Przegląd Bezpieczeństwa Wewnętrznego

2024, nr 31, s. 13–55

 https://doi.org/10.4467/20801335PBW.24.017.20794

ARTYKUŁ

Możliwości wykorzystania modeli analitycznych Cyber Threat Intelligence w badaniach operacji informacyjnych i operacji wpływu

The potential of Cyber Threat Intelligence analytical frameworks in research on information operations and influence operations

KAMIL BARANIUK

Wydział Nauk Społecznych, Uniwersytet Wrocławski
Polskie Towarzystwo Bezpieczeństwa Narodowego

https://orcid.org/0000-0002-8071-434X

PIOTR MARSZAŁEK

Polskie Towarzystwo Bezpieczeństwa Narodowego

https://orcid.org/0009-0000-0362-4132

Abstrakt

Celem autorów była ocena użyteczności wykorzystania podejścia Cyber Threat Intelligence (CTI) w analizie operacji informacyjnych (*information operations*) i operacji wpływu (*influence operations*). Badanie zostało przeprowadzone metodą porównawczą opartą na technice analizy źródeł zastanych. Punktem odniesienia komparatystyki dla metodologii CTI były metody wywodzące się z komunikologii, które są stosunkowo popularne w badaniu propagandy. Autorzy starali się odpowiedzieć na pytanie, jaki wkład metodologiczny w badania omawianych zjawisk – i tym samym dla praktycznego potencjału warsztatu analityka – stanowi przyjęcie paradygmatu analizy operacji informacyjnych i operacji wpływu opartego na modelach rozpoznawania taktyk, technik i procedur (*tactics*,

techniques, and procedures, TTPs), taksonomii incydentów teleinformatycznych czy typizacji aktorów zagrożeń (*threat actors*) w CTI. Główną osią badania była krytyczna analiza anglojęzycznych publikacji na temat wykorzystania CTI w analizie dezinformacji. Zasadniczym wnioskiem płynącym z analizy jest teza o ograniczonych korzyściach metodologicznych metod opartych na CTI, przy jednocześnie dużym ich potencjale techniczno-organizacyjnym dla badania elementów operacji informacyjnych oraz operacji wpływu, w których jest wykorzystywana cyberprzestrzeń.

Słowa kluczowe walka informacyjna, operacje wpływu, operacje informacyjne, dezinformacja, cyberbezpieczeństwo, CTI

Abstract The article's aim is to evaluate the utility of using the Cyber Threat Intelligence (CTI) approach in analysing information and influence operations. The study was carried out by a comparative method based on the technique of desk research. The point of comparison for the CTI methodology were methods originated in communicology, which are relatively popular in the study of propaganda. The authors try to answer the question of what methodological contribute to the study of the discussed phenomena – and thus to the practical potential of the analyst's workshop – is the adoption of a paradigm for the analysis of information operations and influence operations based on models of tactics, techniques, and procedures (TTPs) recognition and taxonomy of ICT incidents or typification of CTI threat actors. The central focus of the study is a critical analysis of English-language publications discussing the use of CTI in disinformation analysis. The main conclusion from the analysis includes a thesis about the limited methodological benefits of CTI based methods, while using their technical and organisational strengths to research elements of information operations and influence operations in which cyberspace is used.

Keywords information warfare, influence operations, information operations, disinformation, cybersecurity, CTI

Wprowadzenie

Cyber Threat Intelligence[1] (CTI) stanowi obecnie nieodłączny element procesu zapewniania cyberbezpieczeństwa[2] w obszarach, w których istnieje domniemany przeciwnik. Rozwój tej dyscypliny, związany z koniecznością reagowania na rosnącą kreatywność i zaawansowanie adwersarzy, pomaga objąć procesem analizy coraz to nowe elementy ewoluujących cyberzagrożeń. Stosowanie wspólnej aparatury pojęciowej, modeli i standardów znacznie zwiększa kooperatywny potencjał specjalistów z zakresu cyberbezpieczeństwa. Ambicją ekspertów ds. CTI jest zapewnienie zdolności organizacji, w tym państwa i jego obywateli, do podjęcia działań wyprzedzających, obliczonych na wyeliminowanie lub zminimalizowanie, np. przez aktywną obronę (*active defense*), skutków szkodliwych działań.

Celem autorów artykułu była ocena użyteczności wykorzystania podejścia CTI w analizie operacji informacyjnych oraz operacji wpływu, czyli propozycji popularyzowanych obecnie m.in. przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (European Union Agency for Cybersecurity, ENISA)[3]. Autorzy starali się odpowiedzieć na pytanie, jaki wkład metodologiczny w badania omawianych zjawisk – i tym samym w praktyczny potencjał warsztatu analityka – stanowi przyjęcie modelu analizy operacji informacyjnych i operacji wpływu opartego na rozpoznawaniu taktyk, technik i procedur (*tactics, techniques, and procedures*, TTPs), aktorów zagrożeń (*threat actors*) oraz inspirowanie się terminologią incydentów teleinformatycznych.

Postawiony cel autorzy osiągnęli z wykorzystaniem założeń metodologii ogólnej – analizy i syntezy – które zostały przeprowadzone z użyciem metody porównawczej oraz techniki analizy źródeł zastanych.

W pierwszej części artykułu dokonano analizy źródeł ukierunkowanej na omówienie podstaw CTI i modeli analitycznych stosowanych w jej ramach. W drugiej części autorzy podjęli próbę zdefiniowania istoty operacji informacyjnych

---

[1] Wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje tej informacji za każdym razem (przyp. red.).

[2] „Cyberbezpieczeństwo" oraz inne terminy wykorzystywane w niniejszym artykule zostały zdefiniowane w dalszej części artykułu. W celu zachowania klarowności części pojęć branżowych z języka angielskiego nie tłumaczono, a w przypadku przetłumaczenia oryginalne brzmienie zostało podane w nawiasie. [Tłumaczenia w artykule pochodzą od autorów – dop. red.].

[3] Zob. szerzej: *Cybersecurity and Foreign Interference in the EU Information Ecosystem*, ENISA, 8 XII 2022 r., https://www.enisa.europa.eu/news/cybersecurity-foreign-interference-in-the-eu-information-ecosystem [dostęp: 20 IX 2024]; *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape*, ENISA, 8 XII 2022 r., https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape [dostęp: 20 IX 2024].

(*information operations*) oraz operacji wpływu (*influence operations*) na podstawie przykładowych publicznie dostępnych materiałów oraz literatury tworzonej przez instytucje, które są zobligowane do zajmowania się tego typu zjawiskami, tj. instytucje sektora siłowego (głównie dokumenty normatywne zachodnich sił zbrojnych w postaci doktryn oraz instrukcji, a także piśmiennictwo związane z funkcjonowaniem służb specjalnych w postaci branżowych glosariuszy, słowników i leksykonów). Zostało w niej omówione rozumienie tych zjawisk przez podmioty z branży platform społecznościowych i IT. Jako przykłady wykorzystano serwisy społecznościowe – Facebook i X oraz firmę Microsoft. Celem tej części artykułu była analiza relacji operacji wpływu i operacji informacyjnych z cyberbezpieczeństwem i cyberprzestrzenią. W trzeciej i czwartej części artykułu autorzy przeprowadzili syntezę piśmiennictwa naukowego oraz innej literatury przedmiotu, aby porównać metody analizy operacji informacyjnych i operacji wpływu wykorzystujące metody badawcze wywodzące się z nauk o komunikacji oraz – zaadaptowanych na te potrzeby – modeli stosowanych w CTI.

Cyber Threat Intelligence jako element zapewniania cyberbezpieczeństwa

Omówienie istoty CTI należy rozpocząć od zarysowania obszaru cyberbezpieczeństwa, za który odpowiada ta dziedzina. Sfera zagrożeń w cyberprzestrzeni[4] dynamicznie się rozwija, zarówno pod względem jakościowym, jak i ilościowym. Wynika to ze stałego przyrostu liczby aktorów zagrożeń, wysoce zmotywowanych do wykorzystania możliwości stwarzanych przez wirtualną rzeczywistość do realizacji

[4] Pojęcie cyberprzestrzeni funkcjonujące w obiegu naukowym oraz eksperckim ma swoją genezę w kulturze popularnej i – w uproszczeniu – można przyjąć, że dotyczy rozległej, alternatywnej wobec świata rzeczywistego (fizycznego) sfery powstałej na bazie powiązań między urządzeniami telekomunikacyjnymi i informacyjnymi. Zob. J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 225–226. Termin „cyberprzestrzeń" funkcjonuje również w polskim obiegu prawnym i oznacza, zgodnie z art. 2 pkt 1 lit. 1b *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*, „(…) przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne (…) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". W polskim prawodawstwie terminem „system teleinformatyczny" określa się natomiast, zgodnie z art. 3 pkt 3 *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*, „(…) zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej".

działań godzących w dobra innych. Podmioty te w zależności od motywacji (np. finansowych bądź politycznych) obierają sobie za cele ataku jednostki (np. kradzież tożsamości), jak również organizacje (np. oszustwa finansowe) i podmioty państwowe (np. cyberszpiegostwo, sabotaż komputerowy).

Zapewnienie dowolnej organizacji, państwu, ale także jednostce szeroko pojętego cyberbezpieczeństwa nie byłoby więc kompletne, gdyby w rozpoznawaniu zagrożeń w cyberprzestrzeni i przeciwdziałaniu im nie dążono do pogłębiania wiedzy o podmiotach kreujących te zagrożenia. Działania podejmowane w cyberprzestrzeni, chociaż korzystają z jej różnych udogodnień[5], nie odbywają się bez pozostawiania śladów i tropów (tj. danych), które mogą zostać zebrane i uwzględnione w analizie retrospektywnej. Dane te można również wykorzystać do podjęcia działań wyprzedzających, będących w pewnych sytuacjach posunięciem najkorzystniejszym.

Dziedziną wiedzy mającą ambicję wzmocnienia w cyberprzestrzeni potencjału defensywnego organizacji, rozwijaną na styku informatyki, cyberbezpieczeństwa i studiów wywiadowczych, jest CTI[6]. Istnieje wiele definicji tego pojęcia[7]. Jest to związane m.in. z komercyjnym rozwojem branży cyberbezpieczeństwa, w obrębie której CTI funkcjonuje jako produkt bądź usługa (np. płatny dostęp do źródeł informacji o zagrożeniach, tzw. *threat intelligence feed*) i podlega prawom rynku komercyjnego oraz potrzebom marketingu[8]. W mniejszym stopniu CTI stanowi domenę badań naukowych, w tym metodologicznych, pozostając obszarem wymagającym refleksji teoretycznej[9].

Na potrzeby artykułu autorzy przyjęli definicję CTI zaproponowaną w dokumencie *CTI-CMM Cyber Threat Intelligence Capability Maturity Model*. Zgodnie z nią jest to dyscyplina skupiona na zrozumieniu zdolności, intencji, motywacji

---

[5] Te udogodnienia, w porównaniu z fizycznym wymiarem środowiska informacyjnego, zwiększają możliwości ukrywania lub fałszowania tożsamości oraz powodują, że podejmowane działania nie mają geograficznych ograniczeń.

[6] K. Oosthoek, Ch. Doerr, *Cyber Threat Intelligence: A Product Without a Process?*, „International Journal of Intelligence and Counter Intelligence" 2021, t. 34, nr 2, s. 301. https://doi.org/10.1080/08850607.2020.1780062.

[7] Nierzadko pojęcie *cyber threat intelligence* jest używane zamiennie z *threat intelligence* (TI), a więc pojęciem znaczeniowo szerszym. Jak wskazują Scott J. Roberts i Rebekah Brown, TI to analiza adwersarzy, ich zdolności, motywacji i celów, CTI zaś jest analizą tego, jak adwersarze wykorzystują cyberprzestrzeń do osiągnięcia swoich celów. Zob. S.J. Roberts, R. Brown, *Intelligence-Driven Incident Response. Outwitting the Adversary*, Sebastopol 2017, s. 2–3.

[8] *An introduction to threat intelligence*, CERT-UK, https://www.ncsc.gov.uk/files/An-introduction-to-threat-intelligence.pdf, s. 2 [dostęp: 10 IX 2024].

[9] K. Oosthoek, Ch. Doerr, *Cyber Threat Intelligence*…, s. 301–302.

i możliwości (*opportunities*) aktorów cyberzagrożeń (*cyber adversaries*) oraz związanych z nimi taktyk, technik i procedur[10] działania (TTPs)[11].

Ujęcie CTI jako procesu obejmuje m.in. zorganizowanie i usystematyzowanie podejmowanych działań w formie cyklu wywiadowczego, zmierzającego do uzyskania użytecznej wiedzy, spełniającej potrzeby informacyjne odbiorcy. Szerokie czerpanie z dorobku analizy wywiadowczej ma na celu zapewnienie, a raczej narzucenie, odpowiedniego rygoru i jakości procesu analitycznego. Dlatego też stałymi elementami wykładów na temat CTI są: wykorzystanie ustrukturalizowanych technik analitycznych (np. analizy hipotez konkurencyjnych) oraz stosowanie ustandaryzowanego języka wyrażającego stopień pewności wydawanych sądów bądź stopień prawdopodobieństwa opisywanych zdarzeń[12].

Podobnie jak w analizie wywiadowczej[13] produkty informacyjne CTI dzielą się na trzy poziomy: taktyczny, operacyjny i strategiczny. Tym samym kierują one uzyskaną wiedzę na odpowiedni szczebel decyzyjny. Najniższy szczebel, taktyczny, obejmuje informacje o krótkim cyklu życia, ale niezbędne do bezpośredniego wykrycia i mitygowania zagrożenia przez techniczne zespoły monitorujące cyberbezpieczeństwo systemów lub zespoły reagowania na incydenty. Na tym poziomie podstawową formą informacji dostarczanej przez CTI są wskaźniki kompromitacji (*indicators of compromise*, IoC), czyli takie artefakty, jak adres IP, domena, *hash* pliku. Ich występowanie w ochranianym systemie wskazuje na naruszenie jego bezpieczeństwa. Poziom operacyjny obejmuje zazwyczaj informacje o kampanii (operacji) prowadzonej przez adwersarzy wraz z charakterystyką sposobu i motywu działania (np. kradzież danych). Poziom ten zawiera wymiar behawioralny (czyli TTPs), opisujący, w jaki sposób atakujący realizuje swój cel. Powiązanie obserwacji behawioralnych z informacją o infrastrukturze wykorzystanej w operacji, jak również interpretacja motywacji i zamierzonych celów działania mogą dać podstawę

[10] Na temat znaczenia TTPs w CTI zob. *TTP in cybersecurity*, Sekoia, https://www.sekoia.io/en/glossary/ttp-cyber-tactics-techniques-and-procedures/ [dostęp: 9 IX 2024].

[11] M. DeBolt i in., *CTI-CMM Cyber Threat Intelligence Capability Maturity Model*, Version 1.0, https://d39ec1uo9ktrut.cloudfront.net/Datasheets/CTI-CMM-Cyber-Threat-Intelligence-Capability-Maturity-Model.pdf, s. 70 [dostęp: 22 VIII 2024]. CTI-CMM (wersja 1.0) jest dokumentem opisującym model dojrzałości programu CTI w organizacji, opublikowanym w 2024 r. i opracowanym jako konsensus grona 27 ekspertów z sektorów: prywatnego i publicznego.

[12] Zob. *Words of Estimative Probability, Analytic Confidences, and Structured Analytic Techniques*, Center for Internet Security, https://www.cisecurity.org/ms-isac/services/words-of-estimative-probability-analytic-confidences-and-structured-analytic-techniques [dostęp: 23 VIII 2023]. Skala rzeczywistego wykorzystania metod i narzędzi zaczerpniętych z analizy wywiadowczej w pracach zespołów CTI może być znacznie przeszacowana i stanowi raczej postulat niż codzienną rutynę praktyków CTI. Zob. K. Oosthoek, Ch. Doerr, *Cyber Threat Intelligence*…, s. 304–305.

[13] Zob. *Words of Estimative Probability, Analytic Confidences*…

do atrybucji, tj. przypisania operacji do danego aktora, np. grupy APT (*advanced persistent threat*)[14]. Poziom strategiczny zaspokaja potrzeby informacyjne odbiorców najwyższego rzędu, np. kreujących politykę cyberbezpieczeństwa organizacji czy państwa, i umożliwia podejmowanie działań strategicznych w dziedzinie cyberbezpieczeństwa, wspartych zorganizowanym procesem wywiadowczym[15].

Modele analityczne i platformy wymiany informacji w CTI

Dynamiczny rozwój metod i technik obrony przed zagrożeniami, wynikający z konieczności zrównoważenia lub przewyższenia potencjałów między obrońcami a atakującymi, zaowocował powstaniem modeli analitycznych (*analytical framework*), taksonomii, ontologii czy standardów wymiany danych (np. formatu STIX, *structured threat information eXpression*)[16]. Do wiodących modeli analitycznych stosowanych w CTI należą: Cyber Kill Chain, MITRE ATT&CK oraz Diamond Model (model diamentu).

Model Cyber Kill Chain, zaproponowany i scharakteryzowany przez Erica M. Huthinsa i innych pracowników koncernu Lockheed Martin w artykule *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*[17], jest dekompozycją cyberataku na siedem następujących po sobie etapów, które atakujący musi zrealizować, aby osiągnąć swój cel. Są to:

1) rekonesans (*reconnaissance*),
2) uzbrojenie (*weaponization*),
3) dostarczenie (*delivery*),

---

[14] Zagadnienie atrybucji w CTI jest jej istotnym elementem, ponieważ odpowiada na zasadnicze pytanie – kto generuje zagrożenie? Na tego rodzaju pytanie zwykle można udzielić odpowiedzi jedynie częściowej bądź niepewnej, co wynika m.in. z faktu ukrywania przez wielu aktorów swojej prawdziwej tożsamości. Na temat atrybucji CTI zob. J. Collier, S. Ronis, *Navigating the Trade-Offs of Cyber Attribution*, https://cloud.google.com/blog/topics/threat-intelligence/trade-offs-attribution/ [dostęp: 22 VIII 2024].

[15] S.J. Roberts, R. Brown, *Intelligence-Driven Incident Response*…, s. 24–25.

[16] Na temat taksonomii, ontologii, standardów wymiany danych (STIX) w CTI zob. V. Mavroeidis, S. Bromander, *Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence*, https://arxiv.org/pdf/2103.03530 [dostęp: 24 VIII 2024] – preprint z referatu wygłoszonego w 2017 r. podczas European Intelligence and Security Informatic Conference; *Introduction to STIX*, https://oasis-open.github.io/cti-documentation/stix/intro.html [dostęp: 24 VIII 2024].

[17] E.M. Hutchins, M.J. Cloppert, R.M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [dostęp: 24 VIII 2024].

4) eksploitacja (*exploitation*),
5) instalacja (*installation*),
6) dowodzenie i kontrola (*command & control*, C2),
7) działanie (*actions on objectives*).

Z perspektywy defensywnej przerwanie ataku na dowolnym etapie, najlepiej jak najwcześniejszym, skutkuje jego udaremnieniem. Model ten wspiera między innymi wyabstrahowanie TTPs atakującego i ułatwia zrozumienie podejmowanych przez niego akcji[18].

Kolejnym narzędziem analitycznym jest model MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)[19], stanowiący bazę wiedzy obejmującą obecnie ponad 200 unikalnych technik i ponad 400 podtechnik (*sub-techniques*) stosowanych przez atakujących, skategoryzowanych w ramach 14 taktyk. Ujęcie tych technik w modelu wynika z obserwacji włamań, które się zdarzyły, dlatego też model ten stale się rozszerza. ATT&CK pozwala na modelowanie działań konkretnego atakującego, np. grupy APT, przez pryzmat technik wykorzystanych we wcześniej przeprowadzonych kampaniach. Na przykład grupa APT29[20], związana ze Służbą Wywiadu Zagranicznego Federacji Rosyjskiej, wykorzystała w ramach kampanii hakerskiej skierowanej przeciwko amerykańskiemu dostawcy usług IT – SolarWinds[21] ponad 40 technik. Wśród nich jako przykład można wymienić technikę pozyskania infrastruktury (technika), tj. domen internetowych (podtechnika)[22] niezbędnych do ustanowienia mechanizmu kontroli i dowodzenia (C2). Defensywne zastosowanie MITRE ATT&CK polega m.in. na wdrożeniu rozwiązań technicznych mitygujących lub wykrywających użycie konkretnej techniki, o której wiadomo, że jest wykorzystywana przez atakującego, interesującego się lub mogącego się interesować chronioną organizacją lub sektorem[23].

---

[18] S.J. Roberts, R. Brown, *Intelligence-Driven Incident Response*…, s. 35–36. Model Cyber Kill Chain doczekał się wielu rozszerzeń, np. w postaci modelu Unified Kill Chain. Zob. szerzej: P. Pols, *The Unified Kill Chain. Raising resilience against advanced cyber-attacks*, https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf [dostęp: 24 VIII 2024].

[19] Zob. *ATT&CK Matrix for Enterprise*, Attack. Mitre, https://attack.mitre.org/ [dostęp: 24 VIII 2024].

[20] *APT29*, Attack. Mitre, https://attack.mitre.org/groups/G0016/ [dostęp: 24 VIII 2024].

[21] *SolarWinds Compromise*, Attack. Mitre, https://attack.mitre.org/campaigns/C0024/ [dostęp: 24 VIII 2024].

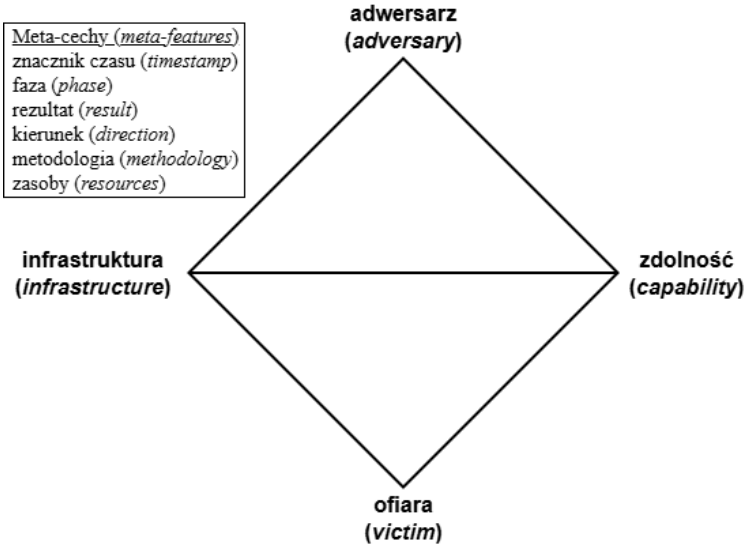
[22] *Acquire Infrastructure: Domains*, Attack. Mitre, https://attack.mitre.org/techniques/T1583/001/ [dostęp: 24 VIII 2024].

[23] Wiele technik ma przyporządkowane metody ich detekcji i mitygacji wraz z identyfikatorem.

Model diamentu (rysunek 1), opisany przez Sergia Caltagirone'a i innych w artykule *The Diamond Model of Intrusion Analysis*, opiera swoją strukturę na czterech współzależnych elementach. Są to: adwersarz (*adversary*), ofiara (*victim*), infrastruktura (*infrastructure*) oraz zdolności (*capabilities*). Jak wskazują autorzy tej publikacji, *adwersarz* wykorzystuje swoje *zdolności* przez określoną *infrastrukturę* przeciwko *ofierze*[24]. Zakłada się, że adwersarz to podmiot, np. jednostka lub organizacja, świadomy swoich celów i środków koniecznych do ich realizacji, mający określone zamiary (intencje), wymagające podjęcia próby włamania do sieci komputerowej czy systemu. Po stronie atakującego odróżnia się operatora (zleceniobiorcę, „hakera") od klienta (zleceniodawcy), który czerpie ostateczną korzyść z działania. Zdolności dotyczą narzędzi i technik użytych w konkretnym akcie włamania (zdarzeniu), np. złośliwego oprogramowania. Element infrastrukturalny to fizyczne bądź logiczne zasoby, którymi atakujący posługuje się w celu dostarczenia i utrzymania zdolności oraz uzyskania efektów ich działania. Są to np. wykorzystane adresy e-mail, konta w mediach społecznościowych, serwery C2, podrzucone pamięci USB. Ofiara, będąca przedmiotem oddziaływania danej zdolności, może być osobą, organizacją (*victim persona*) albo powiązanym z nimi zasobem (*victim asset*), np. siecią, urządzeniem lub witryną internetową. Istotnym pojęciem organizującym analizę w modelu jest zdarzenie (*diamond event*). Zgodnie z aksjomatem modelu dla każdego zdarzenia związanego z atakiem (*intrusion*) istnieje adwersarz podejmujący krok w kierunku realizacji zamierzonego celu przez użycie zdolności. Zdarzenia mają charakter autonomiczny (pojedynczy, niepodzielny krok) i składają się na uporządkowane w czasie wątki aktywności (*activity thread*), czyli ciąg logicznie powiązanych działań adwersarza. Kumulacja informacji z analizowanych zdarzeń pozwala poszerzyć wiedzę o węzłach diamentu, a przemieszczanie się wzdłuż jego krawędzi (*pivoting*) eksponuje relacje zachodzące między nimi. Budowanie dogłębnego obrazu działania adwersarza obejmuje także takie metacechy (*meta-features*), jak: znacznik czasu (*timestamp*), rezultat (*result*), metodologia (*methodology*) i inne[25].

[24] S. Caltagirone, A. Pendergast, Ch. Betz, *The Diamond Model of Intrusion Analysis*, https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf, s. 7 [dostęp: 24 VIII 2024].

[25] Tamże, s. 7–13; S.J. Roberts, R. Brown, *Intelligence-Driven Incident Response*…, s. 49–50.



Rysunek 1. Wizualizacja modelu diamentu.

Źródło: opracowanie własne na podstawie: S. Caltagirone, A. Pendergast, Ch. Betz, *The Diamond Model of Intrusion Analysis*, Active Response, https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf, s. 9 [dostęp: 24 VIII 2024].

Wykorzystanie zaprezentowanych modeli analitycznych zostało ograniczone do trzech najpopularniejszych, jednak wystarczających do wskazania potencjału analitycznego wynikającego z ich zastosowania w badaniu intencjonalnych cyberzagrożeń. Modele te uzupełniają się, co pozwala na uporządkowanie procesu analitycznego, w tym na zidentyfikowanie obszarów o wysokim stopniu pewności i użyteczności lub stanowiących luki informacyjne (*intelligence gaps*)[26].

Organizacje o podobnym profilu zagrożeń lub mierzące się z potencjalnie tym samym przeciwnikiem mają motywację do łączenia wysiłków w obszarze *threat intelligence*[27]. Współpraca ta nierzadko ma charakter zinstytucjonalizowany, np. w ramach centrów wymiany i analizy informacji (*information sharing and analysis center*, ISAC)[28]. Praktyką w tym obszarze jest automatyzacja wymiany

[26] Na temat porównania omawianych modeli zob. F.M. Ferazza, *Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model: a comparison of cyber intrusion analysis models*, https://www.royalholloway.ac.uk/media/20188/techreport-2022-5.pdf.pdf [dostęp: 25 VIII 2024].

[27] Na temat wymiany informacji w obszarze CTI zob. T.D. Wagner i in., *Cyber Threat Intelligence Sharing: Survey and Research Directions*, https://www.open-access.bcu.ac.uk/7852/1/Cyber%20Threat%20Intelligence%20Sharing%20Survey%20and%20Research%20Directions.pdf [dostęp: 24 VIII 2024].

[28] Zob. *Information Sharing and Analysis Centres (ISACs). Cooperative models*, ENISA, 2017 r.,

informacji, zwłaszcza na poziomie taktycznym i operacyjnym, przez wykorzystanie platform TI (*threat intelligence platform*), np. otwartoźródłowej platformy MISP Threat Sharing (Malware Information Sharing Platform)[29] lub OpenCTI[30].

Definiowanie operacji informacyjnych i operacji wpływu

Skonfrontowania wymaga relacja między cyberbezpieczeństwem a operacjami informacyjnymi oraz operacjami wpływu, a także to, na ile rozłącznymi znaczeniowo są te dwa typy działań. Według *Oxford English Dictionary* termin „*operation*" wywodzi się z języka francuskiego i z łaciny. Źródła jego współczesnego rozumienia pojawiły się w XVIII w., wówczas to zaczęto go wykorzystywać m.in. w matematyce i wojskowości[31]. Za *Cambridge Dictionary* można przyjąć, że w znaczeniu ogólnym termin „operacja" oznacza 'aktywność, która jest zaplanowana do osiągnięcia czegoś'[32]. Podobne ujęcie występuje w *Słowniku języka polskiego PWN* (m.in.: 'działania zmierzające do wykonania określonego zadania')[33]. Na potrzeby artykułu autorzy przyjmują, że operacja oznacza zespół celowych czynności, w zależności od branży i dziedziny, zmierzających do realizacji różnych celów.

W dorobku teoretycznym armii amerykańskiej termin „operacje informacyjne" (*information operations*, InfoOps) funkcjonuje od 1996 r., kiedy działania z tego zakresu zostały ujęte w doktrynie C2W (*Joint Doctrine for Command and Control Warfare*)[34]. Terminem „walka w obszarze kontroli i dowodzenia" (*command and control warfare*, C2W) określano walkę informacyjną (tj. działania podejmowane w celu osiągnięcia przewagi informacyjnej) prowadzoną w ramach operacji wojskowych. W ówczesnej amerykańskiej doktrynie C2W obejmowało to zintegrowane użycie operacji psychologicznych (*psychological operations*, PSYOPS), maskowania operacyjnego (*military deception*), bezpieczeństwa operacji (*operations security*,

https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/@@download/fullReport, s. 7–8 [dostęp: 24 VIII 2024].

[29] *MISP. Threat Sharing*, https://www.misp-project.org/ [dostęp: 24 VIII 2024].

[30] *OpenCTI*, https://filigran.io/solutions/open-cti/ [dostęp: 24 VIII 2024].

[31] *Oxford English Dictionary*, https://www.oed.com/dictionary/operation_n?tab=factsheet&tl=true#33665121 [dostęp: 28 XII 2023].

[32] *Cambridge Dictionary*, https://dictionary.cambridge.org/dictionary/english/operation [dostęp: 28 XII 2023].

[33] *Słownik* języka *polskiego PWN*, https://sjp.pwn.pl/szukaj/operacja.html [dostęp: 3 VII 2024].

[34] I.R. Porche i in., *Redefining Information Warfare Boundaries for an Army in Wireless World*, https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf, s. 103 [dostęp: 28 XII 2023].

OPSEC), walki elektronicznej (*electronic warfare*) oraz działań kinetycznych (*physical destruction*), wspieranych przez informacje wywiadowcze (*intelligence*) w celu utrudnienia przeciwnikowi dostępu do informacji, degradowania lub niszczenia jego zdolności dowodzenia bądź wpływania na nie i jednocześnie obrony przed takimi działaniami[35]. W podręczniku polowym (*field manual*) FM 100-6, opublikowanym w 1996 r. przez amerykańską armię, stwierdzono, że w ramach operacji informacyjnych są integrowane wszystkie aspekty informacji, aby w pełni wykorzystać ich potencjał w prowadzeniu operacji wojskowych. Wskazano ponadto, że w erze informacji (*information age*) dowódca funkcjonuje w coraz bardziej złożonym środowisku informacyjnym (*information enviroment*), które obejmuje kwestie zarówno wojskowe (*military information enviroment*), jak i pozamilitarne (*global information environment*). Środowisko to tworzą m.in. rządy innych państw, liderzy polityczni, media, organizacje międzynarodowe, a nawet osoby prywatne. Warto podkreślić, że już wówczas zakres aktywności objętych operacjami informacyjnymi był szeroki – miały one zarówno techno-, jak i antropocentryczny charakter[36]. Pod wpływem kolejnych zmian wprowadzanych w doktrynie armii amerykańskiej termin „operacje informacyjne" zaczęto utożsamiać z wcześniej opisanymi działaniami C2W. Działania te poszerzano o inne typy aktywności, m.in. o operacje w sieciach komputerowych (takie zmiany nastąpiły w dokumencie FM 3-13). W następnych dokumentach doktrynalnych (JP 3-13) pojawia się pojęcie komunikacji strategicznej (*strategic communication*), obejmujące zarówno operacje informacyjne, jak i działania na poziomie komunikacji publicznej (*public affairs*) oraz wsparcia wojskowego dla dyplomacji publicznej (*defence support for public diplomacy*)[37].

W dokumencie doktrynalnym *NATO Allied Joint Publication-10.1* (*Allied Joint Doctrine for Information Operations*) stwierdza się, że operacje informacyjne to działania, które można wykorzystywać zarówno w czasie pokoju, jak i kryzysu i konfliktu, mające na celu zapewnić wszechstronne zrozumienie środowiska informacyjnego, zwłaszcza odbiorców, i dać możliwość planowania konkretnych

[35] *Joint Doctrine for Command and Control Warfare (C2W)*, https://apps.dtic.mil/sti/pdfs/ADA357635.pdf, s. 14–15 [dostęp: 28 XII 2023].

[36] Headquaters Departament of the Army, *FM 100-6, Information Operations*, Washington 1996, https://www.hsdl.org/?view&did=437397, s. 5–12 [dostęp: 28 XII 2023]. Należy podkreślić, że w ujęciu doktrynalnym operacje informacyjne mogą być prowadzone w trzech wymiarach środowiska informacyjnego: kognitywnym (związanym z człowiekiem), informacyjnym (związanym z danymi) oraz fizycznym (związanym ze sferą materialną, realną). Zob. *Information Operations. Joint Publication 3-13*, https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf, s. 7–8 [dostęp: 30 I 2023].

[37] Na temat zmian w doktrynach zob. szerzej: I.R. Porche i in., *Redefining Information Warfare Boundaries…*, s. 103–112.

aktywności, aby uzyskać efekt kognitywny oraz wsparcie w innych obszarach działań[38]. W szczegółach doktryny wskazuje się m.in. na rolę wpływu (*influence*) na odbiorcę przez działanie oparte na wspólnych dla NATO narracjach (*narrative-led execution*)[39].

Zarówno w przypadku doktryny NATO, jak i wcześniej przywołanych dokumentów amerykańskiej armii nie pojawia się pojęcie operacji wpływu, chociaż wpływ na audytoria, proces decyzyjny, morale żołnierzy i sztaby dowodzenia przeciwnika jest wpisany w ich istotę. Próby stworzenia definicji tego pojęcia na potrzeby doktrynalne pojawiają się w opracowaniach eksperckich, jednak najczęściej uwypukla się w nich złożoność działań i ich strategiczny poziom, a więc cechy charakterystyczne dla aktywności z zakresu komunikacji strategicznej[40].

---

[38] Dosłowna definicja: „Information operations (InfoOps) is applicable in peace, crisis and conflict throughout the continuum of competition. It provides a comprehensive understanding of the information environment and, in particular audiences, the ability to plan specific activities for cognitive effect and provides support to planning of all activities in the engagement space, which are then assessed to enable refinement of plans to meet objectives". Zob. *Allied Joint Doctrine for Information Operations (AJP-10.1)*, UK Ministry of Defence, https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations-ajp-101, s. 11 [dostęp: 28 XII 2023].

[39] Tamże, s. 12.

[40] Zob. E.V. Larson i in., *Foundations of Effective Influence Operations. A Framework for Enhancing Army Capabilites*, Rand Corporation, 2009 r., https://www.rand.org/pubs/monographs/MG654, s. 2–6 [dostęp: 18 XI 2024]. Rozumienie operacji wpływu jako zaplanowanej, ukierunkowanej na osiągnięcie wyznaczonych celów, wykorzystującej szerokie zasoby i instrumenty państwa (w ramach polityki zagranicznej, wojska, wywiadu, mediów) oraz skoordynowanej przez najwyższe szczeble administracji państwa może być zasadne, jednak z perspektywy artykułu nie stanowi zmiany jakościowej do aktywności podejmowanych w ramach komunikacji strategicznej. W nomenklaturze NATO *strategic communication* oznacza przede wszystkim koordynowanie oraz odpowiednie wykorzystanie działań komunikacyjnych i zdolności w celu wsparcia polityki, operacji oraz aktywności Sojuszu. Działania StratCom obejmują: dyplomację publiczną, działania z zakresu cywilnego i wojskowego *public affairs*, operacje informacyjne (w tym operacje psychologiczne). Zob. *About Strategic Communications*, NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/about_us/about-strategic-communications/1 [dostęp: 10 VII 2024]. Podstawy doktrynalne StratCom w ramach NATO są rozwijane od 2009 r. Na ten temat zob. szerzej: D. Niedzielski, *Wojskowa doktryna komunikacji strategicznej NATO i jej znaczenie dla Polski*, „Akademickie Centrum Komunikacji Strategicznej" 2022, nr 3, https://www.wojsko-polskie.pl/aszwoj/u/af/14/af143adc-70e6-463a-8448-faaf0df61e9a/biuletyn_nr_3.pdf, s. 46–53 [dostęp: 10 VII 2024]. Podobne, tj. uwypuklające znaczenie koordynacji działań komunikacyjnych, rozumienie tego aspektu jest spotykane w pozamilitarnej części systemu bezpieczeństwa państwa. Świadczy o tym choćby postulat sformułowany w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (dalej: SBN) z 2020 r., wskazujący na konieczność stworzenia jednolitego systemu komunikacji strategicznej kraju w kontekście zapewnienia bezpiecznego funkcjonowania państwa i obywateli w przestrzeni informacyjnej. Zob. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, s. 21 [dostęp: 10 VII 2024]. W SBN z 2020 r. „przestrzeń informacyjna" jest definiowana jako „przenikające się warstwy przestrzeni: wirtualnej

W opinii autorów niniejszego artykułu uzasadnieniem dla wyróżnienia operacji wpływu jako odrębnego typu zaplanowanej aktywności są przede wszystkim ich specyficzne środki realizacji, czyli agentura wpływu (*agents of influence*). Termin ten występuje w glosariuszu definicji i terminów z zakresu wywiadu opublikowanym przez Centralną Agencję Wywiadowczą (Central Intelligence Agency, CIA) i określa osobę zmanipulowaną przez organizację wywiadowczą po to, aby wykorzystać jej pozycję do wpływania na opinię publiczną lub proces decyzyjny w sposób sprzyjający celowi kraju, na którego rzecz działa organizacja[41]. Termin „agent wpływu" występuje również w słowniku terminów opublikowanym w 2011 r. przez jedną z instytucji zajmujących się m.in. kontrwywiadem w resorcie obrony w Stanach Zjednoczonych (Defense Counterintelligence and Human Intelligence funkcjonująca w ramach Defence Intelligence Agency). W tej publikacji także przyjmuje się, że jest to osoba wykorzystująca swoją pozycję do wpływania na opinię publiczną lub podejmowanie decyzji służących uzyskaniu korzyści przez kraj, z którym jest związana służba, na której rzecz działa agent. Wskazano przy tym, że pojęcie pochodzi z terminologii stworzonej przez Sowietów[42]. Podobnie termin ten został zdefiniowany w *Wielkim leksykonie służb specjalnych świata* autorstwa Jana Lareckiego. Tam również podkreśla się świadomą współpracę danej osoby z obcym wywiadem w celu wykorzystania swojej pozycji politycznej, społecznej lub zawodowej do promowania celów innego państwa, wpływania na proces decyzyjny, sytuację gospodarczą itd. Larecki zwraca przy tym uwagę na strategiczny i długofalowy charakter operacji wpływu, ich wysoki stopień utajnienia, a także szczególnie wartościowy charakter agentury wpływu oraz jej odmienność względem „klasycznej" agentury (gromadzącej informacje)[43].

(warstwa systemów, oprogramowania i aplikacji), fizycznej (infrastruktury i sprzętu) i poznawczej (kognitywnej)". Sfera poznawcza przestrzeni informacyjnej jest zatem zasadniczym elementem poszerzającym ją przedmiotowo w porównaniu z pojęciem cyberprzestrzeni (zob. przyp. 4). Należy jednocześnie zwrócić uwagę, że optyka przestrzeni informacyjnej przyjęta w SBN z 2020 r. wpisuje się w postrzeganie wymiarów środowiska informacyjnego na gruncie doktryn NATO. Zob. szerzej: Z. Modrzejewski, *Information operations from the Polish point of view*, „Obrana a strategie" (Defence and Strategy) 2018, nr 1, s. 118–119. https://doi.org/10.3849/1802-7199.18.2018.01.113-130.

41 *Glossary of Intelligence Terms and Definitions*, https://www.cia.gov/readingroom/docs/CIA-RDP-80M00596A000500020003-7.pdf, s. 1 [dostęp: 28 XII 2023].

42 *Terms & Definitions of Interest for DoD Counterintelligence Professionals*, https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf, s. 4 [dostęp: 28 XII 2023].

43 J. Larecki, *Wielki leksykon służb specjalnych świata*, Warszawa 2007, s. 30–31. Mirosław Minkina działania, które swoim zakresem i celami są tożsame z operacjami wpływu, określa terminami: „tajne operacje" i „operacje pozainformacyjne". Podkreśla w ten sposób ich odrębność w stosunku do „klasycznej" działalności wywiadowczej ukierunkowanej na gromadzenie informacji. W tym ujęciu operacjami informacyjnymi/operacjami wpływu są: tajne wspieranie zaprzyjaźnionego państwa, wpływanie na postrzeganie i ocenę przez państwa zainteresowania wywiadowczego, wpływanie na postrzeganie i ocenę przez społeczeństwo państwa zainteresowania wywiadowczego, wspieranie zaprzyjaźnionych

Operacjami wpływu będą więc działania wywiadowcze prowadzone przy wykorzystaniu zasobów wywiadu agenturalnego w celu oddziaływania na inne państwo, np. w sferze polityki zagranicznej i bezpieczeństwa, prowadzenia aktywności społeczno-politycznej skutkującej destabilizacją państwa, finansowania ze źródeł zagranicznych działań z zakresu korupcji politycznej czy prowadzenia nielegalnego lobbingu gospodarczego. Należy podkreślić, że zakres i środki realizacji operacji wpływu stale się poszerzają. Według Federalnego Biura Śledczego (Federal Bureau of Investigation, FBI) do tego typu aktywności aktualnie należy zaliczyć również działania w cyberprzestrzeni. W odniesieniu do tej przestrzeni amerykański kontrwywiad wskazuje przede wszystkim ataki na cele związane z procesem wyborczym, tj. na infrastrukturę do głosowania, kandydatów w wyborach[44]. Postrzeganie cyberprzestrzeni jako obszaru, w którym są realizowane operacje wpływu, to szerszy trend. Kolejnym przykładem przyjmowania takiej perspektywy jest amerykańska agencja właściwa ds. cyberbezpieczeństwa oraz koordynacji działań na rzecz ochrony infrastruktury krytycznej – Cybersecurity & Infrastructure Security Agency (CISA). Agencja ta określa przy tym szeroki wachlarz źródeł generujących zagrożenia, przyjmując, że są to podmioty o wrogich intencjach (*malicious actors*), a same operacje wpływu polegają m.in. na technikach manipulacji informacją (*misinformation, disinformation, malinformation*)[45], za których pomocą aktorzy zagraniczni osiągają własne cele[46].

Z perspektywy nomenklatury stosowanej w sektorze siłowym (wojsko, służby specjalne) operacje informacyjne oraz operacje wpływu są zatem różnymi typami aktywności, chociaż w pewnym zakresie zbliżonymi do siebie. Operacje wpływu ze

ruchów politycznych, a także wpływanie na wydarzenia z wykorzystaniem przemocy. Zob. szerzej: M. Minkina, *Sztuka wywiadu w państwie współczesnym*, Warszawa 2014, s. 227–245.

[44] *Combating Foreign Influence*, FBI, https://www.fbi.gov/investigate/counterintelligence/foreign-influence [dostęp: 2 XI 2024].

[45] Część ekspertów zajmujących się zagrożeniami w przestrzeni informacyjnej stosuje podział na dezinformację oraz pojęcia pokrewne – ale niejednoznaczne – *malinformation* oraz *misinformation*. Pojęcie *disinformation* jest związane ze świadomym i intencjonalnym rozpowszechnianiem fałszywych informacji, mającym na celu spowodowanie szkody. Przyjmuje się, że *misinformation* oznacza rozpowszechnianie fałszywych informacji, ale bez zamiaru wyrządzenia szkody, a *malinformation* – wykorzystanie prawdziwych informacji w celu wyrządzenia szkody. Na ten temat zob. szerzej: C. Wardle, H. Derakhshan, *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe report DGI(2017)09, https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html, s. 20–22 [dostęp: 10 VII 2024].

[46] *Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure*, https://www.cisa.gov/sites/default/files/2023-01/cisa_insight_mitigating_foreign_influence_508.pdf, s. 1 [dostęp: 29 XII 2023].

względu na dostęp do niejawnych (utajonych) środków realizacji są charakterystyczne dla działalności służb wywiadowczych i ich najważniejszym celem jest wsparcie szeroko rozumianej polityki państwa (głównie zagranicznej i bezpieczeństwa). W takim ujęciu definiują je specyficzne, charakterystyczne dla działalności wywiadowczej, atrybuty, m.in.: instytucje przykrycia, metody werbunku i prowadzenia agentury wpływu oraz kanały łączności wykorzystywane do jej finansowania i zadaniowania[47]. Operacje wpływu w cyberprzestrzeni (w dyskursie eksperckim jest używany termin „*cyber influence operation*"[48]) mogą natomiast obejmować np. operacje typu *hack and leak*. Operacje te polegają na uzyskaniu informacji drogą nielegalną (np. przez działania hakerskie), a następnie ich wykorzystaniu w przestrzeni informacyjnej do osiągnięcia określonych celów, np. destabilizacji systemu politycznego przez kompromitację danego polityka, jak to się zdarzyło w Stanach Zjednoczonych w 2016 r., w czasie kampanii do wyborów prezydenckich[49]. W ujęciu doktrynalnym NATO operacje informacyjne obejmują wiele różnych działań, które poza aktywnością informacyjną oraz komunikacyjną ukierunkowaną na osiągnięcie celów kognitywnych[50]

---

[47] Obszerny opis współczesnej operacji wpływu realizowanej przez rosyjską służbę specjalną FSB ukierunkowanej na destabilizację, rozbicie, a następnie przejęcie władzy w Ukrainie w 2022 r. z wykorzystaniem agentury wpływu znajduje się w opracowaniu opublikowanym przez brytyjski ośrodek ekspercki Royal United Services Institute. Zob. J. Watling, O. Danyluk, N. Reynolds, *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023*, https://static.rusi.org/202303-SR-Unconventional-Operations-Russo-Ukrainian-War-web-final.pdf.pdf [dostęp: 10 VII 2024]. W polskim piśmiennictwie pogłębioną analizę tej operacji przeprowadził Marek Świerczek. Zob. M. Świerczek, *Metody działania rosyjskich służb specjalnych w świetle afery Olega Kulinicza*, „Przegląd Bezpieczeństwa Wewnętrznego" 2023, nr 29, s. 63–93. https://doi.org/10.4467/20801335PBW.23.020.18762. Należy podkreślić, że nomenklatura dotycząca operacji wpływu nie jest jednolita również w zachodniej społeczności wywiadowczej i stale się poszerza. W 2024 r. Narodowa Rada Wywiadu Stanów Zjednoczonych opublikowała kilkustronicowy glosariusz terminów dotyczących działań w tzw. szarej strefie. Swoim zakresem obejmuje on m.in. operacje wpływu oraz inne, zbliżone definicyjnie, pojęcia, takie jak np.: tajna operacja (*covert operation*), wpływ zagraniczny (*foreign influence*), walka niekonwencjonalna (*unconventional warfare*). Zob. *Updated IC Gray Zone Lexicon: Key Terms and Definitions*, https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Updated-IC-Gray-Zone-Lexicon-July2024.pdf [dostęp: 11 VIII 2024].

[48] P. Brangetto, M.A. Veenendaal, *Influence Cyber Operations: The Use of Cyberattacks in Support of Cyberaatacks in Support of Influence Operations*, w: *8th International Conference on Cyber Conflict. Proceedings 2016*, N. Pissanidis i in. (red. nauk.), https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf, s. 113–126 [dostęp: 10 VII 2024]; *Cyber Influence Operations*, https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-cyber-influence-operations [dostęp: 10 VII 2024].

[49] J. Shires, *Hack-and-leak operations and U.S. cyber policy*, War on the Rocks, 14 VIII 2020 r., https://warontherocks.com/2020/08/the-simulation-of-scandal/ [dostęp: 10 VII 2024].

[50] Więcej na temat działań komunikacyjnych w dalszej części artykułu. Należy wspomnieć, że rozróżnienie operacji informacyjnych oraz operacji psychologicznych zostało zaadaptowane również

mogą także integrować działania związane m.in. z: ochroną własnego środowiska informacyjnego (OPSEC) i maskowaniem operacyjnym, operacjami w cyberprzestrzeni (*cyberspace operations*), a nawet walką elektroniczną[51]. Wszystkie te typy działań stanowią odrębne, bardzo złożone i wielowymiarowe aktywności. Jeśli cyberprzestrzeń występuje w ramach operacji informacyjnych, to jest jedną z wielu możliwych przestrzeni ich realizacji[52].

Istotna w zrozumieniu możliwości adaptacji dorobku dziedziny wiedzy związanej z cyberbezpieczeństwem na potrzeby rozpoznawania dezinformacji jest również optyka branży platform cyfrowych, a przede wszystkim mediów społecznościowych. Są to środowiska mocno eksploatowane w operacjach informacyjnych i operacjach wpływu prowadzonych w cyberprzestrzeni. Według firmy Meta (dawniej Facebook) operacje wpływu to (…) *skoordynowane wysiłki podejmowane w celu manipulowania debatą publiczną lub jej zakłócenia, ukierunkowane na osiągnięcie założeń strategicznych*[53]. W nomenklaturze firmy operacje wpływu wiążą się z łamaniem jej wewnętrznej polityki bezpieczeństwa dotyczącej zapobiegania skoordynowanym nieautentycznym zachowaniom (*coordinated inauthentic behavior*, CIB) na platformie. W latach 2017–2020 firma rozpoznała 150 takich operacji[54]. Warto podkreślić, że Meta prowadzi w serwisie społecznościowym GitHub publiczne repozytorium, w którym znajdują się m.in. TTPs rozpoznawane w ramach wykrywania CIB, a także informacje bardziej szczegółowe, np. nazwy propagowanych domen, które – podobnie jak w cyberbezpieczeństwie – określono pojęciem wskaźnika kompromitacji. Meta deklaruje wykorzystywanie w tym celu ogólnej metody analizy danych opartej na modelu Kill Chain[55]. Należy zauważyć, że poszczególne platformy prowadzą różne polityki

w rosyjskiej teorii walki informacyjnej. Warto jednak zauważyć, że jednocześnie w rosyjskiej nomenklaturze występuje kategoria operacji kombinowanych, określanych pojęciem operacji informacyjno-psychologicznych. Na ten temat zob. szerzej: M. Wojnowski, *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 15–17.

[51] *Allied Joint Doctrine for Information Operations (AJP-10.1)*…, s. 32–37 [dostęp: 17 XI 2024].

[52] Środowisko informacyjne w tym ujęciu dzieli się na trzy wymiary: wirtualny, fizyczny oraz kognitywny. Zob. tamże, s. 16–17.

[53] *Threat Report. The State of Influence Operations 2017–2020*, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf, s. 3 [dostęp: 10 VII 2024].

[54] *Threat Report: Combating Influence Operations*, Meta, 26 V 2021 r., https://about.fb.com/news/2021/05/influence-operations-threat-report/ [dostęp: 11 VIII 2024].

[55] *Facebook. Threat research*, GitHub, https://github.com/facebook/threat-research [dostęp: 11 VIII 2024]. Przykład raportu: *Facebook. Threat Research. Indicators. CSV. Q4_2023*, GitHub, https://github.com/facebook/threat-research/blob/main/indicators/csv/Q4_2023/Q4_2023_China_based_CIB_network.csv. Szerzej na temat adaptacji metodyki analizy cyberbezpieczeństwa

w zakresie wymiany wiedzy na temat wykrywanych operacji informacyjnych i operacji wpływu oraz przeciwdziałania takim zjawiskom. Kilka lat temu aktywny pod tym względem był również portal społecznościowy Twitter (aktualnie X), który udostępniał badaczom duże zbiory danych dotyczące profili rozpoznanych jako zaangażowane w nieautentyczne i skoordynowane kampanie informacyjne realizowane na tej platformie (określano je terminem „*inauthentic influence campaigns*")[56]. Aktualnie platforma nie prowadzi tak rozbudowanych działań w tym zakresie. Analiza operacji wpływu w cyberprzestrzeni coraz powszechniej wpisuje się w praktykę globalnych firm branży IT i cyberbezpieczeństwa, nie tylko platform społecznościowych. Jako przykład można podać politykę firmy Microsoft. W niektórych z corocznie publikowanych sprawozdań dotyczących zagrożeń cyfrowych poświęciła ona operacjom wpływu odrębny rozdział i wykorzystała do ich opisu zaadaptowane na te potrzeby elementy terminologii z zakresu cyberbezpieczeństwa (np. termin „*advanced persistent manipulators*" nawiązujący do *advanced persistent threat*)[57]. Dorobek teoretyczny firm i platform cyfrowych nie jest tak rozbudowany i pogłębiony jak dorobek państwowych podmiotów sektora bezpieczeństwa narodowego, ponieważ sens znaczeniowy tych definicji wynika z innej praktyki oraz potrzeb tej branży.

Pomimo wskazanych uwag dotyczących rozróżniania operacji informacyjnych i operacji wpływu w dalszej części artykułu autorzy będą posługiwać się tymi terminami zamiennie, ponieważ takiego rozróżnienia nie stosuje się również w literaturze przedmiotu omawianej w dalszej części artykułu. W ramach podsumowania należy jednak podkreślić, że cyberprzestrzeń stanowi tylko jeden z segmentów środowiska informacyjnego, w których tego typu złożone działania są prowadzone.

---

na potrzeby operacji informacyjnych i operacji wpływu w cyberprzestrzeni w dalszej części niniejszego artykułu.

[56] Więcej na ten temat w archiwalnej wersji strony serwisu społecznościowego Twitter. Zob. *Information Operations*, http://web.archive.org/web/20201226185947/https://transparency.twitter.com/en/reports/information-operations.html [dostęp: 11 VIII 2024].

[57] *Microsoft Digital Defence Report 2022*, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/microsoft-digital-defense-report-2022.pdf?culture=en-us&country=us, s. 72 [dostęp: 11 VIII 2024].

Metody analizy operacji informacyjnych/operacji wpływu ze względu na elementy procesu komunikacyjnego

Cechą wspólną operacji informacyjnych/operacji wpływu jest to, że na pewnym etapie ich realizacji mogą one obejmować działania komunikacyjne ukierunkowane na zmianę lub utrwalenie zachowań i postaw określonych osób lub grup społecznych (politycznych, zawodowych, religijnych). W doktrynie operacji informacyjnych NATO tego typu cele są realizowane m.in. przez operacje psychologiczne definiowane jako (…) *zaplanowane działania psychologiczne z wykorzystaniem metod komunikacji i innych środków, wymierzone w określonych odbiorców, aby wpłynąć na ich postrzeganie, postawy i zachowania i w ten sposób osiągnąć cele polityczne i wojskowe*[58]. W przypadku operacji wpływu oddziaływanie na postawy i zachowania odbiorców może mieć różną formę, m.in. postać dezinformacji będącej elementem działalności wywiadowczej obcego państwa. W Polsce taka aktywność została spenalizowana i szczegółowo zdefiniowana w znowelizowanym w 2023 r. Kodeksie karnym. W definicji prawnej pojęcia dezinformacji ustawodawca zawarł nie tylko warunek powiązania osoby zaangażowanej w proces dezinformacji z obcym wywiadem, lecz także wymiar jakościowy tych działań (próba wywołania poważnych szkód dla RP, państwa sojuszniczego lub organizacji międzynarodowej) oraz sprecyzował sposób ich realizacji – jest to rozpowszechnianie konkretnego rodzaju informacji (nieprawdziwych lub wprowadzających w błąd)[59].

---

[58] W oryginale: „planned psychological activities using methods of communications and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives". Zob. *Allied Joint Doctrine for Psychological Operations (AJP-3.10.1)*, UK Ministry of Defence, https://www.gov.uk/government/publications/ajp-3101-allied-joint-doctrine-for-psychological-operations, s. 18 [dostęp: 5 VII 2024]. W cytowanym dokumencie doktrynalnym NATO dotyczącym operacji informacyjnych (AJP-10.1) działania PSYOPS są wymienione jako jedne z dwóch zdolności komunikacyjnych wykorzystywanych w ramach INFOOPS (drugim typem zdolności jest wojskowa komunikacja publiczna, *military public affairs*). Zob. *Allied Joint Doctrine for Information Operations (AJP-10.1)*…, s. 30–31. Operacja informacyjna i operacja psychologiczna są więc odrębnymi terminami, jednak wzajemnie ze sobą powiązanymi, ponieważ INFOOPS ma charakter nadrzędny wobec PSYOPS. Na temat różnic znaczeniowych oraz historii kształtowania się terminu „operacje informacyjne" zob. T. Kacała, *Tendencje rozwojowe współczesnych działań psychologicznych prowadzonych przez Siły Zbrojne RP*, w: *Innowacja i synergia w Siłach Zbrojnych RP*, t. 1, A. Lis, R. Reczkowski (red.), Bydgoszcz 2012.

[59] Art. 130 § 9 Kodeksu karnego: „Kto, biorąc udział w działalności obcego wywiadu albo działając na jego rzecz, prowadzi dezinformację, polegającą na rozpowszechnianiu nieprawdziwych lub wprowadzających w błąd informacji, mając na celu wywołanie poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest Rzeczpospolita Polska, albo skłonienie organu władzy publicznej Rzeczypospolitej Polskiej, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest Rzeczpospolita Polska, do podjęcia lub zaniechania określonych czynności, podlega karze pozbawienia wolności na czas nie krótszy od lat 8".

W literaturze przedmiotu spopularyzowanym i pojemnym znaczeniowo terminem określającym kształtowanie postaw i zachowań jest „propaganda". Spośród wielu definicji tego terminu na potrzeby artykułu przyjmuje się jej rozumienie jako masowe, metodyczne i intencjonalne rozpowszechnianie określonych treści w ramach oddziaływania na określonego odbiorcę[60]. Warto nadmienić, że propaganda może być prowadzona przy wykorzystaniu środków przekazu o różnym stopniu utajnienia. „Białą" propagandą nazywa się działania realizowane przez dobrze zidentyfikowane źródło (np. media państwowe). W przypadku „szarej" propagandy istnieje problem z identyfikacją właściwego źródła danych treści, co jednocześnie utrudnia ocenę intencji autora. „Czarną" propagandę charakteryzuje natomiast pełne utajnienie źródła przekazu oraz rozpowszechnianie fałszywych treści. Ten typ propagandy często utożsamia się z dezinformacją[61]. Propaganda może zatem obejmować część działań prowadzonych w ramach operacji psychologicznych czy dezinformacji, ale jest to pojęcie znacznie szersze. Jednocześnie jest to ugruntowany w literaturze termin odnoszący się do intencjonalnych i usystematyzowanych działań komunikacyjnych ukierunkowanych na wywarcie wpływu na postawy czy zachowania odbiorców.

Tym, co łączy zarówno operacje wpływu, operacje psychologiczne, jak i propagandę, jest to, że można je rozpatrywać jako proces komunikacyjny. Większość modeli procesu komunikacyjnego wyróżnia następujące elementy[62]:

- uczestnicy, czyli nadawcy (właściwi autorzy/źródła przekazu) i odbiorcy (adresaci, audytorium);
- komunikat (przekaz komunikacyjny), którego treść jest zawarta w znaczeniach oraz symbolach zakodowanych przez nadawcę i dekodowanych przez odbiorcę;
- kanał, czyli droga przekazu komunikacyjnego, przez którą jest on transferowany przez nadawcę do odbiorcy (np. media masowe, media społecznościowe, a także komunikacja werbalna i niewerbalna);

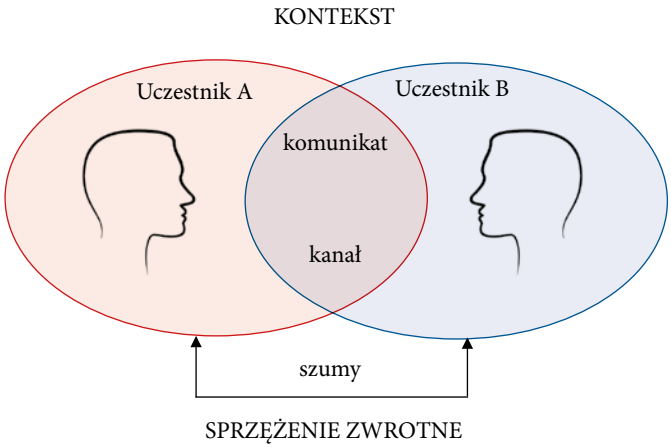
---

[60] W literaturze przedmiotu funkcjonuje wiele definicji propagandy. Edward Bernays, jeden z prekursorów badań dotyczących propagandy i public relations, uważał, że nie należy wartościować etycznie tego terminu, ponieważ ma on znaczenie czysto techniczne i oznacza „(…) konsekwentny i trwały wysiłek ukierunkowany na tworzenie lub kształtowanie wydarzeń mających wpływ na relacje społeczeństwa z przedsiębiorstwem, pomysłem lub określoną grupą". Zob. E.L. Bernays, *Propaganda*, New York 1928, s. 15. Na temat definicji propagandy zob. R. Rajczyk, *Nowoczesne wojny informacyjne*, Warszawa 2016, s. 22–24.

[61] B. Dobek-Ostrowska, J. Fras, B. Ociepka, *Teoria i praktyka propagandy*, Wrocław 1999, s. 36.

[62] B. Dobek-Ostrowska, *Podstawy komunikowania społecznego*, Wrocław 1999, s. 15. W literaturze przedmiotu istnieją również inne, bardziej złożone modele komunikacji, które uwypuklają np. role liderów opinii (model dwustopniowego przepływu komunikowania) oraz selekcjonerów informacji – tzw. gatekeeperów (topologiczny model komunikowania). Zob. szerzej: B. Dobek-Ostrowska, *Komunikowanie polityczne i publiczne*, Warszawa 2007, s. 36.

- sprzężenie zwrotne informujące o reakcji odbiorcy na przekaz komunikacyjny, dzięki czemu nadawca dowiaduje się, czy został on przyjęty i zrozumiany;
- szumy zaburzające skuteczność procesu komunikacyjnego, które mogą mieć charakter wewnętrzny (np. ograniczenia człowieka wynikające z jego predyspozycji psychologicznych czy stanu emocjonalnego), zewnętrzny (np. warunki fizyczne takie jak warunki atmosferyczne czy zakłócenia w funkcjonowaniu kanału przekazu) oraz semantyczny (np. nieodpowiedni dobór lub odbiór znaczenia bądź symbolu zawartego w komunikacie);
- kontekst, czyli warunki (społeczne, kulturowe, historyczne czy fizyczne), w jakich odbywa się proces komunikowania (rysunek 2).



Rysunek 2. Składniki procesu komunikacyjnego.

Źródło: opracowanie własne na podstawie: B. Dobek-Ostrowska, *Komunikowanie polityczne i publiczne*, Warszawa 2007, Wydawnictwo Naukowe PWN, s. 64.

Możliwość wyodrębnienia elementów procesu komunikacyjnego tworzy wspólny metodologiczny punkt wyjścia dla analizy komunikacyjnego aspektu operacji informacyjnych (psychologicznych)/operacji wpływu. W odniesieniu do powyższych składników należy przywołać badania amerykańskiego politologia i badacza propagandy Harolda Lasswella, który prowadził badania procesu komunikacyjnego ze względu na jego funkcję, a w 1948 r. stworzył model aktu perswazyjnego. Jego założenie opierało się na precyzyjnie wyodrębnionych rolach nadawcy i odbiorcy oraz na jednokierunkowym charakterze komunikacji, wykorzystywanym przez nadawcę w jasno wyznaczonym celu – spowodowania określonego skutku (efektu) u odbiorcy.

Istota komunikacji według Lasswella zamyka się w odpowiedzi na pięć pytań dotyczących opisanych wcześniej elementów procesu komunikacyjnego[63]:

1. Kto mówi? (pytanie o nadawcę przekazu).
2. Co mówi? (pytanie o treść przekazu).
3. Za pośrednictwem jakiego kanału mówi? (pytanie o kanał przekazu).
4. Do kogo mówi? (pytanie o odbiorcę przekazu).
5. Z jakim efektem mówi? (pytanie o skuteczność przekazu).

Badania Lasswella w dalszym ciągu mogą być wykorzystywane do analizy działań psychologicznych, o czym świadczy opracowanie Tomasza Kacały i Justyny Lipińskiej pt. *Komunikacja strategiczna i public affairs*, wydane przez Wojskowe Centrum Edukacji Obywatelskiej. Znajduje się w nim schemat analizy wrogiej propagandy uwzględniający pięć kategorii: źródło, treści, odbiorcy, wykorzystywane media oraz osiągnięte efekty[64]. W publikacji szczegółowo omówiono obszary zainteresowania i pytania pomocnicze dla osób badających przekaz propagandowy. Wybrane elementy przedstawiono w tabeli 1.

Tabela 1. Składniki analizy propagandy w odniesieniu do elementów procesu komunikacyjnego na podstawie opracowania Tomasza Kacały i Justyny Lipińskiej.

Element procesu komunikacyjnego (obszar zainteresowania badawczego)	**Przykładowe pytania analityczne**
Nadawca – analiza źródła	**Aktor** Kim jest osoba/grupa realizująca przekaz?
	Autorytet Kto patronuje działalności przeciwnika lub nadaje wartość jego działaniu?
	Autor Kto stworzył/opracował analizowany materiał propagandowy?
	Rozpowszechniający Kto jest odpowiedzialny za rozpowszechnianie przekazu wśród obiektów oddziaływania?
	Autentyczność i wiarygodność Czy źródło przekazu jest możliwe do zidentyfikowania? (typ źródła przekazu ze względu na stopień utajnienia „biały”, „szary”, „czarny”)

[63] B. Dobek-Ostrowska, *Komunikowanie polityczne…*, s. 32.

[64] T. Kacała, J. Lipińska, *Komunikacja strategiczna i public affairs*, Warszawa 2014, s. 155–160.

Element procesu komunikacyjnego (obszar zainteresowania badawczego)	**Przykładowe pytania analityczne**
Przekaz – analiza treści (Co przekazuje propaganda? Do czego stara się nakłonić obiekty oddziaływania?)	Cel przekazu Jakie zachowanie/postawy obiektu oddziaływania usiłuje wywołać nadawca?
	Linie perswazji Jakiej argumentacji, technik i symboliki używa w przekazie nadawca?
	Przypadkowe informacje Jakie niezamierzone informacje zawarł w przekazie nadawca?
	Nieścisłości przekazu Jakie elementy sprawiają, że przekaz jest niespójny lub błędny – również w porównaniu z poprzednimi materiałami?
Odbiorca – analiza odbiorców (Kto jest odbiorcą?)	Pozorny obiekt oddziaływania Kto na początku wydaje się odbiorcą przekazu?
	Ostateczny (docelowy) obiekt oddziaływania Kto jest docelowym, zamierzonym odbiorcą przekazu?
	Pośredni obiekt oddziaływania Kto jest pośrednim odbiorcą przekazu, czyli takim, poprzez którego nadawca usiłuje dotrzeć do ostatecznego obiektu oddziaływania?
Kanał – analiza mediów (Jakie media wykorzystano? Dlaczego właśnie te?)	Typy mediów: radio, telewizja, druk, internet Jakie występują luki informacyjne (np. częstotliwość, lokalizacja, miejsce pochodzenia, charakterystyka techniczna, metoda rozpowszechnienia)?
Sprzężenie zwrotne – analiza efektywności (Jaki skutek przynosi propaganda?)	Jakie wydarzenia, incydenty, reakcje mogą świadczyć o skuteczności oddziaływania przekazu?

Źródło: opracowanie własne na podstawie: T. Kacała, J. Lipińska, *Komunikacja strategiczna i public affairs*, Warszawa 2014, s. 155–160.

Zaletami modelu Lasswella wydają się prostota i stosunkowo wysoka dostępność źródłowa, ponieważ wymagane minimum do jego wykorzystania to treściowa warstwa operacji informacyjnej/operacji wpływu, która – przynajmniej w przypadku komunikowania masowego (np. propagandy) – z założenia jest widoczna

i powszechnie dostępna[65]. Jednocześnie należy podkreślić, że specyfika współczesnych mediów komplikuje oparcie procedury badawczej operacji informacyjnych/operacji wpływu na klarownie określonych elementach procesu komunikacyjnego. Wpływa na to interaktywność nowego typu mediów[66] (szczególnie wysoka w przypadku mediów społecznościowych), która utrudnia precyzyjne wyodrębnienie podstawowych elementów procesu komunikacyjnego (nadawca, medium, adresat), a algorytmizacja doboru treści (powodująca bańki informacyjne) dodatkowo zwiększa znaczenie kontekstu jako istotnego elementu tego procesu[67].

Metody analizy operacji informacyjnych/operacji wpływu oparte na dorobku branży cyberbezpieczeństwa

Refleksja na temat wykorzystania dorobku metodologii badań dotyczących zagrożeń w cyberprzestrzeni w badaniu operacji informacyjnych i dezinformacji jest obecna zarówno w pracach naukowych, jak i w ekspertyzach analityków oraz instytucji rządowych, międzynarodowych, pozarządowych, a także podmiotów komercyjnych branży cyberbezpieczeństwa. Tytułem wprowadzenia można przywołać artykuł trzech amerykańskich badaczy związanych z Uniwersytetem Stanowym Nowego Jorku w Albany (University at Albany, State University of New York) pt. *The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats*. Jego autorzy zwracają uwagę, że stopień, w jakim dezinformacja wpływa na poufność, integralność oraz dostępność informacji, sprawia, że konieczne jest jej postrzeganie nie tylko jako zjawiska zakłócenia informacyjnego, lecz także jako formy cyberataku[68]. W artykule porównano dezinformację z innymi kategoriami cyberzagrożeń, takimi jak socjotechnika,

[65] Do rozwiązania zadania polegającego na przeprowadzeniu analizy według pytań wskazanych w tabeli 1 Tomasz Kacała i Justyna Lipińska podają tylko jeden przykładowy tekst propagandowy z prowincji Diwanija z okresu misji stabilizacyjnej Polskiego Kontyngentu Wojskowego w Iraku w 2006 r. Zob. T. Kacała, J. Lipińska, *Komunikacja strategiczna*…, s. 159–161.

[66] Na temat interaktywności nowych mediów zob. J. van Dijk, *Społeczne aspekty nowych mediów*, Warszawa 2010, s. 18; G.S. Jowett, V. O'Donnell, *Propaganda and Persuasion. Fifth Edition*, Los Angeles–London–New Delhi–Singapore–Washington 2012, s. 366.

[67] Na temat propagandy w warunkach algorytmizacji przekazu zob. S.C. Woolley, P.N. Howard, *Introduction: Computational Propaganda Worldwide*, w: *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, S.C. Woolley, P.N. Howard (red.), Oxford 2018, s. 4. https://doi.org/10.1093/oso/9780190931407.001.0001.

[68] K.M. Caramancion i in., *The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats*, „Data" 2022, t. 7, nr 4, s. 1. https://doi.org/10.3390/data7040049.

ataki na aplikacje webowe, ataki DDoS, malware, ransomware, działania grup APT, zagrożenia typu zero-day. Porównania dokonano ze względu na aktorów zagrożeń, ich źródło (zewnętrzne lub wewnętrzne z perspektywy systemu informacyjnego), motywacje i cele adwersarzy, wektor ataku, atakowaną warstwę sieci według modelu OSI (Open System Interconnection Model), a także wpływ ataku na system i jego użytkowników oraz sposoby mitygacji związanych z nim zagrożeń. Amerykańscy badacze przekonują, że wynik ich analizy porównawczej wykazał wiele podobieństw dezinformacji do typów ataków ugruntowanych w taksonomii cyberzagrożeń. Na przykład podobieństwo dezinformacji i socjotechniki polega na bazowaniu na ludzkich słabościach (np. skłonności do nieprzemyślanych zachowań wywołanych podaniem informacji w zmanipulowanym kontekście), a w przypadku porównania z atakami ransomware i z wykorzystaniem złośliwego oprogramowania (malware) wiąże się z podobnymi skutkami – obniżoną reputacją, generowaniem strat finansowych oraz utratą zaufania ofiary ataku. Badacze wskazują również na podobieństwa do działań grup APT, które charakteryzują się długotrwałym działaniem w sieci ofiary (podobnie jak np. proces dezinformacji w mediach społecznościowych)[69]. Warto zwrócić uwagę, że według nich adwersarz prowadzący dezinformację w cyberprzestrzeni atakuje ostatnią warstwę modelu OSI, czyli warstwę aplikacji, a wektorem ataku są wyszukiwarki internetowe, reklamy internetowe (*online advertisements*) oraz platformy w mediach społecznościowych[70].

Istotny wkład w adaptację dorobku branży cyberbezpieczeństwa do potrzeb rozpoznawania operacji informacyjnych i dezinformacji ma Clint Watts, ekspert ds. bezpieczeństwa, walki informacyjnej i dezinformacji, który w przeszłości był związany z amerykańską armią i FBI, a obecnie jest pracownikiem naukowym w Foreign Policy Research Institute oraz specjalistą w Alliance for Securing Democracy. Watts wskazuje, że media społecznościowe są obiektem oddziaływania grup APM (*advanced persistent manipulators*), definiowanych przez niego jako (…) *aktor lub skoordynowana grupa (kombinacja) aktorów, którzy dokonują rozszerzonego, wyrafinowanego, wieloplatformowego, multimedialnego ataku informacyjnego na określony cel*[71]. Termin „*advanced persistent manipulators*" nawiązuje do powszechnie stosowanego w branży cyberbezpieczeństwa terminu „*advanced persistent threats*", którym – jak wcześniej sygnalizowano – określa się aktorów zagrożeń (głównie państwowych)

[69] Tamże, s. 15.

[70] Tamże, s. 10.

[71] W oryginale: „An actor or combination of actors perpetrating an extended, sophisticated, multi-platform, multi-media information attack on a specified target". Zob. C. Watts, *Advanced Persistent Manipulators, Part One: The Threat to Social Media Industry*, Alliance for Securing Democracy, 12 II 2019 r., https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-one-the-threat-to-the-social-media-industry/ [dostęp: 11 VII 2024].

zdolnych do generowania zaawansowanych i trwałych cyberzagrożeń polegających na penetracji sieci ofiary i niewykrytym funkcjonowaniu w niej przez dłuższy czas. Grupy APM działają podobnie do grup APT w tym sensie, że konsekwentnie dążą do realizacji swoich celów, przez co zagrożenia przez nie generowanego nie mityguje np. zamknięcie czy czasowa blokada konta na platformie społecznościowej. Grupy APM wykorzystują kombinację technik manipulacji i mają wystarczające zasoby, aby prowadzić długotrwałe kampanie propagandowe i dezinformację. Potrafią przy tym gromadzić, agregować oraz analizować dane użytkowników, a także adaptować techniki oraz omijać mechanizmy kontroli kont i treści w mediach społecznościowych. Watts wskazuje wiele różnych grup typu APM: aktorzy państwowi, grupy ekstremistyczne, aktywiści, politycy oraz lobbyści i firmy pijarowe[72].

Silnie rozwiniętym nurtem badań nad możliwością adaptacji doświadczeń branży cyberbezpieczeństwa na potrzeby rozpoznawania dezinformacji jest budowanie modeli (frameworków) analitycznych. Umożliwiają one standaryzację procesu badawczego i tym samym ułatwiają ekspertom wymianę informacji i wiedzy, porównywanie i uogólnianie wniosków analizy, a w konsekwencji osiąganie wymiernych efektów analitycznych, np. atrybucji (przypisanie sprawstwa) operacji informacyjnych (psychologicznych)/operacji wpływu do poszczególnych podmiotów, czyli do APM. Przed omówieniem przykładowych rozwiązań warto przywołać postrzeganie tej problematyki przez ekspertów Centrum Doskonalenia NATO StratCom (NATO Strategic Communication Centre of Excellence) oraz Europejskiego Centrum Doskonalenia ds. Zwalczania Zagrożeń Hybrydowych (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE). Zwracają oni uwagę, że istotnym problemem w rozpoznawaniu operacji informacyjnych/operacji wpływu jest zróżnicowany typ danych, na których podstawie pracują analitycy. Eksperci NATO StratCom i Hybrid CoE podzielili je na trzy kategorie: techniczne, behawioralne oraz kontekstowe. Dodatkowo różnią się one ze względu na stopień dostępności. Pierwsza kategoria źródeł to dane ogólnodostępne (*open source*). W tej kategorii danymi technicznymi będą np. adres IP i właściciel strony internetowej lub jawnie wykazywane powiązania ekonomiczne podmiotów wykorzystanych w konkretnej operacji (np. informacje z rejestrów przedsiębiorców czy sprawozdań finansowych). Danymi behawioralnymi pozyskanymi ze źródeł typu *open source* będą np. przykładowa aktywność konkretnego konta lub strony, zaobserwowane przez analityka wzorce propagacji przekazu i techniki komunikacji oraz powiązania wykazane w wyniku analizy sieci społecznych. Dane kontekstowe w tym przypadku mogą dotyczyć sytuacji geopolitycznej (np. powiązanie danego wydarzenia z aktorem na zasadzie prawdopodobieństwa motywu), a także być wynikiem analizy narracyjnej (treściowej)

[72] C. Watts, *Advanced Persistent Manipulators*…

oraz charakterystyki językowej danego materiału (np. propagandowego). Kolejną kategorią są źródła informacji mające charakter prawnie zastrzeżony (*proprietary source*), a więc takie, do których mają dostęp jedynie właściciele danych (np. platformy społecznościowe), czyli np.: adres IP użytkowników, ich geolokalizacja, cały zakres aktywności konta. Trzecim typem informacji są dane ze źródeł niejawnych (*classified source*), do których dostęp mają głównie instytucje rządowe. Są to dane gromadzone np. za pomocą działań wywiadowczych. Autorzy zwracają również uwagę, że w procesie gromadzenia i przetwarzania wszystkich danych z wyżej wymienionych typów źródeł należy uwzględnić kwestie prawne oraz etyczne (tabela 2)[73].

Tabela 2. Rodzaje danych uwzględnianych w analizie operacji wpływu/operacji informacyjnych według Jamesa Pammenta i Victorii Smith.

	Dowód techniczny (*technical evidence*)	**Dowód behawioralny** (*behavioural evidence*)	**Dowód kontekstowy** (*contextual evidence*)	**Ocena prawna i etyczna** (*legal & ethical assessment*)
Źródło otwarte (*open source*)	właściciel domeny, adresy IP, powiązania ekonomiczne	aktywność konta, aktywność strony, pisanie i publikowanie wiadomości (*posting/cross posting*), udostępnianie, obserwowanie, aktywność sieciowa (*network*)	treści medialne, dyskurs i narracje, językoznawstwo, kontekst polityczny, *cui bono*	ryzyko sporu sądowego (*risk of litigation*), etyka badań, ryzyko stania się celem
Źródło własnościowe / zastrzeżone (*proprietary source*)	dane zbierane przez backend platform (internetowych)	jak wyżej, z większym zakresem danych pochodzących z platform (internetowych)	jak wyżej oraz dane pochodzące z usuniętych treści (*takedowns*) wraz z podejrzanymi linkami	ochrona interesów politycznych i handlowych, ochrona danych
Źródło niejawne (*classified source*)	SIGINT; zastrzeżone dane źródłowe uzyskane w ramach nakazu (*warrant*)	jak wyżej oraz SIGINT, HUMINT	jak wyżej oraz niejawne oceny geopolityczne	strategia charakterystyczna dla aktora, ochrona interesów politycznych, ochrona danych

Źródło: opracowanie własne na podstawie: J. Pamment, V. Smith, *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*, https://stratcomcoe.org/publications/download/Nato-Attributing-Information-Influence-Operations-DIGITAL-v4.pdf, s. 15 [dostęp: 18 VIII 2024].

[73] Zob. szerzej: J. Pamment, V. Smith, *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*, https://stratcomcoe.org/publications/download/Nato-Attributing-Information-Influence-Operations-DIGITAL-v4.pdf, s. 15–24 [dostęp: 18 VIII 2024].

Na podstawie wyników przeprowadzonej analizy zróżnicowania typów oraz źródeł danych eksperci NATO StratCom oraz EU Hybrid CoE zwracają uwagę na problemy w ramach badania, a w konsekwencji również przeciwdziałania, dezinformacji. Jednym z ich argumentów jest to, że platformy cyfrowe niechętnie dzielą się swoimi danymi technicznymi i behawioralnymi. Tłumaczą to np. koniecznością ochrony prywatności użytkowników oraz tajemnicą działalności handlowej[74]. Jako konieczne w przezwyciężeniu trudności eksperci postrzegają budowanie transparentnych metodologii rozpoznawania operacji informacyjnych/operacji wpływu oraz otwarcie się na wymianę informacji na temat rozpoznawanych TTPs oraz stosowanie spójnego formatowania danych umożliwiającego ich międzyplatformową analizę[75]. W dalszej części artykułu zostaną omówione modele (frameworki) analityczne spopularyzowane w literaturze przedmiotu.

Kill Chain

Postulat adaptacji modelu Cyber Kill Chain na potrzeby analizy operacji wpływu w cyberprzestrzeni został sformułowany w artykule *Understanding Influence Operations in Social Media* autorstwa Arlida Bergha z Norweskiego Ośrodka Badań Obronnych (Norwegian Defence Research Establishment). Tekst ukazał się na łamach czasopisma „Journal of Information Warfare" w 2020 r.[76] Bergh podkreśla, że oparcie się na podejściu ilościowym w badaniu operacji wpływu (np. przez analizę liczby udostępnień fałszywych materiałów) jest niewystarczające do ich pełnego rozpoznania i zrozumienia, w związku z czym postuluje konieczność ujęcia w analizie kwestii socjotechnicznych. W jego opinii warstwa socjotechniczna operacji wpływu może zostać pogłębiona przez uwzględnienie w jej analizie metodyki opartej na fazach cyberataku modelu Kill Chain, na które składają się:

- rekonesans – rozpoznanie słabości celu, które mogą zostać wykorzystane podczas ataku;
- uzbrojenie – wybór mediów społecznościowych i stworzenie treści, które zostaną wykorzystane w ataku;
- dostarczenie – wykorzystanie kanałów w mediach społecznościowych do rozpropagowania treści;
- eksploitacja – wywołanie zainteresowania audytorium (np. za pomocą techniki clickbaitu czy oddziaływania na liderów opinii);

[74] Tamże, s. 27.

[75] Tamże, s. 26.

[76] A. Bergh, *Understanding Influence Operations in Social Media: A Cyber Kill Chain Approach*, „Journal of Information Warfare" 2020, t. 19, nr 4, s. 113–121.

- instalacja – utrwalenie propagowanych treści w przekazie informacyjnym audytorium. Bergh w tym kontekście proponuje pojęcie osadów informacyjnych środowiska online (*online information sediments*). Za jego pomocą zwraca uwagę na to, że treści umiejętnie wprowadzone w obieg informacyjny utrzymują się w nim przez dłuższy czas. Nawet jeśli nie mają potencjału oddziaływania, to sama ich obecność (trwałość) w obiegu informacyjnym nadaje im użyteczność z perspektywy operacji wpływu (np. mogą zostać wykorzystane do zwiększania wiarygodności innych narracji lub wpływania na algorytmy rekomendacji treści w mediach społecznościowych);
- dowodzenie i kontrola – oddziaływanie i wywieranie wpływu na proces definiowania znaczeń (*meaning-making process*) określonych jednostek oraz grup;
- działanie (*action on objectives*) – dążenie do wywołania określonych działań (zachowań) zdefiniowanych odbiorców (np. protestów społecznych).

Podsumowując model Kill Chain, warto zwrócić uwagę, że w tym ujęciu operacja wpływu jest skuteczna wtedy, gdy cele zostaną zrealizowane we wszystkich wyżej wymienionych fazach. Efektywność takiego działania znacznie wykracza więc poza sytuację, w której materiał został jedynie skutecznie rozpropagowany w sieci (nawet w wypadku, gdy trwale w niej funkcjonuje), ponieważ największe znaczenie ma skuteczność oddziaływania na sferę poznawczą i – w konsekwencji – kształtowanie określonych postaw lub wywołanie pożądanych zachowań u odbiorców. Bergh wskazuje też, że operacja wpływu ma charakter obiegowy (a nie liniowy), co sprawia, że proces przetwarzania informacji jest silnie uzależniony od czynników zewnętrznych (np. od zaangażowania użytkowników mediów społecznościowych)[77]. To implikuje konieczność rozpatrywania działań będących elementami operacji informacyjnych/operacji wpływu w cyberprzestrzeni w szerokim kontekście i z uwzględnieniem ich długofalowości.

Model diamentu

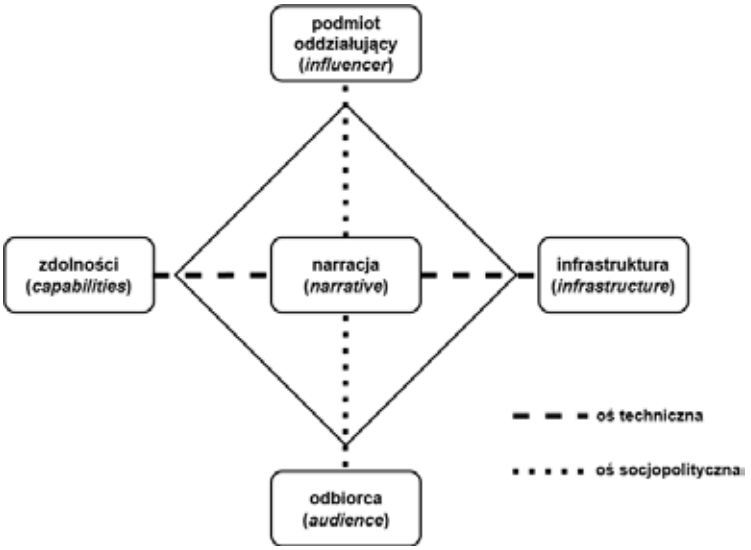
Analityczka Charity Wright związana z Insikt Group (część szerszego podmiotu Recorded Future komercyjnie zajmującego się cyberbezpieczeństwem), a w przeszłości również z amerykańską armią oraz z National Security Agency, opublikowała raport z propozycją wykorzystania modelu diamentu na potrzeby analizy operacji wpływu w cyberprzestrzeni[78]. Założenie tego modelu opiera się na centralności

[77] Tamże, s. 122.

[78] C. Wright, *The Diamond Model for Influence Operations Analysis*, https://go.recordedfuture.com/hubfs/white-papers/diamond-model-influence-operations-analysis.pdf [dostęp: 28 VII 2024].

narracji jako najważniejszego elementu operacji wpływu i jej powiązaniu z czterema elementami[79]:

1) podmiotem oddziałującym (*influencer*), czyli osobą lub organizacją prowadzącą szkodliwą działalność;
2) odbiorcą (*audience*), którym mogą być osoby lub grupy, do których jest skierowana operacja wpływu;
3) infrastrukturą (*infrastructure*), która obejmuje środki techniczne i fizyczne wykorzystywane do tworzenia i rozpowszechniania materiałów wykorzystanych w operacji wpływu;
4) zdolnościami (*capabilities*), na które składają się TTPs stosowane przez wpływającego (rysunek 3).



Rysunek 3. Elementy i powiązania modelu diamentu w analizie operacji informacyjnych/operacji wpływu w ujęciu Recorded Future.

Źródło: opracowanie własne na podstawie: C. Wright, *The Diamond Model for Influence Operations Analysis*, Active Response, https://go.recordedfuture.com/hubfs/white-papers/diamond-model-influence-operations-analysis.pdf, s. 1 [dostęp: 28 VII 2024].

Skuteczność operacji wpływu zależy od tych wszystkich elementów, każdy z nich może być również przedmiotem odrębnej analizy. W modelu diamentu występują dwa typy powiązań z narracją – socjopolityczny oraz techniczny. Pierwszy typ

[79] Tamże, s. 3–7.

to powiązania narracji z podmiotem oddziałującym oraz odbiorcą i może dotyczyć np. znajomości przez podmiot oddziałujący słabych stron odbiorcy, które umożliwiają temu podmiotowi przeprowadzenie skutecznej operacji wpływu. Natomiast powiązanie narracji z infrastrukturą oraz zdolnościami ma charakter techniczny – są to m.in. rozpoznane media wykorzystane w operacji oraz techniki wsparcia oddziaływania lub propagacji przekazu (np. dane dotyczące wykorzystanych materiałów audiowizualnych)[80]. Analiza relacji między poszczególnymi elementami modelu pozwala na lepsze zrozumienie celów kampanii, identyfikację słabych punktów odbiorców, przewidywanie kolejnych działań podmiotu oddziałującego i rekomendowanie sposobów przeciwdziałania[81].

DISARM Framework

DISARM Framework (Disinformation Analysis and Response Measures) ma inny charakter niż wyżej omówione koncepcje, ponieważ w większym stopniu skupia się na zoperacjonalizowaniu procesów związanych z analizą operacji informacyjnych/operacji wpływu i zapobieganiu im, a w mniejszym na problematyce teoretyczno-metodologicznej tego aspektu (chociaż i w tym zakresie wysuwa pewne postulaty). Z informacji podanych przez DISARM Foundation[82] wynika, że DISARM Framework nawiązuje do prac ekspertki Sary-Jayne Terp[83] z lat 2017–2018 nad możliwościami adaptacji narzędzi bezpieczeństwa informacyjnego na potrzeby badania dezinformacji, a sama koncepcja ukształtowała się w latach 2019–2020. Podczas kilku lat jej ewoluowania wpływ na nią miało, jak wskazują informacje podane przez DISARM Framework, wiele organizacji z branży bezpieczeństwa w cyberprzestrzeni (wcześniej model nosił nazwę AMITT). Rozwój koncepcji był oparty na ustandaryzowanym systemie wymiany informacji i uwzględnieniu w procesie gromadzenia informacji TTPs zarówno strony ofensywnej (*red team*), jak i defensywnej (*blue team*). Aktualnie DISARM Framework jest prezentowany jako narzędzie bazujące na rozwiązaniach zbliżonych do MITRE ATT&CK[84]. Założenia DISARM Framework

[80] Tamże.

[81] Tamże, s. 10.

[82] Podmiot założony w celu promowania i rozwijania DISARM Framework. Jego członkami są managerowie, analitycy i eksperci branży bezpieczeństwa informacji z doświadczeniem pracy lub służby w amerykańskich instytucjach publicznych, podmiotach komercyjnych oraz organizacjach trzeciego sektora. Zob. *DISARM Foundation*, https://www.disarm.foundation/about-us [dostęp: 5 VIII 2024].

[83] Zainteresowania Sary-Jayne Terp koncentrują się na bezpieczeństwie kognitywnym oraz analizie i zapobieganiu dezinformacji. Zob. SJ Terp, https://www.infosecurity-magazine.com/profile/sj-terp/ [dostęp: 5 VIII 2024].

[84] Na ten temat zob. *DISARM Disinformation TTP (Tactics, Techniques and Procedures) Framework*, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/ [dostęp: 5 VIII 2024].

zostały przedstawione przez Sarę-Jane Terp oraz Pabla Breuera z DISARM Foundation na konferencji CogSIMA (Conference on Cognitive and Computational Aspects of Situation Management) w 2022 r. Autorzy sugerują, że z perspektywy praktyka użyteczne jest przyjęcie optyki „bezpieczeństwa kognitywnego" (*cognitive security*)[85], co pozwala na postrzeganie dezinformacji w sposób bardziej holistyczny. Sugerują przy tym, że perspektywa bezpieczeństwa kognitywnego jest związana nie tylko z „wielkoskalową inżynierią społeczną", lecz także z problemem uczenia maszynowego w bezpieczeństwie informacji (*machine learning in information security*, MLSec), czyli wykorzystywania technologii sztucznej inteligencji, jej modeli wzorowanych na ludzkich procesach myślowych, do ataków na systemy informacyjne oraz na inne systemy sztucznej inteligencji[86]. Autorzy sugerują więc, aby do rozpoznawania i zapobiegania dezinformacji wykorzystać nie tylko elementy dorobku analityki cyberbezpieczeństwa (szczególnie model Kill Chain oraz platformę wymiany informacji i wiedzy w formule MITRE ATT&CK), lecz także badania sfery kognitywnej, np. związane z technikami marketingowymi (np. oceny danej treści przez grupę lub osobę, które są celem oddziaływania) czy działaniami psychologicznymi[87].

Metoda gromadzenia i przetwarzania informacji DISARM Framework jest oparta na założeniu, że jednostkowy przypadek dezinformacji należy traktować w kategorii incydentu (jak w wypadku incydentów komputerowych), który powinien zostać zaewidencjonowany, a następnie przeanalizowany (np. pod kątem odpowiedzi na pytania o poszczególne komponenty zdarzenia, ich współzależność oraz relacje z innymi wydarzeniami i kampaniami propagandowymi). Terp i Breuer zaprezentowali w referacie szablon incydentu dezinformacji/propagandy, na który składa się dziewięć kategorii informacji. Są to informacje opisowe, takie jak: nazwa i podsumowanie incydentu, hipotezy dotyczące sprawcy ataku (atrybucja), czas trwania incydentu, moment wystąpienia, prawdopodobne cele adwersarzy, ich metody, metody przeciwdziałania oraz inne, potencjalnie powiązane, incydenty. W DISARM Framework dostęp do bazy danych o incydentach odbywa się w trybie *open source* i w założeniach ma być ona zasilana przez różne źródła – naukowców,

[85] Terp i Breuer definiują ten termin jako „wdrożenie założeń, praktyk oraz narzędzi bezpieczeństwa informacyjnego na potrzeby manipulacji, dezinformacji oraz operacji wpływu" (w oryginale: „application of information security principles, practices, and tools to misinformation, disinformation, and influence operations"). Zob. SJ Terp, P. Breuer, *DISARM: A Framework for Analysis of Disinformation Campaigns,* 2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogsSIMA), https://ieeexplore.ieee.org/document/9830669, s. 3 [dostęp: 5 VIII 2024].

[86] Tamże, s. 3.

[87] Tamże, s. 6.

badaczy zjawisk dezinformacji[88]. Z udostępnionych danych wynika, że baza zawiera informacje o 66 incydentach i ogranicza się do lat 2014–2020[89]. Znajduje się w niej lista 142 technik (w przypadku niektórych uwzględniono ich podtypy, więc w rzeczywistości ta liczba jest większa) charakteryzujących działania zespołów ofensywnych i defensywnych. Techniki te obejmują zaobserwowane sposoby manipulacji wykorzystane w przekazie, sposoby wprowadzania lub utrwalania go w obiegu informacyjnym, a także rekomendacje dotyczące działań defensywnych ukierunkowanych na mitygację zagrożeń generowanych przez adwersarzy[90]. Techniki zostały przyporządkowane do 16 taktyk, którym z kolei odpowiadają cztery fazy działań[91].

Podsumowanie

Modele analityczne omówione w tekście nie wyczerpują wszystkich propozycji wykorzystania doświadczeń branży cyberbezpieczeństwa w analizie operacji informacyjnych/operacji wpływu[92]. Zestawienie zawiera jedynie te aspekty, które autorzy uznali za istotne z perspektywy celów niniejszego artykułu. Podsumowując, należy wskazać cechy wspólne uzasadniające adaptację koncepcyjnych i metodologicznych podstaw CTI na potrzeby badania operacji informacyjnych/operacji wpływu:

- Głównym argumentem jest funkcjonowanie w przestrzeniach informacyjnych grup typu APM, czyli podmiotów trwale i metodycznie infekujących infosferę za pomocą różnych metod manipulacji (w tym dezinformacji) w celu wywołania określonego zachowania lub kształtowania postaw decydentów, liderów opinii bądź mniej lub bardziej szerokich grup społecznych. APM mogą mieć motywacje polityczne (np. instytucje sektora siłowego prowadzące operacje wpływu w cyberprzestrzeni na rzecz obcych państw), biznesowe (np. nielegalny lobbing, czarny PR w sieci) oraz ideologiczne (np. organizacje ekstremistyczne). Ich działania mogą wywołać doraźne lub trwałe skutki negatywnie wpływające na funkcjonowanie państw i jego instytucji, społeczeństwa oraz pojedynczych obywateli. W tym sensie

[88] Tamże.

[89] Zob. *DISARM Frameworks – incidents*, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/incidents_index.md [dostęp: 31 VIII 2024].

[90] Zob. *DISARM Frameworks – techniques*, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques_index.md [dostęp: 31 VIII 2024].

[91] Zob. *DISARM Frameworks – phases*, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/tree/main/generated_pages/phases [dostęp: 31 VIII 2024].

[92] Na temat innych modeli analitycznych zob. *IO-Campaign-Collections*, GitHub, https://github.com/tripkrant/IO-Campaign-Collections [dostęp: 31 VIII 2024].

przestrzeń informacyjna jest zatem zagrożona negatywnym oddziaływaniem tych podmiotów w podobny sposób, jak sieci teleinformacyjne są zagrożone działaniami aktorów państwowych (np. APT), grup przestępczych czy haktywistów.

- Aktywność grup typu APM wymaga mitygowania generowanych przez nie różnych rodzajów ryzyka i zagrożeń. W tym celu należy dążyć m.in. do – analogicznie jak w CTI – identyfikowania ich aktywności w przestrzeni informacyjnej przez badanie stosowanych przez nie TTPs, wykorzystywanej infrastruktury oraz dokonywania na tej podstawie atrybucji z konkretnym podmiotem (np. z państwem, instytucją, organizacją, podmiotem komercyjnym).
- Grupy typu APM prowadzą działania w różnych obszarach przestrzeni informacyjnej (np. w różnych mediach społecznościowych), a skutki ich aktywności są badane i analizowane przez społeczność składającą się z różnych osób i podmiotów, stosujących różne modele i metodologie analizy. Konieczna jest zatem standaryzacja procedur w celu umożliwienia wymiany wiedzy oraz uzyskania efektu synergii. W literaturze wskazuje się na zasadność korzystania z technologii platform analitycznych (*threat intelligence platform*, np. OpenCTI), usprawniających gromadzenie i analizę śladów aktywności APM (IoC, TTP itp.) oraz wymianę wiedzy w ramach uzgodnionych taksonomii (są one stosowane np. w bazie w MITRE ATT&CK). Aktualnie są rozwijane rozwiązania zbliżone do MITRE ATT&CK, czego przykładem jest DISARM Framework.
- Autorzy materiałów dotyczących adaptacji CTI na potrzeby analizy operacji informacyjnych/operacji wpływu mają świadomość ich odmienności w stosunku do „klasycznego" CTI z uwagi na społeczno-polityczny charakter badanych zagadnień. Można to dostrzec na poziomie zarówno ogólnych, jak i szczegółowych postulatów i koncepcji, czego przykład stanowi model diamentu, w którym centralnym punktem analizy jest narracja.

Warto zwrócić uwagę na znaczenie ostatniej ze wskazanych kwestii. Gromadzenie i analiza danych tekstowych zawierających określony przekaz (komunikat) są odmienne od przetwarzania danych takich jak pakiety przesłane między określonymi adresami IP czy analiza logów aktywności w sieci zainfekowanej przez działania adwersarza (grupy hakerskiej). Ta cecha badanych zjawisk ogranicza możliwość pełnej adaptacji metodyki i pracy CTI na potrzeby analizy operacji wpływu. Rozwój technologii związanych ze sztuczną inteligencją, zwłaszcza z przetwarzaniem języka naturalnego (*natural language processing*), może jednak zmniejszyć w przyszłości tę lukę metodologiczną.

Należy także nadmienić, że w spopularyzowanych aktualnie frameworkach nie akcentuje się zasadności prewencyjnego wykrywania podatności (odbiorcy) na różne formy manipulacji, które to podatności mogłyby umożliwić przeprowadzenie operacji informacyjnych/operacji wpływu lub zwiększyć ich skuteczność. Takie podatności mogą mieć charakter techniczny (np. możliwość rejestracji lub wykorzystania domen w celu dezinformacji[93] czy możliwość stworzenia i długotrwałego wykorzystania sieci kont w celu trollingu w określonej tematyce) oraz społeczny (np. stopień zaufania do instytucji publicznych, potencjał polaryzacji oraz radykalizacji społecznej czy kompetencje medialne obywateli). Wydaje się, że tego typu działania, ukierunkowane na aktywne poszukiwanie zagrożeń, byłyby bliskie innej koncepcji wspierającej CTI, tj. modelowaniu zagrożeń (*threat modelling*). Sygnałem zainteresowania tymi kwestiami są przywoływane w niniejszym artykule rozważania autorów koncepcji DISARM Framework, dotyczące postrzegania operacji informacyjnych/operacji wpływu z perspektywy „bezpieczeństwa kognitywnego". Można zakładać, że w przyszłości ten nurt refleksji zostanie pogłębiony i wzbogacony konkretnymi studiami przypadków czy też stworzeniem podstaw teoretyczno-metodologicznych w celu badania omawianego typu zjawisk.

Wnioski

Autorzy oceniają, że adaptacja doświadczeń CTI w ramach badania operacji informacyjnych/operacji wpływu w warstwie metodologicznej ma pewne walory badawcze, chociaż nie stanowią one znaczącej zmiany jakościowej w stosunku do omawianego w artykule podejścia rozwijanego w naukach społecznych, przede wszystkim w komunikologii. Zaadaptowana metodyka CTI skupia się bowiem na założeniach zbliżonych do analizy opartej na elementach procesu komunikacyjnego, tj.: adwersarzu (czyli nadawcy przekazu), jego działaniach (przekazie) i wykorzystywanej infrastrukturze (mediach wykorzystanych w komunikowaniu przekazu) oraz na obiekcie ataku (audytorium przekazu). Ponadto wydaje się, że postulaty adaptacji CTI nie akcentują znaczenia analizy skutków operacji informacyjnych/operacji wpływu. To znacznie zmniejsza możliwości całościowego i pogłębionego ich zrozumienia, a ta kwestia jest z kolei immanentnym elementem analizy opartej

[93] O identyfikacji przedsięwzięć polegających na rejestracji domen o nazwach przypominających oficjalne witryny rządowe, które w przyszłości mogłyby zostać wykorzystane w działaniach socjotechnicznych, w tym dezinformacji, informował zespół CSIRT GOV w raporcie z 2023 r. Zob. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*, CSIRT GOV, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html, s. 20 [dostęp: 31 VIII 2024].

na elementach procesu komunikacyjnego. Metodologiczne urozmaicenie w stosunku do wyżej opisanych metod opartych na komunikologii to natomiast uwzględnienie chronologii i faz operacji informacyjnej/operacji wpływu w jej charakterystyce. Przyjęcie takiego podejścia sprawia, że możliwe jest bardziej precyzyjne zdefiniowanie zachowań adwersarzy w postaci TTP.

Niewątpliwą zaletą CTI jest dotychczasowy dorobek w organizacji pracy z informacją, w tym dążenie do standaryzacji procedur (terminologii, typologii) w zakresie gromadzonych i przetwarzanych danych oraz wypracowywania organizacyjnych i technicznych uwarunkowań umożliwiających ich wymianę. Nadaje to duży walor adaptacji CTI na potrzeby badania operacji informacyjnych/operacji wpływu oraz sprawia, że ten postulat powinien być postrzegany nie jako propozycja nowej metody badania tych zjawisk, lecz szerzej – jako pewne podejście organizacyjno-metodyczne. Oceniając dorobek CTI z tej perspektywy i mając na uwadze wnioski z analizy literatury przedmiotu, należy stwierdzić, że zasadność adaptacji CTI na potrzeby rozpoznawania operacji informacyjnych/operacji wpływu zależy od odpowiedzi na następujące pytania:

1. Co jest przedmiotem analizy? Jak wskazano w części dotyczącej definiowania operacji informacyjnych i operacji wpływu, cyberprzestrzeń jest jedynie jednym ze środowisk, w których są one realizowane. Zasadność adaptacji modeli CTI dotyczy więc jedynie określonego typu tych działań.
2. Jaki jest cel analizy? Metodyka CTI umożliwia sprawne tematyczne grupowanie danych, co ułatwia ich przetwarzanie i wymianę wiedzy. Zwiększa tym samym możliwości budowania świadomości sytuacyjnej na temat zagrożeń w cyberprzestrzeni. Nie wydaje się jednak, aby takie podejście przybliżało do odpowiedzi na pytania dotyczące szerszego wymiaru analizy, np. w zakresie skuteczności działań adwersarzy. Wynika to m.in. z pomijania aspektu badania efektu działań (kognitywnego, społecznego, politycznego).
3. Do jakich źródeł analityk ma dostęp? Z przywołanych wyżej badań ekspertów Hybrid CoE oraz NATO StratCom wynika, że zakres danych możliwych do uzyskania w ramach badania operacji informacyjnej/operacji wpływu jest bardzo szeroki. W niektórych przypadkach dostęp do danych jest możliwy jedynie dla określonych organizacji (platform mediów społecznościowych, instytucji państwowych prowadzących działalność wywiadowczą). Dostęp ten wpływa zatem na usytuowanie analityka w procesie gromadzenia informacji na temat danego zjawiska i określa zakres pytań badawczych, na jakie może zostać udzielona odpowiedź na podstawie tych danych.

Bibliografia

Bergh A., *Understanding Influence Operations in Social Media: A Cyber Kill Chain Approach*, „Journal of Information Warfare" 2020, t. 19, nr 4, s. 110–131.

Bernays E.L., *Propaganda*, New York 1928.

Caramancion K.M. i in., *The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats*, „Data" 2022, t. 7, nr 4, s. 1–18. https://doi.org/10.3390/data7040049.

Dijk J. van, *Społeczne aspekty nowych mediów*, Warszawa 2010.

Dobek-Ostrowska B., *Komunikowanie polityczne i publiczne*, Warszawa 2007.

Dobek-Ostrowska B., *Podstawy komunikowania społecznego*, Wrocław 1999.

Dobek-Ostrowska B., Fras J., Ociepka B., *Teoria i praktyka propagandy*, Wrocław 1999.

Jowett G.S., O'Donnell V., *Propaganda and Persuasion. Fifth Edition*, Los Angeles–London––New Delhi–Singapore–Washington 2012.

Kacała T., *Tendencje rozwojowe współczesnych działań psychologicznych prowadzonych przez Siły Zbrojne RP*, w: *Innowacja i synergia w Siłach Zbrojnych RP*, t. 1, A. Lis, R. Reczkowski (red.), Bydgoszcz 2012, s. 87–118.

Kacała T., Lipińska J., *Komunikacja strategiczna i public affairs*, Warszawa 2014.

Larecki J., *Wielki leksykon służb specjalnych świata*, Warszawa 2007.

Minkina M., *Sztuka wywiadu w państwie współczesnym*, Warszawa 2014.

Modrzejewski Z., *Information operations from the Polish point of view*, „Obrana a strategie" (Defence and Strategy) 2018, nr 1, s. 115–132. https://doi.org/10.3849/1802-7199.18.2018.01.113-130.

Oosthoek K., Doerr Ch., *Cyber Threat Intelligence: A Product Without a Process?*, „International Journal of Intelligence and Counter Intelligence" 2021, t. 34, nr 2, s. 300–315. https://doi.org/10.1080/08850607.2020.1780062.

Rajczyk R., *Nowoczesne wojny informacyjne*, Warszawa 2016.

Roberts S.J., Brown R., *Intelligence-Driven Incident Response. Outwitting the Adversary*, Sebastopol 2017.

Świerczek M., *Metody działania rosyjskich służb specjalnych w świetle afery Olega Kulinicza*, „Przegląd Bezpieczeństwa Wewnętrznego" 2023, nr 29, s. 63–93. https://doi.org/10.4467/20801335PBW.23.020.18762.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 225–234.

Wojnowski M., *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 11–36.

Woolley S.C., Howard P.N., *Introduction: Computational Propaganda Worldwide*, w: *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, S.C. Woolley, P.N. Howard (red.), Oxford 2018, s. 3–18. https://doi.org/10.1093/oso/9780190931407.001.0001.

Źródła internetowe

About Strategic Communications, NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/about_us/about-strategic-communications/1 [dostęp: 10 VII 2024].

Acquire Infrastructure: Domains, Attack. Mitre, https://attack.mitre.org/techniques/T1583/001/ [dostęp: 24 VIII 2024].

Allied Joint Doctrine for Information Operations (AJP-10.1), UK Ministry of Defence, https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations-ajp-101 [dostęp: 28 XII 2023].

Allied Joint Doctrine for Psychological Operations (AJP-3.10.1), UK Ministry of Defence, https://www.gov.uk/government/publications/ajp-3101-allied-joint-doctrine-for-psychological-operations [dostęp: 5 VII 2024].

An introduction to threat intelligence, CERT-UK, https://www.ncsc.gov.uk/files/An-introduction-to-threat-intelligence.pdf [dostęp: 10 IX 2024].

APT29, Attack. Mitre, https://attack.mitre.org/groups/G0016/ [dostęp: 24 VIII 2024].

ATT&CK Matrix for Enterprise, Attack. Mitre, https://attack.mitre.org/ [dostęp: 24 VIII 2024].

Brangetto P., Veenendaal M.A., *Influence Cyber Operations: The Use of Cyberattacks in Support of Cyberaatacks in Support of Influence Operations*, w: *8th International Conference on Cyber Conflict. Proceedings 2016*, N. Pissanidis i in. (red. nauk.), https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf, s. 113–126 [dostęp: 10 VII 2024].

Caltagirone S., Pendergast A., Betz Ch., *The Diamond Model of Intrusion Analysis*, https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf [dostęp: 24 VIII 2024].

Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/operation [dostęp: 28 XII 2023].

Collier J., Ronis S., *Navigating the Trade-Offs of Cyber Attribution*, https://cloud.google.com/blog/topics/threat-intelligence/trade-offs-attribution/ [dostęp: 22 VIII 2024].

Combating Foreign Influence, FBI, https://www.fbi.gov/investigate/counterintelligence/foreign-influence [dostęp: 2 XI 2024].

Cybersecurity and Foreign Interference in the EU Information Ecosystem, ENISA, 8 XII 2022 r., https://www.enisa.europa.eu/news/cybersecurity-foreign-interference-in-the-eu-information-ecosystem [dostęp: 20 IX 2024].

Cyber Influence Operations, https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-cyber-influence-operations [dostęp: 10 VII 2024].

DeBolt M. i in., *CTI-CMM Cyber Threat Intelligence Capability Maturity Model*, Version 1.0, https://d39ec1uo9ktrut.cloudfront.net/Datasheets/CTI-CMM-Cyber-Threat-Intelligence-Capability-Maturity-Model.pdf [dostęp: 22 VIII 2024].

DISARM Disinformation TTP (Tactics, Techniques and Procedures) Framework, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/ [dostęp: 5 VIII 2024].

DISARM Foundation, https://www.disarm.foundation/about-us [dostęp: 5 VIII 2024].

DISARM Frameworks – incidents, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/incidents_index.md [dostęp: 31 VIII 2024].

DISARM Frameworks – phases, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/tree/main/generated_pages/phases [dostęp: 31 VIII 2024].

DISARM Frameworks – techniques, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques_index.md [dostęp: 31 VIII 2024].

Facebook. Threat research, GitHub, https://github.com/facebook/threat-research [dostęp: 11 VIII 2024].

Ferazza F.M., *Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model: a comparison of cyber intrusion analysis models*, https://www.royalholloway.ac.uk/media/20188/techreport-2022-5.pdf.pdf [dostęp: 25 VIII 2024].

Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape, ENISA, 8 XII 2022 r., https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape [dostęp: 20 IX 2024].

Glossary of Intelligence Terms and Definitions, https://www.cia.gov/readingroom/docs/CIA-RDP80M00596A000500020003-7.pdf [dostęp: 28 XII 2023].

Headquaters Departament of the Army, *FM 100-6, Information Operations*, Washington 1996, https://www.hsdl.org/?view&did=437397 [dostęp: 28 XII 2023].

Hutchins E.M., Cloppert M.J., Amin R.M., *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [dostęp: 24 VIII 2024].

Information Operations, http://web.archive.org/web/20201226185947/https://transparency.twitter.com/en/reports/information-operations.html [dostęp: 11 VIII 2024].

Information Operations. Joint Publication 3-13, https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf [dostęp: 30 I 2023].

Information Sharing and Analysis Centres (ISACs). Cooperative models, ENISA, 2017 r., https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/@@download/fullReport [dostęp: 24 VIII 2024].

Introduction to STIX, https://oasis-open.github.io/cti-documentation/stix/intro.html [dostęp: 24 VIII 2024].

IO-Campaign-Collections, GitHub, https://github.com/tripkrant/IO-Campaign-Collections [dostęp: 31 VIII 2024].

Joint Doctrine for Command and Control Warfare (C2W), https://apps.dtic.mil/sti/pdfs/ADA357635.pdf [dostęp: 28 XII 2023].

Larson E.V. i in., *Foundations of Effective Influence Operations. A Framework for Enhancing Army Capabilites*, Rand Corporation, 2009 r., https://www.rand.org/pubs/monographs/MG654.html [dostęp: 18 XI 2024].

Mavroeidis V., Bromander S., *Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence*, https://arxiv.org/pdf/2103.03530 [dostęp: 24 VIII 2024].

Microsoft Digital Defence Report 2022, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/microsoft-digital-defense-report-2022.pdf?culture=en-us&country=us [dostęp: 11 VIII 2024].

MISP. Threat Sharing, https://www.misp-project.org/ [dostęp: 24 VIII 2024].

Niedzielski D., *Wojskowa doktryna komunikacji strategicznej NATO i jej znaczenie dla Polski*, „Akademickie Centrum Komunikacji Strategicznej" 2022, nr 3, https://www.wojsko-polskie.pl/aszwoj/u/af/14/af143adc-70e6-463a-8448-faaf0df61e9a/biuletyn_nr_3.pdf, s. 46–53 [dostęp: 10 VII 2024].

OpenCTI, https://filigran.io/solutions/open-cti/ [dostęp: 24 VIII 2024].

Oxford English Dictionary, https://www.oed.com/dictionary/operation_n?tab=factsheet&tl=true#33665121 [dostęp: 28 XII 2023].

Pamment J., Smith V., *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*, https://stratcomcoe.org/publications/download/Nato-Attributing-Information-Influence-Operations-DIGITAL-v4.pdf [dostęp: 18 VIII 2024].

Pols P., *The Unified Kill Chain. Raising resilience against advanced cyber attacks*, https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf [dostęp: 24 VIII 2024].

Porche I.R. i in., *Redefining Information Warfare Boundaries for an Army in Wireless World*, https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf [dostęp: 28 XII 2023].

Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure, https://www.cisa.gov/sites/default/files/2023-01/cisa_insight_mitigating_foreign_influence_508.pdf [dostęp: 29 XII 2023].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku, CSIRT GOV, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html [dostęp: 31 VIII 2024].

Shires J., *Hack-and-leak operations and U.S. cyber policy*, War on the Rocks, 14 VIII 2020 r., https://warontherocks.com/2020/08/the-simulation-of-scandal/ [dostęp: 10 VII 2024].

SJ Terp, https://www.infosecurity-magazine.com/profile/sj-terp/ [dostęp: 5 VIII 2024].

Słownik języka polskiego PWN, https://sjp.pwn.pl/szukaj/operacja.html [dostęp: 3 VII 2024].

SolarWinds Compromise, Attack. Mitre, https://attack.mitre.org/campaigns/C0024/ [dostęp: 24 VIII 2024].

Terms & Definitions of Interest for DoD Counterintelligence Professionals, https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf [dostęp: 28 XII 2023].

Terp SJ, Breuer P., *DISARM: A Framework for Analysis of Disinformation Campaigns*, 2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), https://ieeexplore.ieee.org/document/9830669 [dostęp: 5 VIII 2024].

Threat Report: Combating Influence Operations, Meta, 26 V 2021 r., https://about.fb.com/news/2021/05/influence-operations-threat-report/ [dostęp: 11 VIII 2024].

Threat Report. The State of Influence Operations 2017–2020, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf [dostęp: 10 VII 2024].

TTP in cybersecurity, Sekoia, https://www.sekoia.io/en/glossary/ttp-cyber-tactics-techniques-and-procedures/ [dostęp: 9 IX 2024].

Updated IC Gray Zone Lexicon: Key Terms and Definitions, https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Updated-IC-Gray-Zone-Lexicon-July2024.pdf [dostęp: 11 VIII 2024].

Wagner T.D. i in., *Cyber Threat Intelligence Sharing: Survey and Research Directions*, https://www.open-access.bcu.ac.uk/7852/1/Cyber%20Threat%20Intelligence%20Sharing%20Survey%20and%20Research%20Directions.pdf [dostęp: 24 VIII 2024].

Wardle C., Derakhshan H., *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe report DGI(2017)09, https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html [dostęp: 10 VII 2024].

Watling J., Danyluk O., Reynolds N., *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023*, https://static.rusi.org/202303-SR-Unconventional-Operations-Russo-Ukrainian-War-web-final.pdf.pdf [dostęp: 10 VII 2024].

Watts C., *Advanced Persistent Manipulators, Part One: The Threat to Social Media Industry*, Alliance for Securing Democracy, 12 II 2019 r., https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-one-the-threat-to-the-social-media-industry/ [dostęp: 18 VIII 2024].

Words of Estimative Probability, Analytic Confidences, and Structured Analytic Techniques, Center for Internet Security, https://www.cisecurity.org/ms-isac/services/words-of-estimative-probability-analytic-confidences-and-structured-analytic-techniques [dostęp: 23 VIII 2023].

Wright C., *The Diamond Model for Influence Operations Analysis*, https://go.recordedfuture.com/hubfs/white-papers/diamond-model-influence-operations-analysis.pdf [dostęp: 28 VII 2024].

Akty prawne

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. DzU z 2024 r. poz. 1557).

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. DzU z 2022 r. poz. 2091).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. DzU z 2024 r. poz. 17).

Inne dokumenty

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 10 VII 2024].

Dr Kamil Baraniuk

Doktor nauk o polityce i administracji, absolwent Wydziału Nauk Społecznych Uniwersytetu Wrocławskiego.

Kontakt: kam.baraniuk@gmail.com

Piotr Marszałek

Ekspert ds. cyberbezpieczeństwa w Polskim Towarzystwie Bezpieczeństwa Narodowego.

Kontakt: piotr.marszalek@ptbn.online