron

Sytuacje kryzysowe takie jak katastrofy naturalne czy konflikty zbrojne każdorazowo wywołują niekontrolowane migracje wewnętrzne lub międzynarodowe. W szczególności w dobie konfliktu zbrojnego kluczowa dla budowania odporności i bezpieczeństwa państwa i ich obywateli jest świadomość postępowania na wypadek sytuacji kryzysowej. Odpowiednio przygotowane i przede wszystkim rozdystrybuowane informacje o punktach zbiórek, schronach, szlakach migracji etc. pozwolą zbudować świadomość wśród społeczeństwa i wykształcą dobre praktyki dotyczące zachowań w sytuacjach kryzysowych. Odpowiednia edukacja może pomóc w sprawniejszym zarządzaniu kryzysowym i zminimalizować ryzyko zagrożeń i niekontrolowanego przemieszczania się ludności.

W dobie postępu technologicznego i powszechnego dostępu do Internetu idealnym kanałem komunikacji i edukacji są media społecznościowe. Jednymi z kluczowych czynników determinujących newralgiczną rolę mediów społecznościowych oprócz powszechnego dostępu są również szybkość rozprzestrzeniania się informacji, stale rosnąca liczba użytkowników oraz mnogość kanałów komunikacji. Media społecznościowe pozwalają również na ciągłą komunikację dwustronną oraz śledzenie komunikatów 24/7[76]. Należy jednak pamiętać o istotnym zagrożeniu będącym niejako efektem ubocznym specyfiki mediów społecznościowych, czyli dezinformacji. Dlatego tak ważna jest konieczność budowania odporności społecznej, o której mowa w rozdziale 2. Budowanie odporności w kontekście niekontrolowanych migracji musi zaczynać się od edukacji. Technologia będąca kanałem dystrybucji informacji jest tylko narzędziem, które bez odpowiedniej świadomości może przynieść skutek odwrotny do zamierzonego.

**CASE STUDY**

Wojna ukraińsko-rosyjska spowodowała migrację uchodźców do państw ościennych, w tym głównie Polski, Słowacji, Węgier, jak również Czech. Ambasada Ukrainy w Czechach na początku wojny i kryzysu uchodźczego wraz z partnerem biznesowym stworzyła dla obywateli Ukrainy wirtualnego asystenta, który pomagał tysiącom uchodźców przybywającym do Czech w kwestiach związanych z rejestracją, wizą, zatrudnieniem, podróżami czy usługami prawniczymi[77]. Wirtualni asystenci i chatboty stały się popularnym narzędziem wspierającym obsługę dużej ilości ludzi w krótkim czasie, co znacznie upraszczało kwestie formalne związane z pobytem w obcym kraju.

**CASE STUDY**

Polski rząd kilka tygodni po agresji Rosji na Ukrainę umożliwił uchodźcom zdobycie numeru PESEL, który uprawnia m.in. do świadczeń zdrowotnych czy do podjęcia nauki w Polsce[78]. Dodatkowo polski rząd porozumiał się z Ministerstwem Transformacji Cyfrowej Ukrainy i udostępnił uchodźcom możliwość integracji ukraińskiej mobilnej aplikacji rządowej Diia z polską aplikacją e-gov mObywatel. Dzięki temu partnerstwu ukraińscy uchodźcy mają dostęp do swojego cyfrowego portfela również w Polsce i mogą w pełni korzystać z funkcjonalności Diia[79].

Sytuacje kryzysowe, w tym wojny, zawsze wywołują skutek w postaci niekontrolo wanej migracji wewnętrznej i międzynarodowej ludności. Dla służb i aparatu państwowego jest to ogromne wyzwanie, które jednak może być wspierane nowymi technologiami. Innej natury wyzwaniem dla administracji rządowej i samorządowej w kontekście napływu migrantów bądź uchodźców są kwestie włączenia ich w krajową administrację, tak aby w jak najkrótszym czasie mogli korzystać z usług publicznych dostępnych w danym kraju – urzędów, służby zdrowia, transportu zbiorowego etc. Ponadto ewidencja osób przybywających do danego kraju jest również kwestią bezpieczeństwa, dlatego też istotnym elementem jest prowadzenie odpowiednich rejestrów. Nie każdy obywatel ma dostęp do Internetu w każdym miejscu. Dlatego też informacje rządowe płynące do obywateli w czasie kryzysu lub przygotowujące ich na sytuacje ekstremalne powinny być dystrybuowane także innymi kanałami mediów masowych, czyli radiem, telewizją, jak również SMS-ami.

**CASE STUDY**

Alert RCB – jest to SMS-owy system ostrzegania przed zagrożeniami obsługiwany przez Rządowe Centrum Bezpieczeństwa. Wdrożony w 2018 r. system ma za zadanie informować obywateli kraju lub danego regionu o potencjalnych zjawiskach zagrażających życiu jak katastrofy naturalne. Każdy obywatel posiadający działający i podłączony do sieci telekomunikacyjnej telefon otrzymuje informację o zjawiskach ekstremalnych z krótkimi wskazówkami, co powinien w danej chwili zrobić. Taki system nie wymaga połączenia z Internetem czy ściągnięcia aplikacji[80]. Tak prosty system może zostać wykorzystany również podczas konfliktu zbrojnego i spowodowanej nim niekontrolowanej migracji. Poprzez proste komunikaty SMS służby oraz administracja rządowa mogą informować obywateli o miejscu schronienia, dostępnych w danym regionie usługach czy wskazówkach na temat formalności związanych np. z przekroczeniem granicy.



### 3.4 Zaopatrzenie w wodę i żywność

Maciej Góra

Problemy z dostępem do wody oraz żywności nie są wyzwaniami, z którymi rozwinięte społeczeństwa musiały radzić sobie w ostatnich dekadach. Jednak wzrost napięć na arenie międzynarodowej, zmiany klimatu, rosnąca populacja oraz gwałtowna transformacja cyfrowa doprowadziły do ponownego wzrostu zagrożeń niedoboru tych podstawowych dóbr, których dostępność jest jednym z elementów infrastruktury krytycznej.

W ostatnich latach zaobserwować można było ataki cybernetyczne wymierzone przeciw producentom żywności, z których najgłośniejszy przypadek wymierzony był przeciwko firmie JBS S.A., największemu dostawcy mięsa na świecie. *Malware* typu *ransomware* (oprogramowanie szantażujące), którego użyto do ataku, zatrzymał produkcję w Stanach Zjednoczonych, Kanadzie oraz Australii, zaś firma w celu odblokowania systemów musiała wypłacić 11 milionów dolarów w kryptowalucie Bitcoin[81]. Systemy uzdatniania wody również były celami ataków. Przykładowo, w 2021 r. haker uzyskał dostęp do sieci placówki uzdatniającej wodę w Oldsmar w stanie Floryda i próbował zatruć zasoby wodne, zwiększając ilość cząsteczek wodorotlenku sodu (ługu) ze 100 cząsteczek na milion do 11 100 cząsteczek na milion. Próba ta została udaremniona przez operatora zanim toksyczny poziom substancji przedostał się do wody[82]. Amerykańskie Stowarzyszenie Wodociągów (American Water Works Association) w 2019 r. nazwało cyberryzyko zagrożeniem numer jeden dla amerykańskiego sektora wodnego i z pewnością można stwierdzić, że podobne zagrożenia istnieją również w Europie.

Omawiane elementy infrastruktury krytycznej są szczególnie narażone na cyberataki ze względu na swoją specyfikę. Woda oraz żywność to fundamentalne zasoby, których brak bądź skażenie dotyka nie tylko użytkowników końcowych, ale także całe łańcuchy dostaw. Bez uzdatnionej wody niemożliwa jest nie tylko produkcja żywności na masową skalę, ale też produkcja w sektorach przemysłowych, chemicznych, energetycznych, funkcjonowanie usług zdrowotnych i ratunkowych i wielu innych gałęzi gospodarki i krytycznych usług publicznych. Jednocześnie utrudnienie dostępu do wody pitnej w okresie letnim naraża nie tylko plony i zwierzęta gospodarcze, lecz również życie i zdrowie ludzi. Z kolei przerwy w dostarczaniu podstawowych produktów żywieniowych, takich jak zboża, wpływają na dostępność pasz, a więc również produktów mięsnych i nabiałowych. Jednocześnie te obszary są szczególnie podatne w konkretnych okresach czasowych – w przypadku przemysłu żywieniowego zhakowanie inteligentnych systemów rolniczych w okresie siewów bądź zbiorów skutkować będzie niedoborami produktów rolniczych przez cały rok, przynosząc katastrofalne skutki dla całej gospodarki i bezpieczeństwa żywieniowego. Wreszcie istnieją również „klasyczne" problemy tego obszaru infrastruktury krytycznej, na które mogą odpowiedzieć technologie cyfrowe – takie jak marnotrawienie żywności, odwołania skażonych partii produktów, niska wydajność

części rolnictwa, problemy logistyczne i transportowe czy te związane ze zmianami klimatycznymi. Technologie te wykorzystywane są w procesie Zarządzania Ryzykiem Łańcuchów Dostaw (ang. *Supply Chain Risk Management*, SCRM) obejmującym szeroki wachlarz strategii mających na celu identyfikację, ocenę, łagodzenie i monitorowanie nieoczekiwanych zdarzeń lub warunków, które mogą mieć wpływ, najczęściej niekorzystny, na dowolną część łańcucha dostaw[83].

Jednym z najszerzej użytkowanych rozwiązań w zakresie bezpieczeństwa żywnościowego jest technologia *blockchain*. *Blockchain* to cyfrowy, zdecentralizowany i rozproszony rejestr, który zapisuje i dodaje transakcje w porządku chronologicznym w celu stworzenia trwałych i odpornych na manipulacje zapisów[84]. W dziedzinie badań nad bezpieczeństwem żywności technologia *blockchain* jest stosowana głównie w celu zagwarantowania, że dane generowane w procesie produkcji żywności nie zostaną sfałszowane, aby zapewnić bezpieczeństwo produktów, wzmocnić jej identyfikowalność i zwiększyć zaufanie konsumentów do bezpieczeństwa[85]. Zważywszy na cechy charakterystyczne tej technologii, w tym niemożliwość ingerencji w rejestr oraz jego rozproszoną naturę, istnieje gwarancja, że informacje przekazywane władzom państwowym podczas potencjalnego kryzysu żywnościowego będą rzetelne, pozwalając na lepsze planowanie działań zapobiegawczych. W tym kontekście technologia *blockchain* jest łączona z urządzeniami Internetu Rzeczy, które regulują m.in. bezpieczne przechowywanie i transport żywności.

Kolejną technologią, która pozwala na zwiększenie odporności w kontekście dostępu do żywności jest SI. SI pozwala na zwiększenie plonów poprzez polepszenie wydajności zbiorów, powiększenie ilości wartościowych baz danych dotyczących procesów produkcyjnych żywności oraz analizę zmiennych takich jak pogoda, wilgotność, skład gleby, wykorzystywane pestycydy i cena półproduktów[86]. Jest ona również szeroko używana do optymalizacji wykorzystywanych zasobów energetycznych – produkcja żywności jest procesem energochłonnym, a odpowiednie algorytmy pozwalają na redukcję zapotrzebowania na energię. Ważnym aspektem wykorzystania SI jest także wyznaczenie odpowiednich ścieżek transportu żywności, minimalizujących zużycie paliwa, a przez to redukcję emitowanych gazów cieplarnianych i maksymalnie szybkie dotarcie do użytkowników końcowych. SI była kluczową technologią, która pomogła zoptymalizować alternatywne trasy podczas zablokowania Kanału Sueskiego w 2021 r.[87].

Mając na uwadze krytyczną i wzrastającą rolę zasobów żywnościowych, ich nietrwałą naturę, podatność na ataki oraz naturalne występujące katastrofy, wymienione technologie, takie jak SI, big data, blockchain i Internet Rzeczy pozwalają odpowiednio optymalizować te elementy infrastruktury krytycznej i rozbudowywać odporność cywilną na zagrożenia.



## 3.5 Zdolność do reagowania na zdarzenia z dużą liczbą ofiar

dr Michał Hampel

Zdarzenia z dużą liczbą ofiar nie występują często, jednak w związku z ich masowym charakterem obciążają system ochrony zdrowia w sposób znacznie wykraczający poza normę. Nasze działania, np. zapewnienie wydolności cywilnego systemu służby zdrowia łącznie z zapasami środków zaopatrzenia medycznego, powinny polegać na zwiększeniu zdolności do reagowania na tego typu zdarzenia w sposób kontrolowany i adekwatny.

Podstawowym podziałem z definicji jest ten dzielący zdarzenia na mnogie i masowe. Zdarzenie mnogie to takie, w którym poszkodowanych jest wiele osób, jednak określone zapotrzebowanie na pomoc medyczną i czynności ratunkowe w trybie natychmiastowym nie przekracza możliwości sił i środków podmiotów ratowniczych obecnych na miejscu zdarzenia. Z kolei ze zdarzeniem masowym mamy do czynienia w sytuacji, w której to zapotrzebowanie przekracza możliwości operacyjne obecnych na miejscu sił i środków poszczególnych służb.

Wykorzystanie nowoczesnych technologii może znacząco usprawnić sposób reagowania w sytuacjach kryzysowych i wykraczających poza standardowy zakres pomocy. System ratownictwa medycznego i ochrony ludności powinien dysponować narzędziami takimi jak centralna informacja o dostępności sił i środków na danym terenie z możliwością ich uruchamiania w trybie natychmiastowym. Krajowe centrum zarządzania kryzysowego wraz z wojewódzkimi centrami wydają się być odpowiednimi strukturami pełniącymi nadzór nad sytuacjami nadzwyczajnymi, którymi są między innymi zdarzenia z dużą liczbą ofiar.

Funkcjonować powinien centralny system zbierający aktualizowane w czasie rzeczywistym dane o dostępności i zasobach poszczególnych służb, w tym policji, straży pożarnej, ochrony zdrowia i innych. Informacja o podmiotach leczniczych powinna zawierać informację o dostępności miejsc na poszczególnych oddziałach szpitali z danego regionu, ze szczególnym uwzględnieniem oddziałów chirurgii, intensywnej terapii, oraz informację o obłożeniu szpitalnych oddziałów ratunkowych. Te informacje wraz z dodatkowymi takimi jak dostępność sal operacyjnych, opieki specjalistycznej pozwoliłoby zwiększyć skuteczność udzielanej pomocy, oraz spowodowałoby, że pomoc będzie adekwatna i w żadnym wypadku nieopóźniona. To istotne z punktu widzenia zdarzeń masowych, w których ze względu na znaczne obciążenie systemu obserwujemy deficyt opieki, także tej podstawowej. Istotne jest zatem, aby pacjent trafił od razu do ośrodka, w którym nie będzie opóźnienia w udzieleniu pomocy, ta pomoc będzie odpowiednia, a szpital, w którym się znajdzie, będzie dysponował właściwym zapleczem oraz posiadał wolne miejsce. Dzięki temu możemy uniknąć przeciążenia pojedynczych ośrodków oraz sytuacji, w której opóźnienie udzielenia pomocy miałoby wpływ na przeżycie pacjenta.

System taki powinien być zintegrowany z systemami innych służb, a informacja o zdarzeniu z dużą liczbą ofiar powinna skutkować uruchomieniem odpowiednich służb, a w przypadku czasowego braku dostępności wystarczających sił i środków dać możliwość ich zaangażowania z regionów ościennych. Centrum zarządzania kryzysowego oraz odpowiednie służby powinny dysponować możliwościami geolokalizacji poszczególnych jednostek w czasie rzeczywistym z wyszczególnieniem rodzaju jednostki, personelu, zakresu możliwości wraz z narzędziami pozwalającymi na bezpośredni kontakt.

Istotne z punktu widzenia bezpieczeństwa publicznego oraz odpowiedniej reakcji na zdarzenia z dużą liczbą ofiar jest utworzenie zintegrowanej z systemem aplikacji dla obywateli, której funkcjonalność obejmie możliwość zgłoszenia sytuacji niebezpiecznej (wypadek masowy, atak terrorystyczny, wybuch), co może znacząco skrócić czas poinformowania odpowiednich służb. Aplikacja taka powinna mieć możliwość poinformowania wszystkich osób w pobliżu zdarzenia o jego wystąpieniu, przekazywać informacje o konieczności przygotowania się do ewakuacji lub bezpośrednio o jej rozpoczęciu. Biorąc pod uwagę dzi-

**CASE STUDY**

Wśród milionów ukraińskich uchodźców znajdują się osoby, którym wybuch wojny przerwał leczenie rozpoczęte na Ukrainie. Osoby te najczęściej nie dysponują dokumentacją medyczną, ponieważ uległa zniszczeniu wskutek działań wojennych. Nie ma też możliwości odzyskania dokumentacji ze zbombardowanych ukraińskich szpitali. W takich przypadkach wiele czasochłonnych badań trzeba wykonywać od nowa i podejmować ryzykowne decyzje, zwłaszcza w przypadku nagle przerwanej terapii onkologicznej. Taka sytuacja ma bardzo negatywny wpływ na zdrowie pacjentów.

Opisane powyżej doświadczenia pokazują, jak wielkie znaczenie dla bezpieczeństwa danych ma ich odmiejscowienie. W technologii chmury obliczeniowej dane są przechowywane w tzw. strefach dostępności – fizycznie oddzielonych lokalizacjach w regionie świadczenia usługi. Fizyczna separacja stref dostępności zapewnia odporność chmury na lokalne awarie, klęski żywiołowe czy zdarzenia ekstremalne, jak wybuch bomby czy uderzenie rakiety. Każda z przechowywanych w chmurze informacji jest synchronizowana równocześnie w trzech strefach dostępności, połączonych w wydajną sieć.

Technologia chmury obliczeniowej może nie tylko zapewnić bezpieczeństwo danych medycznych, ale też znacząco ułatwić dostęp do takich danych. Połączenie centrów przetwarzania danych w globalny ekosystem umożliwia też korzystanie z nich w dowolnym miejscu na Ziemi. Dane medyczne mogą w tej sytuacji bezpiecznie podążać za pacjentem, a dostawca chmury przejmuje od szpitala znaczną część odpowiedzialności za ich ochronę.



siejszy system transportu publicznego, metro, komunikację miejską oraz innych przewoźników osobowych, korzystających z aplikacji do przewozu osób, istnieć powinna możliwość centralnego ograniczenia wykonywania kursów w pobliżu rejonu zagrożenia i miejsca wypadku. Znacząco zmniejszyłoby to ryzyko dla osób postronnych oraz usprawniło prowadzenie akcji ratunkowej bezpośrednio w miejscu zdarzenia. Mając na uwadze obecną sytuację w związku z wojną na Ukrainie i zagrożenia z tego wynikające, aplikacja powinna również obejmować informację o najbliżej położonych schronach, miejscach opieki medycznej, punktach pomocy.

System taki powinien również zawierać wykaz magazynów oraz stan ich zaopatrzenia w środki niezbędne na wypadek wystąpienia zdarzenia masowego.

## 3.6 Zapewnienie łączności

Łukasz Gawron

Szybka i niezawodna łączność telekomunikacyjna stanowi podstawę dzisiejszego cyfrowego świata. Obecnie większość społeczeństwa ma dostęp do sieci telekomunikacyjnych czy bezprzewodowego Internetu. Sieć jest też podstawą działania wielu systemów administracji rządowej, wojska, infrastruktury krytycznej czy innego rodzaju służb. Dlatego też wzmacnianie cyberodporności infrastruktury telekomunikacyjnej powinno być traktowane jako pierwszoplanowe działanie mające na celu wzmocnienie odporności całego państwa. Łączność jest zresztą traktowana, podobnie jak zaopatrzenie w energię, jako infrastruktura krytyczna państwa i każde zakłócenie łączności, w szczególności w sytuacjach kryzysowych, może mieć katastrofalne skutki dla jego funkcjonowania. Takie podejście ma wyraz m.in. w komunikacie ministrów obrony państw NATO z listopada 2019 r. Państwa członkowskie zgodziły się zaktualizować bazowe wymagania sojuszu dotyczące telekomunikacji cywilnej, aby odzwierciedlić pojawiające się obawy dotyczące technologii 5G[88] i jej wpływu na cywilną gotowość sojuszu (ang. *civil preparedness*).

Wzmocnienie odporności i niezawodności infrastruktury telekomunikacyjnej jest również przedmiotem regulacji w poszczególnych państwach Unii Europejskiej i Wielkiej Brytanii. Gabinet Premiera Wielkiej Brytanii proponuje pięć podstawowych zasad cyberodporności infrastruktury telekomunikacyjnej, które mogą być również z powodzeniem zastosowane w pozostałych państwach sojuszniczych[89]:

1. Patrz poza rozwiązania techniczne, na procesy i organizacje
   - → Rozważając kwestię odpornej infrastruktury telekomunikacyjnej, duży nacisk kładzie się na rozwiązania techniczne (jak stacje nadawcze czy telefony komórkowe). Jednak procesy i sposób, w jaki aktorzy rynkowi się organizują w celu reagowania na sytuacje awaryjne, powinny być rozpatrywane jako jedna całość.

2. Zidentyfikuj i przejrzyj krytyczne działania komunikacyjne, które stanowią podstawę ustaleń dotyczących reakcji na wydarzenia kryzysowe

- Należy zidentyfikować kluczowe działania komunikacyjne, które stanowią podstawę procesów dotyczących reagowania na sytuacje kryzysowe (np. wyznaczenie odpowiednich osób do kontaktu i wymiana informacji pomiędzy kluczowymi z punktu widzenia bezpieczeństwa instytucjami).

3. Zadbaj o różnorodność swoich rozwiązań technicznych
   - W przypadku działań o znaczeniu krytycznym można rozważyć zwiększenie różnorodności środków technologicznych do prowadzenia komunikacji (jednak ocena rzeczywistej różnorodności rozwiązań technicznych może być trudna ze względu na nieodłączną zależność jednego rozwiązania technicznego od drugiego).

4. Przyjęcie „warstwowych rozwiązań" awaryjnych
   - Żadne rozwiązanie techniczne nie będzie dostępne przez cały czas. Dostępność jest konsekwencją niezawodności systemu (związanej z usterkami i ich naprawą) oraz umiejętnością radzenia sobie z przeciążeniem (wynikającym z nadmiernego zapotrzebowania). Przyjęcie warstwowego podejścia awaryjnego do wyboru rozwiązań technicznych pomaga złagodzić niedostępność.

5. Zaplanuj odpowiednią interoperacyjność
   - Współpraca między służbami, biznesem, administracją publiczną celem lepszej koordynacji działań kryzysowych.

Infrastruktura komunikacyjna jest również podatna na zniszczenie spowodowane klęskami żywiołowymi oraz działaniami zbrojnymi. Dlatego też kolejnym kluczowym czynnikiem wzmacniającym odporność w tym zakresie może być skorzystanie z alternatywnych sposobów komunikacji, czyli łączności satelitarnej. Komunikacja w oparciu o technologie satelitarne daje możliwość szybkiej i niezawodnej komunikacji nawet w niesprzyjających warunkach. Idealnym przykładem użycia tego rozwiązania w czasie konfliktu zbrojnego jest zastosowanie Internetu satelitarnego Starlink zaprojektowanego przez amerykańską firmę SpaceX.

**CASE STUDY**

Tuż po rozpoczęciu rosyjskiej agresji Minister Cyfrowej Transformacji Ukrainy Mychajło Fedorow poprosił założyciela firmy SpaceX Elona Muska o dostęp do autorskiego szybkiego satelitarnego Internetu Starlink. Jest to system nisko orbitujących satelitów (obecnie ok. 2200), które zapewniają połączenie z siecią, gdy inne kanały komunikacji są niedostępne. Starlink okazał się niezwykle przydatny po tym, jak Rosjanie zaczęli celowo niszczyć infrastrukturę telekomunikacyjną. Firma SpaceX odpowiedziała na prośbę ministra Fedorowa i wysłała na Ukrainę odpowiednie terminale pozwalające połączyć się z Internetem satelitarnym. W terminale Starlink w pierwszej kolejności zostały wyposażone obiekty infrastruktury krytycznej m.in. szpitale, banki oraz firmy energetyczne[90]. Obecnie na Ukrainie z systemu Starlink dziennie korzysta ok. 150 tys. użytkowników[91].



Niezawodna łączność telekomunikacyjna jest również niezbędnym komponentem, z którego korzystają służby podczas sytuacji kryzysowych. Prowadząc działania ratownicze na terenach słabo zurbanizowanych w sytuacji klęski żywiołowej, służby nie mają możliwości skorzystania z istniejącej infrastruktury ze względu na zniszczenia infrastruktury lub jej brak na danym obszarze. Rozwiązaniem tego problemu może być szybka instalacja polowej sieci 4G/5G.

**CASE STUDY**

Mission Critical Network in the Box (MC-NIB) to rozwiązanie przeznaczone dla służb ratowniczych, operatorów infrastruktury krytycznej oraz wojska. Został stworzony z myślą o zapewnieniu komunikacji w sytuacjach kryzysowych, takich jak klęski żywiołowe, zagrożenia bezpieczeństwa publicznego, rozległe awarie infrastruktury telekomunikacyjnej czy energetycznej. To rozwiązanie 4G i 5G, które zapewnia specjalną łączność dla branż wymagających niezawodnych i bezpiecznych połączeń, takich jak straż pożarna czy wojsko. Niezależny system komunikacji pozwala na szybkie zbudowanie sieci telekomunikacyjnej 4G lub 5G do wykorzystania w każdej sytuacji i w każdych warunkach, nawet tych najbardziej ekstremalnych. MC-NIB może być szybko wdrożony przez służby mundurowe, a całe rozwiązanie można umieścić w walizce lub plecaku[92].

Nie należy również zapominać o zapewnieniu ciągłości łączności cyfrowej, w szczególności podmiotom administracji rządowej. Utrzymanie stałego dostępu do Internetu w dobie digitalizacji jest równie ważne jak podtrzymanie tradycyjnych kanałów komunikacji telefonicznej. W dobie konfliktu militarnego oprócz możliwości zniszczenia infrastruktury zapewniającej łączność z internetem istnieje ryzyko przejęcia wrażliwych zasobów rządowych. Ponadto administracja rządowa musi zachować ciągłość działania na wypadek prowadzenia działań militarnych na terenie państwa. W związku z tak dużą liczbą ryzyk spowodowanych konfliktem zbrojnym, które mają bezpośrednie przełożenie na ciągłość zachowania łączności, a co za tym idzie ciągłość pracy administracji rządowej, należy budować cyberodporność poprzez odpowiednie przygotowanie planów awaryjnych.

## 3.7 Transport cywilny

Sławomir Łazarek

Punkt ostatni, ale nie najmniej ważny. Tak jak sprawny system łączności jest „układem nerwowym" niezbędnym

**CASE STUDY**

Rozwiązaniem zapewniającym zachowanie łączności cyfrowej oraz ciągłości działania usług rządowych jest chmura obliczeniowa. Rząd Ukrainy 16 marca przyjął ustawę o usługach w chmurze. Ustawa pozwala na korzystanie z usług chmurowych przez agencje rządowe i wprowadza zasadę Cloud First. Zasada ta mówi o konieczności przeniesienia głównych i kluczowych usług IT, z których korzysta administracja, do chmury. Dzięki tej decyzji rząd Ukrainy może bez problemu wykonywać swoje zadania, przy okazji minimalizując ryzyku zakupu skompromitowanego sprzętu i znacząco ograniczając wydatki budżetowe[93].

podsystemu transportu i ruchu wojsk „nic się nie dzieje, dopóki coś się nie ruszy" (ang. *nothing happens till something moves*). Ważne jest, by wskazać, że zapewnienie swobody przemieszczania sił i środków wojsk sojuszniczych (ang. *freedom of movement lub military mobility*) w zdecydowanej mierze zależy od cywilnego wsparcia. Wojsko polega na cywilnych środkach transportu, na cywilnych zdolnościach przeładunkowych oraz na cywilnych rozwiązaniach związanych z zarządzaniem ruchem. Nie mniejszą rolę odgrywa podczas kryzysu zapewnienie dekonfliktacji migracji ludności cywilnej opuszczającej strefę działań wojennych z przemieszczeniami wojskowymi w kierunku tych obszarów.

Mobilność i zdolność do przemieszczenia są istotne dla wszystkich. Od codziennych przejazdów osób prywatnych po prawidłowe funkcjonowanie globalnych łańcuchów dostaw towarów do punktów handlowych oraz na potrzeby produkcji przemysłowej. Transport jest czynnikiem, który umożliwia funkcjonowanie życia gospodarczego, jak również społecznego.

Kryzys związany z pandemią COVID-19 pokazał, jak ważną rolę odgrywa transport oraz jakie koszty społeczne, zdrowotne i gospodarcze niesie ze sobą znaczne ograniczenie lub całkowite wstrzymanie swobodnego przepływu osób, towarów i usług. Utrzymanie łańcuchów dostaw oraz skoordynowane międzynarodowe podejście do połączeń i transportu są kluczowe dla przezwyciężenia każdego kryzysu i wzmocnienia odporności państw i ich społeczeństw.

W dzisiejszych czasach, aby zapewnić działanie wszystkich wcześniej wymienionych obszarów funkcjonowania państwa i społeczeństwa, niezbędne jest posiadanie w kraju sprawnego systemu transportowego odpornego na wszelkiego rodzaju zagrożenia, w szczególności te hybrydowe i cyber.

System transportu cywilnego w ostatnich latach podlegał szybkiej transformacji cyfrowej. W zasadzie cały system transportu zależny jest od wsparcia teleinformatycznego. Systemy kierowania i zarządzania ruchem w każdym rodzaju transportu, systemy obsługi przewozu towarów i osób, systemy zarządzania przeładunkami w portach



morskich, na lotniskach, w terminalach towarowych w zasadzie w całości są zależne od nowoczesnych systemów informatycznych. I to zarówno w skali lokalnej, krajowej, jak i międzynarodowej/globalnej. Stopień ich cyfryzacji będzie się tylko pogłębiał.

Zarządzanie środkami transportu i ładunkami, optymalizacja tras przejazdu oraz obsługa zamówień coraz częściej odbywają się za pomocą systemów informatycznych. To standard zwłaszcza w przypadku dużych operatorów transportowych z gęstą siecią powiązań na rynku. Niestety standardem w transporcie wciąż nie jest odpowiedni poziom cyberbezpieczeństwa używanych systemów IT. Systemy i ich zabezpieczenia przed cyberatakami różnią się w zależności od przewoźnika czy zarządcy infrastruktury transportowej. System transportu charakteryzuje się bardzo rozbudowaną siecią powiązań w globalnym łańcuchu dostaw. A to sprawia, że cyberatak wymierzony w jednego z operatorów automatycznie paraliżuje działanie współpracujących z nim dostawców i partnerów – efekt kaskady.

Luki w systemach zabezpieczeń oraz brak jednolitych standardów ochrony przed cyberatakami, a także przetwarzanie cennych danych na temat transportowanych ładunków – to główne powody, dla których system przewozów jest współcześnie tak bardzo podatny na cyberataki. Jest wartościowy i dochodowy dla cyberprzestępców, którzy chcą wykorzystać pozyskane w ten sposób dane np. do działalności przestępczej (wymuszanie okupów) lub terrorystycznej (np. zamachy na dworce czy zakłócanie ruchu wojsk). A także jako środek walki konkurencyjnej, w celu destabilizacji bądź zerwania łańcuchów dostaw lub wygenerowania znaczących strat finansowych w konkretnych przedsiębiorstwach. Jest on także oczywistym celem ataków towarzyszących działaniom wojennym.

Warto zaznaczyć, że nie tylko „wrogie i zamierzone" działania cyberprzestę-

**CASE STUDY**

W czerwcu 2017 r. miał miejsce cyberatak wirusem NotPetya, który dotknął m.in. duńską firmę transportową A.P. Moller-Maersk – największego światowego operatora morskiego transportu kontenerowego. Systemy informatyczne firmy przez kilka dni były niedostępne. W tym czasie Maersk był zmuszony wyłączyć część swoich systemów zarządzania flotą i obsługi zleceń. Nie doszło do kradzieży danych wrażliwych. Mimo to atak sparaliżował działanie firmy, spowodował znaczne straty finansowe (kwartalny zysk operatora zmniejszył się o 300 mln dolarów) oraz doprowadził również do zakłóceń w globalnym łańcuchu dostaw. To i kilka podobnych wydarzeń związanych z naruszeniem cyberbezpieczeństwa w dużych przedsiębiorstwach zajmujących się transportem, spedycją i logistyką sprawiły, że w 2019 r. firmy Thales i Verint umieściły transport na czwartym miejscu zestawienia sektorów najczęściej atakowanych przez cyberprzestępców[94].

walki konkurencyjnej, w celu destabilizacji bądź zerwania łańcuchów dostaw lub wygenerowania znaczących strat finansowych w konkretnych przedsiębiorstwach. Jest on także oczywistym celem ataków towarzyszących działaniom wojennym.

Warto zaznaczyć, że nie tylko „wrogie i zamierzone" działania cyberprzestępców są źródłem zagrożeń dla prawidłowego funkcjonowania systemu transportowego państwa. Takie zagrożenia wynikają również z podatności systemów IT na „nieprawidłowości w ich funkcjonowaniu – awarie sprzętu", co przy intensywnym użytkowaniu pewnych urządzeń i podzespołów pochodzących od jednego producenta może prowadzić nawet do globalnych zakłóceń w przemieszczaniu osób i towarów. Ponadto należy się zastanowić w takich przypadkach (gdy odpowiednie komisje i służby określą takie zdarzenie jako „awaria podzespołu"), czy potencjalnie za „awarią" nie stoi nasz adwersarz. Celowe wywołanie „incydentu" może w znacznym stopniu utrudnić lub uniemożliwić np. terminowe przemieszczenie sojuszniczych sił wzmocnienia.

**CASE STUDY**

W dniu 17 marca 2022 r. nastąpiła awaria na sieci kolejowej Polski, która objęła 19 z 33 lokalnych Centrów Sterowania wyposażonych przez Alstom. Alstom jest francuskim międzynarodowym producentem taboru kolejowego, działającym na całym świecie na rynkach transportu kolejowego. W Polsce jest największym producentem w branży kolejowej. Na początku PKP PLK oraz pełnomocnik rządu ds. cyberbezpieczeństwa nie wykluczyli, że to atak hakerski. Jak się jednak okazało, problem dotyczył oprogramowania firmy. W jej komunikacie czytamy: „Alstom potwierdza, że nie było żadnego cyberataku ani problemu bezpieczeństwa związanego z błędem formatowania czasu, który wystąpił 17 marca 2022 r. Błędy w formatowaniu czasu są znanym zjawiskiem".

Inny przykład. 27 lutego 2022 r. sparaliżowane zostały Koleje Białoruskie, co mocno utrudniło transport wojsk i zaopatrzenia. O działaniu poinformowała wtedy anonimowa Grupa Cyberpartyzantów z Białorusi. Doszło do ataku na system sterowania ruchem kolejowym, który został wyłączony i zaszła konieczność przejścia na ręczne sterowanie, co spowodowało bardzo duże opóźnienia pociągów w całym kraju. To jednak nie pierwsza akcja hakerów wymierzona w białoruskie koleje. 25 stycznia 2022 r. zaszyfrowano serwery państwowego przewoźnika, domagając się wycofania rosyjskich wojsk z Białorusi, które przygotowywały się do wojny z Ukrainą.



# 4. DROGA DO ODPORNOŚCI PAŃSTWA

**dr inż. Witold Skomra**

Do czasu pojawienia się komputerów i technologii cyfrowych wszystkie obszary bezpieczeństwa były traktowane jako odrębne środowiska, przy czym bezpieczeństwo fizyczne (ochrona przed dostępem osób postronnych) było zasadniczym celem prowadzonych działań. Możliwości integracyjne technologii cyfrowych sprawiły, że od kilkunastu lat bezpieczeństwo zarówno organizacji jak i całych państw ma charakter wielowymiarowy. W Polsce dokumentem, który to zdefiniował jest Narodowy Program Ochrony Infrastruktury Krytycznej. Zgodnie z nim bezpieczeństwo ma sześć wzajemnie przenikających się obszarów. Są nimi bezpieczeństwo fizyczne, techniczne, osobowe, cyber (IT i OT), prawne oraz ciągłość działania. Zgodnie z NPOIK rdzeniem tej wielowymiarowej tablicy zależności pozostaje bezpieczeństwo fizyczne.

Transformacja cyfrowa i pogłębiające się uzależnienie współczesnych społeczeństw od zdobyczy cywilizacyjnych i nowoczesnych technologii sprawia, że podejście zaproponowane w NPOIK wymaga znaczącej korekty. Wspomniana transformacja cyfrowa ma wymiar zarówno indywidualny, grupowy jak i ogólnonarodowy. W wymiarze indywidualnym mało kto uświadamia sobie, że użytkując dedykowaną aplikację staje się uczestnikiem wewnętrznych procesów realizowanych przez bank, dostawcę energii czy organizatora koncertów. Wymiar ogólnonarodowy transformacji cyfrowej ma o wiele większe znaczenie. Wzajemne powiązania procesów realizowanych przez poszczególne podmioty zarówno odrębnie, jak i współzależnie, sprawiają, że państwo staje się jedną strukturą organizacyjną wymagającą wspólnego zarządzania. Proces poszukiwania narzędzi do zarządzania bezpieczeństwem państwa można podzielić na kilka etapów. Etap funkcjonowania autonomicznych podmiotów, etap zarządzania systemami i wreszcie etap zarządzania systemami złożonymi („*system of systems*")[95]. Trudność zarządzania systemami złożonymi wynika z faktu, że poszczególni uczestnicy mogą nawet nie mieć świadomości że ich procesy są częścią szerszej struktury. Jednocześnie nawet pozornie niewielkie zakłócenia w ramach systemu złożonego poprzez efekt domina lub kaskady wywołuje trudne lub niemożliwe do przewidzenia skutki w obszarach pozornie niepowiązanych ze sobą.

Zwrócenie uwagi, że całe społeczeństwo zaczyna funkcjonować jako jeden organizm połączony całą siecią powiązań realizowanych technologiami cyfrowymi lub przy wsparciu tych technologii wymusza konieczność zmiany strategii w budowaniu bezpieczeństwa publicznego. Dotychczasowe podejście „z dołu do góry" oznaczające, że skupiamy się na bezpieczeństwie pojedynczych organizacji (niekiedy tylko obiektów) musi zostać zastąpione podejściem „z góry do dołu". Ta nowa strategia zakłada, że najpierw definiuje się cele społeczne i opisuje skutki ich zakłócenia, a dopiero na tej podstawie poszczególne organizacje (operatorzy

usług kluczowych) dostosowują się do wymaganego poziomu dostępności oferowanych przez siebie usług.

Próbą wprowadzenia tej strategii do przepisów prawa są projekty dwóch dyrektyw. Wielokrotnie przywoływanej już dyrektywy NIS 2 obejmującej bezpieczeństwo cyber oraz projekt dyrektywy CER (Directive on the Resilience of Critical Entities)[96], która to dyrektywa dotyczy pozostałych wymiarów bezpieczeństwa. Powiązane z tymi dwoma projektami jest Rozporządzenie DORA uwzględniające specyfikę sektora bankowego. Te trzy zasadnicze akty prawne wraz z przepisami wykonawczymi stworzą zupełnie nowe środowisko budowania bezpieczeństwa publicznego. Wdrażanie nowej strategii zgodnie z tymi projektami można podzielić na kilka etapów. Po pierwsze kraje członkowskie UE identyfikują procesy kluczowe i ryzyka związane z ich zakłóceniem. Ta część pracy kończy się opracowaniem dokumentu strategicznego wskazującego jaki poziom odporności na zakłócenia państwo zamierza osiągnąć. W kolejnym kroku typuje się operatorów usług kluczowych, a w przypadku dyrektywy CER również infrastrukturę krytyczną zarządzaną przez tych operatorów. Dodatkowym elementem nowej strategii jest całościowy proces oceny ryzyka. Proces uwzględnia specyfikę poszczególnych operatorów, ale jego główną wartością jest nadzorowany przez administrację proces mitygacji ryzyk uznanych za nieakceptowalne z punktu widzenia państwa. Polega on na tym, że poszczególni operatorzy muszą zastosować środki organizacyjne, bezpieczeństwa i techniczne, które są odpowiednie i proporcjonalne do ryzyka, na jakie są narażeni.

Podsumowując należy podkreślić, że zmiany środowiska bezpieczeństwa w połączeniu z trwającą rewolucją technologiczną wymuszają zastosowanie nowych strategii zarządzania sferą bezpieczeństwa publicznego. Bez rozwiązań między i ponadresortowych trudnym lub wręcz niemożliwym jest osiągnięcie odporności państwa na właściwym poziomie. Poziomie, do którego osiągnięcia obowiązaliśmy się w ramach sojuszu NATO akceptując siedem bazowych wymogów odporności. Jednocześnie pierwszym, niezbędnym warunkiem zbudowania odporności państwa na aktualne wyzwania jest wcześniejsze uświadomienie decydentom potrzeby dostosowania się do nowych uwarunkowań. Niniejszy Raport jest elementem budowania tej świadomości.

## PODSUMOWANIE

W aktualnej sytuacji geopolitycznej, z towarzyszącym jej wymiarem zagrożenia dla bezpieczeństwa narodowego krajów UE i NATO, odporność należy postrzegać jako wyzwanie holistyczne, obejmujące wymiar militarny i cywilny, które w tych okolicznościach coraz bardziej się przenikają, warunkują i uzupełniają. Budowanie odporności – we wszystkich jej odsłonach: cyfrowej, cyber i społecznej – wymaga współpracy międzysektorowej i wielowymiarowej, zarówno w ramach poszczególnych krajów, jak i społeczności międzynarodowej.



# BIOGRAMY AUTORÓW

**Izabela Albrycht**
Współtwórca CYBERSEC Forum i Przewodnicząca jego Rady Programowej, członek Rady Doradców Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland. Politolog, od wielu lat specjalizuje się w tematyce strategicznych aspektów bezpieczeństwa, w tym cyberbezpieczeństwa i technologii. Członek Grupy Doradczej NATO ds. nowych i przełomowych technologii oraz Rady do Spraw Cyfryzacji. Od stycznia 2022 r. członek Rady ds. Bezpieczeństwa i Obronności w Kancelarii Prezydenta RP. W l. 2020-2022 z ramienia polskich organizacji branżowych ICT – PIIT, Cyfrowa Polska oraz KIGEIT była członkiem zarządu DIGITALEUROPE, aktualnie w ramach tej organizacji współtworzy Digital Resilience Executive Council. Jest członkiem Rady Nadzorczej Asseco Poland S.A. oraz ComCERT. Była prezesem Instytutu Kościuszki w l. 2010-2021.

**Łukasz Gawron**
Absolwent stosunków międzynarodowych na Uniwersytecie Jagiellońskim w Krakowie, gdzie ukończył również studia licencjackie. Koordynował projekt European Energy Hub w Instytucie Polityk Publicznych. Od wielu lat związany z Instytutem Kościuszki, gdzie odpowiedzialny był za organizację kilkunastu wydarzeń spod szyldu CYBERSEC Forum. Od grudnia 2021 r. pełni rolę Prezesa Zarządu pierwszego w Polsce Klastra Cyberbezpieczeństwa #CyberMadeinPoland. Posiada certyfikat z zarządzania projektami PRINCE2 Foundation oraz Agile PM Foundation.

**Maciej Góra**
Koordynator projektów w Instytucie Kościuszki. Studiował bezpieczeństwo narodowe na Uniwersytecie Jagiellońskim, cyberbezpieczeństwo na Akademii Górniczo-Hutniczej oraz stosunki międzynarodowe na Uniwersytecie Karola w Pradze. W trakcie swojej pracy w Instytucie Kościuszki koordynował liczne inicjatywy i projekty, m. in. tworząc i operacjonalizując wiele punktów agendy Europejskiego Forum Cyberbezpieczeństwa - CYBERSEC, przewodząc zaangażowaniu IK podczas Internet Governance Forum 2021 i IGF Poland 2022, współtworząc podręcznik antydezinformacy dla licealistów i nauczycieli, uczestnicząc jako gość i gospodarz w podcaście General Talks. Jego zainteresowania badawcze i zawodowe obejmują zagadnienia cyfrowe w skali mikro (redukcja śladu cyfrowego, osobiste bezpieczeństwo w sieci) i makro (geopolityczny wymiar cyberbezpieczeństwa, zarządzanie cyberbezpieczeństwem, procesy społeczne związane z digitalizacją, futurologia).

**Michał Hampel**
Lekarz, specjalista chirurgii ogólnej, pracuje w Klinice Chirurgii Gastroenterologicznej i Transplantologii Centralnego Szpitala Klinicznego MSWiA w Warszawie, wykładowca akademicki na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie. Od 2019 r. lekarz w zespole ratunkowym Polskiego Centrum Pomocy Międzynarodowej. W 2020 r. brał udział w tworzeniu Szpitala Tymczasowego na Stadionie Narodowym. Stworzył i koordynował pracę

największego w Polsce Punktu Szczepień Populacyjnych przeciw COVID-19 na Stadionie Narodowym. Pełni funkcję Koordynatora Medycznego Stadionu Narodowego w Warszawie odpowiedzialnego za przygotowanie zabezpieczenia medycznego podczas imprez masowych. Uczestniczył w wielu misjach medycznych związanych z przeciwdziałaniem rozwojowi i zwalczaniem skutków pandemii, brał udział w misji ratunkowej po wybuchu w porcie w Bejrucie (Liban), w misji ewakuacyjnej w Afganistanie, realizując zadania zabezpieczenia medycznego polskiej misji i osób ewakuowanych, a także koordynował prace związane z uruchomieniem i działaniem pociągu medycznego do ewakuacji obywateli Ukrainy do Polski.

**Michał Krawczyk**

Analityk dezinformacji oraz koordynator projektów w Instytucie Kościuszki. Absolwent Uniwersytetu Jagiellońskiego w Krakowie, na kierunku bezpieczeństwo narodowe, gdzie zajmował się zagadnieniem budowania społecznej odporności na dezinformację. Uczestnik szkoły letniej „Changing Security and Hybrid Threats" na Uniwersytecie Jyvaskyla oraz absolwent programu „Digital Scherlocks", prowadzonego przez Atlantic Council. W Instytucie Kościuszki członek zespołu badawczego „Prozodia", autor publikacji z obszaru analizy dezinformacji, w tym badania fake news w kontekście COVID-19 i rosyjskiej dezinformacji w Polsce oraz gospodarz podcastu General Talks.

**Sławomir Łazarek**

Kierownik Wydziału Współpracy Międzynarodowej polskiego Rządowego Centrum Bezpieczeństwa; magister inżynierii lądowej Wojskowej Akademii Technicznej w Warszawie i absolwent studiów podyplomowych ekonomii obronności na Akademii Sztuki Wojennej tamże. Emerytowany pułkownik Wojska Polskiego i były zastępca szefa polskiego krajowego Centrum Koordynacji Ruchu Wojsk. Wcześniej, w okresie 32 lat służby wojskowej, na różnych pełnionych stanowiskach odpowiedzialny za przygotowanie systemów transportu do celów obronności. Współpracując z cywilnym zarządem infrastruktury transportowej w Polsce, brał udział w rozwijaniu minimalnych wymogów wojskowych dotyczących sieci transportu i wymogów przemieszczania wojskowego uzbrojenia i wyposażenia oraz określeniu zasad, procedur i wytycznych systemu transportu i ruchu wojsk Wojska Polskiego i jego przygotowaniu oraz zapewnieniu przez wszystkie gałęzie transportu. Polski przedstawiciel Grupy Roboczej NATO ds. transportu i ruchu wojsk. Obecnie odpowiedzialny za kwestie krajowej i międzynarodowej koordynacji zarządzania kryzysowego i planowania cywilnego, w szczególności systemy reagowania na sytuacje kryzysowe, wzmacnianie odporności oraz zaangażowanie cywilno-wojskowe.

**dr Krzysztof Malesa**

Członek zarządu, dyrektor ds. strategii bezpieczeństwa(National Security Officer) w Microsoft Polska. Ekspert w zakresie zarządzania kryzysowego, ochrony infrastruktury krytycznej oraz odporności. W latach 2010-2021 pracował w Rządowym Centrum Bezpieczeństwa. Był m. in. szefem polskiej delegacji w Komitecie Planowania Cywilnego NATO oraz krajowym delegatem w grupie roboczej przygotowującej Dyrektywę Unii Europejskiej w sprawie odporności podmiotów krytycznych (CER). Krzysztof Malesa jest absolwentem studiów bałtystycznych w Katedrze Językoznawstwa Ogólnego i Bałtystyki na Unwersitecie Warszawskim, na którym uzyskał też stopień doktora nauk humanistycznych w zakresie językoznawstwa. Jest tłumaczem przysięgłym języka litewskiego.

**dr inż. Witold Skomra**

Doradca, a jednocześnie szef Wydziału Ochrony Infrastruktury Krytycznej w Rządowym Centrum Bezpieczeństwa. Ekspert w zakresie planowania cywilnego, zarządzania kryzysowego i ochrony infrastruktury krytycznej. Krajowy delegat do prac grupy przygotowującej projekt dyrektywy Critical Entities Resilience, oraz do działającego w ramach OECD High Level Risk Forum. Wykładowca Wydziału Zarządzania Politechniki Warszawskiej. Prowadzi zajęcia z ciągłości działania, zarządzania ryzykiem, zarządzania bezpieczeństwem publicznym i ochrony infrastruktury krytycznej. Witold Skomra to były strażak – Komendant Główny Państwowej Straży Pożarnej, absolwent Szkoły Głównej Służby Pożarniczej oraz Akademii Obrony Narodowej.

# PRZYPISY KOŃCOWE

1 Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, str. 10.
2 Ibidem, str. 15
3 Ibidem, str. 20
4 „Dla skuteczniejszego osiągnięcia celów niniejszego traktatu, Strony, każda z osobna i wszystkie razem, poprzez stałą i skuteczną samopomoc i pomoc wzajemną, będą utrzymywały i rozwijały swoją indywidualną i zbiorową zdolność do odparcia zbrojnej napaści" – art. 3 T*raktatu Północnoatlantyckiego, sporządzonego w Waszyngtonie dnia 4 kwietnia 1949 r.*, https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/traktat-polnocnoatlantycki-waszyngton-1949-04-04-16885651, [online: 29.06.2022].
5 *Współpraca w ramach NATO*, https://www.gov.pl/web/rcb/wspolpraca-w-ramach-nato#_ftn2, [online: 29.06.2022].
6 Wcześniej w podobnej formule działał Civil Emergency Planning Committee (CEPC), *Resilience and civil preparedness – Article 3*, https://www.nato.int/cps/en/natohq/topics_132722.htm, [online: 29.06.2022].
7 *Resilience and civil preparedness – Article 3*, https://www.nato.int/cps/en/natohq/topics_132722.htm, [online: 29.06.2022].
8 Wspomniania Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej odnosi się bezpośrednio do siedmiu bazowych wymogów odporności NATO wskazując na konieczność budowy odporności w tych obszarach w trybie priorytetowym", por. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, str. 16.
9 *Komunikat ze szczytu NATO w Brukseli wydany 14 czerwca 2021 r.*, https://www.nato.int/cps/en/natohq/news_185000.htm, [online: 29.06.2022].
10 *Komunikat ze szczytu NATO w Madrycie wydany 29 czerwca 2022 r.* https://www.nato.int/cps/en/natohq/official_texts_196951.htm, [online: 29.06.2022].
11 *NATO's Strategic Concept*, https://www.nato.int/strategic-concept/, [online: 29.06.2022].
12 „We will enhance our individual and collective resilience and technological edge", *ibidem*, [online: 29.06.2022].
13 NATO releases its Climate Change and Security Impact Assessment, https://www.nato.int/cps/en/natohq/news_197241.htm, [online: 29.06.2022].
14 https://ec.europa.eu/info/strategy/strategic-planning/strategic-foresight/2020-strategic-foresight-report/resilience-dashboards_en, [online: 24.06.2022].
15 *Resilience*, https://joint-research-centre.ec.europa.eu/resilience_en, [online: 24.06.2022].
16 Szczegółową analizę Krajowych Planów Odbudowy dla 12 krajów członkowskich z Europy Środkowo-Wschodniej można zaleźć w raporcie T*hree Seas United in Cyber Power*, https://ik.org.pl/publikacje/premiera-raport-three-seas-united-in-cyberpower/, [online: 24.06.2022].
17 Skutki pandemii widoczne są w spadku globalnego PKB, spadku produkcji przemysłowej, wzroście poziomu bezrobocia, wzroście długu publicznego, spadku eksportu.
18 *Digital path to recovery and resilience in the European Union*, https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/news/digital-path-recovery-and-resilience-european-union, [online: 24.06.2022].
19 *Ibidem*, https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/news/digital-path-recovery-and-resilience-european-union, [online: 24.06.2022].
20 „Przeciętne gospodarstwo domowe w USA ma obecnie łącznie 25 podłączonych urządzeń w 14 różnych kategoriach (wzrost z 11 w 2019 r.)", więcej: *Connectivity & Mobile Trends 2021 Survey*, Deloitte, https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-pandemic-stress-tested-digital-home.html, [online: 24.06.2022].



21 J. De Groot, *What is Cyber Resilience*, https://digitalguardian.com/blog/what-cyber-resilience, 2019, [online: 24.06.2022].
22 https://www.consilium.europa.eu/pl/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/, [online: 24.06.2022].
23 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Akt-dotyczacy-cyberodpornosci-nowe-przepisy-dotyczace-cyberbezpieczenstwa-produktow-cyfrowych-i-us%C5%82ug-pomocniczych_pl, [online: 24.06.2022].
24 Por. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy, [online:28.06.2022].
25 Por. https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024, [online:28.06.2022].
26 https://www.eesc.europa.eu/pl/our-work/opinions-information-reports/opinions/roadmap-security-and-defence-technologies, [online: 24.06.2022].
27 *United for a new era*, 2021, s. 19, [online]: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.
28 Komisja Europejska, *2018 Code of Practice on Disinformation*, 16 czerwca 2022, [online]: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.
29 Komisja Europejska, *2022 Strengthened Code of Practice on Disinformation*, 16 czerwca 2022, [online]: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.
30 Komisja Europejska, *The Digital Services Act package*, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package, [online: 29.06.2022].
31 EU Disinfo Lab, *Tackling disinformation online: the Digital Services Act opens the era of accountability*, 25 kwietnia 2022, https://www.disinfo.eu/advocacy/tackling-disinformation-online-the-digital-services-act-opens-the-era-of-accountability/, [online: 29.06.2022].
32 K. Mikulski, *Unia Europejska*, [w]: *Europa wobec dezinformacji – budowa odporności systemowej w wybranych krajach*, Instytut Kościuszki, Kraków 2021, s. 16, https://ik.org.pl/wp-content/uploads/raport_dezinformacja_europa_final.pdf, [online: 29.06.2022].
33 *Ibidem*, s. 16.
34 *Ibidem*, s. 16.
35 StrategEast, *Ukrainian Digital Resistance to Russian Aggression*, 2022, s. 6, https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf, [online: 29.06.2022].
36 *Ibidem*, s. 9.
37 *Ibidem*, s. 10.
38 *Ibidem*, s. 11.
39 PolitiFact, https://www.politifact.com/.
40 DebunkEU, https://debunk.eu/about-debunk/.
41 Full Fact, https://fullfact.org/about/.
42 R. Oshikawa, J. Qian, W. Yang Wang, *A Survey on Natural Language Processing for Fake News Detection*, 2020, https://aclanthology.org/2020.lrec-1.747/, [online: 29.06.2022].
43 *Ibidem.*
44 K. Wagner, *Facebook found a new way to identify spam and false news articles in your News Feed*, Vox, https://www.vox.com/2017/6/30/15896544/facebook-fake-news-feed-algorithm-update-spam, [online: 30.06.2022].
45 J. Cook, *Building Resilience Against Misinformation Through a Cartoon Game*, https://www.aaas.org/programs/center-public-engagement-science-and-technology/reflections/building-resilience-against, [online: 30.06.2022].
46 Get Bad News, https://www.getbadnews.pl/#intro, [online: 30.06.2022].

47 Fake News: The Game, https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/fake-news-the-game.html, [online: 30.06.2022].
48 Fake It To Make It, https://www.fakeittomakeitgame.com/, [online: 30.06.2022].
49 Deklaracja końcowa szczytu NATO w Warszawie, 9 lipca 2016 r., https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf, [online: 30.06.2022].
50 PO(2020)0189-Updated Baseline Requirements, Resilience Guidelines and Evaluation Criteria.
51 *Guide to Continuity of Government For State, Local, Tribal and Territorial Governments*, Federal Emergency Management Agency, July 2021, s. 4.
52 *Ibidem*, s. 3.
53 P. Zaskórski P., K. Szwarc, *Modelowanie procesów zapewniania bezpieczeństwa i ciągłości działania organizacji administracji publicznej*, [online]: http://sbn.wat.edu.pl/pdf-129871-56756?filename=MODELING%20OF%20THE%20PROCESSES.pdf, s. 337–340, [online: 27.06.2022].
54 K. Pietryka, *Nowe technologie informacyjno-komunikacyjne w zarządzaniu kryzysowym*, [w]: red. Danielewska A., Maciąg K., *Wybrane aspekty kryminologii, kryminalistyki i bezpieczeństwa w wymiarze narodowym i międzynarodowym*, Wydawnictwo Naukowe TYGIEL, Lublin 2021, s. 25.
55 *Managing uncertainty in government modeling*, https://www.turing.ac.uk/research/research-projects/managing-uncertainty-government-modelling, [online: 27.06.2022].
56 P. Zaskórski, K. Szwarc, *Modelowanie procesów…*, *op. cit.*, s. 337.
57 Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity, s. 18.
58 *Defending Ukraine: Early Lessons from the Cyber War*, raport Microsoft, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK, s. 5, [online: 27.06.2022].
59 K. Sikorski, *Ukraina przechowuje wrażliwe dane w Polsce w specjalnie zaprojektowanej chmurze. Chroni je przed cyberprzestępcami i rakietami wroga*, [online]: https://polskatimes.pl/ukraina-przechowuje-wrazliwe-dane-w-polsce-w-specjalnie-zaprojektowanej-chmurze-chroni-je-przed-cyberprzestepcami-i-rakietami/ar/c1-16435809, [online: 27.06.2022].
60 *The Ukrainian Digital Resistance to Russian Aggression*, https://www.strategeast.org/ukrainian-digital-resistance-to-russian-aggression-report/, [online: 27.06.2022].
61 I. Albrycht, wystąpienie podczas seminarium „Stan zagrożenia – zabezpieczenie systemów teleinformatycznych", https://youtu.be/SHRwsiMW3P4 [online: 28.06.2022].
62 P. Mell, T. Grance, The NIST Definition of Cloud Computing, *Special Publication 800-145*, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf, [online: 27.06.2022].
63 P. Zaskórski, K. Szwarc, *Modelowanie procesów…*, *op. cit.*, s. 353.
64 Dyrektywa Parlamenty Europejskiego i Rady UE 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.
65 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
66 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.
67 Rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa sektora energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów, Ministerstwo Klimatu i Środowiska, wrzesień 2021 r.
68 Scandanve XP, https://www.icsec.pl/scadvance/, [online: 28.06.2022].
69 *IT vs OT Security: The Operational Technology Guide for Professionals*, https://www.otorio.com/blog/it-security-vs-ot-security-the-operational-technology-cybersecurity-guide-for-industry-professionals/, [online: 28.06.2022].
70 *ISO/IEC 27001 Information Security Management*, https://www.iso.org/isoiec-27001-information-security.html, [online: 28.06.2022].



71 *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, U.S. Department of Commerce, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final, [online: 28.06.2022].
72 *ISO 22301: 2019 Business continuity management system*, https://www.iso.org/standard/75106.html [online: 28.06.2022].
73 Rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa sektora energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów, Ministerstwo Klimatu i Środowiska, wrzesień 2021 r.
74 *J. Reed, Disaster Recovery in Cloud Computing: All you need to know*, https://www.nakivo.com/blog/disaster-recovery-in-cloud-computing/, [online: 28.06.2022].
75 *Cloud disaster recovery (cloud DR)*, https://www.techtarget.com/searchdisasterrecovery/definition/cloud-disaster-recovery-cloud-DR, [online: 28.06.2022].
76 M. Kotas, *Media społecznościowe w zarządzaniu kryzysowym organizacji*, Uniwersytet Ekonomiczny w Katowicach.
77 *Virtual assistant launched to help Ukrainian refugees access key services in Czech Republic*, https://www.ibm.com/blogs/southeast-europe/virtual-assistant-launched-to-help-ukrainian-refugees-access-key-services-in-czech-republic/, [online: 28.06.2022].
78 *Ćwierć Miliona numerów PESEL dla obywateli Ukrainy!*, https://www.gov.pl/web/cyfryzacja/cwierc-miliona-numerow-pesel-dla-obywateli-ukrainy, [online: 28.06.2022].
79 *Ukraińcy mogą korzystać z aplikacji mObywatel. Co zrobić, by ją aktywować?*, https://www.portalsamorzadowy.pl/smart-city/ukraincy-moga-korzystac-z-aplikacji-mobywatel-co-zrobic-by-ja-aktywowac,362053.html, [online: 28.06.2022].
80*Alert RCB – Najważniejsze Pytania i Odpowiedzi*, https://www.gov.pl/web/rcb/alert-rcb---najwazniejsze-pytania-i-odpowiedzi, [online: 28.06.2022].
81 F. Batista, M. Hirtzer, *JBS Paid Hackers $11 Million After Hack Crippled Meat Plants*, https://www.bloomberg.com/news/articles/2021-06-09/jbs-paid-11-million-in-ransom-to-resolve-cyberattack-dj, [online: 28.06.2022].
82 J. Magill, *U.S. Water Supply System Being Targeted By Cybercriminals*, https://www.forbes.com/sites/jimmagill/2021/07/25/us-water-supply-system-being-targeted-by-cybercriminals/?sh=4fc9b32728e7, [online: 28.06.2022].
83 G. Baryannisa, S. Validib, S. Danib, G. Antonioua, *Supply Chain Risk Management and Artificial Intelligence: State of the Art and Future Research Directions*, „International Journal of Production Research", t. 57, nr 7, 2179-2202, DOI: 10.1080/00207543.2018.1530476, s. 1.
84 H. Treiblmaier, *The impact of the blockchain on the supply chain: a theory-based research framework and a call for action*, „Supply Chain Management: An International Journal", t. 23, nr 6, s. 545–559, https://doi.org/10.1108/, s. 547.
85 Q. Zhou, H. Zhang, S. Wang, *Artificial intelligence, big data, and blockchain in food safety*, „International journal of food engineering", nr 18, 1-14. doi: 10.1515/ijfe-2021-0299, s. 10.
86 *What is the Impact of AI in the Food Supply Chain?*, https://adroitna.com/what-is-the-impact-of-ai-in-the-food-supply-chain/, [online: 28.06.2022].
87 *Ibidem.*
88 *2019 NATO Leaders' Meeting: In Brief*, Congressional Research Service, 27 listopada 2019.
89 *Resilient communications*, https://www.gov.uk/guidance/resilient-communications, [online: 28.06.2022].
90 *Ukrainian Digital Resistance to Russian Aggression*, StrategEast Center for a New Economy, 2022
91 *About 150,000 people in Ukraine are using SpaceX's Starlink internet service daily, government official says*, [online]: https://www.cnbc.com/2022/05/02/ukraine-official-150000-using-spacexs-starlink-daily.html, [online: 28.06.2022].

92 *Innovation for emergency services and the military: 4G / 5G connectivity in crisis situations*, https://www.is-wireless.com/news/innovation-for-emergency-services-and-the-military-4g-5g-connectivity--in-crisis-situations/, [online: 28.06.2022].
93 *Ukrainian Digital Resistance to Russian Aggression*, op. cit., 2022.
94 Thales, Verint, raport *The Cyberthreat Handbook*, 2019, https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who, [online: 29.06.2022].
95 I. Eusgeld, C. Nan, S. Dietz, "System-of-systems" approach for interdependent critical infrastructures, Reliability Engineering and System Safety, 96(2011) 679–686
96 https://home-affairs.ec.europa.eu/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resiliance_en [online: 28.06.2022].



INSTYTUT KOŚCIUSZKI

Instytut Kościuszki to wiodący pozarządowy ośrodek naukowo-badawczy o charakterze non-profit założony w 2000 r. Naszą misją jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski jako aktywnego członka Unii Europejskiej oraz NATO. Instytut specjalizuje się w tworzeniu strategicznych rekomendacji i kierunków rozwoju kluczowych polityk publicznych, stanowiących merytoryczne wsparcie dla polskich i europejskich decydentów politycznych. Instytut Kościuszki jest pomysłodawcą i głównym organizatorem Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC, corocznej konferencji poświęconej strategicznym aspektom cyberprzestrzeni.

ik.org.pl InstytutKosciuszki @ikosciuszki Instytut Kosciuszki

© Instytut Kościuszki 2022

Instytut Kościuszki

CYBERSEC
EUROPEJSKIE FORUM CYBERBEZPIECZEŃSTWA

Microsoft

PARTNER RAPORTU

RCB
Rządowe Centrum Bezpieczeństwa

PATRONAT

© Instytut Kościuszki 2022