Wojny przyszłości i operacje informacyjne (INFOOPS) w cyberprzestrzeni

Chapter · October 2019

CITATIONS
0

READS
1,585

1 author:

Rafał Karol Kasprzyk
Military University of Technology
102 PUBLICATIONS **297** CITATIONS

SEE PROFILE

Rozdział V

Wojny przyszłości i operacje informacyjne (INFOOPS) w cyberprzestrzeni

Rafał Kasprzyk[1]

1. Wprowadzenie

W niniejszym rozdziale przedstawione zostaną założenia tzw. wojny przyszłości, roli operacji informacyjnych w kształtowaniu środowiska informacyjnego oraz konsekwencji tego typu działań dla środowiska bezpieczeństwa. Następnie w sposób syntetyczny omówiona zostanie ewolucja sieci Internet, mająca fundamentalne znaczenie dla rozważanej tematyki. Powszechny dostęp do sieci Internet i coraz większa rola mediów społecznościowych w kształtowaniu opinii, a szerzej sposobu postrzegania świata, wymaga podjęcia prac nad wypracowaniem metod identyfikacji i rozpoznania operacji informacyjnych w mediach społecznościowych. W kolejnym kroku zasadne jest również wypracowanie modeli i metod przeciwdziałania tego typu zjawiskom, a następnie ich wdrożenie, co jednak w państwach demokratycznych jest z oczywistych powodów dyskusyjne. Związane jest to często z bardzo subtelną różnicą między wrogą operacją informacyjną, a typową i zasadną w państwach demokratycznych debatą publiczną.

Przedstawiona zostanie również istota modelowania operacji informacyjnych na przykładzie teorii sterowania refleksyjnego jako modelu wpływania na proces podejmowania decyzji przeciwnika. Sterowanie refleksyjne polega na ingerowaniu w proces budowy subiektywnego obrazu rzeczywistości przez obiekt atakowany poprzez wytworzenie w świadomości, podświadomości i nieświadomości obiektu warunków do kształtowania się przekonań i poglądów, a w konsekwencji podejmowania decyzji i akcji zgodnych z celem atakującego.

2. Wojny przyszłości i kluczowe pojęcia

Ocena zmian środowiska bezpieczeństwa jest jednym z procesów prowadzonych na poziomie strategicznym państwa, mającym kluczowe znaczenie dla kierunku rozwoju systemu bezpieczeństwa narodowego. Istotą tego procesu jest identyfikacja przyszłych uwarunkowań prowadzenia operacji, w tym wojny, tak aby podsystem militarny i pozamilitarny przygotowywać do tego, co będzie, a nie tego, co miało miejsce w przeszłości. Zmiany zachodzące we współczesnym świecie związane są z dynamiką rozwoju nowoczesnych technologii i jej wpływem na życie niemalże każdego człowieka.

[1] Wojskowa Akademia Techniczna, Wydział Cybernetyki, Instytut Systemów Informatycznych.

Wojny przyszłości, a tym samym największe wyzwania, jakie stoją przed siłami zbrojnymi, w wielu opracowaniach [21], [33], [38] definiowane są przez pryzmat przyszłych uwarunkowań prowadzenia operacji:

- Rozróżnienie pomiędzy stanem „P" i „W" będzie trudne lub niemożliwe;
- Brak linii frontu w tradycyjnym rozumieniu tego słowa oraz coraz większa asymetryczność konfliktów i wojen;
- Trudność w rozróżnieniu podsystemu militarnego i pozamilitarnego, a tym samym żołnierz coraz bardziej podobny do cywila;
- Rozwój robotyki i sztucznej inteligencji będzie prowadził do powstania broni coraz bardziej autonomicznych lub wręcz autonomicznych;
- Działania niekinetyczne, w szczególności operacje cybernetyczne (ang. *CyberOps*) i operacje informacyjne (ang. *InfoOps*), będą oddziaływać na środowisko fizyczne w stopniu determinującym powodzenie operacji militarnych.

Obecnie, jak nigdy w historii ludzkości, wszystko jest ze wszystkim połączone za pomocą sieci i systemów teleinformatycznych, tworząc tzw. **cyberprzestrzeń** (ang. *cyberspace*). Pojęcie cyberprzestrzeni zostało spopularyzowane przez amerykańskiego pisarza *science fiction* Wiliama Gibsona, który poruszał problem świata zdominowanego przez wszechobecną i bardzo tanią zaawansowaną technologię. Jest to wizja świata, w której niemożność wejścia do cyberprzestrzeni spycha człowieka na margines społeczeństwa. Cyberprzestrzeń opisywana jest w książkach Gibsona jako „przestrzeń wypełniona danymi generowana przez połączone ze sobą komputery", do której mogą przedostać się bohaterowie jego opowiadań. Jest podstawową przestrzenią, w której funkcjonują ludzie, podczas gdy świat fizyczny jest „złem koniecznym".

Obecnie trudno mówić o powszechnie obowiązującej definicji cyberprzestrzeni. Często przytaczanymi definicjami są tłumaczenia definicji proponowanych w publikacjach Departamentu Obrony Stanów Zjednoczonych, np. „przestrzeń wytwarzania, gromadzenia, przetwarzania i wymiany danych, informacji i wiedzy tworzona przez systemy i sieci teleinformatyczne (w tym Internet) wraz z zewnętrznymi obiektami (np. użytkownikami) wchodzącymi w interakcje z tymi systemami" [39], [40]. Istotną kwestią z punktu widzenia tematyki poruszanej w niniejszym rozdziale jest fakt, że cyberprzestrzeń jest częścią środowiska informacyjnego współczesnego człowieka, a za sprawą popularności mediów społecznościowych traktowana jest jako nowa przestrzeń społeczna, w której „spotykają" się ludzie. Pojęcie cyberprzestrzeni spopularyzował rozwój Internetu, dlatego też jest ono używane często jako synonim Internetu.

Kolejnym istotnym konceptem jest **świadomość sytuacyjna** (ang. *Situation Awareness*), definiowana jako „cykliczny proces percepcji stanu środowiska informacyjnego rozumienia znaczenia stanu poszczególnych elementów składowych środowiska informacyjnego i projekcji (prognozowania) na tej podstawie przyszłych jego stanów, w celu podejmowania właściwych decyzji, a w konsekwencji działań, które wpływają na nowy stan środowiska informacyjnego" [41].

Koncept świadomości sytuacyjnej pozwala zdefiniować kluczowe dla dalszych rozważań **operacje informacyjne** (ang. *InfoOps*) jako wszelkie operacje na elementach środowiska informacyjnego mające na celu:

- ingerowanie w proces osiągania świadomości sytuacyjnej przeciwnika, a w konsekwencji wpływanie na jego proces podejmowania decyzji [perspektywa ofensywna];
- uniemożliwienie ingerowania zewnętrznym aktorom w proces osiągania świadomości sytuacyjnej przez stronę defensywną, a w konsekwencji uniemożliwienie im wpływania na proces podejmowania decyzji strony defensywnej [perspektywa defensywna].

Nowa przestrzeń – cyberprzestrzeń – wykorzystywana do prowadzenia operacji cybernetycznych (ang. *CyberOps*) i w coraz większym zakresie operacji informacyjnych (ang. *InfoOps*) ma istotny wpływ na potencjalne zagrożenia dla bezpieczeństwa państwa, istniejące zarówno na poziomie technicznym, jak również informacyjnym. Wojny przyszłości prowadzone będą w głównej mierze właśnie w cyberprzestrzeni stanowiącej kluczową część współczesnego środowiska informacyjnego. Jednocześnie coraz częściej „tradycyjne" już operacje cybernetyczne zsynchronizowane będą z operacjami informacyjnymi tworząc *de facto* jedną operację w cyberprzestrzeni [22].

Polem walki staną się więc systemy przetwarzania danych i informacji, ale nie tylko twarda infrastruktura teleinformatyczna (operacje *CyberOps*), lecz wszystko, co do tej infrastruktury jest „podłączone", a więc również ludzie – „mózgi realizujące procesy poznawcze" (operacje *InfoOps*). O ile świadomość zagrożeń technicznych jest systematycznie podnoszona, a zdolności w tym obszarze zarządzane (w głównej mierze) w ramach zespołów CERT/CSIRT, jak również w różnych państwach w ramach nowych rodzajów wojsk, np. w Polsce – Wojska Obrony Cyberprzestrzeni, to świadomość powagi zagrożeń na poziomie informacyjnym jest wciąż niewystarczająca.

3. Ewolucja Internetu

Internet, jak większość przełomowych technologii XX wieku, powstał w odpowiedzi na potrzeby armii Stanów Zjednoczonych i w pierwotnym zamyśle jego twórców miał stanowić rozproszony system kierowania i dowodzenia (ang. *command & control*) zdolny przetrwać zmasowany atak fizyczny. Z armii trafił na uniwersytety, następnie do biznesu i w końcu „pod strzechy". Historia rozwoju Internetu od strony zarówno technicznej jak i użytkowej jest niezwykle ciekawa.

Z punktu widzenia tematyki rozdziału koniecznym jest wskazanie kamieni milowych, określanych jako **Web1.0**, **Web.2.0** oraz **Web3.0**, które pozwalają zrozumieć, jaką drogę przeszliśmy, jeśli chodzi o rozwój technologii i dokąd zmierzamy. W wielkim skrócie i jednak pewnym uproszczeniu, kolejne wersje Internetu można scharakteryzować w następujący sposób:

- *Web1.0* to sieć „tylko do czytania" (ang. *read-only Web*), gdzie istnieje stosunkowo wąskie grono producentów treści umieszczanych na portalach internetowych, a cała reszta użytkowników sieci to konsumenci mający zasadniczo możliwość przeglądania treści (niekiedy z drobnymi wyjątkami np. dodawanie przez czytelników portalu

komentarzy). Historycznie jest to najstarsza kultura użycia Internetu, choć wciąż spotykana: ten charakter ma np. większość współczesnych portali informacyjnych.

- *Web2.0* to sieć „do czytania i pisania" (ang. *read-write Web*), gdzie zacierają się granice pomiędzy rolą producenta i konsumenta treści. W miejsce portali internetowych powstają platformy internetowe stanowiące przestrzeń szeroko rozumianej komunikacji pomiędzy użytkownikami pełniącymi jednocześnie role producentów i konsumentów treści. Tego typu kultura użycia Internetu jest współcześnie bardzo powszechna. W oparciu o ideę sieci Web2.0 powstały internetowe platformy handlowe (np. eBay, Allegro), Wikipedia, media społecznościowe (np. Youtube, Facebook, Twitter) i wiele innych obecnie powszechnych rozwiązań.
- *Web3.0* to również sieć „do czytania i pisania" (ang. *read-write Web*) będąca rozszerzeniem koncepcji Web2.0 o tzw. sztuczną inteligencję (ang. *artificial intelligence*), której zadaniem jest coraz lepsze rozumienie potrzeb i zainteresowań użytkowników sieci. Platformy internetowe migrują w kierunku kultury inteligentnych platform, dzięki czemu możliwym staje się rekomendowanie użytkownikom właściwych dla nich treści, przy jak najmniejszym wysiłku ze strony owych użytkowników. Personalizowanie treści odbywa się poprzez profilowanie użytkowników, co, jak się okazuje, ma daleko idące konsekwencje i staje się tematem wrażliwym.
- *Web4.0* to hipotetyczna kultura Internetu przyszłości, gdy faktycznie wszystkie urządzenia zostaną dołączone do globalnej sieci Internet w wyniku upowszechnienia się koncepcji IoT (ang. *Internet of Things*), inteligentne platformy internetowe zostaną scalone w jeden organizm, umożliwiając wymianę danych, informacji i wiedzy bez dotychczasowych ograniczeń (problemy integracji) przy jednoczesnym przełomie w zakresie możliwości tzw. sztucznej inteligencji, rozumianym jako przejście od istniejącej obecnie wąskiej sztucznej inteligencji (ang. *narrow artificial inteligence*) do wizjonerskiej koncepcji ogólnej sztucznej inteligencji (ang. *general artificial intelligence*). W końcu Web 4.0, określana mianem sieci symbiotycznej, ma spowodować, że interakcja człowieka i maszyny zostanie pozbawiona dotychczasowych barier związanych ze współczesnymi nienaturalnymi interfejsami, takimi jak np. klawiatura czy myszka. Współcześni wizjonerzy (m.in. Ray Kurzweil prezentujący koncepcję tzw. *Sigularity*) przewidują, że w połowie XXI wieku będziemy mogli, a być może musieli, połączyć nasze umysły z komputerami. Programy łączenia mózgu ludzkiego z komputerem nie są fantazją, od lat bowiem prowadzone są – z powodzeniem – prace nad wykorzystaniem m.in. elektroencefalografii (EEG) do komunikacji z osobami sparaliżowanymi lub do sterowania ruchami sztucznych kończyn. Co więcej, obecnie uruchomione zostały bardzo ambitne projekty nad połączeniem komputera z mózgiem, których celem jest nie tyle sterowanie urządzeniem, ile zapis „myśli" na zewnętrznym nośniku danych, w bardzo różnych celach. Projekty takie realizuje firma Neuralink Elona Muska i amerykańska agencja DARPA (ang. *Defence Advanced Research Project Agency*).

Podsumowując: stoimy w obliczu coraz większego przenikania człowieka do cyberprzestrzeni (ang. *immersion*), a tym samym wpływu cyberprzestrzeni na człowieka

w świecie fizycznym. Zmierzamy więc w kierunku zacierania granic między fizycznymi bytami a ich awatarami (ang. *avatars*) w cyberprzestrzeni.

4. Kultura Web3.0 i jej konsekwencje

Współcześnie użytkownicy cyberprzestrzeni to blisko 60% ludzkości (ponad 4,3 mld osób). Większość użytkowników Internetu (ponad 3,4 mld) to aktywni użytkownicy mediów społecznościowych wykorzystujący jako interfejs głównie urządzenia mobilne (ponad 3,2 mld). Standardem obecnie stały się inteligentne platformy internetowe, a więc Internet osiągnął poziom kultury Web3.0, do której wielu jej użytkowników jest „podłączonych" niemal na stałe. Bycie on-line stało się kluczową potrzebą, w szczególności tzw. cyfrowych tubylców (ang. *digital native*) – pokolenia ludzi, którzy nie znają świata bez Internetu. Potrzeba bycia on-line staje się jednak również coraz bardziej powszechna wśród pokoleń starszych, starających się sprostać wymaganiom otaczającego ich świata, tzw. cyfrowych imigrantów (ang. *digital immigrant*).

Media społecznościowe, w których, jak to zostało wspomniane, „spotykają" się ludzie, są zasadniczym elementem środowiska informacyjnego współczesnego człowieka. Dla wielu są niemalże jedynym źródłem informacji o otaczającym ich świecie. Rola mediów społecznościowych, jeśli chodzi o kształtowanie opinii na niemalże każdy temat, jak również możliwość wpływania na sposób postrzegania rzeczywistości i poglądy poszczególnych osób, grup społecznych czy niemalże całych społeczeństw jest obecnie nie do przecenienia [7], [15]. Problem ten staje się przedmiotem debaty publicznej, która wydaje się jednak nieco spóźniona (na co już nie mamy wpływu), bardzo często jest prowadzona jedynie przez i z perspektywy cyfrowych imigrantów, na dodatek w większości przypadków z wykorzystaniem jedynie badań jakościowych.

Użytkownicy kultury Web3.0 generują olbrzymią ilość danych i potężny ruch w Internecie. Wyzwaniem staje się opanowanie gigantycznego szumu informacyjnego oraz szukanie „źródła prawdy" i „źródła fałszu". Media społecznościowe wpływają jednak na to, jak znaczna część społeczeństwa pozyskuje informacje, jak ją konsumuje i jak się tą informacją dzieli. Okazuje się, że proces ten jest bardzo szybki i w większości przypadków bezkrytyczny, niemalże wręcz bezmyślny. Nie ma wówczas mowy o weryfikacji informacji i jej źródeł. Media społecznościowe (ang. *Social Media*) przekształciły komunikację w Internecie w interaktywny dialog, którego uczestnicy odczuwają potrzebę wyrażenia siebie i wyartykułowania „swoich" przekonań i poglądów, szukając aprobaty czy wręcz aplauzu. Trudno więc o jakikolwiek merytoryczny dyskurs. Komunikacja w mediach społecznościowych to przede wszystkim emocje, które potęgują naturalne odruchy, jak np.:

- efekt potwierdzenia (ang. *confirmation bias*) – preferowanie treści, które potwierdzają dotychczasowe przekonania i poglądy,
- efekt przyciągania podobieństwa (ang. *similarity attraction effect*) – nawiązywanie kontaktów z osobami o podobnych przekonaniach i poglądach.

Powyższe skutkuje pojawianiem się w mediach społecznościowych zjawiska tzw. baniek społecznych (ang. *social bubbles*), czyli społeczności, zwykle antagonistycznych i stąd przeważnie minimalizujących wzajemne interakcje związane z realną komunikacją. Co więcej, kultura Web3.0 wykorzystująca inteligentne platformy

internetowe tworzy tzw. bańki filtrujące (ang. *filter bubbles*) dla swych użytkowników, co potęguje wspomniane zjawisko baniek społecznych.

Wolne od uprzedzeń (jak może się wydawać) i nieskrępowane cenzurą interaktywne dialogi w mediach społecznych nieoczekiwanie prowadzą do niespotykanej polaryzacji społecznej. Reasumując powyższe, kultura Web3.0 okazuje się być wyjątkowo podatnym gruntem dla wszelkiego rodzaju manipulacji informacją, a w konsekwencji jej użytkownikami. Paliwem dla manipulacji są tzw. **zaburzenia (patologie) informacji** (ang. *information disorder*), która są rozprzestrzenianie w mediach społecznościowych.

5. Dezinformacja – ujęcie statyczne (klasyfikacja zaburzeń informacji)

Klasyfikacją zaburzeń (patologii) informacji zajmuje się obecnie wiele ośrodków naukowych, instytucji publicznych i prywatnych. Jedna z ogólnych taksonomii wyróżnia wśród zaburzeń informacyjnych [37]:

- informację nieprawdziwą, wprowadzającą w błąd (ang. *mis-information*),
- informację wyrządzającą szkodę/ból (ang. *mal-information*),
- informację celowo wprowadzającą w błąd, mogącą wyrządzić szkodę/ból (ang. *dis-information*).

Przedmiotem dalszego zainteresowania jest właśnie tzw. **dezinformacja** jako informacja mogąca posiadać cechy zarówno informacji nieprawdziwej, jak i wyrządzającej szkodę lub tylko jednej z tych kategorii. W ujęciu jakościowym dezinformacja rozumiana jest jako informacja mającą zdolność kreowania obrazu rzeczywistości, niekoniecznie zgodnego z faktami. W zależności od intencji wprowadzenia odbiorcy w błąd (ang. *intent to deceive*) [36] dezinformację mogą stanowić:

- satyra/parodia (ang. *satire/parody*),
- fałszywe/pokrętne połączenia (ang. *false connection*) np. nagłówki artykułów pokrętnie odpowiadające jego treści,
- wprowadzająca w błąd treść (ang. *misleading content*),
- fałszywy kontekst dla prawdziwej informacji (ang. *false context*),
- informacja o pozornie niesterowanych zdarzeniach (ang. *imposter content*),
- zmanipulowana treść (ang. *manipulated content*),
- w pełni sfabrykowana treść (ang. *fabricated content*).

W ujęciu ilościowym dezinformację można natomiast zdefiniować jako ustaloną ilość informacji mającej kreować obraz rzeczywistości na określony temat, w tym całkowity brak informacji na ten temat lub przeciwnie – szum informacyjny, jak również natłok informacji prowadzący do swego rodzaju przeciążenia informacyjnego odbiorcy.

Zaburzenia informacyjne są więc różnie klasyfikowane i występują pod różnymi postaciami, np. tekst, grafika, nagrania dźwiękowe, wideo. W powszechnym obiegu tego rodzaju zaburzenia informacyjne określane są mianem fake'ów lub fake newsów, jeśli dotyczą spraw bieżących. Bardzo często fake'i, wyglądają na informacje prawdziwe, dopiero po ich analizie i weryfikacji źródła okazują się zaburzeniami informacyjnymi. Zupełną nowością i potężnym zagrożeniem są od niedawna deepfake'i. O ile fake'i są tworzone w całości przez ludzi, oczywiście z wykorzystaniem narzędzi takich jak edytory

tekstu czy edytory graficzne, to deepfake'i powstają w sposób zautomatyzowany z wykorzystaniem narzędzi i algorytmów szeroko rozumianej tzw. sztucznej inteligencji, w szczególności uczenia maszynowego (ang. *machine learning*), a precyzyjniej głębokich sieci neuronowych (ang. *deep neural networks*), rozpoznawania obrazu i syntezy mowy. Wyjątkowo niepokojący jest fakt dostępności w Internecie gotowych narzędzi, które umożliwiają nawet laikowi przygotowanie deepfake'a. Oczywiście, powstają również narzędzia do automatyzacji identyfikacji deepfake'ów.

Niestety, jak już zostało wspomniane, kultura Web3.0 bardzo zniechęca jej użytkowników do krytycznego myślenia. Stąd potrzeba systemowego podejścia do walki z fake'ami, czego jednym z przejawów jest pojawienie się na różnych poziomach (rzetelnego dziennikarstwa, pojedynczych państw, organizacji międzynarodowych, również samych mediów społecznościowych) osób lub całych instytucji zajmujących się kontrolą faktów, tzw. pogromców mitów (ang. *fact checkers*).

6. Dezinformacja – ujęcie dynamiczne

W poprzednim podrozdziale dezinformacja została zdefiniowana w ujęciu statycznym jako zaburzenie informacyjne. Dezinformacja w ujęciu dynamicznym to proces manipulacji, świadomego wprowadzania w błąd, zasianie wątpliwości odbiorcy co do faktycznego stanu rzeczy z wykorzystaniem różnego rodzaju zaburzeń informacyjnych. Dezinformacja jako proces jest więc ofensywną operacją informacyjną, czyli ingerowaniem w proces osiągania świadomości sytuacyjnej, której celem jest wywołanie u odbiorcy określonego obrazu rzeczywistości, a w konsekwencji decyzji (ewentualnie jej braku) zgodnej z założeniami ośrodka planującego operację informacyjną [5]. Dezinformacją jest w swojej istocie ingerencja w proces podejmowania decyzji odbiorcy (obiektu lub grupy obiektów), również poprzez maskowanie pewnych wydarzeń i informacji o tych wydarzeniach lub generowanie szumu informacyjnego celem zdezorientowania odbiorcy. Tym samym w procesie dezinformacji wykorzystywana jest informacja, która nie zawsze jest nieprawdziwa, ale wprowadzane zaburzenia informacyjne mogą powodować u odbiorcy wątpliwości co do faktycznego stanu rzeczy. W tym miejscu warto zwrócić uwagę na olbrzymie podobieństwo procesu dezinformacji do działań marketingowych, w tym reklamowych.

Zaawansowane operacje informacyjne opierają się na wcześniejszym rozpoznaniu odbiorcy (obiektu lub grupy obiektów), do których są kierowane. Efektem rozpoznania są profile, czyli *de facto* sparametryzowane modele subiektywizmu odbiorcy, w oparciu o które kształtuje on swój obraz rzeczywistości. Budowa modeli subiektywizmu jest złożonym procesem, który może polegać na profilowaniu poprzez aktywną komunikację w czasie poprzedzającym proces dezinformacji. W oparciu o zbudowane profile atakujący kształtuje środowisko informacyjne obiektu atakowanego w celu wykreowania obrazu rzeczywistości (w pewnym sensie narzuconego przez atakującego) zbieżnego z celami strony atakującej. Tym samym atakujący zyskuje swego rodzaju przewagę informacyjną, która umożliwia wpływanie na procesy decyzyjne obiektu atakowanego [5]. Warto przypomnieć, że dokładnie według tego schematu, poprzez profilowanie użytkowników, odbywa się personalizowanie treści w kulturze Web3.0 na inteligentnych platformach

internetowych. W tym ujęciu bardzo wyraźnie widać istotę procesu dezinformacji, którą niekoniecznie jest rozprzestrzenianie nieprawdziwych informacji.

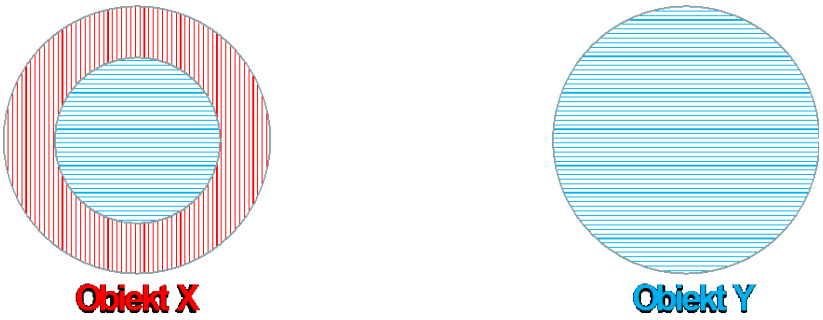
Intuicyjne jest spostrzeżenie, że skuteczność operacji informacyjnej jest tym większa, im dłużej realizowana jest skrycie, a więc im dłużej obiekt atakowany nie jest tego świadomy. Ciekawostką jest jednak to, że nawet uzyskanie przez obiekt atakowany pełnego przekonania o tym, że był przedmiotem operacji informacyjnej, nie oznacza nabycia przez niego odporności na określoną narrację. Zbudowany obraz rzeczywistości przez długi czas może determinować decyzje obiektu atakowanego ze względu na zjawisko dysonansu poznawczego (ang. *cognitive dissonance*) i wspomniany już efekt potwierdzenia (ang. *confirmation bias*) lub prowadzić do trudności z podjęciem jakiejkolwiek decyzji. Co więcej, zdemaskowanie operacji informacyjnej, nawet jeśli pierwotnie niezamierzone przez atakującego, paradoksalnie jest dla niego stanem korzystnym, w szczególności możliwym do wykorzystania w kolejnej operacji informacyjnej.

Proces dezinformacji należy rozpatrywać w krótkim i długim horyzoncie czasowym. W kontekście długoterminowym kluczowa jest próba identyfikacji celu przeciwnika, co zwykle jest bardzo trudne. W przypadku rozpatrywania dezinformacji w długim horyzoncie czasowym istotna jest również możliwość wykorzystywania nawet zdemaskowanych wcześniej produktów dezinformacji jako tła informacyjnego do budowy zmanipulowanego „spójnego" obrazu rzeczywistości w przyszłości [5].

W tym miejscu warto zwrócić uwagę na potrzebę opracowywania metod identyfikacji i rozpoznania operacji informacyjnych (dezinformacji jako procesu), które to metody, aby były skuteczne, nie mogą zostać oparte wyłącznie na identyfikacji i rozpoznaniu informacji nieprawdziwych. Przeciwdziałanie dezinformacji w ujęciu dynamicznym, czyli procesowi manipulacji, wymaga więc mechanizmów dużo bardziej zaawansowanych niż wspomniani wcześniej tzw. pogromcy mitów (ang. *fact checkers*).

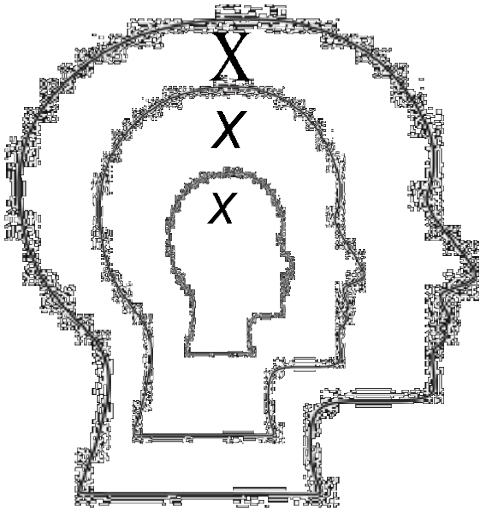
7. Modelowanie operacji informacyjnych

Jednym z najbardziej zaawansowanych matematycznych modeli operacji informacyjnych jest **teoria sterowania refleksyjnego** (szerzej refleksywnego) opracowana w Związku Radzieckim w latach 60. ubiegłego wieku przez Vladimira Lefebvre'a [17–20]. Radziecka koncepcja sterowania refleksyjnego jest zbliżona do amerykańskiej koncepcji zarządzania percepcją, jednak z istotnie mocniej rozwiniętym aparatem formalnym oraz prawdopodobnie bardziej zaawansowanym narzędziami z obszaru m.in. psychologii i socjopsychologii. Punktem wyjścia dla procesu sterowania refleksyjnego jest budowa specyficznego modelu obiektu mającego podlegać sterowaniu. Obiektem tym jest zwykle człowiek, czyli obiekt, który myśli (jest refleksyjny), a w związku z tym tworzy subiektywne obrazy (modele) będący opisem świata, w tym swoich przekonań, poglądów, zasad i reguł postępowania (rysunek 1).



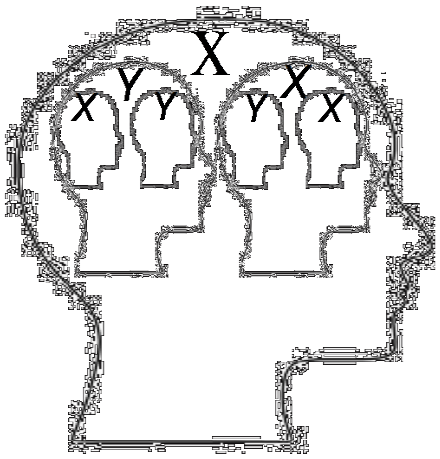
Rys. 1. Budowa modelu obiektu Y przez obiekt X
Źródło: opracowanie własne

Istota budowy tego specyficznego modelu związana jest z pojęciem refleksji (ang. *reflexion*), rozumianej jako zdolność do przyjęcia perspektywy obserwatora w stosunku do swoich własnych przekonań, poglądów, zasad i reguł postępowania. Tak zdefiniowana refleksja to **refleksja pierwszego rodzaju** (ang. *reflexion of the first kind*) lub autorefleksja (ang. *self-reflexion*), która ma charakter rekurencyjny (rysunek 2).



Rys. 2. Refleksja pierwszego rodzaju
Źródło: opracowanie własne

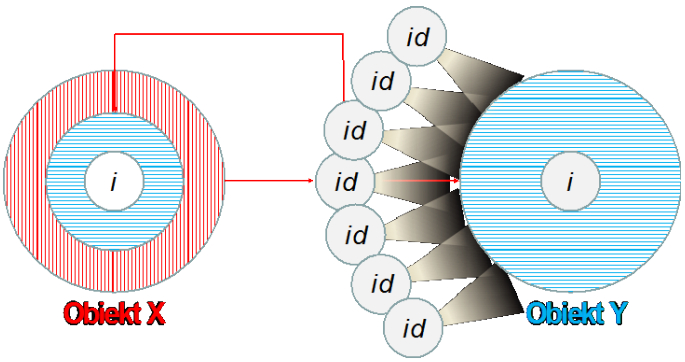
Pojęcie refleksji zostało uogólnione przez Lefebvre'a i w kontekście sterowania refleksyjnego rozumiane jest jako zdolność do przyjęcia perspektywy obserwatora w stosunku do swoich własnych i innego obiektu refleksyjnego, przekonań, poglądów, zasad i reguł postępowania. Tak zdefiniowana refleksja to **refleksja drugiego rodzaju** (ang. *reflexion of the second kind*), która również ma charakter rekurencyjny (rysunek 3), prowadzący do konceptu drzewa hierarchii refleksji rzeczywistości (ang. *hierarchy of realities*).



Rys. 3. Refleksja drugiego rodzaju
Źródło: opracowanie własne

Konstruując model obiektu mającego podlegać sterowaniu refleksyjnemu, najważniejsze jest uwzględnienie w modelu owego konceptu refleksji obiektu modelowanego. Obiekt X chcący sterować obiektem Y buduje model obrazu (modelu) świata zbudowanego przez obiekt Y na określonym poziomie drzewa hierarchii refleksji. Na podstawie tego modelu przygotowuje przeznaczone dla obiektu Y zaburzenia informacji, mające skłonić obiekt Y do podjęcia decyzji, która jest oczekiwana przez X, w taki sposób, aby Y był przekonany, że decyzję podejmuje autonomicznie i że jest ona dla niego najkorzystniejsza z możliwych. Istota sterowania refleksyjnego to zmiana podejścia z próby przewidywania procesów decyzyjnych przeciwnika na wpływanie na jego procesy decyzyjne za pomocą zaburzeń informacji [13], [31].

Jeśli proces sterowania refleksyjnego realizowany jest skrycie, a obiekt X właściwie odczytał subiektywny obraz świata obiektu Y, to każda porcja zaburzenia informacyjnego (oznaczona przez *id* na rysunku 4) przesłana od obiektu X do obiektu Y jest jednocześnie dla X dodatkową informacją o obiekcie Y. Ciekawostką jest możliwość odwrócenia przez obiekt Y procesu, tak aby z roli obiektu sterowanego przejść do roli obiektu sterującego obiektem X, przy jednoczesnym utwierdzaniu obiektu X w przekonaniu o jego pełnej kontroli nad procesem sterowania refleksyjnego.



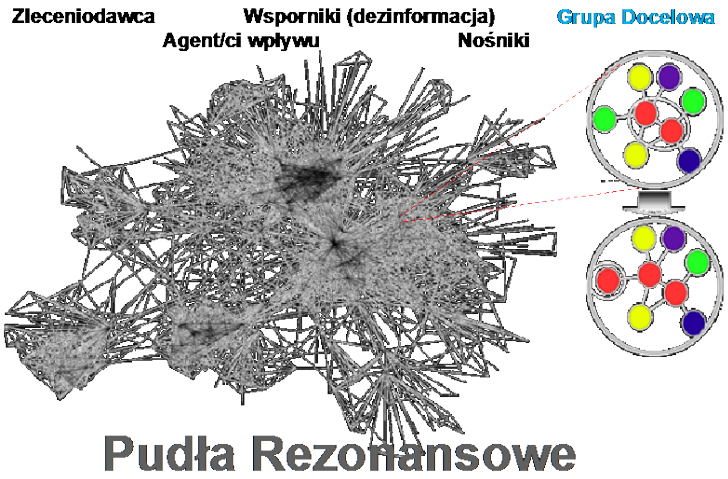
Rys. 4. Szkielet procesu sterowania refleksyjnego obiektem Y przez obiekt X
Źródło: opracowanie własne

Proces sterowania refleksyjnego można uogólnić na sterowanie grupami społecznymi lub całymi społeczeństwami, splątanymi różnego rodzaju więziami społecznymi, jak również grupami powstającymi „spontanicznie" w odpowiedzi na określone bodźce, które to grupy współdzielą w pewnym sensie obraz rzeczywistości.

W sytuacji modelowania operacji informacyjnych prowadzonych w mediach społecznościowych, w szczególności kiedy obiekt poddawany sterowaniu refleksyjnemu jest obiektem złożonym np. grup społecznych, podział na obiekt sterujący i obiekt sterowny jest niewystarczający. Pomocna okazuje się w tym wypadku **teoria dezinformacji** opracowana przez Vladimira Volkoffa [34], w której wyróżnia się różnych aktorów, odgrywających określone role w procesie dezinformacji (rysunek 5):

- zleceniodawca (klient) – osoba lub grupa, która zyskuje na dezinformacji
- agent wpływu – wykonawca/y zleconej dezinformacji
- temat przewodni – motyw będący cechą charakterystyczną dezinformacji
- wsporniki – wydarzenia (prawdziwe, nieprawdziwe) będące „paliwem" dla prowadzonej operacji dezinformacyjnej
- przekaźniki (nośniki) – media w jakimś stopniu związane z agentem wpływu
- pudła rezonansowe – media niezwiązane zarówno ze zleceniodawcą, jak i agentem wpływu, nieświadomie propagujące zaburzenia informacyjne
- grupa docelowa – osoba lub grupa, która jest celem procesu dezinformacji.

W przypadku mediów społecznościowych w procesie dezinformacji bierze udział wiele obiektów odgrywających różne role. Istotne jest zwrócenie uwagi na fakt, że w tym środowisku informacyjnym niezwykle łatwe dotarcie do osób, które propagują dezinformację na zasadzie pudła rezonansowego. Równie prosto jest o przekaźniki za sprawą Social-Botów i całych Social-Botnetów, które dość prosto można zbudować, nawet posiadając stosunkowo niewielką wiedzę techniczną, ewentualnie kupić na zasadzie usługi. Kultura Web3.0 powoduje, że tzw. pudła rezonansowe z jednej strony są powszechne, a z drugiej mają faktycznie realny wpływ na proces dezinformacji; często z powodu swojej liczby są w stanie niemalże w całości przejąć rolę przekaźników.



Rys. 5. Rozprzestrzenianie się dezinformacji w mediach społecznościowych
Źródło: opracowanie własne

Zasadniczym problemem przy modelowaniu operacji informacyjnych w mediach społecznościowych jest zrozumienie procesu rozprzestrzeniania się (dyfuzji) zjawisk w tym środowisku [11], [12], w tym ocena roli i istotności poszczególnych węzłów w sieci oraz prognozowanie dynamiki dyfuzji i zasięgu informacji będącej produktem operacji informacyjnej. Warto zaznaczyć, że istnieją zasadnicze różnice na poziomie tak modelowym, jak i technicznym procesu dezinformacji, gdy przedmiotem ataku informacyjnego jest pojedynczy obiekt bądź grupa obiektów.

8. Podsumowanie

Rzeczywistość na poziomie informacyjnym jest coraz trudniejsza do weryfikacji, a łatwiejsza do manipulacji właśnie za sprawą cyberprzestrzeni. Powszechny dostęp do sieci Internet spowodował, że media społecznościowe odgrywają coraz większą rolę w kształtowaniu opinii na niemalże każdy temat, a szerzej istotnie wpływają na sposób postrzegania świata przez osoby, grupy społeczne czy całe społeczeństwa. Świadomość zagrożeń na poziomie informacyjnym jest wciąż niewielka.

Teoria sterowania refleksyjnego ułatwia analizę procesu podejmowania decyzji własnych i przeciwnika z perspektywy możliwości manipulacji świadomością sytuacyjną. Teoria ta ma już bogatą historię i ugruntowaną pozycję wśród analityków bezpieczeństwa narodowego zarówno w Rosji, jak również w Stanach Zjednoczonych. Przez wielu matematyków zachodnich postrzegana jest jako radziecka alternatywa dla teorii gier [35]. W tym miejscu warto zwrócić uwagę na pojawienie się w latach 70. ubiegłego wieku **teorii hipergier** (ang. *hipergame theory*), nazywanej również teorią metagier (ang. *metagames*) lub gier wyższego rzędu (ang. *higher-order games*), która z kolei może być postrzegana jako zachodnia odpowiedź na teorię sterowania refleksyjnego [6], [16], [25]. Współcześnie teoria sterowania refleksyjnego jest rozwijana, w pewnym stopniu niezależnie, przez kilka grup badawczych proponujących inny aparat formalny do opisu i analizy sterowania refleksyjnego [24], [26], [27], [28], [29], [32]. Za jedną z jej gałęzi, można uznać wspomnianą teorię hipergier. Równolegle budowane są modele operacji informacyjnych wykorzystujące klasyczną teorię gier [10].

Aktualne prace prowadzone w Pracowni Modelowania i Analizy Cyberprzestrzeni, która została powołana w 2018 r. w ramach Instytutu Systemów Informatycznych Wydziału Cybernetyki WAT koncentrują się m.in. wokół modelowania operacji informacyjnych w oparciu o teorię sterowania refleksyjnego (podejście ilościowe), teorię dezinformacji Volkoffa (podejście jakościowe) oraz modele dyfuzji zjawisk w systemach sieciowych. Jednocześnie, Pracownia Modelowania i Analizy Cyberprzestrzeni bazuje na bardzo bogatym doświadczeniu konstruowaniu modeli, metod i informatycznych narzędzi wspomagania decyzji, jakim mogą się poszczycić badacze operacji z Instytutu Systemów Informatycznych Wydziału Cybernetyki Wojskowej Akademii Technicznej [1], [2], [3], [4], [8], [9], [14], [23], [30] (lista publikacji świadomie subiektywna).

LITERATURA

[1] Ameljańczyk A., *Optymalizacja wielokryterialna w problemach sterowania i zarządzania*, Wydawnictwo Polskiej Akademii Nauk, PTC, Wrocław 1984.
[2] Amaljańczyk A., *Optymalizacja wielokryterialna*, WAT, Warszawa 1986.
[3] Ameljańczyk A., *Teoria Gier*, WAT, Warszawa 1978.
[4] Antkiewicz R., *Modelowanie i metody oceny efektywności wybranych podsystemów sieci korporacyjnych*, WAT, Warszawa 2003.
[5] Basaj K., *Dezinformacja – czyli sztuka manipulacji*, Fundacja Bezpieczna Cyberprzestrzeń, 27.12.2018.
[6] Bennett P., „Toward a Theory of Hypergames", *Omega* 5, 749–751 (1977).
[7] Bond R, Fariss Ch., Jones J., Kramer A., Marlow C., Settle J. Fowler J., „A 61-Million-Person Experiment in Social Influence and Political Mobilization", *Nature* 489, 295–298 (2012).
[8] Chojnacki A., *Modelowanie matematyczne*, WAT, Warszawa 1986.
[9] Chudy M., *Wybrane algorytmy optymalizacji*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2014.
[10] Jormakka J., Mölsä J., „Modelling Information Warfare as a Game", *Journal of Information Warfare*, Vol. 4, Issue 2, 12–25 (2005).
[11] Kasprzyk R., „Diffusion in Networks", *Journal of Telecommunications and Information Technology*, No. 2, 99–106 (2012).
[12] Kasprzyk R., „Modele ewolucji systemów złożonych i metody badania ich charakterystyk dla potrzeb komputerowej identyfikacji potencjalnych sytuacji kryzysowych", praca doktorska, Wojskowa Akademia Techniczna, Warszawa 2012.
[13] Kasprzyk R., „The Essence of Reflexive Control and Diffusion of Information in the Context of Information Environment Security", [w:] *Intelligent Systems in Production Engineering and Maintenance*, Advances in Intelligent Systems and Computing, Vol. 835, 720–728, Springer, Cham 2019.
[14] Korzan B., *Elementy teorii grafów i sieci: metody i zastosowania*, Wydawnictwo Naukowo-Techniczne, Warszawa 1978.
[15] Kramer A., Guillory J., Hancock J., „Experimental evidence of massive-scale emotional contagion through social networks", *PNAS Proceedings of the National Academy of Sciences of the United States of America*, 111(24), 8788–8790 (2014).
[16] Kovach N.S., Gibson A.S., Lamont G.B., „Hypergame Theory: A Model for Conflict, Misperception, and Deception", *Game Theory*, Vol. 2015, Article ID 570639 (2015).
[17] Lefebvre V., „Basic ideas of reflexive games logic", *Problemy Issledovania Sistem i Structur*, AN USSR Press, Moscow 1965.
[18] Lefebvre V., Baranov P., Lepsky V., „Internal Currency in Reflexive Games", *Izvestia*, AN USSR, Tekhnicheskaya Kibernetika, No. 4, 1969.
[19] Lefebvre V., *Algebra of Conscience, second enlarged edition*, Kluwer, Holland 2001.
[20] Lefebvre V., *Lectures on reflexive Game Theory*, Leaf & Oaks Publisher, Los Angeles, USA 2010.
[21] Maj M., Basaj K., Grzybowski M., Kasprzyk R., Pohorecki G., Pyznar M., *Koncepcja Rozwoju Zdolności Resoru obrony Narodowej do działań*

w cyberprzestrzeni, Zespół Zadaniowy ds. Cyberbezpieczeństwa w Resorcie Obrony Narodowej, MON, Warszawa, 1 czerwca 2017.

[22] Maj M., Kasprzyk R., Basaj K., *Rozwój CSIRT a obszar działań INFO OPS*, Fundacja Bezpieczna Cyberprzestrzeń, 01.12.2017.

[23] Najgebauer A., *Informatyczne systemy wspomagania decyzji w sytuacjach konfliktowych. Modele, metody i środowiska symulacji interaktywnej*, WAT, Warszawa 1999.

[24] Novikov D., Chkartishvili A., *Refleksivnye igry* (*Reflexive games*), SINTEG, Moscow 2003.

[25] Mateski M., Mazzuchi T., Sarkani S., „The Hypergame Perception Model: A Diagrammatic Approach to Modeling Perception Misperception and Deception", *Military Operations Research*, Vol. 15, No. 2, 21–37 (2010).

[26] Schreider Yu., „Continously-valued logics Lef_m as languages of reflexion", *Nauchnotekhnicheskaya Informatsia*, No. 1–2 (1999).

[27] Taran T., „Model of Reflexive Behavior in Conflict Situation", *Journal of Computer and Systems Sciences Internatioonal*, No. 1, 1998.

[28] Taran T., „Many-valued Boolean Model of Reflexive Agent", *Multi-Valued Logic*, No.7 (2001).

[29] Taran T., „Boolean models of reflexive control and their application for describing information warfare in social-economical systems", *Avtomatika i Telemekhanika*, No. 11 (2004).

[30] Tarapata Z., *Models and Algorithms for Knowledge-Based Decision Support and Simulation in Defence and Transport Applications*, WAT, Warszawa 2011.

[31] Thomas T., „Russia's Reflexive Control Theory and the Military", *Journal of Slavic Military Studies* 17, 237–256 (2004).

[32] Trudolubov A., „Decisions on dependency nets and reflexive polynomials", *VI Symposium po Kibernetike*, Part III, Tibilisi 1972.

[33] U.S. Army Training and Doctrine Command „Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025–2040", Version 1.0, December 2017.

[34] Volkoff V., *Petite histoire de la désinformation*, Les Editions du Rocher, 1999.

[35] Von Neumann J., Morgenstern O., *Theory of Games and Economic Behavior*, John Wiley and Sons, 1944.

[36] Wardle C., „Fake news. It's complicated", https://firstdraftnews.com:443/fake-news-complicated/, 2017.

[37] Wardle C., Derakhshan H., „Information Disorder: Toward an interdisciplinary framework for research and policymaking", *Council of Europe*, Vol. 9 (2017).

[38] William L., Keith N., John S., Joseph S., Gary W., „The Changing Face of War: Into the Fourth Generation", *Marine Corps Gazette*, 22–26, October 1986.

[39] JP 3-13, Cyberspace Operations, U.S. Joint Chiefs of Staff, 8 June 2018.

[40] JP 3-13, Information Operations, U.S. Joint Chiefs of Staff, 20 November 2014.

[41] https://www.definitions.net/definition/situation+awareness