Dyplomacja i ekonomia przemocy w godzinie drapieżnika: od faktów dokonanych do asymetrii kosztów ataku i obrony w ujęciu Giuliano da Empoliego

AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Tekst analizuje ewolucję dyplomacji, która przestała być narzędziem zapobiegającym przemocy, a stała się instrumentem legitymizacji faktów dokonanych. Autor wprowadza pojęcie „dyplomacji kinetycznej", gdzie siła militarna i cybernetyczna staje się pierwszym krokiem w sekwencji działania, a negocjacje następują dopiero po zmianie stanu faktycznego. W dobie „godziny drapieżnika" tradycyjne rokowania ustępują miejsca przymusowi w strefie szarości, co wynika z dynamicznych zmian układu sił i rozwoju technologii. Wykorzystując teorie Thomasa Schellinga i Jamesa Fearona, artykuł ukazuje przemoc jako formę komunikacji strategicznej, w której nowoczesne państwa stosują wielość kanałów przymusu, aby zmienić kalkulację przeciwnika i wymusić korzystne warunki polityczne.

The text analyzes the evolution of diplomacy, which has ceased to be a tool for preventing violence and has become an instrument for legitimizing faits accomplis. The author introduces the concept of 'kinetic diplomacy,' where military and cyber power becomes the first step in the sequence of action, and negotiations follow only after the factual state has been changed. In the era of the 'hour of the predator,' traditional bargaining gives way to coercion in the gray zone, resulting from dynamic changes in the balance of power and technological development. Drawing on the theories of Thomas Schelling and James Fearon, the article presents violence as a form of strategic communication, in which modern states employ multiple channels of coercion to alter an opponent's calculus and force favorable political conditions.

Artykuł analizuje ewolucję dyplomacji w obliczu współczesnych technologii, stawiając tezę, że nie ulega ona anihilacji, lecz radykalnej transformacji funkcjonalnej. Autor dowodzi, że tradycyjna sekwencja działań – gdzie negocjacje miały zapobiegać przemocy – została odwrócona: obecnie to szybkie działania kinetyczne, cybernetyczne i infrastrukturalne tworzą fakty dokonane, a dyplomacja staje się narzędziem zarządzania skutkami tych uderzeń oraz interpretowania nowej rzeczywistości. Głównym motorem tych zmian jest asymetria kosztów ataku i obrony; tanie i skalowalne środki destabilizacji (jak drony czy cyberataki) premiują tzw. „drapieżników", którzy mogą wymuszać ogromne koszty reakcji przy minimalnym nakładzie własnym. W efekcie dyplomacja przesuwa się z obszaru budowania długofalowego pokoju w stronę transakcyjnego zarządzania zależnością i odpornością systemową, gdzie kluczowym wyzwaniem nie jest już sama perswazja, lecz walka o kontrolę nad węzłami globalnej infrastruktury i interpretację zdarzeń w „strefie szarości".

SŁOWA KLUCZOWE

dyplomacja kinetyczna | ekonomia przemocy | fakty dokonane | asymetria kosztów ataku i obrony | strefa szarości | weaponized interdependence | podatek obronny złożoności | dyplomacja transakcyjna | plausible deniability | security dilemma | arbitraż temporalny | asymetria koncentracji | manual override | coercive diplomacy

Dyplomacja nie znika, lecz zmienia sekwencję działania

Dyplomacja po utracie niewinności. Od rokowania do przymusu, faktów dokonanych i wojny poniżej progu wojny

Teza o „śmierci dyplomacji" należy do tych sformułowań Giuliano da Empoliego, które znakomicie organizują wyobraźnię, lecz wymagają starannego przełożenia z języka diagnozy politycznej na język nauk społecznych. Dyplomacja nie umarła. Państwa wciąż utrzymują ambasady, organizują szczyty, prowadzą negocjacje i zawierają porozumienia; pośredniczą w wymianie jeńców, ustalają zawieszenia broni, nakładają sankcje, handlują dostępem do rynków, budują koalicje oraz wykorzystują organizacje międzynarodowe. Nawet w trakcie najbardziej brutalnych konfliktów

strony posługują się kanałami komunikacyjnymi, pośrednikami i nieformalnymi sygnałami. Zmienia się zatem nie samo istnienie dyplomacji, lecz jej miejsce w sekwencji działania.

W klasycznym wyobrażeniu porządku powojennego rokowanie miało poprzedzać przemoc lub służyć jej powstrzymaniu. W porządku opisywanym przez da Empoliego coraz częściej dominuje odwrotna sekwencja: najpierw tworzy się nowy stan faktyczny, a dopiero potem negocjuje warunki jego politycznego uznania, ograniczenia bądź częściowego odwrócenia. Książka radykalizuje tę diagnozę, przeciwstawiając tradycyjną dyplomację profesjonalnych negocjatorów „dyplomacji kinetycznej" – rozumianej jako wykorzystanie siły militarnej, cybernetycznej i innych form przymusu w charakterze pierwszego instrumentu zmiany sytuacji.

W szerszej konstrukcji notatki jest to element obrazu świata, w którym prywatne potęgi technologiczne oraz polityczni aktorzy zdolni do błyskawicznego działania zyskują przewagę nad instytucjami wymagającymi uzgodnień, kontroli i czasu proceduralnego. Wersja naukowo defensywna tej tezy powinna być jednak bardziej precyzyjna. Siła i dyplomacja nie są przeciwieństwami; pozostają ze sobą splecione od zarania historii stosunków międzynarodowych. Nowość polega raczej na rozszerzeniu katalogu środków przymusu, skróceniu czasu ich użycia oraz rosnącej możliwości prowadzenia działań, których status pozostaje celowo niejednoznaczny.

Klasyczna teoria negocjacji strategicznych pokazuje wyraźnie, dlaczego nie należy romantyzować dyplomacji jako świata uprzejmej rozmowy przeciwstawionego brutalności wojny. Thomas Schelling analizował przemoc jako formę komunikacji. Państwo może grozić użyciem siły nie tylko po to, by zniszczyć przeciwnika, lecz aby zmienić jego kalkulację. Odstraszanie ma przekonać adresata, by czegoś nie robił; przymuszanie, czyli **compellence**, ma doprowadzić do wykonania działania, którego inaczej by nie podjął. Alexander George rozwijał później pojęcie coercive diplomacy, opisując strategię, w której presja, groźba i ograniczone użycie siły pozostają podporządkowane celowi negocjacyjnemu.

Dyplomacja nigdy zatem nie była wyłącznie sztuką perswazji. Często była sztuką wiarygodnego komunikowania kosztów. „Dyplomacja kinetyczna" nie stanowi więc zupełnie nowego gatunku polityki, lecz jest radykalizacją starego mechanizmu. Gunboat diplomacy XIX wieku, blokady morskie, demonstracje wojskowe, ultimata, ograniczone bombardowania czy mobilizacja wojsk już wcześniej pełniły funkcję argumentów negocjacyjnych. Nawet słynne powiedzenie Clausewitza o wojnie jako kontynuacji polityki innymi środkami nie przeciwstawia wojny polityce, lecz umieszcza przemoc wewnątrz szerszego procesu realizacji celów politycznych.

Tym, co odróżnia początek XXI wieku, jest wielość kanałów przymusu oraz możliwość ich jednoczesnego, szybkiego i częściowo zaprzeczalnego stosowania. Państwo może równocześnie

przesunąć wojska, przeprowadzić cyberoperację, użyć sankcji sektorowych, ograniczyć eksport technologii, prowadzić działania informacyjne, oddziaływać na diasporę, wspierać podmiot zastępczy i jednocześnie pozostawić otwarty kanał rokowań.

Fakty dokonane i strefa szarości jako narzędzia przymusu

James Fearon, analizując racjonalistyczne przyczyny wojen, postawił problem w sposób radykalny: skoro konflikt jest kosztowny, racjonalni aktorzy powinni być w stanie wypracować porozumienie, które przyniesie obu stronom więcej niż oczekiwana wartość wojny. Skoro jednak konflikty mimo to wybuchają, konieczne są mechanizmy wyjaśniające niepowodzenie negocjacji. Fearon wskazywał tu przede wszystkim na asymetrię informacji i pokusę jej fałszywego przedstawiania, problemy wiarygodnego zobowiązania oraz – w określonych sytuacjach – niepodzielność przedmiotu sporu.

Teoria ta pozwala inaczej spojrzeć na "godzinę drapieżnika". Jeśli technologia zwiększa zdolność do szybkiej zmiany układu sił, pogłębiają się problemy z wiarygodnością zobowiązań: dlaczego jedna strona miałaby zaakceptować kompromis dziś, skoro spodziewa się, że jutro będzie silniejsza? I dlaczego słabszy gracz miałby zaufać porozumieniu, wiedząc, że przeciwnik po uzyskaniu przewagi może zmienić jego warunki? Dynamiczna zmiana siły tworzy jedno z najtrudniejszych środowisk dla stabilnych rokowań. Porozumienie musi bowiem regulować nie tylko aktualny podział korzyści, ale i oczekiwania co do przyszłości. Gwałtowny rozwój technologiczny, wyścig zbrojeń, zmiana sojuszy czy pojawienie się nowej broni sprawiają, że układ satysfakcjonujący strony obecnie szybko przestaje być akceptowalny. W takiej sytuacji obietnica przestrzegania kompromisu traci na wiarygodności.

Drapieżnik w ujęciu da Empoliego jest zatem groźny nie tylko wtedy, gdy łamie reguły, ale już wtedy, gdy druga strona spodziewa się, że może to zrobić w przyszłości. Samo oczekiwanie naruszenia zmienia dzisiejszą strategię. Z tego powodu kluczową rolę odgrywają fakty dokonane.

Fait accompli polega na przeprowadzeniu ograniczonej zmiany wystarczająco szybko, by przeciwnik stanął przed niekorzystnym wyborem: zaakceptować nowy stan rzeczy albo ponieść znacznie większy koszt jego odwrócenia. Różnica względem klasycznego ultimatum jest zasadnicza. Ultimatum daje adresatowi wybór przed zmianą rzeczywistości; fakt dokonany najpierw zmienia rzeczywistość, a wybór pozostawia na później. Z punktu widzenia teorii gier inicjator przenosi ciężar eskalacji na stronę broniącą status quo. To ona musi zdecydować, czy sporna korzyść jest warta wojny, sankcji, mobilizacji politycznej lub ogromnych kosztów gospodarczych.

Strategia ta okazuje się skuteczna zwłaszcza wtedy, gdy pojedyncza zmiana jest zbyt mała, by automatycznie uruchomić maksymalną reakcję. Schelling opisywał trudność obrony granic, których znaczenie polityczne nie jest wystarczająco ostre; wcześniejsza literatura strategiczna posługiwała się również metaforą "salami tactics", czyli uzyskiwania kolejnych niewielkich zdobyczy, z których żadna osobno nie uzasadnia przeciwnikowi poniesienia najwyższego kosztu reakcji. Problem ten pojawia się współcześnie między innymi w działaniach hybrydowych i strefie szarości.

Aktor dąży do osiągnięcia korzyści, pozostając poniżej progu, przy którym przeciwnik czuje się politycznie lub prawnie zobowiązany do odpowiedzi pełną siłą. Strefa szarości nie oznacza braku prawa, lecz celowe wykorzystywanie niejasności dotyczących faktów, autorstwa, intensywności działania lub właściwego sposobu reakcji. Cyberatak może pochodzić z infrastruktury rozproszonej w wielu państwach, a kampania informacyjna być prowadzona przez formalnie prywatne podmioty.

Sabotaż może przypominać awarię lub działalność przestępczą. Organizacja paramilitarna może utrzymywać relacje z państwem, które jednocześnie zaprzecza operacyjnej kontroli nad nią. Instrument gospodarczy można przedstawić jako zwyczajną decyzję regulacyjną. Problemem nie jest zatem niewidzialność działania, lecz możliwość utrzymania sporu o jego interpretację na tyle długo, by utrudnić wspólną odpowiedź. Nie jest to jedynie abstrakcyjny model.

Dyplomacja jako narzędzie zarządzania interpretacją

W oficjalnych dokumentach z 2025 i 2026 roku Unia Europejska definiuje działania hybrydowe obserwowane na swoim terytorium jako cyberataki, sabotaż, manipulację informacyjną, ingerencję w procesy wyborcze, uszkodzenia infrastruktury krytycznej oraz instrumentalizowanie migracji. W wielu przypadkach UE przypisuje odpowiedzialność za te zdarzenia Rosji lub podmiotom z nią powiązanym; należy jednak zachować rygor metodologiczny i traktować to jako oficjalną atrybucję instytucji europejskich, a nie automatycznie udowodnioną przyczynowość każdego incydentu. NATO również wskazuje na nasilenie naruszeń przestrzeni powietrznej, cyberataków i aktów sabotażu w zmienionym po 2014 i 2022 roku środowisku bezpieczeństwa europejskiego. W lipcu 2026 roku UE opisała rosyjski ekosystem cyberoperacji jako strukturę obejmującą zarówno służby państwowe, jak i cyberprzestępców, haktywistów oraz prywatne przedsiębiorstwa, wskazując m.in. na infiltrację sieci rządowych i ataki na infrastrukturę krytyczną.

Jest to stanowisko i atrybucja UE, lecz jego znaczenie analityczne wykracza poza konkretny konflikt. Obrazuje ono model przeciwnika sieciowego, w którym granica między państwem a aktorem niepaństwowym, przestępczością a operacją strategiczną czy pokojem a konfliktem staje się znacznie trudniejsza do uchwycenia niż w klasycznym obrazie dwóch armii stojących naprzeciw

siebie. W takim środowisku problem dyplomacji zmienia charakter. Ambasador może negocjować z państwem, lecz niekoniecznie ma do czynienia z partnerem posiadającym pełną kontrolę nad wszystkimi elementami sieci. Prawo międzynarodowe operuje kategoriami odpowiedzialności państwa, podczas gdy współczesne działania są celowo organizowane tak, by utrudnić ich przypisanie. Mechanizm ten zwiększa wartość plausible deniability – możliwości wiarygodnego lub politycznie użytecznego zaprzeczenia odpowiedzialności. Jeśli identyfikacja sprawcy trwa tygodnie lub miesiące, reakcja dyplomatyczna jest zawsze spóźniona względem działania. Powraca zatem opisany wcześniej arbitraż temporalny: operacja zostaje wykonana w czasie technologicznym, podczas gdy odpowiedzialność ustalana jest w czasie instytucjonalnym.

Nie oznacza to jednak, że tradycyjna dyplomacja staje się bezużyteczna. Paradoksalnie wzrost niejednoznaczności może zwiększać znaczenie kanałów nieformalnych, poufnych kontaktów, komunikacji wojskowej i mechanizmów deeskalacyjnych. Im bardziej skomplikowany jest system oddziaływania, tym większe ryzyko błędnego przypisania drugiej stronie zamiaru lub odpowiedzialności. Teoria bezpieczeństwa od dawna operuje pojęciem security dilemma: działania podejmowane przez jedno państwo dla zwiększenia własnego bezpieczeństwa mogą być odczytywane przez drugie jako przygotowanie agresji, co uruchamia spiralę wzajemnego zbrojenia. W środowisku cybernetycznym i hybrydowym problem ten się pogłębia, gdyż narzędzia ofensywne i defensywne są technologicznie podobne, a penetracja systemu informatycznego może służyć zarówno rozpoznaniu, jak i przygotowaniu ataku. Dyplomacja staje się w takich warunkach technologią zarządzania interpretacją. Pozwala pytać nie tylko „co zrobiłeś?”, ale również „jak mamy rozumieć to, co zrobiłeś?” i „co zamierzasz zrobić dalej?”.

Robert Jervis w analizach percepcji i błędnej percepcji w polityce międzynarodowej dowodził, że państwa reagują nie tyle na samo zachowanie przeciwników, co na znaczenie, jakie mu przypisują. Dwie identyczne koncentracje wojsk mogą zostać zinterpretowane jako odstraszanie albo przygotowanie ofensywy, zależnie od wcześniejszych przekonań. Dyplomacja pozostaje jednym z niewielu mechanizmów pozwalających testować te interpretacje przed użyciem siły. Da Empoli trafnie zauważa jednak sytuacje, w których komunikat zostaje całkowicie podporządkowany działaniu. Szczególnie wymownym przykładem są wydarzenia z 27 września 2024 roku.

W Nowym Jorku trwały wówczas intensywne zabiegi dyplomatyczne Stanów Zjednoczonych, Francji i innych państw, zmierzające do czasowego przerwania walk między Izraelem a Hezbollahem. Tego samego dnia premier Izraela Benjamin Netanjahu wystąpił przed Zgromadzeniem Ogólnym ONZ, deklarując kontynuowanie działań przeciwko Hezbollahowi. Wkrótce potem izraelskie lotnictwo przeprowadziło potężny atak na kwaterę Hezbollahu w

południowych przedmieściach Bejrutu, w wyniku którego zginął lider organizacji, Hassan Nasrallah.

Dyplomacja transakcyjna jako zarządzanie kosztami i faktami dokonanymi

Źródła opisujące ówczesne negocjacje wskazują, że Stany Zjednoczone nie zostały wcześniej poinformowane o konkretnym uderzeniu. Sekwencja ta obrazowo ilustruje napięcie między forum dyplomatycznym a logiką operacyjną, nie daje jednak podstaw do dalszego kroku, który bywa wyprowadzany: nie można wiarygodnie stwierdzić, że sama obecność Netanjahu w Nowym Jorku została świadomie wykorzystana jako fortel mający uśpić czujność przeciwnika. Potwierdzony jest atak, wystąpienie w ONZ oraz decyzja izraelskiego kierownictwa o eliminacji Nasrallaha. Brakuje jednak materiału, by z tej sekwencji wydarzeń wyprowadzić konkretną intencję dezinformacyjną dotyczącą wizyty na forum ONZ. Naukowa rekonstrukcja powinna zatem zachować paradoks wydarzenia, a odrzucić psychologiczne dopowiedzenie.

Ten przypadek ujawnia coś głębszego: negocjacje i operacja wojskowa mogą przebiegać równolegle, a nie kolejno. Strona konfliktu może prowadzić rozmowy, jednocześnie próbując poprawić swoją pozycję negocjacyjną poprzez zmianę sytuacji militarnej. To stary mechanizm, jednak współczesna technologia drastycznie skraca czas między decyzją a skutkiem.

W wojnie koreańskiej, wietnamskiej, konfliktach bliskowschodnich czy podczas rokowań bałkańskich wielokrotnie próbowano wpływać na negocjacje działaniami wojskowymi. Współczesna różnica polega przede wszystkim na precyzji, zasięgu i szybkości rozpoznania oraz zdolności uderzenia, która pozwala zmieniać układ personalny przeciwnika niemal w czasie trwania politycznego szczytu. Dlatego oddzielanie dyplomacji od wojny bywa poznawczo mylące; lepiej traktować je jako dwa sposoby oddziaływania w ramach jednego procesu strategicznego. Dyplomacja ustala warunki dobrowolnej lub półdobrowolnej zmiany zachowania; przemoc modyfikuje koszty odmowy.

Sankcje gospodarcze zajmują pozycję pośrednią. Cyberoperacje mogą służyć jako ostrzeżenie, sabotaż lub bezpośrednia degradacja zdolności. Presja finansowa bywa bronią negocjacyjną bez jednego wystrzału, a kontrola dostępu do technologii może zmieniać możliwości przeciwnika w perspektywie lat. Granica „dyplomacji” staje się przepuszczalna, gdyż współczesne państwo dysponuje bogatszym zestawem narzędzi wpływu. Joseph Nye ujmował ten problem poprzez rozróżnienie hard power i soft power, później rozwinięte w pojęciu smart power. Współczesne

konflikty ujawniają jednak inny wymiar: władza może wynikać z kontroli nad sieciami współzależności. Henry Farrell i Abraham Newman nazwali ten mechanizm „weaponized interdependence".

Podmiot zajmujący centralną pozycję w globalnej sieci finansowej, informacyjnej lub infrastrukturalnej może wykorzystać ją do pozyskiwania informacji bądź ograniczania dostępu innym. Sankcja nie musi wówczas polegać na fizycznym niszczeniu zasobów przeciwnika – wystarczy odciąć go od infrastruktury, od której zdążył się uzależnić. To kolejny powód, dla którego język „kinetyczny" okazuje się zbyt wąski. Współczesny przymus może być militarny, finansowy, prawny, technologiczny, informacyjny lub infrastrukturalny.

W każdym przypadku pytanie brzmi podobnie: jaki koszt możemy nałożyć na przeciwnika, jaki poniesiemy sami i jak wiarygodnie przekazać, że koszt będzie narastał, jeśli druga strona nie zmieni zachowania? Teoria dyplomacji przymusu pozostaje aktualna, choć repertuar narzędzi jest szerszy niż w czasach, gdy Schelling analizował głównie broń konwencjonalną i nuklearną.

Aktualne trendy w procesach pokojowych potwierdzają tę diagnozę. SIPRI opisuje rok 2025 jako okres, w którym procesy te stawały się bardziej fragmentaryczne, transakcyjne i oparte na przymusie, z mniejszym naciskiem na rozwiązania kompleksowe i inkluzywne, a większym na szybkie porozumienia, zawieszenia broni i negocjacje prowadzone bezpośrednio przez liderów. Nie oznaczało to całkowitego braku osiągnięć, lecz część uzgodnień pozostawała krucha lub niepełna. Jest to istotna empiryczna korekta pojęcia „śmierci dyplomacji": dyplomacja nie znika, lecz staje się bardziej transakcyjna. Transakcyjność oznacza zmianę ambicji.

Klasyczny liberalny model peacebuilding zakładał, że zakończenie konfliktu powinno wiązać się z budowaniem instytucji, pojednaniem, reformą państwa i długoterminową transformacją źródeł przemocy. Model transakcyjny stawia cele skromniejsze: zatrzymanie ostrzału, uzgodnienie wymiany, ustanowienie linii rozdzielenia czy uzyskanie konkretnej koncesji. Jego przewagą jest szybkość rezultatu; słabością – ryzyko pozostawienia nierozwiązanych mechanizmów, które konflikt wytworzyły.

Z perspektywy da Empoliego jest to środowisko sprzyjające Borgianom. Przywódca potrafiący szybko zaoferować wymianę korzyści lub zagrozić natychmiastowym kosztem może uzyskać przewagę nad wielostronnym procesem wymagającym długotrwałej harmonizacji stanowisk. Z perspektywy teorii instytucjonalnej obraz jest bardziej ambiwalentny.

Szybka transakcja może uratować życie, jeśli zatrzymuje walki, ale może także utrwalić przewagę strony, która wcześniej skutecznie wytworzyła fakt dokonany. Nie można zatem normatywnie oceniać „transakcyjności" w oderwaniu od przedmiotu porozumienia, relacji sił oraz dostępnych

alternatyw. Wydarzenia pokazują jednak, że po fazie intensywnej przemocy klasyczna dyplomacja często powraca.

We wrześniu 2026 roku europejscy i arabscy przywódcy oraz dowódcy wojskowi spotykali się w Paryżu w sprawie przyszłej architektury bezpieczeństwa Libanu, podczas gdy równolegle toczyły się negocjacje dotyczące izraelskiego wycofania, rozbrojenia Hezbollahu i wzmocnienia libańskich sił państwowych.

Dyplomacja jako zarządzanie faktami dokonanymi i zależnością

Nie przesądza to o trwałości żadnego rozwiązania, pokazuje jednak, że nawet po radykalnym użyciu siły problem polityczny powraca do stołu negocjacyjnego. Przemoc potrafi zmienić parametry rokowania, lecz nie jest w stanie samodzielnie ustanowić reguł nowego porządku. Pojawia się tu paradoks istotniejszy niż hasła o końcu dyplomacji: im skuteczniej przemoc zmienia stan faktyczny, tym większe staje się zapotrzebowanie na polityczną interpretację jej rezultatów. Zdobycie terytorium nie rozstrzyga samoistnie o jego statusie prawnym. Zniszczenie infrastruktury nie tworzy stabilnego systemu bezpieczeństwa, a eliminacja dowódcy przeciwnika nie określa automatycznie przyszłej struktury organizacji. Sankcja może uszczuplić zasoby, ale sama w sobie nie generuje porozumienia. Technologia wymusza zdarzenia; polityka musi następnie nadać im ramy. Dlatego dyplomacja nie znika nawet w świecie drapieżników. Zostaje jednak zdegradowana: z mechanizmu zapobiegania zmianie do narzędzia zarządzania zmianą dokonaną przez innych.

Różnica jest zasadnicza. W pierwszym wariancie dyplomata uczestniczy w konstruowaniu przyszłości przed użyciem siły. W drugim przybywa do rzeczywistości, której podstawowe parametry zostały już określone przez armię, algorytm, sankcję, cyberoperację lub kontrolę infrastruktury. Stół negocjacyjny pozostaje ten sam, lecz mapa na nim leżąca jest już inna. To właśnie w tym miejscu należy umieścić figurę „szerpy” jako wymierającego profesjonalnego negocjatora. Twierdzenie o jego całkowitym zaniku byłoby jednak nieprawdziwe.

Aparaty dyplomatyczne pozostają rozbudowane, a liczba wielostronnych problemów wręcz zwiększa zapotrzebowanie na ekspertów zdolnych negocjować szczegóły sankcji, handlu, klimatu czy przepływów migracyjnych. Trafniejsza jest hipoteza o utracie monopolu dyplomaty na kształtowanie stosunków między państwami. Obok niego pojawiają się wojskowi, służby wywiadowcze, korporacje technologiczne, operatorzy infrastruktury, instytucje finansowe i naukowcy.

Klasyczna dyplomacja była w dużej mierze relacją państwo-państwo. Dzisiejsza coraz częściej staje się negocjowaniem ekosystemu. Państwo może potrzebować porozumienia z innym krajem w sprawie bezpieczeństwa, a jednocześnie kontaktu z firmą posiadającą infrastrukturę satelitarną, platformą kontrolującą komunikację obywateli czy producentem półprzewodników z trzeciej jurysdykcji. Suwerenność nie znika, lecz jest wykonywana w środowisku głębokiej współzależności infrastrukturalnej. Stąd bierze się kolejna cecha „godziny drapieżnika": przesunięcie od kontroli terytorium do kontroli węzłów. Klasyczna geopolityka pytała o cieśniny, porty i szlaki morskie; współczesna musi pytać również o centra danych, kable podmorskie, systemy pozycjonowania i modele sztucznej inteligencji.

Elementy te nie zastępują terytorium geograficznego, lecz nakładają na nie drugą warstwę strategicznej topologii. Dyplomacja transformuje się zatem z praktyki reprezentowania suwerena wobec innego suwerena w zarządzanie wielowarstwową zależnością. Kluczowym problemem pozostaje wiarygodność zobowiązania, ale zmienia się jego przedmiot. Państwo może zobowiązać się nie tylko do niewprowadzania wojsk, lecz także do zaniechania cyberoperacji, przestrzegania kontroli eksportu czy respektowania standardów technicznych. Dyplomacja technologiczna przestaje być dziedziną poboczną i staje się integralną częścią polityki bezpieczeństwa.

W takim świecie reguły są potrzebne bardziej niż kiedykolwiek, choć trudniej je ustalać przed upowszechnieniem danej technologii. Prawo międzynarodowe dotyczące broni nuklearnej rozwijało się, gdy jej konstrukcja była domeną nielicznych państw i ogromnych zakładów przemysłowych. Cybernarzędzia rozpowszechniają się znacznie łatwiej, drony korzystają z cywilnych łańcuchów dostaw, a algorytmy AI są modyfikowane w rytmie nieznanym klasycznym systemom broni.

Im niższy próg wejścia, tym więcej aktorów zdolnych wywoływać skutki o znaczeniu strategicznym. Prowadzi to do kluczowego pytania: czy rzeczywiście weszliśmy w epokę, w której atak stał się strukturalnie tańszy od obrony? Teza ta, zestawiająca tanie drony i cyberataki z kosztownymi systemami obronnymi, znajduje w aktualnych danych wystarczające podstawy, by traktować ją poważnie.

Asymetria kosztów ataku i obrony premiuje drapieżników

SIPRI wskazuje, że w 2025 roku pociski i uzbrojone bezzałogowce były wykorzystywane w szerokim katalogu misji: od uderzeń dalekiego zasięgu i ataków saturacyjnych zmierzających do przeciążenia

obrony, po roje UAV oraz operacje prowadzone z wnętrza terytorium przeciwnika. Materiał ten zawiera jednak konkretne dane i przykłady, które wymagają głębszej analizy niż efektowne porównanie ceny drona z kosztem rakiety przechwytującej. Kluczowe staje się zatem zbadanie asymetrii kosztów ataku i obrony poprzez syntezę teorii offense-defense, ekonomii konfliktu, odstraszania nuklearnego oraz nowoczesnych technologii – od dronów i broni precyzyjnej po cyberbezpieczeństwo i biologię syntetyczną. Należy przy tym odrzucić zbyt proste przekonanie, że niska cena pojedynczego środka ataku automatycznie oznacza strategiczną przewagę ofensywy.

Dopiero taka perspektywa pozwoli odpowiedzieć na pytanie, czy "godzina drapieżnika" jest również godziną ekonomicznego zwycięstwa napastnika, czy raczej kolejnym etapem nieustannego wyścigu między mieczem i tarczą. W analizie ekonomii ataku i obrony – gdzie dron staje przed rakietą, a kod przed infrastrukturą – musimy precyzyjnie określić granice tezy o przewadze ofensywy.

Jedna z najmocniejszych intuicji w materiale inspirowanym myślą Giuliano da Empoliego dotyczy zmiany ekonomii przemocy. Współczesność jawi się tu jako epoka "asymetrycznej atrycji", w której środki ofensywne tanieją szybciej niż systemy konieczne do ich powstrzymywania. Symbolicznym obrazem tej transformacji jest tani bezzałogowiec atakujący obiekt chroniony przez wielomilionowy system przeciwlotniczy, cyberatak wymierzony w infrastrukturę wartą miliardy dolarów czy niedrogi środek rażenia zagrażający platformie wojskowej, której budowa trwała lata. Zależność ta jest sformułowana kategorycznie: obecna epoka charakteryzuje się dramatycznym spadkiem kosztów ataku przy równoczesnym wzroście kosztów obrony, co systemowo premiuje drapieżników. Hipotezę tę należy jednak rozbić na kilka odrębnych mechanizmów.

W przeciwnym razie łatwo pomylić niską cenę pojedynczej amunicji z przewagą strategiczną całej ofensywy. Teoria stosunków międzynarodowych od dawna analizuje problem offense-defense balance, czyli względnej łatwości prowadzenia ofensywy i obrony. Jej podstawowa intuicja jest prosta: jeśli zdobywanie terytorium, niszczenie przeciwnika lub naruszanie jego bezpieczeństwa jest relatywnie łatwe, państwa wykazują większą skłonność do działań wyprzedzających, zbrojeń i agresji. Gdy natomiast przewagę ma obrona, utrzymanie status quo staje się łatwiejsze, a koszt podboju gwałtownie rośnie.

Przewaga ofensywy wynika z systemu, nie z technologii

Klasyczna literatura podkreśla jednak, że bilans ten nie wynika wyłącznie z technologii. Zależy on również od geografii, organizacji sił zbrojnych, doktryny, mobilizacji, jakości informacji, sojuszy oraz sposobu, w jaki politycy postrzegają istniejący układ. MIT Press, podsumowując rozwój offense-defense theory, wskazuje właśnie na zmienność względnej łatwości ataku i obrony oraz na

wielość czynników kształtujących ten balans. To rozróżnienie jest niezbędne, gdyż sama technologia rzadko bywa „ofensywna” lub „defensywna” w oderwaniu od sposobu jej zastosowania. Samolot może przeprowadzać nalot, ale może też bronić przestrzeni powietrznej. Dron może uderzać, prowadzić rozpoznanie lub wykrywać nadlatujące środki ataku. Satelita służy zarówno do przygotowania ofensywy, jak i do wczesnego ostrzegania. Cybernarzędzie pozwala penetrować system przeciwnika, lecz podobne kompetencje techniczne są niezbędne do testowania własnej infrastruktury.

Nawet fortyfikacja, klasyczny symbol obrony, może uwolnić siły potrzebne do prowadzenia ofensywy w innym miejscu. Współczesny bilans ofensywy i defensywy jest więc cechą systemu, a nie pojedynczego przedmiotu. Książka słusznie kieruje uwagę na historyczne momenty, w których innowacje wojskowe destabilizowały wcześniejsze równowagi. Da Empoli sięga w tym kontekście do włoskich wojen przełomu XV i XVI wieku oraz doświadczeń Leonarda da Vinci, zestawiając świat włoskich państw-miast z nowym sposobem prowadzenia wojny przez wielkie monarchie wyposażone w artylerię i liczniejsze armie. Historyczny mechanizm jest tu ważniejszy od malowniczości analogii. Fortyfikacja, która przez dziesięciolecia stanowiła skuteczne zabezpieczenie, traci na wartości, gdy pojawia się technologia pozwalająca zniszczyć ją szybciej lub ominąć. Wówczas nie traci się tylko muru. Traci się inwestycje, doktryny, struktury administracyjne i oczekiwania polityczne zbudowane wokół założenia, że mur będzie działał. Barry Posen, analizując rozwój doktryn wojskowych między wojnami światowymi, zwracał uwagę, że strategia jest zawsze połączeniem celów politycznych, zasobów wojskowych, organizacji oraz doktryny. Ta sama technologia może przynosić odmienne skutki w zależności od sposobu jej włączenia do większej architektury działania. Stąd wniosek wobec popularnego powiedzenia o nieustannym wyścigu „miecza i tarczy”: miecz i tarcza nie walczą same.

Walczą organizacje, które muszą je produkować, utrzymywać i integrować z rozpoznaniem, logistyką, personelem oraz komunikacją. Wojna dronowa stanowi jednak szczególnie wyrazisty przykład tego, dlaczego teza da Empoliego jest dziś atrakcyjna. SIPRI uznaje szybki rozwój uzbrojonych bezzałogowców, ich relatywną dostępność i elastyczność za trend zmieniający charakter współczesnego pola walki. W 2025 roku drony wykorzystywano do rozpoznania, precyzyjnych uderzeń na dużą odległość, ataków saturacyjnych mających na celu przeciążenie obrony, działań rojowych oraz operacji prowadzonych z wnętrza terytoria przeciwnika. Ich proliferacja wywołała równoległy wyścig w rozwoju systemów przeciwdronowych. Jest to kluczowe: każda przewaga ofensywna wytwarza bodziec do stworzenia tańszej defensywy. Dlatego przykład „drona za kilkaset dolarów przeciwko rakiecie za miliony” należy traktować ostrożnie. Bywa przywoływany dron Huti kosztujący około 200 dolarów i przeciwstawiany mu wielomilionowy

pocisk przechwytujący, jednak nie ma podstaw do uznawania tej kwoty za uniwersalny koszt bezzałogowców używanych przez tę grupę.

Kategoria „dron" obejmuje bardzo różne konstrukcje o zróżnicowanych zasięgach, systemach naprowadzania, ładunkach i kosztach. Również obrona nie stosuje jednego rodzaju efektora przeciwko każdemu celowi; w zależności od sytuacji może wykorzystywać pociski różnych klas, artylerię, broń pokładową, walkę radioelektroniczną, zakłócanie czy systemy skierowanej energii. Sama skala różnicy cenowej nie jest jednak wymysłem. Budżet marynarki Stanów Zjednoczonych wskazuje, że jeden SM-6 Block IA w roku budżetowym 2025 miał koszt jednostkowy około 5,5 miliona dolarów. Jest to jednak pocisk o znacznie szerszych zdolnościach niż zwalczanie prostego bezzałogowca – przeznaczony do obrony przed różnorodnymi zagrożeniami powietrznymi i rakietowymi.

Jego użycie przeciwko tańszemu celowi nie dowodzi samo w sobie irracjonalności systemu. Obrona nie porównuje ceny pocisku z ceną atakującej amunicji, lecz koszt przechwycenia z oczekiwanym kosztem nieprzechwycenia. To jedno z najważniejszych rozróżnień ekonomiki bezpieczeństwa. Jeśli pocisk wart kilka milionów dolarów chroni okręt, infrastrukturę lub ludzi wartych znacznie więcej, jego użycie pozostaje ekonomicznie racjonalne nawet przeciwko urządzeniu kosztującemu ułamek tej sumy. W ujęciu decyzyjnym właściwe porównanie przyjmuje postać oczekiwanej straty: prawdopodobieństwo skutecznego trafienia pomnożone przez potencjalny koszt skutków. Cena agresora i cena obrońcy to tylko jedna warstwa analizy. Atakującego interesuje często współczynnik wymiany zasobów, obrońcę zaś wartość chronionego aktywa. Morze Czerwone dostarczyło rzeczywistego laboratorium tej nierównowagi.

Asymetria kosztów a strategiczne przeciążenie obrony

Amerykańskie dowództwo już na początku operacji Prosperity Guardian informowało o przechwytywaniu kombinacji bezzałogowców, pocisków manewrujących oraz przeciwokrętowych pocisków balistycznych. Reuters zauważył, że ataki Huti stały się pierwszym udokumentowanym bojowym użyciem tej ostatniej klasy broni, co znacząco zwiększyło światowe zainteresowanie zintegrowaną obroną powietrzną i przeciwrakietową.

Nie jest zatem właściwe redukowanie całego zagrożenia do kwestii „taniego drona". Obrona musiała mierzyć się z heterogenicznym pakietem środków, różniących się prędkością, trajektorią i potencjalnymi skutkami. Jednocześnie operacje te obnażyły problem cost imposition. Atakujący nie musi zatopić okrętu, aby wymusić koszt. Jeśli każda próba ataku zmusza przeciwnika do utrzymywania kosztownej obecności, częstszych rotacji załóg, zużywania amunicji, przyspieszenia

remontów, reorganizacji żeglugi czy budowania dodatkowej osłony, efekt ekonomiczny powstaje nawet przy niskiej skuteczności kinetycznej. Przymus strategiczny można zatem realizować poprzez samo wymuszanie reakcji. Jest to w istocie przeciążanie systemu: nie trzeba go całkowicie przełamać, jeśli można sprawić, że utrzymywanie ochrony stanie się stale kosztowne.

W teorii wojskowej dotyczy to relacji między skutecznością taktyczną a trwałością kampanii. Obrona może przechwycić 95 czy nawet 99 procent pocisków, lecz jeśli atakujący produkuje je znacznie szybciej, a obrońca zużywa kosztowne zapasy w tempie przekraczającym ich odtwarzanie, wysoka skuteczność pojedynczego starcia nie gwarantuje strategicznego zwycięstwa. Kluczowym parametrem przestaje być wtedy samo probability of kill; znaczenie zyskują szybkość produkcji, koszty uzupełniania magazynów, dostępność sensorów, odporność sieci dowodzenia oraz zdolność do utrzymania tempa działań przez miesiące lub lata. Tę samą lekcję dostarcza wojna rosyjsko-ukraińska.

Dron nie jest tam pojedynczym typem broni, lecz całą rodziną platform służących do rozpoznania, korygowania ognia, ataków krótkiego i dalekiego zasięgu, minowania, logistyki oraz walki elektronicznej. Jego strategiczne znaczenie wynika m.in. z faktu, że pozwala zwiększyć liczbę sensorów i efektorów na polu walki przy kosztach często niższych niż w przypadku klasycznych systemów załogowych. SIPRI opisuje proliferację UAV jako proces wpływający nie tylko na uderzenia, ale również na ISR (intelligence, surveillance and reconnaissance), czyli zdolność widzenia i rozumienia pola walki. Jeszcze bardziej spektakularnym przykładem była ukraińska operacja „Spider's Web” z 1 czerwca 2025 roku.

Według podsumowania SIPRI wykorzystano w niej ponad sto dronów, rozmieszczonych wcześniej na terytorium Rosji i skoordynowanych przeciwko odległym bazom lotniczym. Z cytowanych przez instytut doniesień wynika, że uszkodzenia miało odnieść 41 rosyjskich samolotów, co wymusiło rozproszenie części lotnictwa strategicznego oraz zmiany logistyczne.

Asymetria kosztów i pułapka skalowalności ataku

Rzeczywisty zakres zniszczeń pozostaje przedmiotem rozbieżnych ocen, dlatego należy zachować ostrożność wobec szacunków maksymalnych. Znaczenie tego przypadku wykracza jednak poza sam bilans uszkodzonych maszyn: stosunkowo małe platformy bezzałogowe mogą wymusić zmianę sposobu ochrony aktywów o ogromnej wartości. To właśnie ten przymus jest najciekawszym aspektem asymetrii. Pojawienie się nowego sposobu ataku sprawia, że wszystkie podobne obiekty potencjalnie wymagają dodatkowej ochrony. Koszt ofensywy można ponieść jednorazowo, koszt defensywy rozlewa się na cały system. To klasyczny problem bezpieczeństwa perymetrycznego:

napastnik wybiera punkt uderzenia, podczas gdy obrońca musi zabezpieczyć wiele potencjalnych wejść. W cyberbezpieczeństwie zasada ta przybrała popularną, choć uproszczoną formę twierdzenia, że obrońca musi chronić wszystko, a napastnik znaleźć tylko jedną lukę. Choć w rzeczywistości atakujący również ponosi koszty rozpoznania, infrastruktury i kompetencji, problem asymetrycznego wyboru celu pozostaje realny.

Tutaj jednak nauka ostrzega przed nadmiernym uproszczeniem. Rebecca Slayton, analizując cybernetyczny offense-defense balance, wykazała, że teza o stałej premii dla ofensywy jest zbyt powierzchowna. Skuteczność i koszty zależą od konkretnej technologii, kompetencji organizacyjnych oraz jakości zarządzania systemami. Precyzyjne operacje zdolne wywołać fizyczne skutki mogą być niezwykle kosztowne; w przypadku Stuxnet analiza Slayton wskazywała wręcz, że przygotowanie ofensywy mogło kosztować więcej niż bezpośrednia obrona. Cyberprzestrzeń nie znosi więc ekonomii wojny, lecz przenosi ją w obszar kompetencji i niewidocznych nakładów. Prowadzi to do ogólniejszej zasady: niski koszt fizycznego nośnika nie jest równy niskiemu kosztowi zdolności bojowej. Dron to nie tylko kadłub i silnik, lecz cały system obejmujący wykrywanie celu, łączność, nawigację, logistykę i wywiad. Cybernarzędzie nie jest jedynie fragmentem kodu – wymaga miesięcy rozpoznania i testów. Pocisk z kolei nie jest samą rakietą; jego skuteczność zależy od sensorów i integracji z systemem dowodzenia.

Jeśli analizujemy tylko cenę końcowego efektora, widzimy zaledwie najbardziej fotogeniczny element kosztu. Można to ująć w kategoriach kosztów stałych i krańcowych. Nowoczesne technologie wymagają ogromnych inwestycji początkowych w badania i infrastrukturę, po których koszt wytworzenia kolejnego egzemplarza drastycznie spada. W oprogramowaniu zjawisko to jest najwyraźniejsze: opracowanie produktu jest drogie, lecz jego kopiowanie niemal bezkosztowe. Podobna logika dotyczy broni autonomizowanej czy algorytmów rozpoznania, choć ogranicza ją konieczność aktualizacji i reakcje obrońcy. Strategicznie niebezpieczna jest więc nie tyle „taniość" ataku, co jego skalowalność po poniesieniu kosztu początkowego.

Da Empoli trafnie uchwyciła intuicję dotyczącą demokratyzacji środków oddziaływania. Technologie zarezerwowane dawniej dla mocarstw są dziś zastępowane lub uzupełniane rozwiązaniami komercyjnymi. Komponenty elektroniczne, komunikacja satelitarna i AI obniżają barierę wejścia dla mniejszych państw i aktorów niepaństwowych. Nie oznacza to jednak zaniku znaczenia wielkich budżetów. SIPRI szacuje światowe wydatki militarne w 2025 roku na około 2,9 biliona dolarów – poziom rekordowy. Epoka taniego drona jest równocześnie epoką rekordowo drogiego systemu wojskowego. Ten paradoks jest centralny.

Asymetria kosztów zakłócania i budowania odporności systemowej

Tanieje możliwość wyrządzenia konkretnych szkód, lecz niekoniecznie tanieje zdolność kontrolowania całego konfliktu. Mały aktor może zagrozić żegludze, infrastrukturze czy pojedynczym instalacjom, jednak zdobycie i utrzymanie terytorium, zapewnienie logistyki milionom ludzi, ochrona przestrzeni powietrznej, rozpoznanie strategiczne czy budowa odporności przemysłowej wciąż wymagają gigantycznych zasobów.

Należy zatem odróżnić demokratyzację zakłócania od demokratyzacji pełnoskalowej potęgi. Współczesna technologia drastycznie obniża próg przeszkadzania, destabilizowania, nękania i wymuszania kosztów; znacznie mniej jednoznacznie obniża jednak próg trwałego rządzenia tym, co zostało zaatakowane. To rozróżnienie pozwala lepiej zrozumieć naturę „drapieżnika". Drapieżnik w ujęciu Empoliego nie musi być silniejszy w sensie całościowym. Wystarczy, że potrafi zidentyfikować obszar, w którym marginalny koszt zakłócenia jest dużo niższy niż marginalny koszt przywrócenia odporności. Taka asymetria występuje w terroryzmie, cyberprzestrzeni, dezinformacji, atakach na infrastrukturę krytyczną oraz w części działaniach dronowych.

Podmiot niewielki może zmusić znacznie większy system do poniesienia kosztów, których sam nie byłby zdolny finansować symetrycznie. Ekonomia publiczna zna zbliżony problem w odniesieniu do dóbr publicznych. Bezpieczeństwo ma charakter częściowo dobra publicznego: ochrona infrastruktury, przestrzeni powietrznej czy systemu finansowego przynosi korzyść wielu uczestnikom, podczas gdy koszt musi zostać sfinansowany zbiorowo. Napastnik może skoncentrować zasoby na pojedynczym celu; obrońca musi natomiast finansować szeroką przestrzeń odporności. Ochrona wymaga redundancji, zapasów i nadmiarowych zdolności, z których korzysta się rzadko. W logice krótkoterminowej może to wyglądać jak marnotrawstwo, lecz w logice odporności jest ceną za zdolność przetrwania zdarzeń skrajnych.

W tym punkcie pojawia się koncepcja resilience. Tradycyjna defensywa próbuje zapobiec trafieniu. Odporność zakłada natomiast, że nie każde uderzenie uda się powstrzymać, dlatego system powinien potrafić absorbować szok, kontynuować działanie i szybko się odtwarzać. Zmienia to rachunek strategiczny. Jeśli infrastruktura funkcjonuje mimo lokalnych uszkodzeń, dane są rozproszone, zdolności zastępowalne, a organizacja sprawnie się regeneruje, napastnik traci część przewagi wynikającej z taniego uderzenia. Najtańszym sposobem obrony nie zawsze jest zatem zestrzelenie każdego pocisku; czasem jest nim zmniejszenie wartości, jaką przeciwnik uzyskuje po trafieniu.

Teoria systemów wskazuje tu na różnicę między robustness a resilience. Pierwsza oznacza odporność na zmianę – system zachowuje działanie pomimo zakłócenia. Druga obejmuje zdolność adaptacji i odbudowy po szoku. Fortyfikacja jest klasycznym przykładem rozwiązania robust: ma nie dopuścić przeciwnika do środka. Sieć rozproszona jest natomiast resilience-oriented: zakłada utratę części węzłów, ale zapobiega paraliżowi całego systemu. W świecie dronów i cyberataków to przesunięcie akcentów może mieć znaczenie równie duże, co rozwój kolejnego pocisku przechwytującego. Ukraina dostarczyła licznych przykładów takiego podejścia poprzez rozproszenie logistyki, adaptację infrastruktury i improwizowane metody przeciwdziałania nowym zagrożeniom. Rosja z kolei adaptowała własne sposoby ochrony i użycia bezzałogowców.

Charakterystyczna jest szybkość tego cyklu. Innowacja dająca wyraźną przewagę przez kilka miesięcy może szybko stracić skuteczność wskutek zakłócania, nowych sensorów lub zmian taktyki. Wojna technologiczna staje się zatem procesem koewolucji. Nie istnieje trwały „zwycięski dron"; istnieje populacja rozwiązań ewoluujących pod presją kontrśrodków. To właśnie dlatego prosta teoria historycznych „epok ofensywy" i „epok defensywy" wymaga ostrożności. Jednocześnie w różnych domenach bilans sił może być odmienny.

Obrona lądowa może zyskać przewagę dzięki fortyfikacjom, minowaniu i dronom, podczas gdy ataki dalekiego zasięgu na infrastrukturę mogą pozostać stosunkowo łatwe. Cyberobrona konkretnej, dobrze zarządzanej sieci bywa bardzo skuteczna, lecz ogromny ekosystem słabo aktualizowanych urządzeń tworzy idealne środowisko ofensywne. System przeciwrakietowy może chronić niewielki obszar z wysokim prawdopodobieństwem, ale nie nadaje się ekonomicznie do ochrony całego terytorium. Bilans ofensywa-defensywa jest więc lokalny i zależny od misji.

Jeszcze inaczej wygląda odstraszanie nuklearne. Pojawia się sugestia, że powojenny wysoki koszt agresji wynikał między innymi z odstraszania nuklearnego, a współczesne technologie miałyby ten porządek stopniowo rozmontowywać. Intuicja ta jest częściowo trafna, lecz wymaga rozróżnienia poziomów.

Broń nuklearna nie sprawiła, że każda forma agresji stała się nieopłacalna. Wojny konwencjonalne, interwencje, konflikty zastępcze czy terroryzm trwały przez całą zimną wojnę. Odstraszanie nuklearne podniosło przede wszystkim koszt bezpośredniej, pełnoskalowej konfrontacji między mocarstwami zdolnymi do odwetu. Nuklearna rewolucja strategiczna polegała więc nie na „defensywie" w klasycznym znaczeniu, lecz na możliwości zadania przeciwnikowi nieakceptowalnego kosztu po ataku. Schelling rozróżniał zdolność do obrony od zdolności do ukarania. W świecie wzajemnie gwarantowanej destrukcji państwo nie musi przechwycić wszystkich głowic, jeśli zachowuje wiarygodną możliwość odwetu. To logika deterrence by

punishment, zasadniczo inna od deterrence by denial. Pierwsza mówi: jeżeli zaatakujesz, zapłacisz. Druga: jeżeli zaatakujesz, nie osiągniesz celu.

Wielowarstwowość odstraszania i asymetria kosztów kompetencji

Współczesna obrona przed dronami, cyberatakami i działaniami hybrydowymi musi łączyć oba mechanizmy. Według danych SIPRI z 2026 roku wszystkie dziewięć państw posiadających broń nuklearną kontynuowało modernizację swoich arsenałów, a wiele z nich wdrażało nowe systemy nuklearne lub zdolne do przenoszenia broni jądrowej.

Instytut zwraca jednocześnie uwagę na rosnące ryzyko błędnej kalkulacji i eskalacji. Nie mamy zatem do czynienia z prostym zanikiem odstraszania nuklearnego, lecz z coraz bardziej złożonym systemem, w którym klasyczne odstraszanie współistnieje z precyzyjnymi środkami konwencjonalnymi, cyberzdolnościami, systemami przeciwrakietowymi i rosnącą rolą automatyzacji. Im silniej te warstwy się przenikają, tym trudniej przewidzieć, jak przeciwnik zinterpretuje konkretne działanie. Do rachunku ofensywy i obrony dołącza także domena biologiczna.

Spotyka się ujęcie przedstawiające ją w najbardziej dramatycznej postaci, sugerujące możliwość osiągnięcia ogromnego efektu destrukcyjnego przy stosunkowo niskim koszcie technologicznego wejścia. Takie porównanie cenowe należy jednak odrzucić jako zbyt uproszczone. Sam dostęp do aparatury czy informacji nie jest równoważny zdolności stworzenia skutecznego zagrożenia biologicznego. Pomiędzy urządzeniem, wiedzą laboratoryjną a stabilnym czynnikiem biologicznym i rzeczywistą zdolnością powodowania szkody istnieją zasadnicze bariery kompetencyjne, techniczne i organizacyjne. Wyolbrzymianie łatwości tych działań może paradoksalnie tworzyć niebezpiecznie fałszywe wyobrażenie o dostępności takich zdolności. Nie oznacza to jednak, że problem dual-use jest fikcyjny. WHO podkreśla rosnącą złożoność oceny badań podwójnego zastosowania w naukach o życiu — w tym wyzwania wynikające z połączenia nowych technologii biologicznych z AI — i wskazuje na potrzebę harmonizacji procesów oceny ryzyka, odpowiedzialnego zarządzania danymi oraz szerszej edukacji środowisk naukowych. Właściwą kategorią nie jest więc „tania broń biologiczna", lecz stopniowe obniżanie barier dostępu do wiedzy i narzędzi przy jednoczesnym utrzymywaniu się wysokich barier skutecznego zastosowania.

To obraz bardziej skomplikowany, a zarazem realistyczny. Podobny problem pojawia się w odniesieniu do sztucznej inteligencji. AI nie jest samodzielnym środkiem ofensywnym

porównywalnym z pociskiem; jest technologią ogólnego zastosowania, która może obniżać koszt niektórych procesów poznawczych: analizy danych, rozpoznawania wzorców, generowania kodu, automatyzacji obserwacji, planowania czy przetwarzania ogromnych ilości informacji. Jej strategiczna wartość polega więc potencjalnie na obniżaniu kosztu kompetencji, a nie tylko kosztu fizycznego efektora. Jeśli zadanie, które wcześniej wymagało dużego zespołu ekspertów, dzięki systemowi wspomagającemu może być wykonane przez mniejszą grupę, zmienia się ekonomia dostępu do zdolności. Nie oznacza to jednak, że AI automatycznie zwiększa przewagę ofensywy. Obrońcy również wykorzystują modele do wykrywania anomalii, analizy zagrożeń, przetwarzania obrazu, cyberbezpieczeństwa i zarządzania systemami. Właściwsze jest zatem pytanie, po której stronie sztuczna inteligencja bardziej obniża koszt krańcowy działania. Może się okazać, że w jednej domenie premiuje napastnika, a w innej zwiększa efektywność obrony.

Asymetria koncentracji i podatek obronny złożoności

Technologia ogólnego zastosowania nie determinuje politycznego rezultatu, lecz przekształca funkcję kosztu wielu uczestników jednocześnie. Wojskowa asymetria przypomina tu logikę ekonomii platform i teorii sieci. W wielu domenach atakujący wybiera punkt koncentracji, podczas gdy obrońca musi zabezpieczyć całą powierzchnię. Haker uderza w konkretną słabość; administrator utrzymuje tysiące urządzeń. Terrorysta wybiera miejsce i czas; państwo chroni tysiące potencjalnych celów. Dezinformator tworzy jedną atrakcyjną, fałszywą narrację; instytucje wiedzy muszą stale produkować wiarygodną informację.

Firma projektująca nowy model może skoncentrować najlepszych ekspertów nad jednym produktem, podczas gdy regulator musi rozumieć cały ekosystem rynku. Choć podobieństwo to nie oznacza tożsamości, wspólnym mianownikiem pozostaje problem asymetrii koncentracji. Tę asymetrię można określić mianem podatku obronnego złożoności. Im bardziej skomplikowany system chcemy chronić, tym więcej relacji, interfejsów, procedur i punktów potencjalnego zakłócenia musimy monitorować. Rozwój technologiczny zwiększa możliwości systemu, ale jednocześnie powiększa jego powierzchnię ataku. Nowoczesny samochód jest bezpieczniejszy mechanicznie od dawnego, lecz stał się systemem komputerowym.

Szpital zyskał na skuteczności dzięki cyfryzacji, jednak awaria IT może dziś całkowicie sparaliżować jego funkcjonowanie. Państwo stało się sprawniejsze przez usługi elektroniczne, ale musi chronić infrastrukturę przed nową klasą zagrożeń. Postęp zwiększa zatem zarówno możliwości, jak i zależności. Charles Perrow w teorii normal accident zwracał uwagę, że w systemach charakteryzujących się dużą złożonością interakcji i ścisłym sprzężeniem pewne typy awarii stają

się trudne do przewidzenia i lokalizowania. Problem ten ma wymiar strategiczny: napastnik nie musi niszczyć całego systemu, jeśli odkryje komponent, którego utrata uruchomi kaskadę zależnych zakłóceń. Obrona nie może więc ograniczać się do ochrony poszczególnych obiektów, lecz musi obejmować analizę zależności między nimi.

Ekonomia ataku i obrony staje się przez to ekonomią systemowego efektu, nie cen katalogowych. Dron kosztujący dziesięć tysięcy, sto tysięcy czy milion dolarów jest „drogi" lub „tani" wyłącznie w relacji do efektu, jaki osiąga. Pocisk przechwytujący za pięć milionów może być ekonomicznie absurdalny wobec niegroźnego celu, a całkowicie racjonalny, jeśli chroni aktywo o wartości miliardów lub zapobiega dziesiątkom ofiar. Cyberoperacja może wydawać się niemal bezkosztowa, jeśli liczymy tylko wysłanie pakietów danych, lub bardzo kosztowna, gdy uwzględnimy lata pracy zespołu i utratę luki po jej ujawnieniu.

Asymetria widoczności i pokusa pominięcia instytucjonalnych hamulców

Cena jednostkowa jest wskaźnikiem użytecznym, lecz jedynie pierwszego rzędu. Z punktu widzenia da Empoliego kluczowy jest skutek polityczny. Gdy społeczeństwo obserwuje, że potężny system państwowy wydaje miliony na zwalczanie tanich zagrożeń, rodzi się wrażenie przewagi małego drapieżnika nad wielkim aparatem. Jest ono częściowo prawdziwe, choć psychologicznie wyolbrzymiane przez asymetrię widoczności. Koszt ataku jest konkretny i łatwy do zobrazowania: dron, telefon, komputer, niewielka grupa ludzi. Koszt obrony pozostaje rozproszony: radary, infrastruktura, szkolenia, dyżury, logistyka, wywiad, normy prawne i rezerwy.

Napastnik staje się bohaterem spektakularnego epizodu, podczas gdy skuteczna defensywa polega właśnie na tym, że nic się nie wydarza. Ekonomia bezpieczeństwa cierpi więc na szczególny problem polityczny: sukces obrony jest kontrfaktyczny. Trudno bowiem zaprezentować katastrofę, która nie nastąpiła. Nakłady na odporność mogą wydawać się przesadne aż do momentu wystąpienia kryzysu, po którym nagle zaczynają wyglądać na oczywiście niewystarczające. Ten sam mechanizm utrudnia politykę zdrowia publicznego, zapobieganie powodziom czy przygotowanie na pandemię. Efektywny system bezpieczeństwa produkuje brak zdarzenia – dobro niezwykle cenne, ale komunikacyjnie niewdzięczne. Dlatego „drapieżnik" posiada jeszcze jedną przewagę: medialną. Spektakularny atak generuje obraz, emocję i narrację sprawczości.

Wielowarstwowa obrona generuje natomiast protokoły, magazyny, procedury serwisowe i niewidzialną redundancję. Współczesna polityka, podporządkowana logice uwagi, może zatem

przeceniać widowiskową ofensywę, niedoceniając nudnej odporności. To, co daje się łatwo pokazać, zaczyna być mylone z tym, co ma największe znaczenie. Da Empoli ma rację w kwestii fundamentalnej: współczesna technologia rzeczywiście tworzy obszary, w których relatywnie mały nakład może wywołać nieproporcjonalnie wysoki koszt reakcji. SIPRI określa dostępność i elastyczność bezzałogowców jako trend zmieniający charakter wojny, dokumentując równoległy wyścig środków przeciwdziałania. Błędem byłoby jednak wyprowadzenie z tego uniwersalnego prawa, że ofensywa „wygrała". Technologia wywołuje raczej serię lokalnych asymetrii, na które obrona z czasem zaczyna adaptować. Wojna pozostaje procesem uczenia się. Prawdziwie niepokojącym elementem "godziny drapieżnika" jest więc coś subtelniejszego niż zwykła taniość broni: obniżenie minimalnego kosztu wejścia do gry w naruszanie porządku, podczas gdy koszt utrzymywania tego porządku pozostaje wysoki.

Atakujący może wybierać moment, obiekt i metodę. Obrońca musi zachować gotowość nawet wtedy, gdy nic się nie dzieje. Napastnik może eksperymentować; obrońca ponosi pełną odpowiedzialność za błąd. Atakujący potrzebuje czasem jednego sukcesu, podczas gdy obrońca jest oceniany przez pryzmat każdego niepowodzenia. Ta nierównowaga łączy ekonomię przemocy z polityką „manual override". Skoro istnieje możliwość wywołania szybkiego i widocznego rezultatu przy niskim koszcie wejścia, rośnie pokusa pominięcia wolniejszego systemu instytucjonalnego. Działanie zaczyna poprzedzać uzasadnienie. Najpierw zmienia się sytuację, później wyjaśnia, dlaczego było to konieczne. Można najpierw dokonać uderzenia, zatrzymania, reorganizacji albo blokady, a następnie zmusić aparat prawny i polityczny do interpretowania faktu już dokonanego. W tej przestrzeni „manual override" przestaje być tylko barwnym określeniem politycznej brutalności. Staje się teorią szczególnego rodzaju sprawczości: przewagi aktora zdolnego skrócić drogę między wolą a skutkiem poprzez pominięcie elementów systemu, które zaprojektowano jako hamulce, kontrole lub miejsca negocjacji. Nie każda szybka decyzja jest jednak sprawna, nie każdy hamulec jest zbędną biurokracją i nie każdy stan wyjątkowy usprawiedliwia zawieszenie reguł.

> W świecie, w którym tani dron może zmusić mocarstwo do kosztownej reorganizacji całej strategii obronnej, prawdziwa przewaga przestaje wynikać z posiadania najsilniejszej broni, a zaczyna z poziomu systemowej odporności. Czy w epoce „godziny drapieżnika" dyplomacja zdoła odzyskać rolę architekta przyszłości, czy pozostanie jedynie kronikarzem faktów dokonanych? Być może największym paradoksem nowoczesności jest to, że im szybciej potrafimy niszczyć i zmieniać rzeczywistość, tym bardziej jesteśmy uzależnieni od powolnych, nudnych i niewidocznych procedur, które tę rzeczywistość stabilizują.

Inspiracje

[1] "The Hour of the Predator" Giuliano da Empoli

Giuliano da Empoli (ur. 27 sierpnia 1973) jest włosko-szwajcarskim pisarzem, eseistą politycznym i politologiem. Studiował na Uniwersytecie La Sapienza w Rzymie i w Instytucie Nauk Politycznych w Paryżu, łącząc karierę w sprawach publicznych, środowisku akademickim i literaturze. Da Empoli był starszym doradcą premiera Włoch Matteo Renziego oraz wicemerem Florencji ds. kultury. Jest wykładowcą w Instytucie Nauk Politycznych w Paryżu i prezesem-założycielem Volty, mediolańskiego think tanku zajmującego się polityką europejską. Jego prace analityczne badają narrację polityczną, manipulację algorytmiczną i mechanizmy współczesnej władzy politycznej. Da Empoli zyskał międzynarodową sławę literacką dzięki swojej debiutanckiej powieści „Czarodziej z Kremla" („Le Mage du Kremlin", 2022), która zdobyła Grand Prix du roman de l'Académie française i była finalistą Nagrody Goncourtów.

Giuliano da Empoli *(born August 27, 1973) is an Italian-Swiss writer, political essayist, and political scientist. Educated at Sapienza University of Rome and Sciences Po Paris, he has combined careers in public affairs, academia, and literature. Da Empoli served as senior advisor to Italian Prime Minister Matteo Renzi and as Florence's deputy mayor for culture. He is a lecturer at Sciences Po Paris and the founding chairman of Volta, a Milan-based European policy think tank. His analytical works investigate political storytelling, algorithmic manipulation, and the mechanics of modern political power. Da Empoli achieved major international literary renown with his debut novel, The Wizard of the Kremlin (Le Mage du Kremlin, 2022), which won the Grand Prix du roman de l'Académie française and was a finalist for the Prix Goncourt.*

Sciences Po

Literatura uzupełniająca

Książki

Książki autorów przywoływanych i literatura pokrewna:



[1] "Restraint"

Barry Posen

Cornell University Press | ISBN: 9781501700729



[2] **"Normal accidents : living with high-risk technologies : with a new afterword and a postscript on the Y2K problem"**

Charles Perrow

Princeton University Press | ISBN: 9780691004129



[3] **"Normal Accidents"**

Charles Perrow

Princeton University Press | ISBN: 9781400828494

Artykuły naukowe

Prace autorów przywoływanych w tekście:

[1] **"The Diplomacy Of Violence"**

Thomas C. Schelling

1970 | Theories of Peace and Security | DOI: 10.1007/978-1-349-15376-3_4

Źródło

[2] **"Strategic Problems of an International Armed Force"**

Thomas C. Schelling

1963 | International Organization | DOI: 10.1017/s0020818300033853

Źródło

[3] **"Why Does Economics Only Help with Easy Problems?"**

Thomas C. Schelling

1997 | economic science and practice | DOI: 10.4337/9781035362950.00015

Źródło

[4] **"Hussein's Lessons to Learn" From the Desert War""**

Carl VON Clausewitz

1992 | DOI: 10.21236/ada437372

Źródło

[5] **"The Sources of Military Doctrine: France, Britain and Germany between the World Wars"**

Andrew J. Pierre, Barry R. Posen

1985 | Foreign Affairs | DOI: 10.2307/20042486

Źródło

[6] **"European Union Security and Defense Policy: Response to Unipolarity?"**

Barry R. Posen

2006 | Security Studies | DOI: 10.1080/09636410600829356

Źródło

[7] **"Political Institutions and Military Change: Lessons from Peripheral Wars, by Deborah D. Avant"**

Barry R. Posen

1995 | Political Science Quarterly | DOI: 10.2307/2152373

Źródło

[8] **"Technology, Doctrine, Strategy, and Stability"**

Barry r. Posen

2019 | Technology and Strategy | DOI: 10.4324/9780429308437-7

Źródło

[9] **"What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment"**

Rebecca M. Slayton

2017 | International Security | DOI: 10.1162/isec_a_00267

Źródło

[10] **"Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards"**

Aaron Clark-Ginsberg, Rebecca M. Slayton

2018 | Science and Public Policy | DOI: 10.1093/scipol/scy061

Źródło

[11] **"Continental Defense in the Eisenhower Era: Nuclear Antiaircraft Arms and the Cold War (review)"**

Rebecca Slayton

2012 | Technology and Culture | DOI: 10.1353/tech.2012.0153

Źródło

[12] **"The Logic of Collective Action: Public Goods and the Theory of Groups."**

Charles B. Perrow, Mancur Olson

1973 | Social Forces | DOI: 10.2307/2576430

Źródło

[13] "The Modern Corporation Statement on Management"

Hugh Christopher Willmott, Martin Parker, C. Perrow, R. ten Bos, A. Beverungen

2016 | DOI: 10.2139/ssrn.2863077

Źródło

[14] "FROM 'POLITICS AS A VOCATION'"

Max Weber

1991 | Edinburgh University Press eBooks | DOI: 10.1515/9781474469654-020

Źródło

Artykuły naukowe autora:

[15] "Architettura Open Source. Verso una progettazione aperta"

Elke Pohl, Assaf Biderman, Michele Bonino, Richard Burdett, Pierre Alain Croset, Giuliano da Empoli

2014

Źródło

[16] "Open Source Architecture"

Ethel Baraona Pohl, Assaf Biderman, Michele Bonino, Ricky Burdett, Pierre Alain Croset, Giuliano da Empoli

2015

Źródło

[17] "L'heure des prédateurs"

Giuliano da Empoli

2026 | Gallimard eBooks | DOI: 10.3917/gall.empol.2026.01

Źródło

[18] "Entretien avec Giuliano Da Empoli autour de L'Heure des prédateurs"

Giuliano da Empoli, Patrick Suter, Fabien Dubosson, Helena Goncalves Leal, Dominik Wüthrich

2026 | Open Access CRIS of the University of Bern | DOI: 10.48620/96620

Źródło

[19] "Riyad, novembre 2024"

Giuliano da Empoli

2025 | Cairn.info

Źródło

[20] "Chicago, novembre 2017"

Giuliano da Empoli

2025 | Cairn.info

Źródło

[21] "Florence, mars 2012"

Giuliano da Empoli

2025 | Cairn.info

Źródło

[22] "Présentation"

Giuliano da Empoli

2025 | Cairn.info

Źródło

[23] "Montréal, septembre 2024"

Giuliano da Empoli

2025 | Cairn.info

Źródło

[24] "Berlin, décembre 2024"

Giuliano da Empoli

2025 | Cairn.info

Źródło

Treść tworzy Fundacja Dobre Państwo.
Redaguje i publikuje APA ONE, autorski system redakcyjny Fundacji oparty na AI.
APA ONE Publishing System
Fundacja Dobre Państwo © 2026
Article ID: 38376f0e-58c4-457c-aefa-35c7accf9ef4