Cyberprzestrzeń i kryzys odstraszania w dobie wojny kognitywnej

AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Tekst stanowi głęboką analizę transformacji bezpieczeństwa narodowego w erze cyfrowej, gdzie tradycyjne modele odstraszania ustępują miejsca asymetrycznym konfliktom. Autor przywołuje przełomowe wydarzenia, takie jak atak Stuxnet na irańskie instalacje nuklearne oraz wycieki Edwarda Snowdena, które obnażyły nową naturę globalnej rywalizacji. Artykuł zgłębia koncepcję wojny kognitywnej, dezinformacji oraz strategii 'Left of Launch', wskazując na rosnące znaczenie sabotażu infrastruktury krytycznej i systemów SCADA. To kompendium wiedzy o tym, jak państwa takie jak Rosja, Chiny czy Iran redefiniują pojęcie suwerenności i ataku w świecie pozbawionym jasnych linii frontu.

This article provides a deep analysis of the transformation of national security in the digital age, where traditional models of deterrence are giving way to asymmetric conflicts. The author revisits groundbreaking events, such as the Stuxnet attack on Iranian nuclear facilities and the Edward Snowden leaks, which exposed the new nature of global competition. The article explores the concepts of cognitive warfare, disinformation, and left-of-launch strategies, pointing to the growing importance of sabotaging critical infrastructure and SCADA systems. This compendium examines how states like Russia, China, and Iran are redefining the concepts of sovereignty and attack in a world devoid of clear battle lines.

Artykuł analizuje zmieniającą się naturę bezpieczeństwa strategicznego w erze cyfrowej, kwestionując tradycyjne zimnowojenne koncepcje odstraszania oparte na równowadze strachu. David E. Sanger argumentuje, że w cyberprzestrzeni posiadanie potężnego arsenału nie gwarantuje skutecznego odstraszania, a Stany Zjednoczone, inicjując operacje takie jak Stuxnet, paradoksalnie przyczyniły się do osłabienia globalnego bezpieczeństwa. Rewelacje Snowdena obnażyły asymetrię między retoryką a praktyką

państwa, podważając zaufanie i legitymizując autorytarne tendencje. W efekcie, cyberprzestrzeń stała się polem gry dla nowych aktorów, takich jak Iran, Korea Północna i Chiny, wykorzystujących ją do niwelowania przewagi militarnej Zachodu i osiągania własnych celów. Artykuł wskazuje na potrzebę nowego podejścia do odstraszania, uwzględniającego odporność, normy i normatywne tabu, a także na rosnącą rolę korporacji w zapewnianiu bezpieczeństwa w cyfrowym świecie, gdzie wojna o uwagę i pamięć staje się kluczowym polem walki.

SŁOWA KLUCZOWE

cyberprzestrzeń | kryzys odstraszania | wojna kognitywna | Stuxnet | operacja Olympic Games | efekt Snowdena | sabotaż cyfrowy | doktryna Gierasimowa | wojna hybrydowa | atrybucja ataku | infrastruktura krytyczna | systemy SCADA | ransomware | dezinformacja | Left of Launch

Brak atrybucji paraliżuje tradycyjne odstraszanie

Przywykliśmy do myślenia o bezpieczeństwie strategicznym przez pryzmat zimnowojennej kliszy, w której stabilność porządku światowego gwarantowała równowaga skrajnego ryzyka. W tej logice żadna ze stron nie mogła rozpocząć wojny atomowej bez pewności własnego unicestwienia. W tym horyzoncie wyobraźni odstraszanie przez groźbę nieakceptowalnej szkody stanowiło nie tyle instrument polityki, ile swoistą metafizykę nowoczesności. David E. Sanger proponuje jednak radykalne zerwanie z tym odruchem analogii. Jego teza jest prosta i wywrotowa: w erze cybernetycznej posiadanie najpotężniejszego arsenału nie przekłada się automatycznie na skuteczne odstraszanie. Stany Zjednoczone stały się pionierem nowej broni w świecie, który nie zdołał jeszcze wytworzyć równoważących ją norm i instytucji. Cyberprzestrzeń okazała się nie tyle kolejną domeną wojny, ile laboratorium rozsadzającym tradycyjne pojęcie równowagi strachu.

Olympic Games: cyberatak niszczy infrastrukturę fizyczną

Pierwszym doświadczeniem, które w tym laboratorium przekroczyło skalę zwykłej operacji wywiadowczej, była operacja Olympic Games, publicznie znana jako Stuxnet. W wymiarze technicznym był to kod o niezwykłej złożoności, zaprogramowany niczym cyfrowy pocisk samonaprowadzający, by spośród milionów systemów sterowania przemysłowego odnaleźć jedną, unikalną konfigurację wirówek w irańskim ośrodku wzbogacania uranu w Natanz. W wymiarze politycznym stanowił on próbę rozwiązania podwójnego dylematu: jak skutecznie opóźnić irański program nuklearny, nie prowokując jednocześnie izraelskiego nalotu, który nieuchronnie wciągnąłby Stany Zjednoczone w kolejną wojnę na Bliskim Wschodzie. Amerykańscy decydenci, cytowani przez Davida Sangera, potrzebowali broni, która zniszczy wirówki, a nie flagę – i to w sposób pozwalający wszystkim stronom udawać, że nic się nie stało.

W tym sensie Stuxnet był czymś znacznie więcej niż technologicznym majstersztykiem. Był przede wszystkim decyzją, by po raz pierwszy w czasie formalnego pokoju użyć kodu komputerowego do fizycznego zniszczenia infrastruktury innego państwa. Generał Michael Hayden, były dyrektor CIA i NSA, porównał ten moment do sierpnia 1945 roku, kiedy bomba atomowa objawiła światu zupełnie nowy wymiar destrukcji. Jego słowa, że w powietrzu czuć było „zapach sierpnia czterdziestego piątego roku", nie były banalną analogią historyczną. Wskazywały na jakościową zmianę: oto użyto broni, której skutków nie sposób było cofnąć ani politycznie, ani technologicznie.

Techniczna logika Stuxnetu opierała się na precyzyjnym połączeniu sabotażu z iluzją. Kod z jednej strony subtelnie manipulował prędkością obrotową wirówek, doprowadzając je do fizycznej destrukcji, z drugiej zaś generował fałszywe odczyty, które utwierdzały irańskich operatorów w przekonaniu, że cała instalacja pracuje stabilnie. W języku ekonomii można by to przyrównać do ataku na system księgowy, który jednocześnie fabrykuje fikcyjne zyski i po cichu niszczy realne aktywa firmy, aż do momentu jej gwałtownego bankructwa. W sferze antropologicznej mamy tu do czynienia z doświadczeniem, w którym świat przeżywany – codzienny horyzont zawodowej kompetencji inżynierów – zostaje potajemnie wypaczony przez niewidzialnego przeciwnika.

Jednak to nie taktyczny sukces operacji, lecz jej niekontrolowane efekty uboczne stały się zarzewiem kryzysu odstraszania. Kod wymknął się bowiem poza hermetyczne środowisko w Natanz i zaczął replikować się w globalnej sieci. Firmy z branży cyberbezpieczeństwa, analizując go warstwa po warstwie, doszły do nieuchronnego wniosku, że jego autorem musiało być państwo dysponujące olbrzymimi zasobami. W ten sposób świat otrzymał dowód, że Stany Zjednoczone nie tylko posiadają broń zdolną do niszczenia infrastruktury krytycznej, ale są też gotowe jej użyć.

Równocześnie, skoro broń cyfrowa jest w swej istocie kodem, a więc informacją, jej analiza stała się wzorem i zachętą dla innych państw. Grzech pierworodny polegał na tym, że państwo, które samo chciało utrzymać monopol, zarazem ujawniło reguły gry.

Efekt Snowdena: fragmentacja globalnej architektury

Drugi próg w genealogii współczesnego kryzysu odstraszania wyznacza afera Edwarda Snowdena. Z perspektywy teorii systemów nieistotna jest tu osobista motywacja sygnalisty, lecz fakt, że jego działania obnażyły fundamentalną asymetrię między oficjalną retoryką państwa a jego rzeczywistą praktyką. Stany Zjednoczone publicznie odgrywały rolę ofiary agresywnych działań Rosji, Chin czy Iranu, podczas gdy w cieniu prowadziły masową inwigilację własnych obywateli i sojuszników. Co więcej, ingerowały w infrastrukturę globalnych dostawców sprzętu i instalowały tylne furtki w urządzeniach firm, które o te same praktyki oskarżały.

Snowden nie dokonał tego za pomocą genialnego hakerskiego wyczynu, lecz przy użyciu prostego programu typu web crawler. To szczegół o ogromnym znaczeniu symbolicznym, dowodzi bowiem, że budowa najbardziej wyrafinowanej technologicznej fortecy jest daremna, jeśli jej wewnętrzne procedury opierają się na anachronicznym zaufaniu do własnych administratorów. Używając języka ekonomii, można rzec, że NSA poniosła klęskę nie wskutek zewnętrznego szoku, lecz wewnętrznego kryzysu ładu korporacyjnego i fatalnego zarządzania ryzykiem agencyjnym.

W wymiarze geopolitycznym efekt Snowdena był dwojaki. Po pierwsze, zdemolował zaufanie między rządem USA a kluczowymi firmami technologicznymi. Ujawnienie ataków typu man-in-the-middle na łącza między centrami danych Google czy praktyki masowego pozyskiwania metadanych telefonicznych sprawiło, że giganci tacy jak Google czy Apple zaczęli traktować własne państwo jako jednego z głównych adwersarzy. Odpowiedź była natychmiastowa i radykalna: gwałtowna ekspansja szyfrowania, od komunikacji wewnętrznej po domyślną ochronę pamięci urządzeń mobilnych.

Po drugie, rewelacje Snowdena dostarczyły autorytarnym reżimom wymarzonego pretekstu do legitymizacji własnej cenzury. Chiny i Rosja mogły odtąd twierdzić, że wprowadzają przepisy o lokalizacji danych nie z żądzy kontroli, lecz w obronie przed wszechobecną inwigilacją NSA. W rezultacie cyfrowa utopia, która w liberalnej wizji miała być uniwersalnym medium wolnej informacji, uległa bałkanizacji. Przestrzeń cyfrową pocięto na narodowe i blokowe segmenty, zmuszając transnarodowe korporacje do nieustannej ekwilibrystyki i negocjowania lojalności między sprzecznymi reżimami prawnymi.

Sanger trafnie diagnozuje tu paradoks, który w filozofii prawa można określić jako aporię legalizmu. Państwo, które maksymalizuje swoje zdolności wywiadowcze z pominięciem demokratycznej kontroli, podkopuje własną legitymację. Tym samym odbiera sobie zdolność do budowania międzynarodowych norm, które miałyby ograniczać agresję innych. O ile w sferze nuklearnej Ameryka potrafiła być współarchitektem globalnego porządku, o tyle w cyberprzestrzeni w dużej mierze utraciła moralny autorytet niezbędny do odgrywania roli normatywnego hegemona.

Cyberprzestrzeń niweluje technologiczną przewagę Zachodu

Na tej scenie pojawiają się aktorzy, których David Sanger trafnie określa mianem nowych graczy, choć geopolitycznie są to państwa doskonale znane. Ich nowość polega na odkryciu, że cyberprzestrzeń to doskonały instrument do niwelowania tradycyjnej przewagi militarnej Zachodu. Iran potraktował cyfrową konfrontację jako asymetryczny rewanż za Stuxnet i sankcje. Zamiast celować w infrastrukturę wojskową, uderzył w miękkie podbrzusze gospodarki: finanse i energetykę. Ataki DDoS na amerykańskie banki czy niszczycielski Shamoon wymierzony w Saudi Aramco były tego brutalnym dowodem. Trzydzieści tysięcy dysków twardych nie tylko wyczyszczono, ale ich zawartość zastąpiono obrazem płonącej flagi – to był czytelny komunikat dla elit gospodarczych: wasza potęga militarna nie ochroni waszych łańcuchów wartości.

Korea Północna poszła o krok dalej, traktując cyberwojnę jako „wszechstronny miecz" – narzędzie totalne, służące jednocześnie do zastraszania, kradzieży i obchodzenia sankcji. Atak na Sony Pictures za film kpiący z przywódcy był manifestacją siły. Próba kradzieży miliarda dolarów z Banku Centralnego Bangladeszu, częściowo udana, pokazała zuchwałość. Globalny atak ransomware WannaCry, oparty na narzędziach wykradzionych z NSA przez grupę Shadow Brokers, dowiódł z kolei, że reżim w Pjongjangu pojął logikę globalnego systemu finansowego znacznie lepiej, niż chciałoby to przyznać wielu bankierów z Wall Street.

W ten sposób państwowa cyberprzestępczość staje się de facto formą finansowania programów nuklearnych i rakietowych. To swoisty podatek nakładany na globalny system, którego płatnikami są nieostrożne instytucje finansowe i najsłabsze ogniwa cyfrowej infrastruktury. Z perspektywy ekonomii politycznej jesteśmy świadkami narodzin nowej formy ekstrakcji renty. Tutaj jednak narzędziem nie jest już własność ziemi czy przewaga w produkcji przemysłowej, lecz coś znacznie bardziej ulotnego: dostęp do luk w oprogramowaniu i ludzka podatność na socjotechnikę.

Model chiński: masowy drenaż własności intelektualnej

Chiński model działania w cyberprzestrzeni stanowi jednak osobny paradygmat. Jego celem nie jest demonstracyjne niszczenie, lecz cierpliwa, systematyczna akumulacja danych i własności intelektualnej. Wyspecjalizowane struktury, jak osławiona Jednostka 61398, przez lata prowadziły operacje będące w istocie długotrwałą kradzieżą planów, kodów źródłowych i tajemnic handlowych. Kulminacją tej strategii było włamanie do amerykańskiego Biura Zarządzania Personelem (OPM), skąd pozyskano dane 22 milionów urzędników. Ich szczegółowe dossier, obejmujące życie prywatne i zawodowe, stworzyło nie tylko potężny potencjał szantażu, lecz także precyzyjną mapę powiązań wewnątrz amerykańskich elit administracyjnych.

Z perspektywy antropologii państwa autorytarnego takie zbiory danych przekształcają się w instrument kontroli nad transnarodowymi przepływami kompetencji oraz lojalności. Chińska strategia jest zatem bardziej cierpliwa niż koreańska i mniej spektakularna niż irańska. W długim okresie może się jednak okazać groźniejsza, ponieważ nie niszczy istniejących zasobów, lecz systematycznie zmienia samą strukturę przewag komparatywnych w gospodarce opartej na wiedzy.

Ukraina i USA: rosyjskie poligony wojny hybrydowej

Rosja pod rządami Władimira Putina potraktowała cyberprzestrzeń nie jako zwykłe narzędzie szpiegowskie, lecz jako medium do ingerencji w samą tkankę społecznego doświadczenia Zachodu. Tak zwana doktryna Gierasimowa, czyli strategia zakładająca permanentny konflikt poniżej progu otwartej wojny, unieważnia tradycyjny podział na czas pokoju i czas konfrontacji. Granica między nimi ulega celowemu rozmyciu, a wojna nie potrzebuje już formalnej deklaracji.

Ukraina stała się poligonem doświadczalnym dla tej doktryny. Wyłączenie fragmentów sieci energetycznej przez zdalne operacje na systemach SCADA, z użyciem takich narzędzi jak BlackEnergy i KillDisk, było brutalnym dowodem, że klasyczne środki militarne – czołgi, artyleria i osławione „zielone ludziki” – można bezszwowo połączyć z niewidzialną ofensywą cyfrową. Ofensywą, która uderza w codzienność ludności cywilnej. Atak NotPetya, który zainfekował ukraińskie oprogramowanie księgowe, by następnie sparaliżować globalne łańcuchy dostaw, z gigantem logistycznym Maersk na czele, pokazał, jak lokalny konflikt hybrydowy potrafi zmutować w globalny kryzys gospodarczy, liczony w setkach milionów dolarów strat.

Kulminacją tej strategii stała się ingerencja w wybory prezydenckie w Stanach Zjednoczonych w 2016 roku. Nie chodziło w niej jednak wyłącznie o techniczne włamanie na serwery Partii Demokratycznej czy do skrzynki Johna Podesty, ani nawet o precyzyjne publikowanie

wykradzionych e-maili w kluczowych momentach kampanii. Kluczowy okazał się komponent psychologiczny: użycie farm trolli i operacji w mediach społecznościowych do rozniecania istniejących już podziałów rasowych, religijnych i politycznych. Rosyjska interwencja była zatem nie tyle zewnętrznym atakiem na instytucje, ile katalizatorem wewnętrznych konfliktów, które i tak wrzały w amerykańskim społeczeństwie.

Patrząc przez pryzmat teorii społecznej, można postawić tezę, że rosyjska wojna hybrydowa instrumentalnie wykorzystuje media komunikacji do swoistej refeudalizacji sfery publicznej. Tam, gdzie racjonalna debata miała być fundamentem, pojawia się gęsta mgła dezinformacji, teorii spiskowych i emocjonalnych zrywów. Jej strażnikami nie są już instytucje prawa, lecz algorytmy rekomendacyjne i anonimowe kampanie wpływu, napędzane ukrytym kapitałem.

Left of Launch: zawodna prewencja przed startem rakiet

Strategia Left of Launch, opracowana w odpowiedzi na koreański program rakietowy, stanowi próbę przeniesienia logiki prewencji chirurgicznej wprost do arsenału cyfrowego. Zamiast podejmować niemal niemożliwą próbę zestrzelenia pocisku pędzącego z prędkością hipersoniczną, system ma za zadanie zainfekować go jeszcze na ziemi. Celem jest sabotowanie kodu na etapie testów, zakłócanie procesu tankowania czy paraliżowanie systemów nawigacyjnych tuż przed zapłonem.

Rachunek ekonomiczny wydaje się tu bezlitosny. Obrona kinetyczna jest niebotycznie droga i obarczona wysoką niepewnością, a każdy udany test przeciwnika wzmacnia jego wiarygodność odstraszania. Cyfrowy sabotaż jawi się jako rozwiązanie tańsze i bardziej finezyjne. David Sanger dowodzi jednak, że sukces tej strategii jest w najlepszym razie chwilowy. Rok 2016 zdawał się potwierdzać jej skuteczność serią spektakularnych awarii północnokoreańskich rakiet Musudan, co w Pentagonie odczytano jako cichy triumf. Radość była jednak przedwczesna. Już rok później Korea Północna wdrożyła nowe silniki, radykalnie poprawiła niezawodność startów i przystąpiła do testów międzykontynentalnych oraz broni termojądrowej.

W tle tych technicznych zmagań narasta jednak świadomość znacznie głębszego ryzyka strategicznego. Jak wskazuje Jon Lindsay, próby ingerencji w systemy dowodzenia i kontroli broni jądrowej mogą podważyć zaufanie decydentów do własnego arsenału. To z kolei niebezpiecznie zwiększa prawdopodobieństwo działań impulsywnych lub katastrofalnych w skutkach błędów w sytuacji kryzysowej. Innymi słowy, narzędzie zaprojektowane do redukcji ryzyka w krótkiej perspektywie, w długiej perspektywie może erodować same fundamenty stabilności opartej na odstraszaniu nuklearnym.

Anonimowość sprawców blokuje odwet w cyberprzestrzeni

David Sanger stawia brutalną diagnozę: przeciwnicy USA, jak ujął to generał Paul Nakasone, po prostu się ich nie boją. Nie widzą bowiem realnej groźby poniesienia dotkliwych kosztów za swoje działania. W języku teorii odstraszania oznacza to, że zawodzi co najmniej jeden z czterech warunków koniecznych, sformułowanych przez Martina Libickiego. Chodzi o zdolność do wiarygodnego przypisania ataku, jasne wyznaczenie czerwonych linii, wiarygodność zapowiedzianej kary oraz rzeczywiste zdolności do jej wymierzenia.

W cyberprzestrzeni każdy z tych filarów kruszeje w specyficzny sposób. Atrybucja się rozmywa, gdyż agresor może ukryć się za labiryntem serwerów pośredniczących, zaprzęgnąć do działania botnet albo użyć kodu skradzionego wcześniej komuś innemu. Czerwone linie toną we mgle celowej niejednoznaczności, ponieważ państwa wolą nie precyzować, które działania uznają za casus belli, czyli powód do wojny. Wiarygodność odpowiedzi słabnie, gdy reakcja jest albo symboliczna, ograniczona do mało dotkliwych sankcji, albo tak tajna, że nie pełni funkcji odstraszającej – pozostaje niewidoczna dla opinii publicznej i potencjalnych naśladowców. Wreszcie potężne zdolności odwetowe muszą być nieustannie korygowane przez świadomość własnej kruchości; społeczeństwo i infrastruktura USA są tak głęboko scyfryzowane, że stają się bardziej podatne na cios niż systemy ich przeciwników.

Joseph Nye proponuje zatem, by poszerzyć klasyczną koncepcję odstraszania o cztery uzupełniające się mechanizmy: karę, zapobieganie przez obronę, uwikłanie i normatywne tabu. W cyfrowym świecie można bowiem odstraszać nie tylko groźbą odwetu. Można to robić również poprzez budowanie tak wysokiej odporności, że atak staje się nieopłacalny, poprzez wzajemne powiązania gospodarcze, które czynią agresję aktem ekonomicznego samobójstwa, oraz przez powolne tworzenie globalnych norm, zakazujących na przykład ataków na szpitale czy sieci energetyczne w czasie pokoju.

Jednocześnie spora część literatury naukowej podaje w wątpliwość samo pojęcie cyberodstraszania. Niektórzy autorzy sugerują, by porzucić je jako anachronizm z innej epoki. Inni chcą ograniczyć jego zastosowanie wyłącznie do relacji międzypaństwowych i zagrożeń o najwyższej skali. Jeszcze inni próbują budować szerokie, syntetyczne ujęcie, łączące wszystkie wymiary, o których pisze Nye. W tym akademickim sporze teza Sangera jawi się jako głos realizmu, krytyczny wobec nazbyt optymistycznych projektów, które zakładają, że cyberprzestrzeń da się zamknąć w ramach analogicznych do epoki nuklearnej.

Aby uchwycić istotę tej aporii w skondensowanej formie, posłużmy się prostym modelem z rachunku zdań. Niech zdanie p oznacza, że broń jest widoczna i policzalna, jak w przypadku arsenału jądrowego. Niech zdanie q oznacza, że sprawca ataku jest łatwo identyfikowalny. Wreszcie, niech zdanie r oznacza, że klasyczne odstraszanie, oparte na groźbie odwetu, jest skuteczne.

W modelu zimnowojennym przyjmujemy dwie przesłanki. Po pierwsze, jeśli broń jest widoczna i policzalna (p), a sprawca łatwo identyfikowalny (q), to klasyczne odstraszanie działa (r). W logice zapisujemy to jako implikację: $(p \wedge q) \rightarrow r$. Po drugie, doświadczenie epoki nuklearnej potwierdza, że zarówno p, jak i q są prawdziwe; mocarstwa znały swoje arsenały, a atak rakietowy nie mógł być skutecznie ukryty. Z tych dwóch przesłanek logicznie wynika, że r jest prawdziwe. Odstraszanie działało, czego historycznym dowodem był brak bezpośredniego starcia nuklearnego.

Tu pojawia się zagadka. W cyberprzestrzeni obserwujemy, że r jest fałszywe – liczne ataki uchodzą płazem, a odstraszanie zawodzi. Gdzie zatem pęka ten klasyczny model? Czy fałszywe stało się zdanie p? A może q? Czy też może cała implikacja, która łączy je z r, straciła ważność?

Rozwiązanie tej łamigłówki wymaga zrozumienia, że w cyberprzestrzeni fałszywe są jednocześnie p i q, przez co cała implikacja traci moc opisową. Broń cyfrowa nie jest widoczna i policzalna w tym samym sensie co głowice; jej zasób jest płynny, można go kopiować, modyfikować i kraść. Jednocześnie tożsamość sprawcy może pozostać na tyle niejednoznaczna, że przypisanie winy staje się przedmiotem politycznych sporów, a nie twardym faktem. W rezultacie przesłanki klasycznego modelu nie są spełnione, a zatem nie ma podstaw, by oczekiwać, że jego konkluzja będzie prawdziwa. Innymi słowy, logiczna forma pozostaje poprawna, lecz przestaje mieć zastosowanie do nowej rzeczywistości. Kryzys odstraszania nie jest więc porażką rozumu, lecz skutkiem upartego stosowania starych map do opisu nowego, nieznanego terytorium.

Cyberataki: ryzyko systemowe dla globalnego biznesu

Jeżeli ta rekonstrukcja jest trafna, to jej konsekwencje dla globalnego biznesu są fundamentalne. Cyberprzestrzeń przestaje być domeną zastrzeżoną dla służb specjalnych i staje się polem gry strategicznej, na którym korporacje występują jako równorzędni gracze. Uderzenie w łańcuch dostaw koncernu motoryzacyjnego, atak na systemy księgowe międzynarodowego operatora logistycznego czy paraliż placówek medycznych przez ransomware to operacje o skutkach porównywalnych z klasycznymi sankcjami gospodarczymi. To już nie jest problem techniczny – to nowa forma ekonomicznej presji.

Potwierdzają to twarde dane. Raporty Światowego Forum Ekonomicznego, zarówno Global Cybersecurity Outlook, jak i Global Risks Report, konsekwentnie umieszczają zagrożenia cyfrowe w ścisłej czołówce ryzyk postrzeganych przez kadrę zarządzającą na świecie. Ponad siedemdziesiąt procent respondentów najnowszego Outlooka przyznaje, że zagrożenia cybernetyczne nasiliły się w ostatnim roku, a największy niepokój budzą cyberoszustwa, phishing i ataki na infrastrukturę krytyczną. W innym badaniu, przeprowadzonym wspólnie przez Marsh i Microsoft, podobny odsetek członków rad nadzorczych zalicza cyberyzyko do pięciu najważniejszych zagrożeń dla organizacji. Jednocześnie zaledwie niewielka grupa deklaruje wysoką pewność co do zdolności firmy do skutecznej obrony.

Najnowsze dane z rynku europejskiego tylko wzmacniają ten obraz. Niemal co trzeci menedżer odpowiedzialny za zakupy odnotował w ostatnich miesiącach wzrost liczby ataków na łańcuchy dostaw. Spektakularne incydenty, takie jak ataki na producentów samochodów, sieci handlowe czy firmy z sektora spożywczego, przyniosły straty liczone w setkach milionów euro, wymuszając gwałtowną rewizję strategii budowania odporności.

Z perspektywy teorii przedsiębiorstwa oznacza to sejsmiczną zmianę. Cyberbezpieczeństwo przestaje być domeną działu IT, a staje się kluczowym elementem ładu korporacyjnego, który bezpośrednio wpływa na wycenę firmy, koszt kapitału i zdolność do utrzymania reputacji. Inwestorzy instytucjonalni coraz częściej traktują odporność cyfrową jako integralny składnik oceny czynników ESG, jasno komunikując, że zarządy bagatelizujące to ryzyko narażają spółkę na katastrofalne straty finansowe i regulacyjne.

W tym sensie wojna hybrydowa, którą Sanger opisuje na przykładzie państw narodowych, przenosi się wprost do świata korporacji. Firma staje się jednocześnie celem potencjalnych ataków i aktorem odpowiedzialnym za utrzymanie stabilności własnego ekosystemu. Nie wystarczy już bronić własnych serwerów; trzeba monitorować bezpieczeństwo dostawców, klientów i partnerów. Logika ryzyka systemowego, którą znamy z kryzysu finansowego z 2008 roku, powraca w nowej, cyfrowej odsłonie. Tym razem jednak toksyczne aktywa nie kryją się w bilansach banków. Są nimi podatności w kodzie i zaniedbania w procesach aktualizacji oprogramowania.

Cyfrowy impas: brak zgody na międzynarodowe normy

Broniąc zasadniczej intuicji Sangera, musimy zadać sobie pytanie o naturę obecnego kryzysu. Czy mamy do czynienia z trwałym, strukturalnym paraliżem odstraszania, czy raczej z chorobą wieku dziecięcego ery cyfrowej? Część badaczy słusznie przypomina, że pierwsze lata epoki atomowej również naznaczone były chaosem, brakiem spójnych doktryn i niebezpiecznymi, przypadkowymi

eskalacjami. Dopiero po kilkunastu latach wyłonił się z tego zgiełku stabilniejszy reżim wzajemnie gwarantowanego zniszczenia.

Można zatem argumentować, że obecny nieład jest jedynie stadium przejściowym, w którym normy, doktryny i praktyki dopiero krystalizują się w ogniu codziennych starć. Rozwijane w amerykańskich dokumentach strategicznych pojęcie integrated deterrence, czyli odstraszania zintegrowanego, zakłada zharmonizowanie wszystkich domen – od nuklearnej, przez konwencjonalną, aż po cybernetyczną i kosmiczną – oraz włączenie w ten system aktorów prywatnych. To program o niemal utopijnej ambicji, jeśli weźmiemy pod uwagę fragmentaryzację cyfrowej przestrzeni, rozbieżność korporacyjnych interesów i narastające napięcia geopolityczne.

Z drugiej strony, krytycy podnoszą fundamentalny zarzut: nacisk na odstraszanie w cyberprzestrzeni może prowadzić do jej dalszej militaryzacji kosztem inwestycji w odporność, edukację i regulacje. Jeśli każde stworzone przez nas narzędzie ofensywne może zostać skradzione i obrócone przeciwko nam, logika wyścigu zbrojeń zaczyna przypominać próbę gaszenia pożaru benzyną. W tym sensie teza Sangera o grzechu pierworodnym operacji Olympic Games rozciąga się na wszystkie współczesne programy ofensywne. Nie chodzi tu o moralne potępienie, lecz o chłodną konstatację: każdy nowy precedens poszerza pole tego, co inni uznają za dopuszczalne.

Jako ekonomista i doradca gospodarczy muszę podkreślić, że żadne rozwiązanie nie będzie polegało na mechanicznym przeniesieniu modeli z przeszłości. Współczesność domaga się tego, co można nazwać racjonalnością profetyczną – zdolności do łączenia trzeźwej analizy z odwagą wyobraźni. Wydaje się, że konieczne jest działanie na co najmniej trzech płaszczyznach.

Po pierwsze, budowa normatywnego tabu wokół określonych kategorii celów, na wzór zakazu stosowania broni chemicznej. Propozycja tak zwanej Cyfrowej Konwencji Genewskiej, wysuwana między innymi przez liderów sektora technologicznego, wskazuje na pilną potrzebę ochrony ludności cywilnej przed atakami na szpitale, sieci energetyczne czy wodociągi w czasie pokoju. Trudność polega na tym, że państwa musiałyby zrezygnować z części własnych zdolności ofensywnych, na przykład z uśpionych implantów w cudzych sieciach, aby wiarygodnie domagać się tego samego od innych.

Po drugie, budowa odporności rozumianej nie tylko technicznie, lecz także organizacyjnie i kulturowo. Oznacza to redefinicję bezpieczeństwa korporacyjnego jako wspólnego zasobu całej organizacji, a nie zadania wąsko wyspecjalizowanego działu IT. Wymaga to nie tylko inwestycji w technologię, lecz także transformacji logiki raportowania i odpowiedzialności na poziomie zarządu. Zarządy i rady nadzorcze, które traktują cyberbezpieczeństwo jak kolejną pozycję w macierzy

ryzyka, nie rozumieją, że jest ono dziś warunkiem fundamentalnego zaufania, bez którego rynki po prostu przestają funkcjonować.

Po trzecie, realistyczna rewizja doktryny odstraszania w cyberprzestrzeni, oparta na brutalnym założeniu, że pełne przeniesienie wzorca nuklearnego jest niemożliwe. Należy przyjąć, że część wrogich działań zawsze będzie rozgrywać się poniżej progu

Wojna kognitywna: AI automatyzuje manipulację umysłem

Jeżeli dotychczasowa analiza prowadziła od operacji Olympic Games, grzechu pierworodnego cyberwojny, przez rewelacje Snowdena i nową kartografię sił, aż po kryzys odstraszania w sferze infrastruktury, to logicznym zwieńczeniem musi być zejście o jeden poziom głębiej. Schodzimy z warstwy przewodów, serwerów i sieci energetycznych do samej tkanki, która nadaje im realność: do uwagi, pamięci i aksjologicznych przekonań ludzi zanurzonych w cyfrowej przestrzeni. To tutaj klasyczny język bezpieczeństwa państwa spotyka się z teorią mediów i antropologią poznania. Decydujące staje się bowiem nie to, jakie dane posiadamy, lecz to, w jaki sposób są one filtrowane i prezentowane – proces w coraz większym stopniu modelowany przez sztuczną inteligencję, która kształtuje świat przeżywany obywateli i konsumentów.

To, co w literaturze strategicznej określa się dziś mianem wojny kognitywnej, nie jest prostym rozwinięciem propagandy. W dokumentach NATO pojawia się definicja, która opisuje ją jako sztukę posługiwania się technologią w celu przekształcania procesów poznawczych jednostek. Kluczowe jest to, że ani cele ataku, ani znacząca część ich otoczenia nie są świadome, że znajdują się w polu oddziaływania. Inne ujęcie jest jeszcze bardziej dosadne: w tej odmianie konfliktu ludzki umysł staje się jednocześnie polem walki i bronią. Gra toczy się o zdolność do formowania percepcji, pamięci zbiorowej oraz fundamentalnych kryteriów odróżniania prawdy od fałszu.

Gdy do tej definicji dodamy współczesne systemy sztucznej inteligencji – zwłaszcza te działające w tle jako silniki rekomendacji, mechanizmy rankingowe czy generatory przekazów – otrzymujemy obraz, w którym walka o infrastrukturę krytyczną jest zaledwie potyczką na powierzchni. Prawdziwa wojna toczy się o fundamenty: o to, jakie bodźce ciekawości, jakie ramy interpretacyjne i jakie pakiety informacji zostaną w ogóle dopuszczone do świadomości użytkownika. Logika nowoczesnych algorytmów, projektowanych dla maksymalizacji zaangażowania, prowadzi do sytuacji, którą Światowe Forum Ekonomiczne w swoim raporcie o globalnych ryzykach nazywa

wprost: dezinformacja i błędna informacja, turbodoładowane przez AI, stają się najpoważniejszym krótkoterminowym zagrożeniem dla stabilności społecznej.

Można zatem powiedzieć, że o ile klasyczne cyberataki, wymierzone w sieci energetyczne czy systemy bankowe, uderzają w to, co fizycznie umożliwia funkcjonowanie społeczeństwa, o tyle wojna kognitywna ingeruje w to, co nadaje temu funkcjonowaniu sens. Atak na elektrownię powoduje przerwę w dostawie prądu; atak na pamięć zbiorową i strukturę uwagi niszczy zdolność do wspólnego zdefiniowania, czym w ogóle jest sytuacja, w której się znaleźliśmy. Analitycy NATO podkreślają, że wojna kognitywna niejako wchłania dotychczasowe kategorie wojny informacyjnej i psychologicznej. W zmienionej architekturze cyfrowego środowiska wszystko, co publiczne, staje się potencjalnym instrumentem walki o percepcję.

W tym środowisku sztuczna inteligencja odgrywa rolę potężnego katalizatora. Po pierwsze, pozwala generować treści na niewyobrażalną dotąd skalę i z takim stopniem personalizacji, że każdy odbiorca otrzymuje własną, skrojoną na miarę wersję rzeczywistości. Badania nad kampaniami dezinformacyjnymi pokazują, że systemy uczące się potrafią segmentować populację według wrażliwości emocjonalnej i uprzedzeń poznawczych, by następnie projektować przekazy maksymalizujące długotrwały wpływ na przekonania. Po drugie, te same aksjologicznie obojętne mechanizmy sterują rekomendacjami

Politycy bagatelizują dezinformację dla doraźnych zysków

Pozostaje jednak fundamentalne pytanie: dlaczego wojna o uwagę i pamięć, mimo rosnącej literatury strategicznej i ostrzeżeń ze strony globalnych instytucji, wciąż nie jest traktowana z powagą należną atakom na infrastrukturę krytyczną? Odpowiedź wymaga rozróżnienia dwóch fundamentalnie odmiennych typów zagrożeń. Pierwsze można opisać metaforą nagłej ciemności. Gdy cyberatak paraliżuje sieć energetyczną wielkiego miasta, gdy milkną terminale płatnicze, a samoloty grzęzną na lotniskach, każdy decydent wie, że ma do czynienia z namacalnym kryzysem. Będzie on relacjonowany przez media, mierzony w utraconych punktach PKB i straconych głosach wyborców.

Drugi typ zagrożenia przypomina raczej mgłę. Pojawia się stopniowo, zagęszcza powoli i nie daje się sprowadzić do jednego, spektakularnego incydentu. Rozproszone kampanie dezinformacyjne, subtelne przesuwanie ram debaty publicznej, postępująca erozja zaufania do instytucji czy aksjologiczna polaryzacja społeczeństwa to procesy, których nie sposób przypisać do konkretnego

zdarzenia i jednego sprawcy. Politycy, funkcjonujący w krótkim rytmie kadencji, sondaży i medialnych cykli, instynktownie reagują na ciemność. Mgłę natomiast rozumieją słabo, jeśli w ogóle. Atak na elektrownię ma bowiem bezpośrednie przełożenie na słupki poparcia, podczas gdy atak na strukturę przekonań rozciąga się na lata i rozmywa się wśród wielu aktorów, także tych krajowych.

Tu właśnie odsłania się kolejny paradoks. Walka o uwagę toczy się nie tylko między państwami i ich służbami, lecz także wewnątrz nich: między partiami politycznymi, mediami, influencerami i korporacjami technologicznymi. Politycy są w tej grze jednocześnie ofiarami, uczestnikami i beneficjentami. Wiele narzędzi, które w literaturze o wojnie kognitywnej opisuje się jako instrumenty wrogiego wpływu, znajduje swoje lustrzane odbicie w arsenałach narodowych kampanii. Mikrotargetowanie przekazów, testowanie komunikatów przez sztuczną inteligencję czy manipulacja emocjami w mediach społecznościowych to techniki z powodzeniem wykorzystywane również przez partie demokratyczne. Trudno zatem oczekiwać, by ci sami aktorzy, którzy z nich korzystają, definiowali je jako zagrożenie wymagające ostrych regulacji.

Do tego dochodzi poważny problem normatywny. O ile atak na elektrownię jest jednoznacznym naruszeniem suwerenności, o tyle kampania wpływu, polegająca na rozpowszechnianiu treści kontrowersyjnych, lecz formalnie mieszczących się w granicach swobody wypowiedzi, jest niezwykle trudna do zaklasyfikowania jako akt wrogi w sensie prawnym. Każda próba regulacji sfery przekonań i światopoglądów natychmiast natrafia na zarzut cenzury i tłumienia pluralizmu. W rezultacie powstaje próżnia normatywna, w której aktorzy państwowi, platformy technologiczne i globalny biznes przerzucają się odpowiedzialnością za utrzymanie integralności informacyjnej społeczeństwa.

Wreszcie, sama kategoria cyberbezpieczeństwa została ukształtowana w cieniu paradygmatu infrastrukturalnego. Przez lata koncentrowano się na ochronie sieci, serwerów i danych, a nie na ochronie delikatnych procesów formowania opinii publicznej. Jednym ze skutków ubocznych tego podejścia jest strukturalne niedoszacowanie roli, jaką architektury algorytmiczne odgrywają w kształtowaniu pamięci i uwagi, zwłaszcza w perspektywie międzypokoleniowej. UNESCO, pracując nad wytycznymi dotyczącymi etyki AI w edukacji, alarmuje, że brak refleksji nad tym, jak młode pokolenie będzie odróżniać prawdę od fałszu, stanowi zagrożenie dla samej idei edukacji jako procesu emancypacyjnego.

Edukacja krytyczna buduje odporność w ekonomii uwagi

Z perspektywy ekonomii wojna o uwagę jest przede wszystkim bitwą o zasób rzadki i, co kluczowe, nieodnawialny. W przeciwieństwie do mocy obliczeniowej czy przepustowości sieci, czas i zdolność koncentracji człowieka nie rosną wraz z postępem technologicznym. Pozostają tragicznie stałe, podczas gdy liczba bodźców, komunikatów i ofert pęcznieje w tempie wykładniczym. Platformy cyfrowe, które opanowały sztukę monetyzacji uwagi – poprzez reklamy, subskrypcje czy analizę danych behawioralnych – działają w modelu, gdzie każdy ułamek sekundy spędzony przed ekranem jest potencjalnym źródłem przychodu.

W tym kontekście generatywna sztuczna inteligencja, zdolna do nieprzerwanego tworzenia nowych treści, nie jest neutralnym narzędziem. Stanowi raczej radykalizację już istniejącego modelu ekonomicznego. Gdy połączymy ją z architekturą rekomendacji, której jedynym celem jest optymalizacja zaangażowania, powstaje potężne sprzężenie zwrotne. System w sposób naturalny faworyzuje treści skrajne, emocjonalne i kontrowersyjne, ponieważ to one najskuteczniej przebijają się przez informacyjny szum. Badania nad nowoczesną wojną informacyjną dowodzą, że państwa i grupy interesu doskonale rozumieją tę logikę, projektując kampanie, które wykorzystują zjawiska viralowości i polaryzacji, zamiast próbować je powstrzymać.

Jeśli nałożymy na to mapę ryzyk globalnych elit biznesowych, obraz staje się jeszcze wyraźniejszy. W horyzoncie od dwóch do pięciu lat dezinformacja napędzana przez AI oraz polaryzacja społeczna jawią się jako jedne z najpoważniejszych zagrożeń dla stabilności systemów. Z perspektywy zarządów jest to czytelny sygnał: neutralność wobec wojny o uwagę przestała być opcją, stając się luksusem, na który nikogo nie stać. Sposób, w jaki firma uczestniczy w obiegu informacji, przestaje być kwestią wizerunku, a staje się fundamentem bezpieczeństwa operacyjnego i długoterminowej legitymizacji.

Jeśli klasyczny model odstraszania, oparty na groźbie odwetu za atak na fizyczną infrastrukturę, okazuje się bezradny wobec wojny o przekonania, musimy znaleźć nową kategorię porządkującą. Obiecującym kandydatem jest odporność kognitywna, rozumiana jako zdolność jednostek i wspólnot do obrony autonomii myślenia w środowisku nasyconym manipulacją. Nie polega ona na budowaniu murów i izolacji od informacji, lecz na rozwijaniu kompetencji krytycznych, transparentności algorytmów i tworzeniu instytucji, które mogą pełnić rolę zaufanych pośredników. Propozycje UNESCO, akcentujące prawa człowieka, przejrzystość i edukację medialną w kontekście AI, wyznaczają właściwy kierunek, choć wciąż brakuje im mechanizmów egzekwowania.

Dla globalnego biznesu oznacza to konieczność porzucenia roli biernego adresata regulacji i wejścia w rolę aktywnego współtwórcy standardów. Korporacje technologiczne muszą wreszcie przyjąć do wiadomości, że architektura ich systemów rekomendacyjnych jest elementem infrastruktury społecznej, równie ważnym jak sieci energetyczne. Inne sektory, od finansów po przemysł, muszą z kolei zrozumieć, że inwestycje w cyfrową edukację pracowników czy przejrzyste relacje z mediami to nie koszt, lecz inwestycja w odporność kognitywną całej organizacji.

Politycy natomiast muszą porzucić iluzję, że bezpieczeństwo da się zamknąć w kategoriach infrastrukturalnych, pozostawiając sferę uwagi wolnej grze rynkowej. W przeciwnym razie obudzimy się w rzeczywistości, w której gigantyczne środki przeznaczone na ochronę sieci i rurociągów okażą się bezużyteczne. Społeczeństwa, które miały z

> W świecie, gdzie granica między prawdą a fałszem zaciera się w mglistym krajobrazie informacyjnym, a sztuczna inteligencja kształtuje nasze myśli, czy potrafimy odzyskać kontrolę nad własnym umysłem? Czy w dobie algorytmicznej orkiestracji percepcji, jesteśmy skazani na symfonię dezinformacji, czy też zdołamy skomponować własną melodię prawdy i autonomii poznawczej? Może kluczem jest nie tylko ochrona danych, ale przede wszystkim pielęgnowanie umiejętności krytycznego myślenia, które staną się naszym osobistym cyfrowym kompasem?

Inspiracje

[1] **"Perfect Weapon: War, Sabotage, and Fear in the Cyber Age"** David E. Sanger

2018 | Crown Publishing Group

David E. Sanger jest amerykańskim dziennikarzem i głównym korespondentem „The New York Times" w Waszyngtonie. Specjalizuje się w bezpieczeństwie narodowym, polityce zagranicznej, globalizacji i proliferacji broni jądrowej. Jest autorem wielu książek na temat polityki zagranicznej USA i członkiem zespołów nagrodzonych Nagrodą Pulitzera.

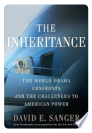
David E. Sanger *is an American journalist and the chief Washington correspondent for The New York Times. He specializes in national security, foreign policy, globalization, and nuclear proliferation. He has authored multiple books on U.S. foreign policy and has been a member of Pulitzer Prize-winning teams.*

The New York Times; Harvard Kennedy School

Literatura uzupełniająca

Książki

Autorzy przywoływani w artykule:



[1] **"The Inheritance: The World Obama Confronts and the Challenges to American Power"**

David E. Sanger

2009 | Crown | ISBN: 9780307451675

[2] **"Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power"**

David E. Sanger

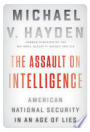
2012 | Crown | ISBN: 9780307718020

[3] "New Cold Wars: China's Rise, Russia's Invasion, and America's Struggle to Defend the West"

David E. Sanger

2024 | Scribe Publications | ISBN: 9781761385759

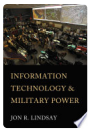
Literatura pokrewna (Google Scholar):



[4] "The Assault on Intelligence: American National Security in an Age of Lies"

Michael V. Hayden

2018 | Penguin | ISBN: 9780525558583



[5] "Information Technology and Military Power"

Jon R. Lindsay

2020 | Cornell University Press | ISBN: 9781501749575

[6] "Cyberspace in Peace and War"

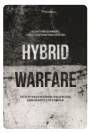
Martin Libicki

2021 | Naval Institute Press | ISBN: 9781682476178

[7] "Soft Power: The Means to Success in World Politics"

Joseph Nye

2004 | Public Affairs | ISBN: 9781586482251



[8] "Hybrid Warfare: Security and Asymmetric Conflict in International Relations"

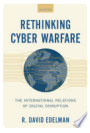
Mikael Weissmann

2023 | Bloomsbury Academic | ISBN: 9781350429093

[9] "Cognitive Warfare: Grey Matters in Contemporary Political Conflict"

Adam Henschke

2024 | Taylor & Francis | ISBN: 9781040112588



[10] "Rethinking Cyber Warfare: The International Relations of Digital Disruption"

R. David Edelman

2024 | Oxford University Press | ISBN: 9780197509685

Artykuły naukowe

Autorzy przywoływani:

[1] "Cognitive warfare - the human mind as the new battlefield"

Arijana Marjanović, Dražen Smiljanić

2025 | Proceedings of the Defence and Security Conference

Google Scholar

[2] "Prediction and judgment: Why artificial intelligence increases the importance of humans in war"

Avi Goldfarb, Jon R. Lindsay

2021 | International Security

[3] "Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack"

Jon R. Lindsay

2015 | Journal of Cybersecurity

Google Scholar

[4] "POSTURE STATEMENT OF GENERAL PAUL M. NAKASONE"

Paul M. Nakasone

2023

Google Scholar

[5] "The Convergence of Information Warfare"

Martin C. Libicki

2017 | Strategic Studies Quarterly

Google Scholar

[6] "Why Cyberspace is not a Warfighting Domain"

Martin C. Libicki

2012 | I/S: A Journal of Law and Policy for the Information Society

[7] "Soft power"

Joseph S. Nye

1990 | Foreign Policy

[8] "Deterrence and Dissuasion in Cyberspace"

Joseph S. Nye Jr.

2017 | International Security

Google Scholar

Tekst opracowany z udziałem sztucznej inteligencji.
Redakcja i kontrola merytoryczna: Fundacja Dobre Państwo.
APA ONE Publishing System

Article ID: fae50058-2cf4-4072-b68d-24bba919dfba