WOJSKOWA AKADEMIA TECHNICZNA
im. Jarosława Dąbrowskiego

WYDZIAŁ BEZPIECZEŃSTWA, LOGISTYKI I ZARZĄDZANIA

ROZPRAWA DOKTORSKA

Temat: **Wzorzec oddziaływań operacji informacyjnych na bezpieczeństwo jednostki i grupy**

Autor:
mgr inż. Krzysztof Zaborek

Promotor:
dr hab. Janusz Świniarski, prof. ndzw. WAT

Promotor pomocniczy:
dr Joanna Skulska

Warszawa 2023

STRESZCZENIE

W ramach rozprawy doktorskiej opracowano i zweryfikowano wzorzec oddziaływań operacji informacyjnych na bezpieczeństwo jednostki (osoby) i grupy (wspólnoty). Za fundament rozważań przyjęto koncepcje związane z Polską Szkołą Cybernetyki (jakościowa teoria informacji, psychocybernetyka, socjocybernetyka i teoria systemów autonomicznych) oraz filozofią neotomistyczną i tomistyczną ze szczególnym uwzględnieniem metafizyki i antropologii filozoficznej. Korzystając z analizy systemowej wyróżniono elementy przestrzeni sterowania (cyberprzestrzeni), takie jak zasoby, jednostki, grupy i komunikaty (informacje). Następnie przeanalizowano każdy z wyróżnionych elementów wraz z możliwymi relacjami między nimi pod kątem operacji informacyjnych, na które składają się zarówno oddziaływania na zasoby (oddziaływania techniczne), jak i ludzi wraz z grupami (oddziaływania psychologiczne). Jako źródła pomocnicze zostały użyte matematyczna teoria komunikacji, teorie bezpieczeństwa (bezpieczeństwo subiektywne i obiektywne Freia, teoria bezpieczeństwo Świniarskiego i Chojnackiego, model *instrusion kill chain* i kostka McCumbera) oraz dokumenty doktrynalne SZ RP dotyczące operacji informacyjnych i operacji w cyberprzestrzeni. Wzorzec został zweryfikowany przez porównanie go do modelu dywersji ideologicznej opisanej przez Bezmienowa. Dodatkowo wzorzec został zestawiony z teorią metod pokojowych i wojennych Świniarskiego.

ABSTRACT

Within the framework of the dissertation, a pattern of impacts of information operations on the security of an individual (person) and a group (community) was developed and verified. Concepts related to the Polish School of Cybernetics (qualitative information theory, psychocybernetics, sociocybernetics and autonomous systems theory), as well as neo-Thomistic and Thomistic philosophy with a focus on metaphysics and philosophical anthropology, were taken as the foundation for consideration. Using systems analysis, elements of the control space (cyberspace) were distinguished, such as resources, individuals, groups and signals (information). Each of the distinguished elements was then analyzed along with possible relationships between them in terms of information operations, which consist of both interactions with resources (technical interactions) and people along with groups (psychological interactions). The mathematical theory of communication, security theories (Frei's subjective and objective security, Świniarski and Chojnacki's security theory, the instrusion kill chain model and McCumber's cube), and the Polish Armed Forces doctrinal documents on information operations and cyber operations were used as supporting sources. The pattern was verified by comparing it to the model of subversion described by Bezmienov. In addition, the pattern was juxtaposed with Świniarsky's theory of peace and war methods.

Spis treści

WSTĘP

W literaturze naukowej pojawiają się ujęcia związane z oddziaływaniem informacji na bezpieczeństwo ujmowane zarówno przedmiotowo, jak i podmiotowo przy wykorzystaniu różnych teorii, natomiast w żadnym z nich nie wytworzono ogólnego wzorca teoretycznego (systemu teoretycznego wyprowadzonego z dedukcji, a następnie porównanego z empirią) korzystając jednocześnie z ujęcia cybernetycznego i filozoficznego. Dzięki takiemu układowi dziedzin możliwe będzie zarówno zdefiniowanie każdego z elementów (systemów) biorących udział w operacjach informacyjnych (zarówno po stronie atakujących, jak i broniących się), wskazanie ich właściwości i relacji między tymi systemami, co pozwoli na dogłębną analizę problemu wyrażonego w temacie pracy.

Zgłębienie tematu opierające się na powyższych ujęciach wydaje się potrzebne, gdyż wokół operacji informacyjnych (nazywanych również innymi, pokrewnymi terminami, takimi jak wojna informacyjna, walka informacyjna etc.) narastają wielkie emocje, pod których wpływem niektórzy autorzy szukają pewnych nowości i rewolucji w zjawiskach, które de facto trwają od początku istnienia ludzkości. Człowiek od kiedy tylko istnieje posługuje się informacją. W dziedzinie wojskowej Sun Tzu, w swojej Sztuce Wojny napisanej w VI wieku przed Chrystusem, opisywał użyteczność opłacanych szpiegów, których celem miało być zdobywanie informacji[1]. Juliusz Cezar posługiwał się tzw. szyfrem Cezara, aby uczynić przekaz swoich wiadomości trudnym lub niemożliwym do odczytania przez tych, którzy nie znali klucza lub zasady działania algorytmu szyfrującego[2]. Opis próby osłabienia morale przeciwnika występuje e.g. w Starym Testamencie, gdzie zawarta jest mowa wysłannika króla asyryjskiego do oblężonych obrońców Jerozolimy (w VIII wieku przed Chrystusem), wygłoszona w celu nakłonienia ich do poddania się[3]. Operacje informacyjne zatem nie są pewną, nową jakością dzisiejszych czasów, a ilościową zmianą akcentu z wojen

1 v. Sun Tzu, *Sztuka wojny*, in: *Sztuka wojny*, B. Oczko (red.), Helion, Gliwice 2014, p. 92-93.
2 v. G. Trankwillus, *Żywoty cezarów*, Zakład Narodowy im. Ossolińskich, Wrocław 1960, p. 37. Warto dodać, iż tzw. szyfr Cezara jest możliwy do złamania z pomocą względnie prostych metod z dziedziny kryptoanalizy.
3 2 Krl 18, 17-37.

wykorzystujących oddziaływania kinetyczne (energomaterialne) w stronę wykorzystania oddziaływań informacyjnych.

Analizowanie tematu operacji informacyjnych musi zatem odbywać się z użyciem metod, które pozwalają konkretnie, jak najbardziej jednoznacznie, rzetelnie i trafnie opisać zjawiska związane z oddziaływaniem informacyjnym. Polska Szkoła Cybernetyki (PSC) zaproponowała metodę, która ma na celu integrować naukę pod czujnym okiem cybernetyki[4] lub metacybernetyki[5]. Skorzystanie z dostępnych wzorców teoretycznych opracowanych w ramach PSC (teorii systemów, jakościowej teorii informacji, psychocybernetyki i socjocybernetyki) i pewne ich zaktualizowanie z wykorzystaniem filozofii neotomistycznej (przy wykorzystaniu metafizyki, antropologii filozoficznej i etyki) pozwoli na całościowe ujęcie tematu rozprawy na zadanym poziomie ogólności. Wybór ograniczonej liczby źródeł jest podyktowany tym, że z każdej teorii mogą wynikać wnioski, które mogą być (i takie też bywają) sprzeczne z wnioskami, które zostały wyciągnięte na podstawie innych źródeł. Zatem, aby efektem końcowym był wzorzec teoretyczny służący do oceny bezpieczeństwa jednostek i grup pod kątem oddziaływań informacyjnych należy podjąć decyzje projektowe, które źródła zostaną wykorzystane i w jaki sposób. Praca zatem nie ma charakteru opisania wszystkich, czy nawet większości, teorii związanych z bezpieczeństwem jednostek, grup i oddziaływań informacyjnych, ale przeprowadzenia analizy narzędziami przyjętymi a priori.

Problemem jednak jest w jaki sposób egzemplifikować uzyskany wzorzec i wykazać jego właściwości prognostyczne i diagnostyczne. Dodatkową trudnością jest ogólny charakter rozważań, który obejmuje jednocześnie oddziaływania psychologiczne i techniczne, na poziomie pojedynczej jednostki, jak i całych grup. Wykorzystanie metafizyki będącej częścią tomizmu pozwoli na opisanie zależności między bytami w cyberprzestrzeni (rozumianej szeroko jako przestrzeń sterowania), jak i właściwości samych tych bytów, a więc uznanie, które są pierwotne (realne, samodzielne, istniejące niezależnie od myśli), a które są

4 v. M. Mazur, *Cybernetyka i charakter*, Państwowy Instytut Wydawniczy, Warszawa 1976, p. 2-15.
5 v. J. Kossecki, *Metacybernetyka*, Narodowa Akademia Informacyjna, Warszawa 2015, p. 8-10.

wtórne do rzeczywistości (myślne, które są tylko umysłowym ujęciem pewnego wycinka rzeczywistości). Z punktu widzenia cybernetyki i analizy systemowej nie ma rozróżnień między bytami realnymi i myślnymi, zatem bez dodatkowych założeń metafizycznych nie jest możliwe określenie prymatu jednego systemu nad drugim. Uznanie człowieka za główne odniesienie w poniższej pracy pozwala na skupienie wysiłków egzemplifikacji właśnie na człowieku, gdyż od jego bezpieczeństwa będzie zależało bezpieczeństwo wszystkich innych rodzajów systemów w cyberprzestrzeni. Dodatkowo sam tomizm posiada obok metafizyki również antropologię filozoficzną, która zawiera w sobie etykę. Zarówno metafizyka i etyka będą cennym uszczegółowieniem i weryfikacją wzorca.

Sposobem egzemplifikacji wzorca będzie porównanie wzorca z modelem dywersji ideologicznej KGB opisanej przez Bezmienowa, który był z powodzeniem wykorzystywany w praktyce. Zatem jeśli wzorzec teoretyczny wykaże zgodność z tym modelem, to zostanie to uznane za skuteczną egzemplifikację. A sam wzorzec bezpieczeństwa za wiarygodny.

Problemem jest również wykorzystanie samej cybernetyki wraz z neotomizmem do tworzenia wzorca ze względu na niedostateczny stan tych nauk w kontekście teorii bezpieczeństwa jako takiego i brak w nich terminu operacji informacyjnych. Dlatego też zostaną wykorzystane dodatkowe koncepcje takie jak teoria bezpieczeństwa Świniarskiego i Chojnackiego (de facto arystotelesowsko-tomistyczna ze względu na użyte do jej tworzenia źródła) lub teoria bezpieczeństwa subiektywnego i obiektywnego Freia. Operacje informacyjne zostaną opisane według dokumentów doktrynalnych SZ RP – DD 3.10 (A) o operacjach informacyjnych i DD 3.20 o operacjach w cyberprzestrzeni. Dodatkowymi źródłami będą również modele z zakresu bezpieczeństwa informacyjnego jak intrusion kill chain, kostka bezpieczeństwa McCumbera i podstawy kryptologii. W pracy wykorzystano również matematyczną teorię komunikacji Shannona i Weavera.

Struktura pracy składa się z pięciu rozdziałów. Pierwszy z nich opisuje metodologię badań, przedstawia cel główny, cele utylitarne i poznawcze, pytania

badawcze i hipotezy. Przedstawione są w nim również źródła badawcze (cybernetyka, filozofia neotomistyczna i źródła pomocnicze). Rozdział drugi dotyczy ogólnych właściwości systemów i zawiera rozważania związane z systemami w kontekście metafizyki, ogólne oddziaływania między systemami, wyróżnia rodzaje systemów, ich parametry takie jak moc, energia, współczynnik swobody, stany systemów i kończy się opracowaniem zbioru możliwości systemów w cyberprzestrzeni. Trzeci rozdział dotyczy systemów w cyberprzestrzeni i dzieli się na rozważania dotyczące systemów substancjalnych (jednostki) i myślnych, nazwanych addycyjnymi (grup i zasobów). W ramach tego rozdziału opisany został proces poznawczy i decyzyjny jednostki wraz z aktualizacją wzorca psychocybernetycznego Mazura, jak i zasoby, grupy i relacje między nimi. Czwarty rozdział dotyczy bezpieczeństwa systemów (głównie jednostek) w cyberprzestrzeni i bezpieczeństwa komunikatów (informacji). W rozdziale piątym opisano zagadnienie operacji informacyjnych, wzorzec bezpieczeństwa cyberprzestrzeni (jednostek, grup, zasobów i komunikatów) wobec operacji informacyjnych, porównanie wzorca do metody pokojowej i wojennej Świniarskiego i Chojnackiego, a w końcowej części rozdziału również do modelu dywersji ideologicznej KGB.

Rozdział I.
METODOLOGIA BADAŃ

„Nie ma nic bardziej praktycznego niż dobra teoria”
K. Lewin

W ramach pierwszego rozdziału opisano proces zgłębiania tematu niniejszej rozprawy. Informacje uzyskane z analizy źródeł zostaną opracowane za pomocą metod i narzędzi badawczych, aby móc osiągnąć założone cele badań. Autor nie porusza się w ugruntowanym paradygmacie naukowym w ramach nauk społecznych[6], więc poszczególne elementy niniejszego rozdziału zostaną proporcjonalnie do potrzeby rozbudowane. Co więcej, autor ma świadomość, że zupełnie naturalnym jest zjawisko tzw. zaślepienia teoretycznego, które objawia się kurczowym trzymaniem się systemów teoretycznych, które są wyznawane, nawet pomimo naocznych dowodów (kontrprzykładów), na to, że nie są prawdziwe, a przynajmniej mniej prawdopodobne, niż się to powszechnie przyjmuje[7]. Dodatkowo badacze mogą zupełnie nie zdawać sobie sprawy z tego, że przyjmują pewien paradygmat i związane z nim założenia zarówno filozoficzne, jak i metodologiczne[8].

Aby ustrzec się tych błędów wymagane jest, aby opisać założenia ujęć, na których opiera się praca, czyli filozofii neotomistycznej i koncepcji Polskiej Szkoły Cybernetyki. Finalna synteza (wzorzec teoretyczny) zostanie porównany z modelem dywersji ideologicznej opisanej przez Bezmienowa, aby zweryfikować

6 Paradygmat jest tutaj rozumiany za Kuhnem jako dorobek działalności szkoły, który jest atrakcyjny i oryginalny, a do tego pozostawia pewne problemy do rozwiązania. W paradygmacie danej szkoły mieszczą się zarówno prawa, teorie, ich zastosowania, jak i narzędzia techniczne. cf. T. Kuhn, *Struktura rewolucji naukowych,* Państwowe Wydawnictwo Naukowe, Warszawa 1968, p. 26-27. Nauki o bezpieczeństwie są relatywnie młodą dziedziną, zatem autor nieskromnie pozwala sobie na pewne innowacje w tej materii (i formie).

7 v. D. Kahneman, *Pułapki myślenia. o myśleniu szybkim i wolnym*, Media Rodzina, Poznań 2012, p. 367-368.

8 v. B. Sławecki, *Znaczenie paradygmatów w badaniach jakościowych,* in: *Badania jakościowe. Podejścia i teorie*, vol. 1, D. Jemielniak (red.), Wydawnictwo Naukowe PWN, Warszawa 2012, p. 60.

użyteczność uzyskanej koncepcji. Powyższe zjawiska wymuszają, aby cała praca miała charakter sekwencyjny, tak aby, uczynić zadość słowom św. Tomasza z Akwinu do jego współbrata Jana – „Nie nurkuj prosto do oceanu wiedzy. Toruj sobie drogę mniejszymi strumieniami. Najlepiej jest zaczynać od rzeczy łatwiejszych i dopiero potem zajmować się trudniejszymi.”[9]. Każdy skrót myślowy może prowadzić do niezrozumienia przekazu, zatem wydaje się, że szczegółowe i dokładne opisanie każdego elementu pracy jest konieczne dla prześledzenia myśli autora, tak aby dyskutowanie wyników tejże pracy odnosiło się do meritum, a nie do pewnej wymiany skojarzeń. Według najlepszej wiedzy autora nie próbowano łączyć jednocześnie ujęcia Polskiej Szkoły Cybernetyki i ujęcia (neo)tomistycznego.

1.1. Cele badań

W pracy wyróżniono cel główny, jak i cele poznawcze i utylitarne. Celem głównym jest opracowanie wzorca teoretycznego oddziaływania operacji informacyjnych na bezpieczeństwo jednostek i grup w cyberprzestrzeni[10]. Biorąc pod uwagę cel głowny można postawić główne pytanie badawcze: „Czy możliwe jest opracowanie wzorca teoretycznego oddziaływania operacji informacyjnych na bezpieczeństwo jednostek i grup w cyberprzestrzeni?”.

Do celów poznawczych należą:

1 Identyfikacja systemów w cyberprzestrzeni (jednostki, grupy, zasoby, komunikaty).
2 Ustalenie elementów zawierających się w zidentyfikowanych systemach (ustalenie, czy któreś z systemów zawierają się w innych, czyli czy są nadsystemami albo podsystamami innych systemów).
3 Ustalenie właściwości systemów w cyberprzestrzeni pod kątem ich bezpieczeństwa w kontekście oddziaływania informacyjnego.

9 v. J. Cumming, *Listy świętych do grzeszników*, Instytut Wydawniczy PAX, Warszawa 2003, p. 38-39.
10 Wzorzec został w całości opisany w podrozdziale 5.2.

4 Ustalenie relacji między wyróżnionymi systemami.

W ramach celów utylitarnych można wymienić:

1 Ustalenie zupełnego katalogu możliwych zagrożeń bezpieczeństwa jednostek i grup w kontekście operacji informacyjnych na zadanym poziomie ogólności.
2 Opracowanie wzorca teoretycznego pozwalającego ocenić bezpieczeństwo jednostek i grup (własnych, jak i przeciwnika) wobec operacji informacyjnych.
3 Opracowanie wzorca teoretycznego pozwalającego przewidzieć trendy bezpieczeństwa jednostek i grup (własnych, jak i przeciwnika) wobec operacji informacyjnych.
4 Ustalenie ograniczeń uzyskanego wzorca teoretycznego (w kontekście diagnostyki i prognozy poziomu bezpieczeństwa).
5 Ustalenie możliwości poprawienia bezpieczeństwa własnych jednostek i grup w kontekście operacji informacyjnych i zmniejszenia bezpieczeństwa jednostek i grup przeciwnika.

Z powyższych celów badawczych wypływają następujące szczegółowe pytania badawcze:

1 Jakie, istotne dla bezpieczeństwa jednostek i grup, systemy i ich elementy występują w cyberprzestrzeni?
2 Jakie są właściwości systemów występujących w cyberprzestrzeni?
3 Jakie są relacje między systemami w cyberprzestrzeni?
4 Od czego zależy bezpieczeństwo jednostek i grup w ujęciu systemowym? Od jakich parametrów systemów zależy bezpieczeństwo jednostki, a od jakich parametrów systemu zależy bezpieczeństwo grup?
5 W jaki sposób można oddziaływać informacyjnie na drugi system, aby zmniejszyć jego bezpieczeństwo?

6 W jaki sposób można chronić się przed zmniejszającym bezpieczeństwo oddziaływaniem informacyjnym przeciwnika?
7 W jaki sposób diagnozować bezpieczeństwo jednostek i grup wobec operacji informacyjnych dla danego stanu systemów w cyberprzestrzeni?
8 W jaki sposób prognozować bezpieczeństwo jednostek i grup wobec operacji informacyjnych dla danego stanu systemów w cyberprzestrzeni?
9 Z jakimi ograniczeniami wiązać się będzie zarówno diagnoza, jak i prognoza bezpieczeństwa jednostek i grup wobec operacji informacyjnych?

Osiągnięcie celów badawczych i uzyskanie odpowiedzi na główne, jak i szczegółowe pytania badawcze pozwoli na zweryfikowanie następujących hipotez badawczych:

1 Opracowany wzorzec teoretyczny posiada właściwości diagnostyczne w zakresie oddziaływania operacji informacyjnych na bezpieczeństwo jednostki.
2 Opracowany wzorzec teoretyczny posiada właściwości diagnostyczne w zakresie oddziaływania operacji informacyjnych na bezpieczeństwo grup.
3 Opracowany wzorzec teoretyczny posiada właściwości prognostyczne w zakresie oddziaływania operacji informacyjnych na bezpieczeństwo jednostki.
4 Opracowany wzorzec teoretyczny posiada właściwości prognostyczne w zakresie oddziaływania operacji informacyjnych na bezpieczeństwo grup.

Krokiem do osiągnięcia celu pracy będzie uporządkowanie, głównie za pomocą analizy systemowej (rozumianej w ramach koncepcji Polskiej Szkoły Cybernetyki), zagadnień związanych z bezpieczeństwem jednostek (rozumianych jako pojedynczych ludzi) i grup (rozumianych jako wspólnoty ludzkie) wobec oddziaływań na ich tor informacyjny. Poza ujęciem Polskiej Szkoły Cybernetyki zostaną użyte, teorie z zakresu filozofii (neo)tomistycznej (głównie antropologii

filozoficznej i metafizyki) oraz, w charakterze pomocniczym, matematyczna teoria komunikacji, teoria bezpieczeństwa Świniarskiego i Chojnackiego i opis operacji informacyjnych według DD SZ RP, które będą miały na celu pogłębienie koncepcji Polskiej Szkoły Cybernetyki i wskazanie rozbieżności ujęć. Efektem końcowym będzie wypracowanie wzorca przeprowadzania operacji informacyjnych w cyberprzestrzeni ze szczególnym uwzględnieniem parametru bezpieczeństwa, wraz ze wskazaniem mocnych i słabych stron takiego ujęcia, które pozwoli na dalsze badania nad zagadnieniem.

1.2. Źródła i narzędzia badawcze

Jak zostało już wcześniej wspomniane, praca będzie opierała się na trzech filarach – cybernetyce (ze szczególnym uwzględnieniem Polskiej Szkoły Cybernetyki), filozofii (neo)tomistycznej i źródłach pomocniczych (matematycznej teorii komunikacji, dokumentach doktrynalnych Sił Zbrojnych RP i wybranych ujęciach z zakresu bezpieczeństwa).

1.2.1. Cybernetyka

Początki cybernetyki sięgają już starożytności. Sama nazwa cybernetyka pochodzi z języka greckiego (gr. κυβερνήτης) i oznacza sternika[11]. Platon w swoim Gorgiaszu, ustami Sokratesa, opisuje ją jako tę, która „chroni od największych niebezpieczeństw nie tylko dusze, lecz również ciała i dobytek”[12]. Trentowski cybernetykę określa jako „trudną sztukę rządzenia narodem”[13] i stawia ją, obok teologii, jako jedną z dwóch „potężnych pań gminu”, które są wiedzione przez filozofię idącą naprzód „z rozpaloną pochodnią w ręku”[14]. Z kolei Ampère zalicza cybernetykę do części polityki odpowiedzialną za metody rządzenia[15]. Wiener,

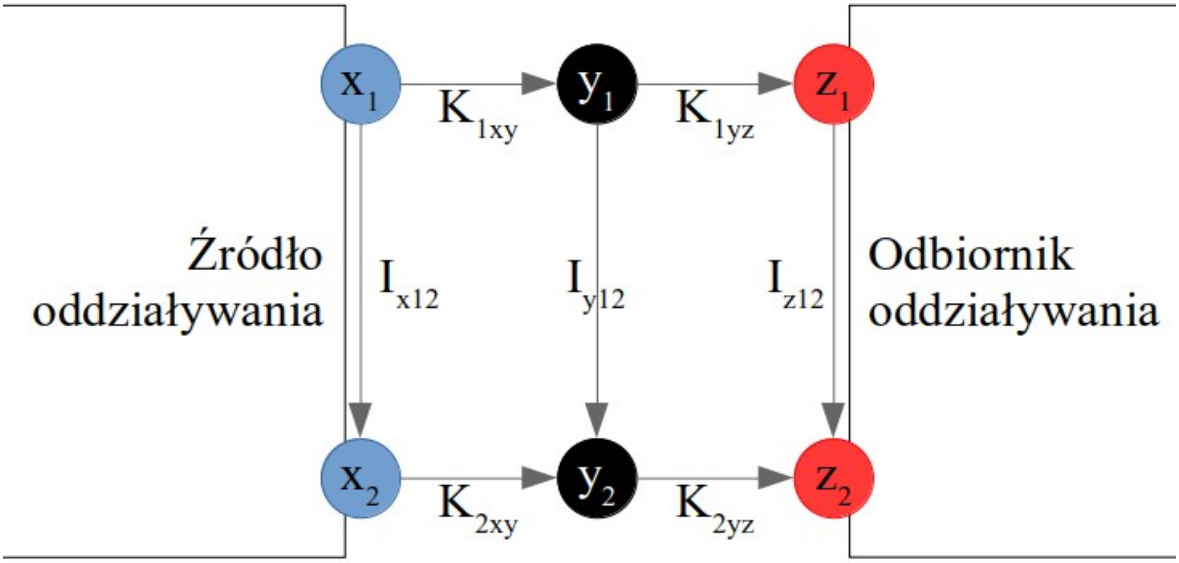
11 v. N. Wiener, *Cybernetyka, czyli sterowanie i komunikacja w zwierzęciu i maszynie*, Państwowe Wydawnictwo Naukowe, Warszawa 1971, p. 35.
12 v. M. Mazur, *Cybernetyka a zarządzanie*, Ministerstwo Spraw Wewnętrznych Departament Szkolenia i Wydawnictw, Warszawa 1969, p. 7.
13 v. B. Trentowski, *Stosunek filozofii do cybernetyki*, PWN, Warszawa 2014, p. 10.
14 cf. ibid., p. 203-204.
15 v. M. Mazur, *Cybernetyka a zarządzanie*, op. cit, p. 7;

który jest uważany za twórcę współczesnej cybernetyki jako nauki[16], określał tę dziedzinę jako „teorię sterowania i komunikacji w maszynach i zwierzętach”[17]. Wchodząc na wyższy poziom ogólności, Mazur określał cybernetykę jako „naukę o sterowaniu”[18]. W takim też znaczeniu będzie w pracy używany termin cybernetyka ze względu na przyjęty paradygmat związany z PSC.

W ramach Polskiej Szkoły Cybernetycznej została opracowana koncepcja metodologiczna oparta na wzorcach teoretycznych i modelach teoretycznych. Aby móc przeanalizować zagadnienie modeli i wzorców teoretycznych należy najpierw zdefiniować pojęcia komunikatu, oryginału, obrazu i informacji. Komunikat jest „stanem fizycznym różniącym się w określony sposób od innych stanów fizycznych w torze sterowniczym”[19]. Obraz jest zakodowanym oryginałem. Różnica między nimi jest taka, że oryginał jest komunikatem generowanym przez system, który oddziałuje na inny system, a obraz jest komunikatem odbieranym przez inny system, na który się oddziałuje[20]. Przykładem obrazu może być kartka papieru, na której zapisuje się pewne zdania (oryginał), które są odczytywane przed pewną osobę i pojawiają się w jej umyśle jako myśli (obraz). Inaczej można powiedzieć, że oryginał jest na wejściu toru sterującego, a obraz na jego wyjściu. Idąc dalej – transformacja jednego komunikatu w drugi w poprzecznym zbiorze komunikatów w torze sterowania nazywana jest informacją[21], gdzie „poprzeczny zbiór komunikatów” należy rozumieć jako zbiór komunikatów znajdujących się w dowolnym miejscu toru sterującego[22]. Przykładem poprzecznego zbioru komunikatów może być aktualny stan pamięci człowieka lub komputera, znaki topograficzne na mapie lub fala akustyczna rozchodząca się w powietrzu. Można te pojęcia zobrazować na poniższym rysunku:

---

16 cf. P. Sienkiewicz, *Poszukiwanie golema*, Krajowa Agencja Wydawnicza, Warszawa 1988, p. 11-14.
17 v. N. Wiener, op. cit., p. 35.
18 v. M. Mazur, *Cybernetyka i charakter,* op. cit., p. 7.
19 v. M. Mazur, *Jakościowa teoria informacji*, Wydawnictwo Naukowo Techniczne, Warszawa 1970, p. 34.
20 cf. ibid., p. 33-35.
21 cf. ibid., p. 70.
22 cf. ibid., p. 35.



Rys. 1: Komunikat, informacja i kod

źródło: opracowanie własne na podstawie: M. Mazur, *Jakościowa...*, op. cit.

Na rysunku koła symbolizują komunikaty. Kolorem czarnym oznaczono specjalny rodzaj komunikatów nazywany interkomunikatami. Na niebiesko zostały oznaczone oryginały, a na czarno i czerwono obrazy, które nie są interkomunikatami. Literą I oznaczono transformacje w poprzecznym torze sterowania, czyli informacje. Literą K oznaczono transformacje w podłużnym torze sterowania, czyli kody. x_1 i x_2 są wyjściem źródła oddziaływania, a z_1 i z_2 wejściem odbiornika oddziaływania.

Twierdzenia są informacjami w zbiorze obrazów[23]. Wynika z tego, że twierdzenie jest zawsze wtórne wobec oryginału. Dla przykładu, jeśli jakiś przedmiot oddziałuje na człowieka odbijając w stronę jego oczu wiązki fotonów, to dochodzi do pewnego kodowania oryginałów w obrazy. Oryginałem jest sam przedmiot (jego wygląd), a obraz, który powstaje w umyśle człowieka pod wpływem światła jest obrazem. Równie dobrze obrazem może być książka lub plik tekstowy zawierający zapis teorii naukowej w jakimś języku. Idąc dalej, w ramach

23 v. J. Kossecki, *Metacybernetyka*, op. cit., p. 39.

Polskiej Szkoły Cybernetyki nauka posiada twierdzenia oraz procedury dowodowe[24]. Aby zweryfikować prawdziwość danego twierdzenia należy zweryfikować czy informacje w zbiorze obrazów są zgodne z informacjami w zbiorze oryginałów pierwotnych (czyli faktów obiektywnie istniejących). Przyjęte (świadomie lub nie) przez badacza założenia ontologiczne wpływają na to jakie byty przyjmuje się za oryginały pierwotne[25]. Oznacza to, że inne założenia filozoficzne (inny paradygmat), przyjęte na samym początku danej rozprawy, mogą dawać różne wyniki. w tym miejscu warto odwołać się do przykładu przedmiotu jako oryginału. Dla pewnych ujęć filozoficznych oryginałem pierwotnym może być dopiero umysłowa reprezentacja danego przedmiotu, a nie sam przedmiot. z tego też powodu szczególnie istotne wydaje się wyakcentowanie z jakich zasad ontologicznych (metafizycznych) wychodzi dany autor.

W przypadku procedur dowodowych można wyróżnić procedury empiryczne i teoretyczne. Empiryczne polegają na badaniu zbioru oryginałów (w dużej mierze za pomocą indukcji), a teoretyczne – zbioru obrazów (korzystając z dedukcji). Jeśli dana teoria (rozumiana jako zbiór twierdzeń) spełnia postulaty definicyjne zbioru oryginałów i relacji między nimi, to jest modelem teoretycznym. Proces tworzenia modeli teoretycznych nazywa się teoretycznym modelowaniem. Jeśli dochodzi do sytuacji odwrotnej, a więc do tego, iż zbiór oryginałów i relacji między nimi spełnia postulaty definicyjne wcześniej opracowanej teorii (wypracowanej za pomocą dedukcji), wtedy teoria jest wzorcem teoretycznym, a sam proces dowodzenia wzorca nazywa się egzemplifikacją. Egzemplifikację przeprowadza się za pomocą metod empirycznych. Jeśli twierdzenia zawarte w teorii spełniają warunki ogólności (dane informacje są powtarzalne, typowe), intersubiektywnego komunikowania (możliwe jest takie zakodowanie informacji, aby była możliwość zaznajomienia się z nimi i ich zrozumienia przez inne osoby) i sprawdzalności (możliwa jest weryfikacja prawdziwości danych informacji za pomocą

24 v. ibid., p. 40.
25 cf. ibid., p. 37.

teoretycznych lub empirycznych procedur dowodowych), to można powiedzieć, że dana teoria jest teorią naukową[26].

Zaletą wzorców teoretycznych jest to, że na ich podstawie możliwe jest stworzenie tzw. mocnych teorii, czyli teorii, które potrafią przewidywać informacje, które nie zostały do tej pory stwierdzone empirycznie. Dzieje się tak, gdyż teoria oparta na modelowaniu teoretycznym jest przedstawieniem rzeczywistości (zbioru oryginałów i relacji między nimi) w uproszczony sposób (ograniczając się do właściwości, które wybrał badacz), a więc nie dodaje niczego dodatkowego do opisu rzeczywistości. Wzorzec teoretyczny nie posiada takiego ograniczenia. Jedynym warunkiem jest egzemplifikacja, czyli znalezienie takiego systemu w rzeczywistości, który spełnia postulaty definicyjne wzorca lub takiego, którego dotyczą twierdzenia wynikające z postulatów definicyjnych wzorca teoretycznego. Tym sposobem również wszystkie właściwości wydedukowane z postulatów definicyjnych będą dotyczyły również i wyegzemplifikowanego systemu, co może wykraczać poza dotychczasowe badania empiryczne[27].

Celem pracy jest opracowanie wzorca teoretycznego, a więc pewnego systemu teoretycznego, który został wyprowadzony za pomocą dedukcji z założonych źródeł (głównie z koncepcji Polskiej Szkoły Cybernetyki i neotomizmu oraz źródeł pomocniczych), a następnie sprawdzony (wyegzemplifikowany) przez porównanie z modelem dywersji ideologicznej KGB. Na wzorzec bezpieczeństwa jednostek i grup wobec operacji informacyjnych składają się kryteria bezpieczeństwa jednostki, z których wynikają kryteria bezpieczeństwa grup, zasobów i komunikatów, a co zostało wymienione, opisane i wyjaśnione w podrozdziale 5.2. Wykorzystanie wzorca pozwoli w pewnym zakresie (na zadanym poziomie ogólności) na diagnozę i prognozę bezpieczeństwa zarówno jednostek, jak i grup. Egzemplifikacja zostanie przeprowadzona przez odwołanie się do modelu dywersji ideologicznej KGB Bezmienowa i porównanie uzyskanych koncepcji do tego modelu, który był wykorzystywany z powodzeniem w praktyce.

---

26 cf. ibid., p. 40-44.
27 cf. ibid., p. 41-45.

1.2.2. Filozofia neotomistyczna

Filozofia jest dziedziną, która potrafi wzbudzić wiele emocji również w środowisku naukowym. Z jednej strony nie przez każdego jest uważana za naukę, ale coś ponad lub pod nią. Istnieją ujęcia, w których uznaje się, że celem filozofii jest rozjaśnianie myśli, a nie wytwarzanie tez filozoficznych[28]. Pojawiają się również ujęcia deprecjonujące filozofię twierdzące, że jest to albo zbiór twierdzeń, których jeszcze nie można zbadać naukowo[29], albo pewna nieracjonalna (lub wręcz nadracjonalna) sztuka pisarska, poezja[30]. Z drugiej strony filozofia rozumiana jest jako nauka uniwersalna, która korzysta z każdej dostępnej metody, uwzględniając dosłownie każdą dziedzinę. Zajmuje się jednocześnie zagadnieniami fundamentalnymi i granicznymi[31]. Co interesujące, zjawisko wydzielania i usamodzielniania się od filozofii wielu dziedzin nauki, nie prowadzi do ograniczania rozważań filozoficznych, ale skutkuje tworzeniem się kolejnych dziedzin filozofii[32]. Jako przykład tego zjawiska można podać e.g. filozofię bezpieczeństwa. Wyjątkiem w tej tendencji jest ontologia (metafizyka) i filozofia badająca wartości same w sobie (aksjologia). Obydwie te dziedziny nie posiadają swojego odpowiednika w innych dziedzinach nauki[33].

W ramach filozofii wyróżnia się dwa główne działy, którymi są teoria bytu (zwana też metafizyką) i teoria poznania (epistemologia, gnozeologia). Wszelkie inne działy filozoficzne są pewnym uszczegółowieniem tych dwóch. Z metafizyki wypływa antropologia filozoficzna[34], która, obok metafizyki, szczególnie zostanie

---

28 cf. L. Wittgenstein, *Tractatus logico-philosophicus*, Wydwanictwo Naukowe PWN, Warszawa 2012, p. 27: „Myśli skądinąd mętne i niewyraźne filozofia ma rozjaśnić i ostro odgraniczyć.”.
29 cf. J. Bocheński, *Ku filozoficznemu myśleniu,* Instytut Wydawniczy PAX, Warszawa 1986, p. 14-15. w tym miejscu warto zacytować fragment ze strony 15: „Już Arystoteles przeciwstawił przeciwnikom filozofii następujące rozumowanie: albo należy filozofować, albo nie należy filozofować; ale jeżeli nie należy filozofować, to tylko w imieniu filozofii. a więc nawet jeśli nie należy filozofować, należy filozofować. i to jest prawdą do dziś.”.
30 cf. ibid., p. 15-17.
31 cf. ibid., p. 20: „Tak rozumiała filozofię większość wielkich filozofów wszystkich czasów. Nauka a nie twórczość pisarska, nie muzyka, lecz poważne, trzeźwe badania. Nauka uniwersalna w tym sensie, że nie wyklucza żadnej dziedziny i korzysta z każdej dostępnej metody. Nauka o zagadnieniach granicznych i o podstawach - czyli nauka radykalna, która nie zadowala się założeniami innych dyscyplin, lecz pragnie badać dalej - dotrzeć do samych korzeni.”.
32 cf. ibid., p. 19.
33 cf. ibid., p. 20.
34 cf. A. Stępień, *Elementy filozofii*, Redakcja Wydawnictw KUL, Lublin 1982, p. 56.

zaakcentowana w tej pracy ze względu na potrzebę przebadania właściwości zarówno jednostki (człowieka jako takiego), jak i grupy (której człowiek jest częścią). Aby zgłębić byty należy odnieść się do ich przyczyn (łac. principia), a więc do tego co wyjaśnia dlaczego dany byt jest tym czym jest (czyli do jego przyczyn wewnętrznych) i zewnętrznych przyczyn jego powstania (jeśli jest bytem przygodnym). Dzięki czemu możliwe jest rozumowe uchwycenie danego bytu[35]. Co więcej w ramach filozofii umysłu, która daje podstawę pod rozważania nauk społecznych (psychologii, socjologii czy nauk o bezpieczeństwie), wciąż występuje spór dotyczący relacji między umysłem a ciałem (ang. mind-body problem)[36], w którym neotomizm bierze czynny udział prezentując Tomaszowy wariant hylemorfizmu (poglądu, że człowiek jest jednością duchowo-cielesną)[37], który jest konkurencyjny wobec kartezjańskiego dualizmu i różnych wariantów monizmu (materializmu, mentalizmu, teorii identyczności)[38]. Zatem nie da się zrozumieć jednostki i grupy bez metafizyki.

Metafizyka i antropologia filozoficzna będą głównie opisywane w duchu filozofii tomistycznej i neotomistycznej. Neotomizm jest współczesnym tomizmem. Wywodzi się od św. Tomasza z Akwinu działającego w XIII wieku po Chrystusie. Nawiązuje do tradycji ruchu perypatetyckiego (Arystotelesa)[39] szczególnie akcentując metafizykę jako fundament swoich badań. Neotomizm nie jest jednak jednolitym ruchem. Jedną ze szkół tomistycznych jest tomizm egzystencjalny zapoczątkowany przez Maritaina i Gilsona, którzy odkryli, niezauważone przez wieki, ubogacenie przez Akwinatę metafizyki Arystotelesowskiej o akt istnienia, który stał się podstawą do wyróżnienia nowego złożenia subontycznego.

35 cf. T. Stępień, *Wprowadzenie do antropologii filozoficznej św. Tomasza z Akwinu*, Warszawskie Towarzystwo Teologiczne, Warszawa 2013, p. 16.
36 cf. A. Grobler, L. Koczanowicz, *Elementy filozofii dla psychologów*, in: *Psychologia podręcznik akademicki*, vol. 1, J. Strelau, D. Doliński (red.), Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2008, p. 42.
37 cf. M. Zembrzuski, *Problem mind-body w świetle Tomaszowej koncepcji hylemorfizmu*, in: *Rocznik tomistyczny*, 7 (2018), p. 163-164.
38 cf. J. Kalat, *Biologiczne podstawy psychologii*, Wydawnictwo Naukowe PWN, Warszawa 2006, p. 5.
39 z tego też powodu w pracy będą wykorzystywane również koncepcje Arystotelesa ze Stagiry, z których korzystał sam św. Tomasz z Akwinu, jak i neotomiści.

Zwolennicy tej szkoły niechętnie przyznają niezależność teorii poznania od metafizyki. Jej głównym ośrodkiem w Polsce jest Katolicki Uniwersytet Lubelski[40].

Inną odmianą neotomizmu jest szkoła tomizmu konsekwentnego zapoczątkowana przez Gogacza[41]. Jej głównymi założeniami jest realizm poznawczy (uznanie, że rzeczywistość istnieje niezależnie od naszego postrzegania), metafizyka jako punkt wyjścia do wszelkich rozważań, postulowanie pluralistycznego sposobu istnienia bytów (istnienia jakościowych różnic między gatunkami e.g. pomiędzy człowiekiem, a psem lub rośliną), rozróżnienia przyczyn i skutków, wiedzy i bytu, stwarzania i tworzenia, wartości i własności, monizmu i pluralizmu, ujęć genetycznych i strukturalnych, pryncypiów i bytu w sobie. Co więcej badania w tomizmie konsekwentnym wychodzą od przyczyn i substancji (zamiast wartości i celów), a przyczyny są ustalane za pomocą porządku istotowego a więc związanego z tym czym byt jest. Tomizm konsekwentny dąży do doprecyzowania tomizmu egzystencjalnego, oczyszczenia tekstów Akwinaty z twierdzeń Awicenny, odróżnienia metafizyki Arystotelesa od Tomaszowej oraz rozróżnienia i niemieszania różnych odmian tomizmu ze sobą w poszczególnych twierdzeniach i zagadnieniach[42].

W pracy wykorzystano rozwiązania wypracowane z jednej strony przez św. Tomasza z Akwinu (oczyszczonego z wpływów arabskich i pogańskich filozofów), jak i szkołę tomizmu konsekwentnego. Identyfikacja bytów istotnych z punktu widzenia operacji informacyjnych i ich wpływu na jednostki i grupy i ustalenie sposobu ich bytowania dało podstawę teoretyczną pod podział rzeczywistości na systemy i podsystemy w ramach analizy systemowej. W aspekcie związanym z celem jednostki i grupy autor wykorzystał elementy teologii tomistycznej zamiast filozofii ze względu na to, że użyta w pracy teoria bezpieczeństwa (Świniarskiego i Chojnackiego) powołuje się na traktat teologiczny Akwinaty O władzy, w którym poruszono zagadnienia stricte teologiczne. Wybór teologii tomistycznej w ujęciu celu jednostek i grup został dodatkowo uargumentowany źródłami pomocniczymi.

40 cf. A. Stępień, op. cit., p. 104-107.
41 v. A. Andrzejuk, M. Zembrzuski, *Mieczysław Gogacz jako twórca tomizmu konsekwentnego*, in: *Opera philosophorum Medii Aevi*, 11 (2012)., p. 22.
42 v. ibid., p. 19-20.

1.2.3. Źródła pomocnicze

Wśród pozostałych źródeł uzupełniających do opisania bezpieczeństwa jednostek i grup wykorzystano matematyczną teorię komunikacji i teorie związane z bezpieczeństwem subiektywnym i obiektywnym, opis efektów możliwości i pewności, wraz z teorią bezpieczeństwa Świniarskiego i Chojnackiego opracowaną na podstawie źródeł tomistycznych. Wykorzystano również modele intrusion kill chain i kostki bezpieczeństwa McCumbera wraz z podstawowymi koncepcjami kryptologii do opisu bezpieczeństwa komunikatów (informacyjnego). Operacje informacyjne zostały opisane zgodnie z dokumentami doktrynalnymi SZ RP 3.10 (A) dotyczącego operacji informacyjnych i 3.20 dotyczącego operacji w cyberprzestrzeni. W aspekcie tez poruszanych w ramach teologii tomistycznej powołano się na podział podejść w ramach psychologii religii. W części dotyczącej operacji informacyjnych wykorzystano koncepcję związaną z psychologią wojskowości odnoszącą się do wpływu posiadanej broni na morale.

1.3. Metody badawcze

Główną metodą badawczą w pracy jest analiza i krytyka piśmiennictwa. Podstawą analiz są wytworzone wzorce teoretyczne w ramach Polskiej Szkoły Cybernetyki, które będą sukcesywnie rozbudowywane i weryfikowane w oparciu o inne, już wymienione źródła. Do głównych problemów jakie wystąpiły w pracy należą rozbieżności terminologiczne. Każda szkoła poruszająca się w ramach swojego paradygmatu wypracowuje z czasem swój własny słownik. Tak też się stało w przypadku filozofii (neo)tomistycznej. Co więcej w źródłach dodatkowych mogą pojawić się fragmenty tekstów, które pisane są językiem potocznym, bez dbałości o konsekwentne używanie terminów i definicji (o ile takie się kiedykolwiek pojawiły). Sprawia to, że wymagane jest, aby z takiego tekstu zidentyfikować istotę danego zjawiska i porównać ją do koncepcji PSC lub neotomistycznej. Kolejnym utrudnieniem są różne charaktery tekstów – zarówno formalne, jak i nieformalne.

Jednak te przeszkody nie przekreślają użycia danych dokumentów[43]. Trud włączania niecybernetycznych źródeł do cybernetycznego trzonu będzie wymagał uzgodnienia słownika, a w niektórych przypadkach wprowadzenia nowych terminów na podstawie konwencji terminologicznej[44]. Oczywiście wszelkie dodatkowe definicje i terminy będą wprowadzane tylko i jedynie jeśli zajdzie taka potrzeba, aby, według zasady brzytwy Ochkama, nie mnożyć bytów ponad potrzebę[45].

Do metod badawczych wykorzystywanych w pracy należy również analiza systemowa (zwana również metodą systemową, ujęciem systemowym lub podejściem systemowym[46]). Mazur wymienia jej następujące zalety[47]:

- jest wolna od dowolności interpretacyjnej,
- nadaje się do analizowania systemów złożonych z dużej ilości elementów,
- umożliwia przedstawianie danych w postaci schematów cybernetycznych (co poprawia ich czytelność),
- cechuje się zwięzłością.

---

43 cf. M. Łuczewski, P. Bednarz-Łuczewska, *Analiza dokumentów zastanych*, in: *Badania jakościowe. Metody i narzędzia*, vol. 2, D. Jemielniak (red.), Wydawnictwo Naukowe PWN, Warszawa 2012, p. 164: „Nie ma bowiem żadnego powodu, żeby badacz społeczny rezygnował z cennego, a często jedynego źródła informacji. Dziś coraz częściej badacze poświęcają swoją energię nie na wytwarzanie danych, które można zdobyć, lecz na analizę i interpretację danych zebranych przez innych. Można tu wręcz mówić o prawdziwej rewolucji."; p. 184: „Dokumenty z racji olbrzymiego zróżnicowania swojej treści i formy mogą posłużyć do realizacji wszystkich podstawowych celów badania oraz analizy wszystkich sfer rzeczywistości społecznej. Zarówno dokumenty formalne, jak i nieformalne są bardzo dobrym źródłem hipotez i problemów badawczych, choć literatura pozostaje przez badaczy zdecydowanie niedoceniona.".

44 cf. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 118-119.

45 cf. K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, p. 65:

„Mając na uwadze zasadę brzytwy Ockhama, można zadać osobom używającym terminów «cybercoštam» na przykład takie pytania:

1 Dlaczego nie używać istniejącego już w naszym prawie terminu «terroryzm»? Jaki ma sens wyróżnianie cyberterroryzmu? Zakładając na roboczo, bo powszechnie uznanej definicji nie ma, że cyberterroryzm to terroryzm prowadzony w cyberprzestrzeni (cokolwiek miałoby to znaczyć) można zapytać, czy terrorystów działających na pokładach samolotów zaczniemy nazywać «aeroterrorystami» a wysyłających pocztą paczki z bombami «postterrorystami»?
2 Co to jest «atak cybernetyczny»? Atak przeprowadzony przez cybernetyków? a kto jest cybernetykiem? Członek Polskiego Towarzystwa Cybernetycznego? a może chodzi o atak prowadzony w «cyberprzestrzeni»? Jeżeli tak, to mamy «niezdefiniowane do kwadratu». (...)"

46 cf. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 47.

47 cf. ibid., p. 47-49.

Aby móc wykorzystać analizę systemową należy, w ramach jednej analizy jednoznacznie i niezmiennie określić systemy w badanym wycinku rzeczywistości. Systemy powinny być rozłączne, a podział badanej rzeczywistości zupełny[48]. Zatem wszystkie istotne, z punktu widzenia założonego problemu, byty w badanej rzeczywistości powinny zostać przydzielone do któregoś z systemów. Przy spełnieniu tych wymagań możliwe będzie określenie zbioru możliwości, a więc wszystkich rodzajów relacji między wyróżnionymi w analizie systemami[49]. Posiadanie zupełnego zbioru rodzajów relacji umożliwi ich szczegółowy opis z pewnością, że nie został przeoczony żaden fragment rzeczywistości.

Opracowywanie wzorca bezpieczeństwa jednostek i grup w cyberprzestrzeni wobec operacji informacyjnych w zakresie analizy systemowej uzupełniono o przeprowadzenie analizy ryzyka cyberprzestrzeni. Analizę ryzyka można przeprowadzić zarówno w celu zabezpieczenia własnych systemów, jak i przygotowania ataku na cudze systemy[50]. Może również dotyczyć zasobów, jak i procesów[51]. Nie istnieje jeden sposób na szacowanie (analizę) ryzyka. Jednym z kroków wyboru algorytmu analizy ryzyka jest określenie klas zmiennych, które będą używane w procesie szacowania. Zmienną można zaklasyfikować do jednej z czterech klas zmiennych[52]:

- nominalnej - w ramach, których można rozważać relację równy lub nierówny (e.g. zmienna płeć przyjmująca wartości: mężczyzna i kobieta),
- porządkowej - w ramach, których można rozważać relacje równy, nierówny, większy i mniejszy (e.g. zmienna straty przyjmująca wartości: brak, niskie, średnie i wysokie),
- przedziałowej - w ramach, których występuje umowne zero i można rozważać relacje jak przy zmiennych porządkowych, ale dodatkowo możliwe jest interpretowanie różnic między kolejnymi wartościami zmiennej

48 cf. ibid., p. 47.
49 cf. ibid., p. 49.
50 cf. G. Watson, A. Mason, R. Ackroyd, *Social Engineering Penetration Testing. Executing Social Engineering Pen Tests, Assesments and Defense*, Syngress, Coppell 2020, p. 120-122.
51 cf. K. Liderman, op. cit., p. 180.
52 cf. G. Ferguson, Y. Takane, *Analiza statystyczna w psychologii i pedagogice*, Wydawnictwo Naukowe PWN, Warszawa 2003, p. 31-32.

(w przypadku porządkowej zmiennej straty różnice między kolejnymi wartościami zmiennej nie są równe tj. różnica między wartością brak a niskie nie jest taka sama jak między średnie a wysokie. Przykładem zmiennej porządkowej może być temperatura liczona w stopniach Celsjusza, gdzie występuje umowne zero).

- stosunkowej - w ramach których występuje naturalne zero i można dodatkowo mówić o stosunku między konkretnymi wartościami zmiennej (e.g. że dana wartość jest dwa, trzy etc. razy większa lub mniejsza. Przykładem takiej zmiennej może być wartość strat wyrażona w złotówkach, gdzie wartość zero złotych jest naturalnym zerem).

W tym kluczu możliwe jest użycie zmiennych ilościowych – przedziałowych lub stosunkowych i wyrażania e.g. prawdopodobieństwa wystąpienia zagrożenia w procentach, a strat w złotówkach. z drugiej strony możliwe jest wykorzystywanie zmiennych porządkowych i określenia zarówno prawdopodobieństwa, jak i strat jako e.g. niskich, średnich lub wysokich, a samą wartość ryzyka można wyczytać z przygotowanej wcześniej macierzy ryzyka. Liczba cech (zmiennych) brana pod uwagę też nie musi ograniczać się do dwóch, ale może obejmować takie zmienne jak[53]:

- możliwość realizacji zagrożenia,
- stopień podatności,
- możliwość poniesienia szkód,
- wycena strat,
- i inne.

Z drugiej strony możliwe jest też uproszczone przeprowadzanie analizy ryzyka (wykorzystywane podczas testów penetracyjnych z wykorzystaniem socjotechniki), które polega na odpowiedzeniu na pytania[54]:

53 cf. K. Liderman, op. cit., p. 182.
54 cf. G. Watson, A. Mason, R. Ackroyd, op. cit., p. 122-124.

- Jaki zasób wziąć pod uwagę? Jaki zasób jest kluczowy dla danej organizacji lub osoby?
- Dlaczego ten zasób jest istotny?
- Kto ma do niego dostęp?
- Gdzie się znajduje dany zasób (w znaczeniu fizycznym i logicznym)?
- Jak jest aktualnie chroniony? Jak przebiega proces dostępu do danego zasobu?

Ze względu na ogólny poziom wzorca wyróżniono najistotniejsze kluczowe zasoby bezpieczeństwa cyberprzestrzeni, możliwe wektory ataku, możliwości ich wykorzystania i opisania potencjalnych skutków, które zmniejszają bezpieczeństwo danego elementu cyberprzestrzeni. Z punktu widzenia użytych klas zmiennych rozważa się w ramach prawdopodobieństwa ryzyko możliwe i niemożliwe (w ramach skali porządkowej), a straty jako istniejące lub nieistniejące (również w ramach skali porządkowej). W pracy nie korzystano z macierzy ryzyka. Z drugiej strony finalny wzorzec teoretyczny jest platformą do przeprowadzania analiz ryzyka w zakresie bezpieczeństwa jednostek, grup, zasobów i komunikatów w cyberprzestrzeni, gdyż wyróżniono konkretne kryteria, od których zależy bezpieczeństwo tych elementów, a bez których można mówić o znajdowaniu się danego systemu w stanie obiektywnego niebezpieczeństwa. Zatem dalsze badania, jak i implementacja wzorca do szczegółowych zadań umożliwia, z jednej strony, rozszerzenie skal jakościowych lub wykorzystanie skal ilościowych. W kontekście bezpieczeństwa komunikatów użyto modeli intrusion kill chain i kostki bezpieczeństwa McCumbera, które uogólniono i włączono do wzorca.

Podsumowując, w pracy zostaną użyte następujące metody badawcze:

- analiza i krytyka piśmiennictwa,
- analiza systemowa,

- analiza ryzyka systemów w cyberprzestrzeni uzupełniająca analizę systemową,
- egzemplifikacja uzyskanych wzorców teoretycznych wynikami badań w ramach źródeł uzupełniających,
- porównanie wzorca do teorii metod pokojowych i wojennych.

Do tworzenia wzorca użyto metody analizy i krytyki piśmiennictwa oraz analizy systemowej wraz analizą ryzyka. Wzorzec został sprawdzony przez porównanie do modelu dywersji ideologicznej Bezmienowa, jak i do koncepcji metod pokojowych i wojennych, aby wykazać podobieństwa i różnice i dokonać na tej podstawie egzemplifikacji samego wzorca bezpieczeństwa jednostek i grup wobec operacji informacyjnych. Porównanie odbyło się przez porównanie kryteriów bezpieczeństwa jednostek i grup do elementów modelu dywersji ideologicznej oraz teorii metod pokojowych i wojennych, jak i podstaw metafizycznych, które są podłożem przyjętych w pracy teorii.

Rozdział II.
OGÓLNE WŁAŚCIWOŚCI SYSTEMU

„Metafizyka zawsze ostatecznie grzebie swoich grabarzy”
E. Gilson

W drugim rozdziale opracowano zbiór możliwości według zasad analizy systemowej i opisano ogólne właściwości systemów. Skonfrontowanie ujęcia cybernetycznego z metafizyką uprawianą w ramach neotomizmu pozwoliło na dookreślenie właściwości systemów jako takich. Przy wykorzystaniu metafizyki dokonano zhierarchizowania systemów pod kątem ich sposobu istnienia (jako systemów substancjalnych lub systemów addycyjnych). Dzięki temu umożliwiono odpowiednie położenie akcentów w dalszych rozdziałach. Poza samymi właściwościami systemów zostały wyróżnione oddziaływania między systemami. Opisane zostały zarówno rodzaje sprzężeń, jak i sposoby informowania między systemami.

W ramach uwzględniania właściwości systemów uwzględniono możliwe ich podsystemy, z jakich mogą się składać, co pozwoliło na wyróżnienie konkretnych rodzajów systemów. Opisano zagadnienia związane z przetwarzaniem energii systemu wyróżniając współczynnik swobody i moc systemu, które służą do oceny poziomu możliwości oddziaływania danego systemu na otoczenie. Cybernetyka walki Koniecznego pozwoliła na wyróżnienie dodatkowo stanów systemu, które mogą się zmieniać w czasie oddziaływań informacyjnych zarówno wrogich, jak i własnych.

Rozdział zamknięto rozważaniami nad pojęciem cyberprzestrzeni i wyróżnieniem jej elementów istotnych z punktu widzenia oddziaływań informacyjnych. Na tej podstawie opracowano zbiór możliwości wszystkich istotnych dla tematu pracy rodzajów relacji, które występują w cyberprzestrzeni. Ich wyróżnienie zdeterminowało kolejne rozdziały pracy, a odpowiednie

usytuowanie otrzymanych relacji w metafizyce (neo)tomistycznej pozwoliło na potraktowanie ich proporcjonalnie do ich faktycznej istotności.

2.1. System a metafizyka

Zasadniczo same odwołanie się do metody analizy systemowej wymusza przyjęcie pewnych założeń terminologicznych związanych z systemami. Zatem system będzie za Mazurem rozumiany jako „zbiór elementów i relacji między nimi”[55]. Jeśli elementy w ramach pewnego systemu są również systemami, to są podsystemami tego systemu, a sam system odniesienia jest ich nadsystemem[56]. Według Mazura szukanie odpowiedzi na pytanie „Co to jest system?” jest bezzasadne, gdyż istotne jest nadanie nazwy pojęciu „zbioru elementów i relacji między nimi”, a nie szukanie znaczenia słowa system jako takiego[57]. Naturalnie, każde ujęcie związane z tym słowem jest poprawnie użyte, jeśli tylko zostało zdefiniowane i konsekwentnie używane w zdefiniowanym znaczeniu.

Przyjęta definicja (lecz nie sam wyraz system) jest problematyczna przy zestawieniu z metafizyką przyjmowaną w ramach neotomizmu. Centralnym pojęciem metafizyki jest byt[58] rozumiany jako to co jest (byt jest, niebytu nie ma). Zatem wszystko co istnieje jest bytem. W ramach tej koncepcji byt można podzielić na trzy rodzaje[59]:

- rzecz,
- cecha,
- relacja.

O ile definicja systemu obejmuje rzeczy i relacje, to jednak nie bierze pod uwagę cech samego systemu i jego elementów. Analizowanie samych elementów danego systemu i relacji między nimi może okazać się niewystarczające, gdyż

55 v. M. Mazur, *Pojęcie systemu i rygory jego stosowania*, http://autonom.edu.pl/publikacje/mazur_marian/pojecie_systemu_i_rygory_jego_stosowania-ocr.pdf, dostęp na: 29.07.2021, p. 3.
56 cf. ibid, p. 4.
57 cf. ibid., p. 2-3.
58 v. M. Gogacz, *Elementarz metafizyki*, https://www.katedra.uksw.edu.pl/gogacz/ksiazki/elementarz_metafizyki.pdf, dostęp na 25.09.2022. p. 123-124.
59 cf. J. Bocheński, *Współczesne metody myślenia*, W drodze, Poznań 1992, p. 13.

poza funkcją jaką dany system spełnia, lub wypadkową jego elementów i relacji między nimi, istotną rolę może mieć e.g. jakość występująca w danym systemie bądź elemencie. Dla przykładu kwanty nie są szorstkie, ale pewne ich nadsystemy już mogą posiadać tę cechę. Podobnie rozumność nie jest udziałem żadnej z części człowieka, ale jest właściwością typową dla całego człowieka jako takiego. Jednym z rozwiązań tego problemu może być zmienienie definicji systemu na „zbiór elementów, relacji między nimi i cech odnoszących się do tego zbioru". Możliwy jest również wariant, że dodatkowych cech niewynikających z elementów zbioru i relacji między nimi po prostu nie będzie. Drugim rozwiązaniem jest zapisywanie dodatkowych cech danego systemu w myśl aksjomatycznej teorii poznania Kosseckiego, która polega na określeniu, że dany system należy do zbioru, który reprezentuje daną cechę[60]. Dla przykładu system kwantów i relacji między nimi może należeć do zbioru bytów szorstkich, a system obejmujący wszystkie części człowieka do zbioru bytów rozumnych. Tym sposobem możliwe jest zapisywanie dodatkowych cech systemów, które nie wynikają z wypadkowej jego elementów i relacji tych elementów, bez modyfikowania definicji systemu. Autor przyjął w pracy rozwiązanie drugie.

Co więcej rzeczy mogą mieć różny status ontyczny. Istota części z nich istnieje niezależnie od ludzkiej myśli, a pozostała część jest z myślą ludzką ściśle związana (a wręcz jest treścią ludzkiej myśli)[61]. Dla przykładu człowiek zawsze będzie człowiekiem, niezależnie od tego jak jest ujmowany myślowo przez innych ludzi (lub inne byty zdolne do abstrakcji). Innym przykładem są byty w rodzaju krzesła lub komputera stacjonarnego. Zasadniczo istotą komputera stacjonarnego jest wykonywanie obliczeń, obsługa aplikacji etc. Zbiór cząsteczek, które tworzą dany komputer, człowiek ujmuje jako jedną całość ze względu na funkcję jaką pełni komputer jako taki (dlatego też został tak, a nie inaczej zaprojektowany i wytworzony przez człowieka). Ta funkcja jest tylko i jedynie treścią ludzkiej myśli

60 cf. J. Kossecki, *Metacybernetyka*, op. cit., p 23-24.

61 Warto zauważyć, że kategoryzacja bytów na podstawie ich zależności od ludzkiej myśli odnosi się do teorii poznania, a nie stricte metafizyki. Taki kierunek rozważań może być nieakceptowany w niektórych ujęciach metafizycznych. Autor przedstawia zagadnienie w ten sposób, dlatego iż w ramach nauk społecznych, niestety, nie naucza się metafizyki (bądź ontologii), więc głównym celem jest wytłumaczenie tego zjawiska w jak najprostszy sposób.

(twórcy komputera i jego użytkownika), wynikającej z celu postawionego sobie przez projektanta, gdyż komputer równie dobrze może służyć jako bardzo dobra broń improwizowana podczas karczemnych bijatyk. Zatem nowe użycie (jako pewien rodzaj broni) narzuca nową istotę komputera stacjonarnego przy braku zmiany jego struktury fizycznej[62].

Wydaje się zatem zasadne wprowadzenie podziału systemów na systemy substancjalne i addycyjne[63]. Idąc za Arystotelesem, każdy byt składa się z aktu i możności, czyli tego co aktualizuje daną możność w tej właśnie chwili i tego co może być aktualizowane, czyli pewnego zbioru możliwości, stanów jakie może przyjąć lub jakich może się podjąć dany byt[64]. W przypadku bytów substancjalnych można wyróżnić dwa główne złożenia aktu i możności. Pierwsze z nich przebiega na linii istota i istnienie (gdzie istnienie jest aktem, a istota możnością). Wynika z tego, że istnienie nie jest cechą bytu, ale podstawą jego istoty, zatem nie byłoby zgodne z (neo)tomizmem uznanie, że system, który istnieje posiada taką cechę, ale wymusza to opracowanie nowej kategorii systemów. Drugie złożenie aktu i możności dotyczy istoty, która składa się z formy i materii. Forma substancjalna jest aktem, który odpowiada za tożsamość danego bytu, a materia jest sferą fizyczną, która może ulegać zmianie. Warto dodać, że Gogacz wyróżnił w przypadku bytów rozumnych, jako jedno ze złożeń subontycznych, możność intelektualną, która obok możności materialnej, byłaby aktualizowana przez formę[65]. Innymi słowy zmieniać się (rozwijać lub degenerować) może nie tylko materia w człowieku, ale też i sfera intelektualna. Byty addycyjne (posiadający jedność tylko addycyjnie)[66] nie posiadają formy substancjalnej, a więc są różne

62 cf. M. Gogacz, *Elementarz...*, op. cit., p. 35: „Jedność addycyjna spełnia się w ludzkich wytworach i polega na przyznaniu każdemu elementowi strukturalnemu wytworu tej samej pozycji elementu niezależnego od innych. Przypisuje się tym samym temu elementowi pozycję samodzielności, co powoduje, że wytwór jest sumą samodzielnych elementów. Nie mogą one wtedy tworzyć jednego i o wewnętrznej jedności samodzielnego bytu. Nie stanowią bytowej kompozycji, lecz sumę bytów powiązanych relacjami wyznaczonymi przez naturę elementów. Człowiek połączył te elementy na miarę celu, który wyznaczył tej kompozycji."
63 cf. ibid. p. 36.
64 cf. M. Krąpiec, *Metafizyka*, Redakcja Wydawnictw Katolickiego Uniwersytetu Lubelskiego, Lublin 1995, p. 207-211.
65 cf. T. Stępień, op. cit., p. 129-130.
66 W ramach metafizyki istnieją pewne rozbieżności terminologiczne. Według Gogacza byt nie jest tym czym jest, ale jest rzeczą, która jest aktualizowana przez formę substancjalną, a więc jest

jakościowo od bytów substancjalnych. Jedność bytów addycyjnych wynika tylko i jedynie z zewnętrznego działania[67]. Inaczej można to zagadnienie wyrazić w ten sposób, że forma substancjalna jest wewnętrzną podstawą tożsamości danego bytu. Zatem tożsamość człowieka wynika z jego formy (podobnie jak tożsamość zwierzęcia i rośliny), a więc zasada tożsamości człowieka jest w samym człowieku. Z drugiej strony tożsamość krzesła (lub komputera) nie jest w samym krześle (lub komputerze), tylko jest narzucana z zewnątrz na zasadzie pewnej konwencji. Mimo to cząsteczki z jakich składa się krzesło posiadają formę substancjalną, która określa tożsamość każdej z cząsteczek osobno.

Biorąc pod uwagę powyższe rozważania w pracy proponuje się rozróżnienie systemów addycyjnych (systemów, których istota jest zależna od ludzkiej myśli, a więc związanych z pewną konwencją, wytworzonych przez człowieka w pewnym celu) i systemów substancjalnych, czyli takich, których istota jest niezależna od ludzkiej myśli, niezależnych od jakiejkolwiek konwencji, gdyż obejmowane są przez formę substancjalną, a więc są samodzielnymi, odrębnymi bytami. Będzie to istotne, chociażby w przypadku wyznaczenia kierunku zależności między bezpieczeństwem jednostki a bezpieczeństwem grupy, jak i tworzenia zbioru możliwości w ramach analizy systemowej.

2.2. Oddziaływania między systemami

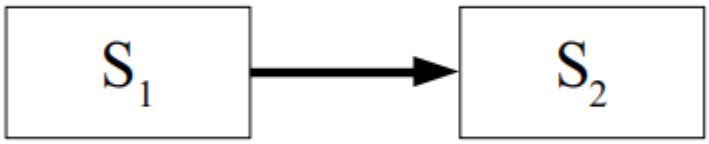
Systemy mogą oddziaływać na siebie (i często tak się właśnie dzieje). Można wyróżnić dwa podstawowe rodzaje takich oddziaływań, czyli sprzężeń prostych i sprzężeń zwrotnych[68].

---

pewną jednostkową strukturą z odrębnym aktem istnienia. Zatem zwrot *byt addycyjny* jest według tego ujęcia błędny. Autor, co zostało wcześniej opisane, rozumie byt jako „to co jest", co uniesprzecznia termin *byt addycyjny* z ogólnym terminem *byt*. cf. M. Gogacz, *Elementarz*..., op. cit., p. 36, 115.

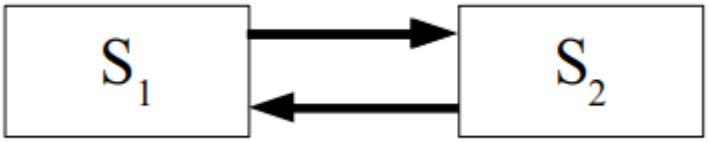
67 cf. M. Gogacz, *Elementarz...*, op. cit., p. 35-36.

68 cf. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 63.



Rys. 2: Sprzężenie proste

źródło: opracowanie własne na podstawie: M. Mazur, *Cybernetyka i charakter*, op. cit., p. 63.



Rys. 3: Sprzężenie zwrotne

źródło: opracowanie własne na podstawie: M. Mazur, *Cybernetyka i charakter*, op. cit., p. 63.

Oddziaływania, które prowadzą do zmian w innym systemie nazywane są inaczej sterowaniem[69]. Oddziaływanie na inny system nazywane będzie bodźcem (S). Bodziec może wywoływać reakcję systemu (R). Obydwa zjawiska można powiązać terminem reaktywności (r)[70], którą można również wyrazić wzorem[71]:

$$r = \frac{R}{S}$$

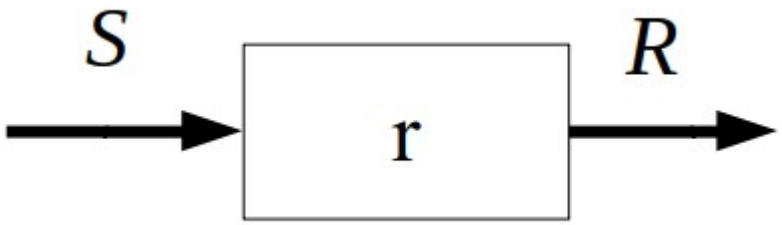
Znajomość reaktywności danego systemu na dany bodziec i samego bodźca umożliwia obliczenie reakcji na ten bodziec[72]:

$$R = r * S$$

Podaną sytuację można zobrazować w poniższy sposób. Należy dodać w tym miejscu uwagę, że jeśli na schemacie strzałka nie kończy się na innym systemie,

69 cf. ibid., p. 107.
70 cf. ibid., p. 64.
71 v. ibid.
72 v. ibid., p. 65.

to oznacza, że reakcja dotyczy otoczenia. Jeśli strzałka nie zaczyna się od innego systemu, to znaczy, analogicznie, że bodziec pochodzi z otoczenia.



Rys. 4: Reaktywność systemu

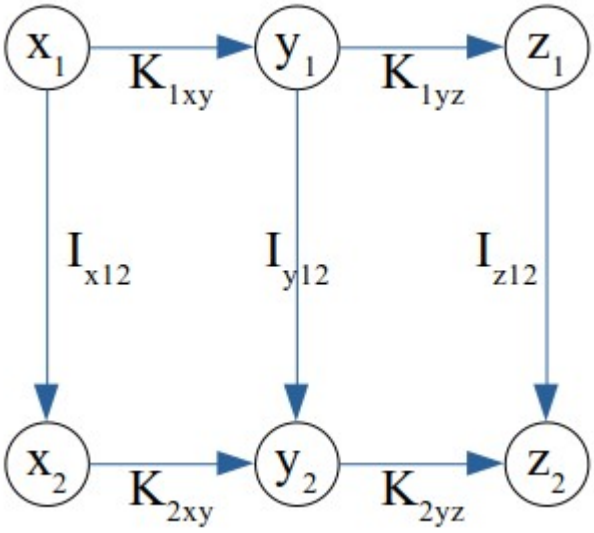
źródło: opracowanie własne na podstawie: M. Mazur, *Cybernetyka i charakter*, op. cit., p. 64-65.

Rozważane w pracy bodźce oddziałujące na system i jego reakcje mają zawsze charakter energomaterialny, a więc są pewną ilością energii lub materii w odpowiedniej konfiguracji. W zależności od tego co jest istotne w danej analizie dla badacza, możliwe jest analizowanie konkretnych bodźców (a wręcz całych sprzężeń) jako informacyjnych bądź energetycznych. W ramach toru informacyjnego przenoszone są informacje, a w ramach toru energetycznego – pozostała energomateria[73]. Ten sam bodziec może, w zależności od podejścia, być ujmowany jako informacyjny lub energetyczny. Przykładem może być sygnał wysłany światłowodem, który może, z jednej strony, być analizowany pod kątem przenoszonej przez niego informacji, albo pod kątem jego parametrów energetycznych. Na rysunkach kolorem niebieskim oznaczany będzie tor informacyjny, a kolorem czerwonym – energetyczny. Kolor czarny używany będzie do oznaczenia sprzężeń (torów) jako takich. Co więcej w pracy główny ciężar analizy spoczywa na oddziaływaniach informacyjnych, a więc tor energetyczny będzie najczęściej uwzględniany tylko i jedynie dla zachowania porządku.

73 cf. J. Kossecki, *Metacybernetyka*, op. cit., p. 85-87.

W ramach jakościowej teorii informacji informowanie definiuje się jako „transformowanie informacji zawartych w łańcuchu oryginałów w informacje zawarte w łańcuchu obrazów”[74]. Wyróżnia się następujące rodzaje informowania:

- transinformowanie, w którym informacje w zbiorze oryginałów są takie same jak w zbiorze obrazów[75]. Można to przedstawić następującym rysunkiem, na którym spełniona jest zależność $I_{x12}=I_{z12}$(I_{y12} nie musi być równa I_{x12} i I_{z12}):

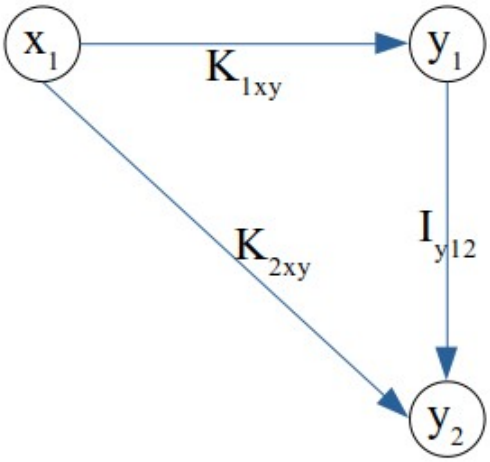


Rys. 5: Transinformowanie

źródło: opracowanie własne na podstawie: M. Mazur, *Jakościowa...*, op. cit., p. 87-88.

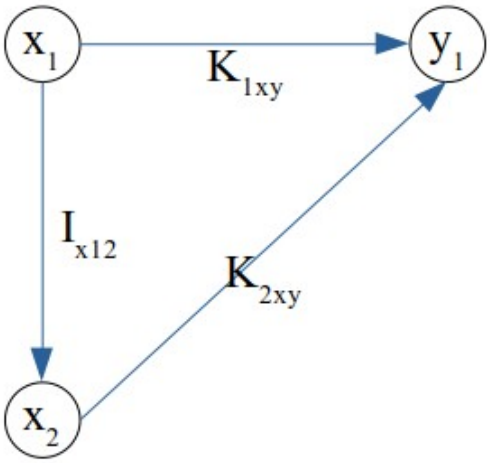
- pseudoinformowanie (informowanie pozorne), w którym niektóre komunikaty mają wspólne komunikaty w zbiorze oryginałów lub obrazów. Pseudoinformowanie dzieli się dodatkowo na pseudoinformowanie symulacyjne (informowanie rozwlekłe) posiadające wspólne komunikaty w zbiorze obrazów i pseudoinformowanie dysymulacyjne (informowanie ogólnikowe) posiadające wspólne komunikaty w zbiorze oryginałów[76].

74 v. M. Mazur, *Jakościowa...*, op. cit., p. 82.
75 v. ibid., p. 87.
76 cf. J. Kossecki, *Metacybernetyka*, op. cit., p. 74-75.



Rys. 6: Pseudoinformowanie symulacyjne

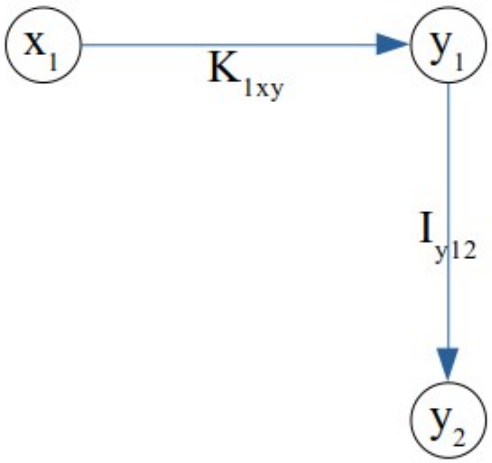
źródło: opracowanie własne na podstawie: J. Kossecki, *Metacybernetyka*, op. cit., p. 75.



Rys. 7: Pseudoinformowanie dysymulacyjne

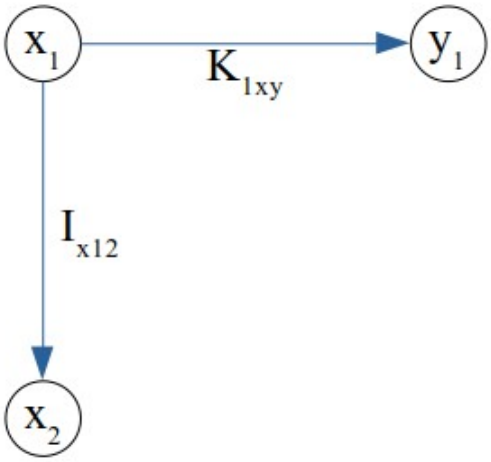
źródło: opracowanie własne na podstawie: J. Kossecki, *Metacybernetyka*, op. cit., p. 75.

- dezinformowanie (informowanie fałszywe), w ramach którego niektóre ciągi kodów są niepełne, ale jednoznaczne. Dezinformowanie dzieli się na dezinformowanie dysymulacyjne (zatajanie) i dezinformowanie symulacyjne (zmyślanie).



Rys. 9: Dezinformowanie symulacyjne

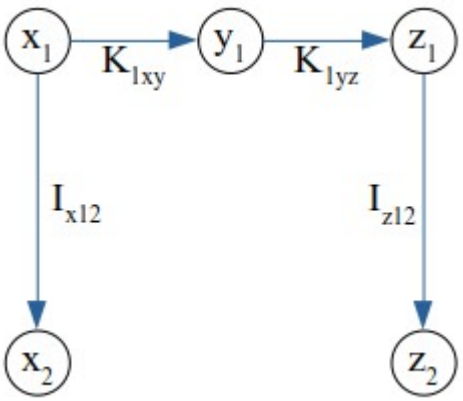
źródło: opracowanie własne na podstawie: J. Kossecki, *Metacybernetyka*, op. cit., p. 75.



Rys. 8: Dezinformowanie dysymulacyjne

źródło: opracowanie własne na podstawie: J. Kossecki, *Metacybernetyka*, op. cit., p. 75.

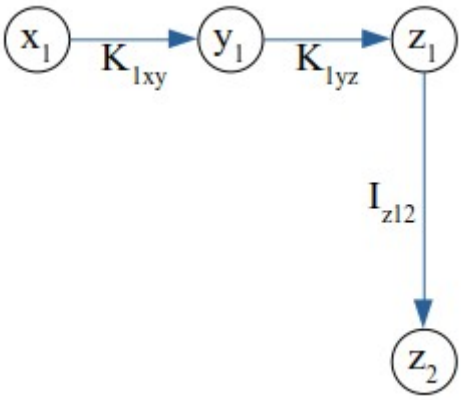
- parainformowanie, ściśle związane jest z parakomunikatami, które występują w łańcuchu informacyjnym, ale nie w łańcuchu kodowym. Informowanie, w którym występuje parakomunikat jest parainformowaniem. Może być zarówno paratransinformowaniem (jeśli informacje w łańcuchu informacyjnym są takie same po parainformowaniu), jak i paradezinformowaniem (jeśli informacje w łańcuchu informacyjnym nie są takie same)[77]. Innymi słowy kodowane są tylko niektóre komunikaty w nadziei, że system, który je odbiera wytworzy asocjację, która była zamierzona w systemie oddziałującym. Jeśli dojdzie do niezrozumienia przekazu, to dochodzi do paradezinformowania, który skutkuje wytworzeniem informacji, których nie było w intencji nadawcy, albo niezauważenie tych, które miały zostać przekazane. Przykładem paratransinformowania może być język, dzięki któremu posługujący się nim ludzie kodują tylko część komunikatów, co nie przeszkadza w tym, żeby odbiorcy zrozumieli całość przekazu. Innymi przykładami są niezrozumiałe przez drugą stronę metafory (paradezinformowanie dysymulacyjne) lub doszukiwanie się aluzji tam, gdzie jej nie ma (paradezinformowanie symulacyjne).



Rys. 10: Paratransinformowanie

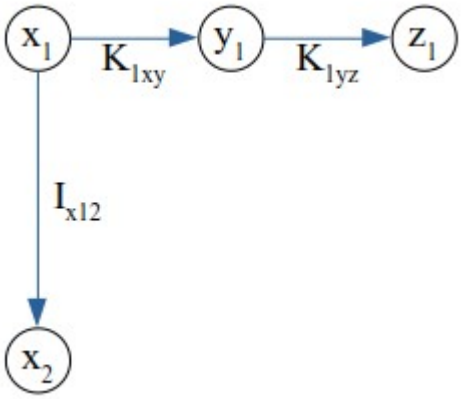
źródło: opracowanie własne na podstawie:
M. Mazur*, Jakościowa...*, op. cit., p. 156.

77 cf. M. Mazur, *Jakościowa...*, op. cit., p. 153-161.



Rys. 11: Paradezinformowanie symulacyjne

źródło: opracowanie własne na podstawie: M. Mazur, *Jakościowa ...*, op. cit., p. 160.

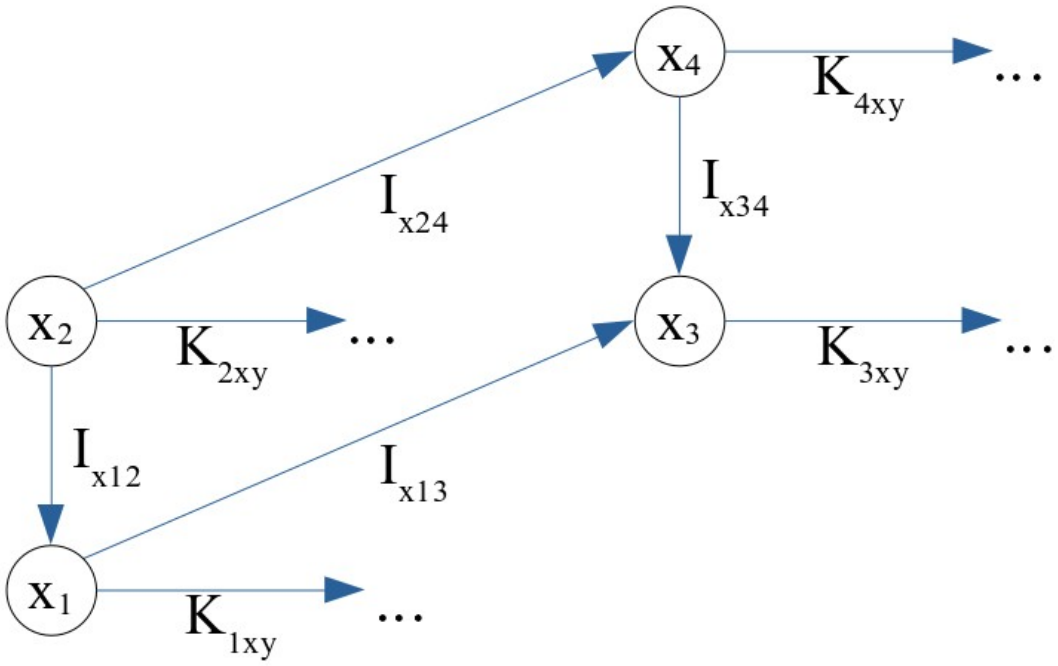


Rys. 12: Paradezinformowanie dysymulacyjne

źródło: opracowanie własne na podstawie: M. Mazur, *Jakościowa...*, op. cit., p. 161.

- metainformowanie jest informowaniem o informowaniu. Polega na relacji komunikatów złożonych (przynajmniej dwóch komunikatów, między którymi występuje informacja) między sobą. Na poniższym schemacie komunikatem złożonym jest x_1, x_3 i informacja między nimi I_{x13}. Drugim komunikatem złożonym jest x_2, x_4 wraz z informacją I_{x24}. Jeśli jeden komunikat złożony odnosi się do drugiego komunikatu złożonego i go opisuje, to staje się metakomunikatem[78]. Wśród metainformowań można wyróżnić zarówno metatransinformowanie (metainformowanie wierne), jak i metapseudoinformowanie, metaparainformowanie lub metadezinformowanie. Przykładem metainformowania wiernego może być stwierdzenie, że dana osoba skłamała, jeśli faktycznie skłamała, a przykładem metadezinformowania stwierdzenie kłamstwa u kogoś kto powiedział prawdę[79]. Zarówno komunikaty wykorzystywane w ramach informowania, jak i metainformowania mogą być kodowane dalej w ramach swoich torów informacyjnych (stąd uwzględniono na rysunku kodowania K_{1xy}, K_{2xy}, K_{3xy} i K_{4xy}).

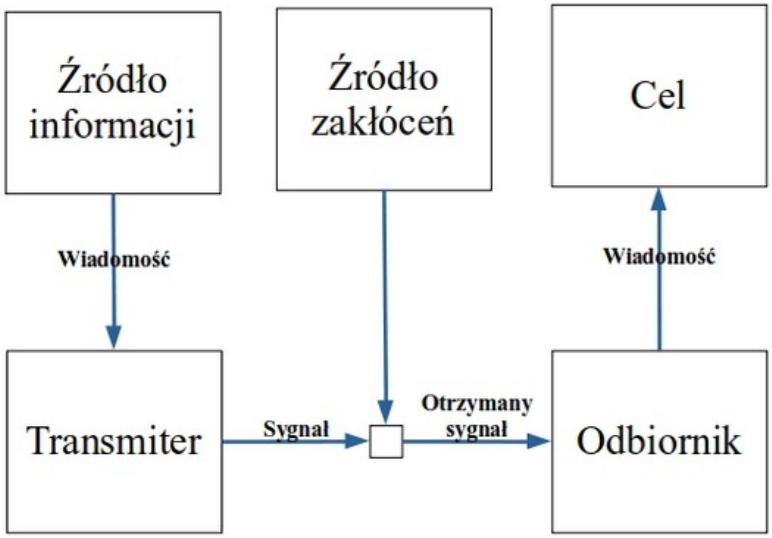
78 cf. ibid., p. 171-178.
79 v. ibid., p. 184-185.



Rys. 13: Metainformowanie

źródło: opracowanie własne na podstawie: M. Mazur, *Jakościowa ...*, op. cit., p. 171, 184.

Podczas przesyłania informacji mogą nastąpić zakłócenia, które zniekształcają komunikaty generowane w torze informacyjnym. W pracy szczególnie istotne będą intencjonalne zakłócenia generowane przez zarówno jednostki, jak i całe grupy. Proces przesyłania informacji można wyrazić poniższym modelem.



Rys. 14: Model komunikacji w matematycznej teorii komunikacji

źródło: opracowanie własne na podstawie: C. Shannon, W. Weaver, *The mathematical theory of communication*, The University of Illnois Press, Urbana 1964, p. 7.

Na powyższym rysunku wiadomość z źródła informacji jest przekształcana na sygnał, który za pomocą odbiornika z powrotem przekształca sygnał w wiadomość. Jeśli wiadomość z źródła informacji i ta, która osiągnęła cel są tożsame, to doszło do transinformowania. Na schemacie uwzględniono również źródło zakłóceń, które może zmieniać sygnał w torze sterującym.

2.3. Rodzaje systemów

W jednym bycie może zachodzić wiele różnych jakościowo procesów (spełniających różne funkcje), które można rozdzielić za pomocą analizy systemowej. Podsystemy spełniające poszczególne funkcje można podzielić na[80]:

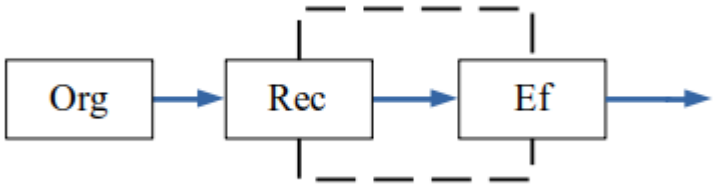
- efektor (oznaczany na rysunkach przez Ef) – odpowiedzialny za wytwarzanie reakcji na zewnątrz systemu. System może posiadać wiele efektorów,

80 cf. J. Kossecki, *Metacybernetyka*, op. cit., p. 85-87, 89, 91-92.

- receptor (oznaczany na rysunkach przez Rec) – odbierający bodźce o charakterze informacyjnym (dla danego bodźca). System może posiadać wiele receptorów,
- korelator (oznaczany na rysunkach przez Kor) – przetwarzający i przechowujący informacje w systemie,
- alimentator (nazywany również zasilaczem i oznaczany na rysunkach przez Z) – odbierający bodźce o charakterze energetycznym. System może posiadać wiele alimentatorów (zasilaczy),
- akumulator (oznaczany na rysunkach przez Ak) – przetwarzający i przechowujący energomaterię, która nie jest traktowana jako informacja, ale jako zasilanie,
- homeostat (oznaczany na rysunkach przez Hom) – zapewniający równowagę funkcjonalną systemu i samosterowność danego systemu,
- organizator (oznaczany na rysunkach przez Org) – w niektórych przypadkach (w niektórych systemach lub w przypadku niektórych rodzajów bodźców) system jest sterowany przez zewnętrznego organizatora, a nie własny homeostat.

Na podstawie różnej konfiguracji powyższych podsystemów można wyróżnić następujące rodzaje systemów:

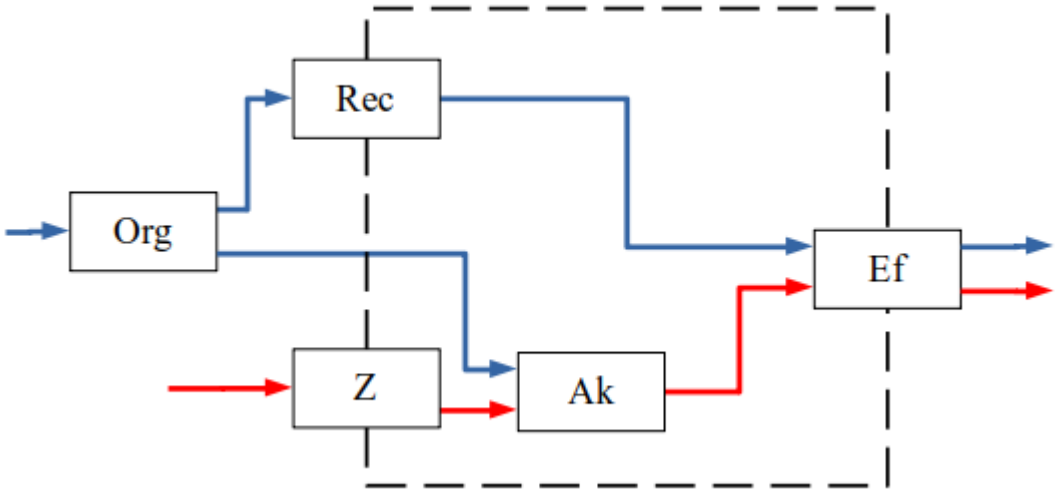
- układ zorganizowany (system zorganizowany), który transportuje informacje z wejścia receptora na wyjście efektora (przy uwzględnieniu reaktywności tych podsystemów),



Rys. 15: System zorganizowany

źródło: opracowanie własne na podstawie: M. Mazur, *Cybernetyczna teoria układów samodzielnych*, Państwowe Wydawnictwo Naukowe, Warszawa 1966, p. 51.

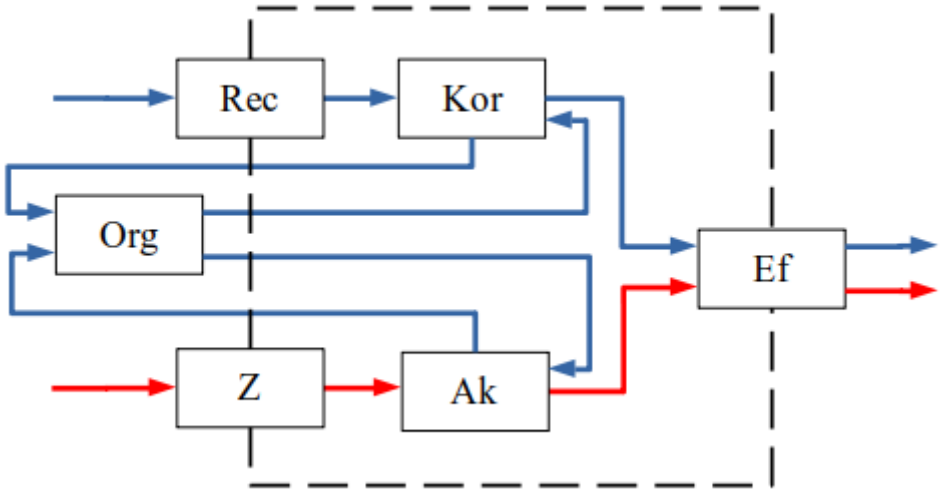
- system sterowny, który poza przenoszeniem informacji i wyzwalaniem reakcji, samodzielnie pobiera (przez zasilacz) i przetwarza (w akumulatorze) energomaterię. Organizator jedynie steruje systemem sterownym, ale nie musi dostarczać mu energomaterii jako zasilania,



Rys. 16: System sterowny

źródło: opracowanie własne na podstawie: J. Kossecki, *Metacybernetyka*, op. cit., p. 88.

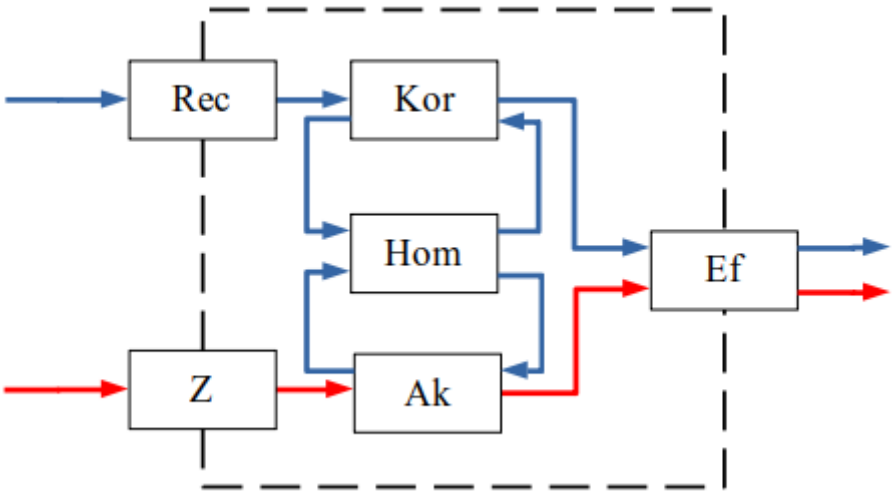
- system samosterowny, który posiada wszystkie cechy systemu sterownego, ale dzięki korelatorowi może przetwarzać i przechowywać informacje, które pozyskał z receptorów,



Rys. 17: System samosterowny

źródło: opracowanie własne na podstawie: J. Kossecki, *Metacybernetyka*, op. cit., p. 90.

- system autonomiczny, który potrafi pobierać i przetwarzać zarówno informacje, jak i zasilanie. Dzięki homeostatowi system autonomiczny posiada zdolność do sterowania samym sobą i utrzymania tej zdolności w czasie[81].



Rys. 18: System autonomiczny

źródło: opracowanie własne na podstawie: J. Kossecki, *Metacybernetyka*, op. cit., p. 92.

81 v. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 163.

W dalszej pracy zostaną głównie wykorzystywane schematy systemu zorganizowanego i systemu autonomicznego.

2.4. Moc i stany systemu

Aby system autonomiczny mógł trwać i oddziaływać na otoczenie potrzebuje energii. Energię można podzielić na zewnętrzną, czyli taką, która pochodzi spoza systemu, i wewnętrzną, która pochodzi z samego systemu, a więc która może być produkowana na potrzeby działania tego systemu. W przypadku człowieka energię zewnętrzną nazywa się energią socjologiczną, a wewnętrzną - energią fizjologiczną[82]. Energia (E), która jest przetwarzana w pewnym czasie (t) jest mocą (P). Można to wyrazić wzorem[83]:

$$P = \frac{E}{t}$$

Moc powstała z przetwarzania energii socjologicznej nazywa się mocą socjologiczną, a moc powstała w wyniku przetwarzania energii fizjologicznej nazywa się mocą fizjologiczną[84]. W ramach zagadnienia mocy systemu autonomicznego można wyróżnić kilka jej rodzajów[85]:

- moc całkowita (P),
- moc jałowa (P_0), którą system zużywa w celu utrzymania się przy życiu,
- moc robocza (P_r), którą system zużywa na zdobycie mocy jałowej,
- moc dyspozycyjna (P_d), jest mocą, która pozostaje po odjęciu od mocy całkowitej mocy jałowej,
- moc swobodna (P_s), która jest mocą, która pozostaje po odjęciu od mocy całkowitej mocy jałowej i roboczej.

Używając powyższych rodzajów mocy systemu autonomicznego możliwe jest określenie następujących zależności między nimi[86]:

$$P_d = P - P_0$$

82 cf. J. Kossecki, *Metacybernetyka*, op. cit., p. 102.
83 v. ibid.
84 cf. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 224-225.
85 cf. ibid., p. 238-239.
86 cf. ibid.

$$P_s = P - \left(P_r + P_0\right)$$

$$P = P_0 + P_r + P_s$$

$$P_d = P_r + P_s$$

Współczynnikiem, który jest związany z mocą systemu autonomicznego jest współczynnik swobody (s). Dzięki niemu możliwe jest dokładniejsze ocenienie jak dużą swobodę posiada dany system autonomiczny. Dla $s = 0$ system nie posiada żadnej swobody, a więc całą moc zużywa na pokrycie mocy jałowej i mocy roboczej. Dla $s = 1$ system autonomiczny zużywa moc tylko na pokrycie mocy jałowej. W przypadku niedoborów mocy roboczej system autonomiczny może kompensować braki energetyczne przez zdobywanie energii socjologicznej (a więc i mocy socjologicznej). Współczynnik swobody określa się wzorami[87]:

$$s = \frac{P_s}{P_d} = \frac{P_s}{P_r + P_s} = \frac{P - P_0 - P_r}{P - P_0} = 1 - \frac{P_r}{P - P_0}$$

Analizowanie współczynnika swobody jest cenne w kontekście oceniania bezpieczeństwa, zagrożeń analizowanych systemów wynikających z różnego udziału homeostatu systemu i zewnętrznego organizatora na sterowanie tym systemem.

Zagadnienie mocy systemu można również opisać odnosząc się do właściwości samego materiału, z którego składa się system. Wyróżnić można następującego jego cechy[88]:

- c - ilość materiału z jakiego składa się system,
- a - jakość materiału z jakiego składa się system,
- v - moc jednostkowa przypadająca na jednostkę jakości i jednostkę ilości tworzywa,
- w - stratność, czyli moc jałowa przypadająca na jednostkę ilości materiału.

Na ich podstawie możliwe jest opisanie mocy następującymi wzorami[89]:

$$P = c * a * v$$

$$P_0 = c * w$$

87 cf. ibid., p. 239-240.
88 v. ibid., p. 227; 232.
89 v. ibid., p. 227-232.

Aby system mógł istnieć musi zajść warunek $P \geq P_0$[90], a więc:

$$c * a * v \geq c * w$$

Dzieląc obydwie strony nierówności przez c (które jest zawsze dodatnie) otrzymujemy:

$a * v \geq w$, czyli (dzieląc przez$v$, które jest zawsze dodatnie)

$$a \geq \frac{w}{v}$$

Zakładając, że $v = const$ i $w = const$, to wynika z tego, że zakończenie istnienia sytemu zależy tylko od jednej zmiennej jaką jest jakość tworzywa z którego się dany system składa[91].

Każdy z systemów może dodatkowo znajdować się w jednym z trzech (a nawet czterech) stanów, które wynikają z trzech kategorii stanów[92]:

- stan żywotności (p),
- stan gotowości (q),
- stan aktywności (h[93]).

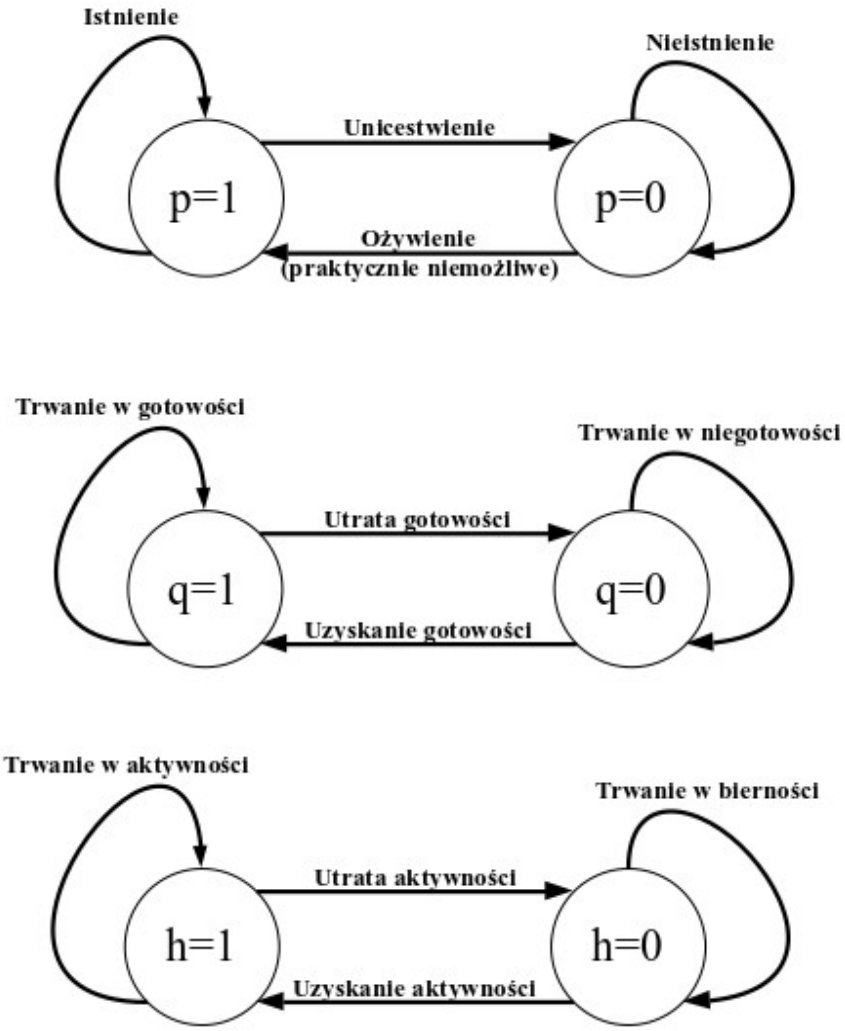
Możliwymi stanami jakie może osiągnąć system są stany (rozpatrywane jako uporządkowana trójka $<p,q,h>$)[94]:

- $<0,0,0>$ - system nie istnieje,
- $<1,0,0>$ - system istnieje, ale nie jest gotowy do działania,
- $<1,1,0>$ - system istnieje, jest gotowy do działania, ale nie działa,
- $<1,1,1>$ - system istnieje, jest gotowy do działania i właśnie oddziałuje na otoczenie.

Przechodzenia między stanami można zobrazować grafami:

---

90 v. ibid., p. 232-233.
91 cf. ibid., p. 234-235.
92 v. J. Konieczny, *Cybernetyka walki*, Wydawnictwo Naukowe PWN, Warszawa 1970, p. 55.
93 Konieczny oznacza stan aktywności przez literę *r*, ale została ona już użyta w pracy na rzecz reaktywności systemu.
94 v. ibid., p. 56-57.



Rys. 19: Przejścia między stanami w systemie

źródło: opracowanie własne na podstawie: J. Konieczny, *Cybernetyka walki*, op. cit., p. 56.

W konkretnych stanach mogą znajdować się dowolne systemy. Zarówno system zorganizowany, sterowny, samosterowny lub autonomiczny, ale również podsystemy, z których się składają.

2.5. Zbiór możliwości systemów w cyberprzestrzeni

Przed ustaleniem zbioru możliwości cyberprzestrzeni, należy określić w jaki sposób rozumieć sam termin cyberprzestrzeń. Nie istnieje jedna definicja cyberprzestrzeni. Do przykładowych ujęć należą[95]:

- cyberprzestrzeń jako internet (zasoby, usługi i użytkownicy),
- cyberprzestrzeń jako wirtualna rzeczywistość generowana przez internet, komputer i sieć,
- cyberprzestrzeń jako sieć sieci - megasieć, której zasoby są eksploatowane przez jej użytkowników,
- cyberprzestrzeń jako dynamiczny system złożony (bez wyróżniania konkretnych aspektów – zarówno technicznych, społecznych czy informacyjnych).

Etymologicznie cyberprzestrzeń należy rozumieć jako przestrzeń sterowania. Jako, że w ramach przestrzeni, w której możliwe jest sterowanie znajdują się różne byty, to można uznać, że cyberprzestrzeń jest nadsystemem wobec wszystkich systemów, które generują lub odbierają bodźce informacyjne[96]. Ujęcie etymologiczne jest najbliższe rozumieniu cyberprzestrzeni jako dynamicznemu systemu złożonemu (nadsystemu). Cyberprzestrzeń zatem nie będzie się ograniczała do internetu, czy innych aspektów technicznych. Tak rozumiana cyberprzestrzeń zawiera się całkowicie w rzeczywistości (uniwersum rozumiane jako zbiór wszystkich bytów), a być może jest z nią tożsama.

W ramach analizy systemowej nie istnieje jeden sposób podziału badanej rzeczywistości na systemy. Podziału dokonuje się pod kątem właściwości, które są istotne dla badacza[97]. Z pewnością wyróżnionymi systemami muszą być jednostka i grupa, jako że celem pracy jest przeanalizowanie tych systemów pod kątem ich bezpieczeństwa w kontekście różnych oddziaływań informacyjnych. Jaka jest

95 cf. P. Sienkiewicz, *Ontologia cyberprzestrzeni*, in: Zeszyty Naukowe WWSI, 13 (2015), p. 93.
96 Przetwarzanie informacji przez system prowadzi do jego zmiany, a więc jest sterowaniem.
97 cf. P. Sienkiewicz, *Analiza systemowa. Podstawy i zastosowania*, Wydawnictwo Bellona, Warszawa 1994, p. 36.

relacja między jednostką i grupą? Grupa zawiera w sobie jednostki i relacje między nimi[98], a więc jest nadsystemem dla jednostki. Określając kolejne właściwości tych systemów należy odwołać się do rodzajów bytów substancjalnych jakie wyróżnia się w rzeczywistości. Według Akwinaty należą do nich sinole (najmniejsze cząstki, z których złożona jest rzeczywistość), composity (złożenia sinoli), rośliny, zwierzęta i ludzie[99]. Wszystkie inne byty są pewnymi wytworami, czyli bytami, które nie są niczym więcej jak treściami ludzkich myśli, albo są złożeniem sinoli i compositów, aby móc pełnić jakieś funkcje (a więc posiadają tylko i jedynie jedność addycyjną). W ramach bytów substancjalnych jako systemy zostaną wyróżnione tylko i jedynie ludzie (jednostki), a więc wszystkie inne systemy będą systemami addycyjnymi (dla przykładu grupy, które są treściami ludzkich myśli). Dodatkowo ludzie będą traktowani jako systemy autonomiczne.

Człowiek kompensuje pewne braki w swojej naturze (na przykład brak pazurów, kłów, rogów i futra) przez tworzenie narzędzi i życie we wspólnocie[100]. Nie inaczej dzieje się w przypadku oddziaływań informacyjnych. Ograniczenia w postaci zasięgu widzenia, donośności ludzkiego głosu można pomijać przez zastosowanie środków organizacyjnych i pewnych wytworów. Dobrze zorganizowana poczta może przenosić listy (zawierające informacje) na duże odległości. Podobnie można wykorzystywać infrastrukturę teleinformatyczną. Dlatego też porządku organizacyjnego (lub jego braku) nie można odwzorować w analizie systemowej przez badanie tylko i jedynie relacji między jednostkami w ramach grupy, gdyż poza relacjami międzyludzkimi (i relacjami jednostki do grupy) rozwiązania organizacyjne obejmują również używanie różnych przedmiotów. Zarówno kabel, komputer, książka etc. mogą przysłużyć się

98 cf. M. Gogacz, *Mądrość buduje państwo*, Wydawnictwo Ojców Franciszkanów, Niepokalanów 1993, p. 162. Gogacz dodatkowo używa zwrotu *osoba* zamiast *jednostka* lub *człowiek*. Nie zmienia to jednak wniosków wyprowadzonych z tego fragmentu dla analizy systemowej. Dodatkowo jako relacje Gogacz wymienia szczegółowo relacje myślne i realne, które zostaną opisane w dalszej części pracy.
99 v. S. Swieżawski, *Święty Tomasz na nowo odczytany*, W drodze, Poznań 1995, p. 120-122.
100 cf. Tomasz z Akwinu, O *władzy*, in: *Św. Tomasz z Akwinu. Dzieła wybrane*, W drodze, Poznań 1984, p. 135,

w oddziaływaniu informacyjnym. Wszystkie tego typu przedmioty (nazywane dalej zasobami) mogą wspomóc działanie człowieka w jednym lub kilku jego podsystemach wyróżnionych w ramach systemu autonomicznego. A zatem zasoby mogą wspierać działalność człowieka w ramach:

- receptora - pozwalając odbierać większy zakres bodźców,
- korelatora - pozwalając na przechowywanie i przetwarzanie większych ilości informacji, niż wynika to z ograniczeń ludzkiej natury,
- efektora - oddziaływać w większym zakresie na otoczenie,

Ze względu na specyfikę homeostatu nie jest możliwe wspieranie tego podsystemu bezpośrednio przez zasoby. Z drugiej strony możliwe jest wspieranie człowieka przez zasoby w ramach akumulatora, aczkolwiek nie jest to istotne zagadnienie w kontekście oddziaływań informacyjnych. Dodatkowo istotnym elementem cyberprzestrzeni są komunikaty, które wymieniane są między systemami. Ich analiza również będzie istotna, aczkolwiek nie ma potrzeby ich specjalnego wyróżniania jako systemu, gdyż są nierozdzielnym elementem torów informacyjnych. Komunikaty będą analizowane w kontekście relacji między wyróżnionymi poniżej elementami.

Wyróżnia się zatem następujące elementy cyberprzestrzeni:

- systemy substancjalne:
  - jednostka (człowiek).
- systemy addycyjne:
  - grupa,
  - zasób.

Uwzględniając dodatkowo otoczenie można wyróżnić następujący zbiór możliwości:

- jednostka-otoczenie,
- jednostka-jednostka,

- jednostka-grupa,
- jednostka-zasób,
- grupa-otoczenie,
- grupa-grupa,
- grupa-zasób,
- zasób-otoczenie,
- zasób-zasób.

Systemy addycyjne zawsze związane są z pewną konwencją narzucaną przez jednostkę, a więc są wobec niej wtórne. Sprawia to, że szczególnie istotna jest analiza człowieka jako takiego, która pozwoli na pełniejsze ujęcie tematu przy zmniejszeniu ryzyka przeakcentowania ważnych, ale mniej istotnych elementów badanego wycinka rzeczywistości z punktu widzenia przeprowadzania operacji informacyjnych.

Rozdział III.
SYSTEMY W CYBERPRZESTRZENI

„Prawidłowość, o ile zachodzi w zjawiskach społecznych i historycznych nie jest odbiciem prawa: «podobne przyczyny wywołują podobne skutki», lecz wyrazem psychologicznej prawdy, że «podobne impulsy wywołują na ogół u ludzi podobne reakcje, choć nigdy nie mamy pewności, że nie wywołają wręcz odwrotnych»”

J. Mosdorf

W poniższym rozdziale opisano podstawowe charakterystyki systemów w cyberprzestrzeni – zarówno jednostki, zasobów, jak i grup. Jako, że istota wszystkich innych systemów poza człowiekiem jest zależna od myśli jednostki (konwencji jaką on przyjmie), to sprawia, że człowiek jest centrum rozważań w temacie oddziaływań informacyjnych, a więc i operacji informacyjnych jako takich. Oczywiście myśl ludzka nie jest w stanie zmienić e.g. kłody drewna w coś innego, albo sprawić, żeby przestała istnieć, ale przez narzucenie pewnej konwencji na zbiór elementarnych cząsteczek (sinoli – bez wchodzenia w szczegóły czym są) możliwe jest ujmowanie danego zbioru jako całości ze względu na funkcję, którą może spełniać.

Aby móc oddziaływać na otoczenie człowiek musi podjąć decyzję. Z drugiej strony decyzja nie jest możliwa bez przetwarzania odpowiednich informacji, które są zdobywane na drodze poznania. Jednak człowiek nie poznaje w sposób absolutny, gdyż w rzeczywistości występuje wiele szczegółów, a jednostka może odebrać i przetworzyć tylko część z nich. Sprawia to, że nawet to co człowiek poznaje może zależeć od jego decyzji. Zarówno poznawanie, jak i podejmowanie decyzji są ze sobą ściśle sprzężone, co jest uwzględnione w toku analizy, w której jednostka (człowiek) będzie traktowana jako system autonomiczny, którego

reakcja na bodziec jest poprzedzona procesem poznawczym i procesem decyzyjnym[101].

W podrozdziale dotyczącym jednostki szczególny nacisk położono na tor informacyjny w człowieku, lecz należy pamiętać iż również przebieg toru energetycznego może wpływać na proces przetwarzania informacji. Wynika z tego, iż zarówno poznanie, jak i podejmowanie decyzji jest uzależnione od energomaterii różnej od informacji. Z tego też powodu opisano podstawowe właściwości toru energetycznego, które są istotne z punktu widzenia oddziaływań informacyjnych.

Rozdział zamknięto rozważaniami związanymi z systemami addycyjnymi (zasobami i grupami). W ramach opisywania zasobów opisano ich rodzaje odwołując się do wzorców systemu autonomicznego i systemu zorganizowanego, jak i podsystemów systemu autonomicznego jednostki, które mogą być wspierane przez zewnętrzne zasoby. Opisano ogólny wzorzec komunikacji między systemami, jak i proces obsługi zasobów. Problem grup opracowano przez odwołanie się do koncepcji nadsystemu autonomicznego. Przywołano również zagadnienia związane z cnotą sprawiedliwości według Doktora Anielskiego, która odpowiada za regulację relacji społecznych, cnotą roztropności w zakresie przyjmowania i dawania rad innym, jak i relacje podsystemu sterującego do podsystemu sterowanego.

3.1. Systemy substancjalne w cyberprzestrzeni

W poniższym podrozdziale opisano proces poznawczy i decyzyjny jednostki powołując się na psychocybernetykę Mazura, którą skonfrontowano i uzupełniono o ujęcie (neo)tomistyczne. Rozbudowano proces decyzyjny o teorię cnót i uczuć Akwinaty, jak i teorię motywacji Kosseckiego i potencjału swobodnego. Podrozdział został zamknięty aktualizacją wzorca psychocybernetycznego Mazura.

---

101 J. Kossecki, *Tajniki Sterowania Ludźmi*, Krajowa Agencja Wydawnicza, Warszawa 1984, p. 75-76.

3.1.1. Proces poznawczy jednostki

Według Mazura system autonomiczny składa się z receptorów, korelatora, homeostatu, efektora, zasilacza i akumulatora. W fazie poznawania biorą udział wszystkie z tych podsystemów, ale w różnym stopniu. Z jednej strony receptory odbierają bodźce odpowiedniego dla nich typu i interpretują je jako informacje. Korelator powinien uzyskiwać informacje, przechowywać je, przetwarzać i wykorzystywać[102]. Zasilacz doprowadza energomaterię do systemu dzięki czemu może ona być kumulowana w akumulatorze i wykorzystywana e.g. do przetwarzania informacji i działania efektorów. Część efektorów jest w stanie skierować receptory w pożądanym przez system kierunku e.g. obrócić głowę, aby jednostka mogła zobaczyć co jest za nią. W końcu homeostat nadzoruje, aby zarówno akumulator, jak i korelator działały, tak aby równowaga funkcjonalna systemu była ciągle zachowana.

Postrzeganie człowieka nie ogranicza się tylko i jedynie do odbioru pewnych obrazów, ale również na badaniu relacji w tym co zostało podane przez zmysły zewnętrzne (receptory). Poza tym, że człowiek widzi psa, to również kojarzy go z innymi psami klasyfikując go właśnie jako psa. Słyszane szczekanie przyporządkowuje właśnie do tego czworonoga, a nie e.g. do jego właściciela, który idzie obok. Sam odbiór bodźców wiąże się od razu z przetwarzaniem uzyskanych informacji. Według ujęcia (neo)tomistycznego za odbiór i przetwarzanie informacji z bodźców odpowiada forma substancjalna człowieka, która ma do dyspozycji pewne władze, czyli pewne właściwości tejże formy[103]. Zmysły zewnętrzne (w przypadku człowieka wzrok, słuch, dotyk, węch i smak) przechwytują bodźce, które są łączone w jedną postać zmysłową, która jest poddawana przetwarzaniu przez dalsze władze[104]. W psychocybernetyce na

---

102 cf. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 176.

103 cf. T. Stępień, op. cit., p. 71. Władze człowieka można podzielić na:

- władze wegetatywne (odżywianie, wzrost, rozmnażanie) i władze ruchu przestrzennego,
- zmysłowe zewnętrzne (smak, dotyk, węch, słuch i wzrok),
- zmysłowe wewnętrzne (zmysł wspólny, wyobraźnia, zmysł osądu, pamięć wraz z przypominaniem, uczucia związane z władzą pożądliwa i władzą gniewliwa),
- intelektualne, nazywane też duchowymi (intelekt czynny, intelekt możnościowy i wola).

cf. ibid., p. 75.

104 cf. ibid., p. 82.

receptor oddziałuje bodziec, który prowadzi do powstania potencjału receptorowego (V_r) na wejściu korelatora[105]. Pojawia się zatem problem w jaki sposób, za pomocą języka cybernetyki, opisać zjawiska e.g. zmysłów zewnętrznych, zmysłu wspólnego[106]. Problem ten nie jest istotny dla operacji informacyjnych, zatem jest tylko zaznaczony jako istotny do rozważenia na polu psychocybernetyki, antropologii filozoficznej, a być może i psychologii. W pracy przyjmuje się, że wytworzenie potencjału receptorowego wiąże się z opisanymi powyżej zjawiskami.

Mazur podzielił zagadnienie pamięci na korelaty (działanie mocy korelacyjnej) i rejestraty (przewodności korelacyjne dla różnych bodźców)[107]. Korelator zbudowany jest ze środowiska korelacyjnego, w którym znajdują się elementy korelacyjne, które można zmieniać oddziałując bodźcem[108]. Każde oddziaływanie bodźca wiąże się z powstaniem mocy korelacyjnej (K), która zwiększa przewodność korelacyjną (G). Im wyższa przewodność korelacyjna tym informacja wynikająca z bodźca jest lepiej zapamiętana (lub po prostu zapamiętana). Zwiększanie przewodności korelacyjnej nazywane jest procesem rejestracji, w wyniku którego powstają rejestraty. Derejestracja polega na zmniejszaniu się przewodności korelacyjnej w czasie, co związane jest z zanikiem rejestratów[109]. Dodatkowo mogą nastąpić zjawisko detrakcji, w której moc korelacyjna została przyłożona do innych miejsc środowiska korelacyjnego, a więc jednostka nie ma dostępu do informacji odłożonych w niektórych rejestratach. Innym zjawiskiem jest przywrócenie takiego dostępu przez ponowne skierowanie mocy korelacyjnej do pożądanego miejsca środowiska korelacyjnego, który to proces nazwany jest retrakcją[110].

---

105 cf. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 176-177.
106 Za przechowywanie informacji odpowiedzialny jest korelator, a zatem wydaje się, że nawet receptory muszą mieć swoje korelatory do przechowywania informacji do ich obróbki. Też nie jest jasne czy zmysł wspólny jest jeszcze receptorem (receptor wewnętrzny), czy już korelatorem, a być może jest pewną formą pośrednią (pewnym układem będącym za receptorem, a przed korelatorem).
107 cf. ibid., p. 126.
108 cf. ibid., p. 175-176.
109 cf. ibid., p. 177-180.
110 cf. ibid., p. 183-184.

Według koncepcji (neo)tomistycznej człowiek jest istotą duchowo-cielesną[111], a więc poza przebiegami energomaterialnymi również przetwarza informacje nieenergomaterialne nazywane duchowymi lub intelektualnymi. Próbując osadzić wzorzec Mazura dotyczący pamięci w ujęciu neotomistycznym należy odwołać się ponownie do władz człowieka. W ramach władz zmysłowych zapamiętywanie postaci zmysłowych (wypadkowej wszystkich bodźców oddziałujących na zmysły zewnętrzne, które zostały scalone przez zmysł wspólny) odbywa się w wyobraźni, która je zapamiętuje i ma możliwość ich przypominania. Co więcej postacie zmysłowe są oceniane przez zmysł osądu jako przyjemne lub nieprzyjemne (bezpieczne lub jako pewne źródło zagrożenia), a ocena odciska się w pamięci, skąd te oceny mogą być też wydobywane przy następnych ocenach[112]. Zatem środowiskiem korelacyjnym wewnętrznych władz zmysłowych człowieka jest jego mózg, który jest organem wewnętrznych władz zmysłowych.[113] To właśnie w nim pod wpływem korelatów (sygnałów w mózgu) powstają rejestraty. Potwierdzają to również odkrycia neuronauk, które wskazują na cechę neuroplastyczności mózgu[114]. Podobnie sytuacja się ma z wyabstrahowanymi (a więc pozbawionymi szczegółowych, fizycznych cech), przez intelekt czynny, postaciami intelektualnymi. Przechowywane są w intelekcie możnościowym a wydobywane są z niego przez intelekt czynny[115]. Środowiskiem korelacyjnym postaci intelektualnych jest więc intelekt możnościowy, a moc korelacyjna jest generowana przez intelekt czynny. Co więcej według Doktora Anielskiego intelekt nie posiada swojego organu cielesnego, a więc przechowywanie i przetwarzanie postaci intelektualnych odbywa się poza mózgiem[116]. Pomimo różnych charakterów rejestratów władz zmysłowych i intelektualnych obydwa biorą udział w procesie myślenia[117]. Należy zaznaczyć sprzeczność ujęcia tomistycznego

111 cf. T. Stępień, op. cit., p. 33.
112 cf. ibid., p. 78-82.
113 cf. ibid., p. 72.
114 v. N. Carr, *The Shallows. What the Internet is doing to our brains*, W.W. Norton & Company, Nowy York, Londyn 2010, p. 25-29.
115 cf. T. Stępień, op. cit., p. 86.
116 cf. ibid., p. 72, 82.
117 cf. ibid., p. 83-84.

z ujęciem jakościowej teorii informacji Mazura. Mazur definiował komunikat (który składa się na informację) jako stan fizyczny, natomiast tomizm zakłada istnienie komunikatów intelektualnych (w ramach postaci intelektualnych), które nie posiadają fizycznych właściwości. Zaistniała aporia nie wpływa jednak na dalsze analizy przeprowadzane w pracy.

Mazur wyróżnił dodatkowo rodzaje intelektu, które są wypadkową trzech właściwości korelatora, a które wpływają na proces przetwarzania informacji[118]:

- inteligencji – odnoszącej się do pojemności korelatora (im większa pojemność, tym większa inteligencja),
- pojętności – odnoszącej się do szybkości zapamiętywania informacji (im większa szybkość zapamiętywania, tym większa pojętność),
- talentu – odnoszącego się do preferencyjności w przetwarzaniu informacji danego typu.

Wedle (neo)tomizmu istnieją specyficzne dla jednostki struktury poznawcze, które działają na zasadzie, że jeśli dana osoba słyszy mowę w znanym przez nią języku, to musi ją odebrać, zrozumieć i przetworzyć na swoją mowę wewnętrzną, aby nowe informacje były kompatybilne z wcześniej uporządkowaną przez daną jednostkę wiedzą[119].

Rejestraty w korelatorze można dodatkowo podzielić za Kosseckim na pojęcia i stereotypy. Według Kosseckiego pojęcia posiadają charakter czysto poznawczy, natomiast stereotypy są silnie wartościujące, co związane jest z generowaniem silnych emocji. Stereotypy mogą być zarówno pozytywne, albo negatywne[120]. Siłą rzeczy kojarzenie negatywnie lub pozytywnie dużej grupy ludzi najprawdopodobniej będzie prowadziło do błędów poznawczych, a więc i błędów decyzyjnych.

---

118 v. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 281-282.
119 cf. M. Gogacz, *Elementarz...*, op. cit., p. 87.
120 cf. J. Kossecki, *O pewnych stereotypach wykorzystywanych do działań dezinformacyjnych i dezintegracyjnych*, in: *Socjotechnika w polityce - wczoraj i dziś*, vol. 2, A. Kasińska-Metryka, A. Kasowska-Pedrycz (red.), Wydawnictwo Uniwersytetu Humanistyczno-Przyrodniczego Jana Kochanowskiego, Kielce 2009, p. 113-114.

Co więcej Mazur wyróżnia trzy problemy poznawcze, które jednostka musi rozwiązać w procesie poznawania rzeczywistości. Na każdym tym etapie mogą pojawić się zakłamania wynikające z natury ludzkiego poznania lub nieprawdziwych rejestratów. Do tych problemów należą[121]:

- eksploracja – określenie czy dany system istnieje,
- klasyfikacja – określenie z jakich elementów się składa,
- eksplikacja – określenie relacji między tymi elementami.

Również analiza ryzyka, która może służyć atakowi na system (zarówno jednostkę, jak i grupę) musi wiązać się z rozwiązaniem problemów wyróżnionych przez Mazura w tym zakresie, że trzeba ustalić strukturę atakowanego systemu (elementy z jakich się składa i relacje między nimi), aby wykorzystać jej słabości do skutecznego ataku.

3.1.2. Proces decyzyjny jednostki

Wśród wszystkich systemów wyróżnionych w ramach analizy systemowej tylko ludzie są zdolni do podejmowania decyzji. Grupy są tylko myślą ujmowaną przez jednostki. Podobnie zasoby nie posiadają zdolności decyzyjnej. Dla przykładu komputery nie podejmują decyzji, ale po prostu działają tak jak zostały zaprojektowane przez człowieka[122]. W ujęciu filozoficznym św. Tomasz z Akwinu twierdzi, że władza ludzka jaką jest wola jest wolna, czyli nie podlega konieczności przymusu[123]. Według tej szkoły wolę można usprawniać. Sposobem na usprawnienie woli jest zdobywanie stałych dyspozycji ku dobru, które nazywane są cnotami[124]. Cnoty można kształtować przez popełnianie czynów równych lub większych od aktualnie posiadanych sprawności[125]. Głównymi cnotami (sprawnościami) woli są[126]:

---

121 cf. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 99-101.
122 cf. ibid., p. 110.
123 cf. T. Stępień, op. cit., p. 107.
124 cf. ibid., p. 137-141.
125 cf. ibid., p. 140.
126 cf. ibid., p. 152-154.

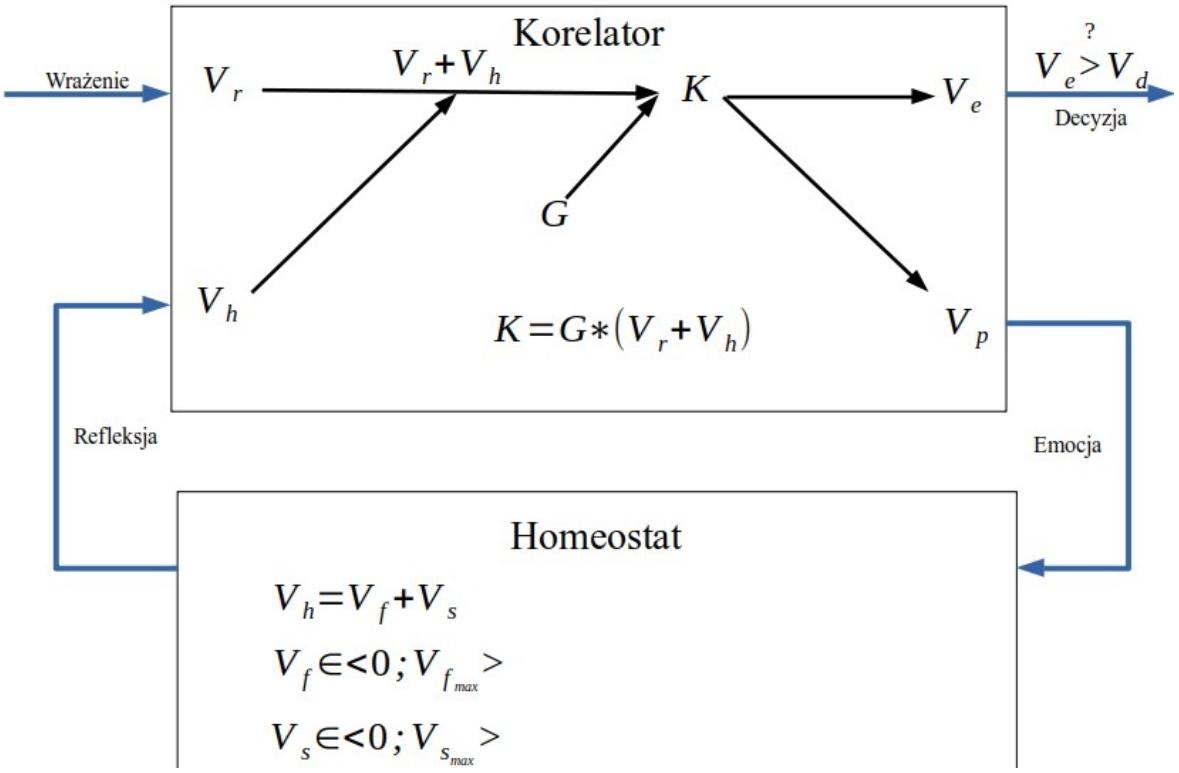
- roztropność – kierowanie się dobrem wykrytym przez rozum,
- sprawiedliwość – dotyczy ładu w relacjach międzyludzkich, czyli tego, aby oddawać każdemu to co mu się słusznie należy,
- męstwo – przeciwstawianie się niebezpieczeństwu i znoszenie cierpień świadomie i z rozwagą,
- umiarkowanie – kierowanie się umiarem w dziedzinie ludzkiego pożądania.

Kierowanie się cnotami prowadzi do prawdziwego szczęścia i trwałego zadowolenia[127]. Tradycja tomistyczna, upatruje źródła sukcesów zawodowych, towarzyskich i tych związanych z życiem osobistym i z interesami w cnotach, a więc usprawnieniach woli[128].

Aby ustalić rolę wolnej woli w psychocybernetycznym wzorcu podejmowania decyzji należy najpierw opisać ten proces. Wrażenie jest bodźcem z receptorów i powoduje powstanie na wejściu korelatora potencjału receptorowego (V_r). Potencjał receptorowy oddziałuje na rejestraty przez co wytwarza się potencjał efektorowy (V_e) i potencjał perturbacyjny (V_p). Potencjał perturbacyjny oddziałuje jako emocja na homeostat, który reaguje na cały proces refleksją wytwarzając potencjał homeostatyczny (V_h). Jeśli korelat, powstały w wyniku oddziaływania sumy potencjału receptorowego i potencjału homeostatycznego dla danej przewodności korelacyjnej (G), wytworzy taki potencjał efektorowy, który przekroczy potencjał decyzyjny (V_d), wtedy dochodzi do wyzwolenia reakcji w efektorach[129]. Kossecki określił potencjał homeostatyczny jako sumę oddziaływania homeostatu fizykalnego (V_f) i potencjału swobodnego (V_s). Potencjał swobodny występuje tylko i jedynie u ludzi i reprezentuje właśnie wolną wolę (zdolność do samoregulacji)[130]. Dzięki potencjałowi swobodnemu jednostka może się samosterować nawet wbrew swojemu interesowi energomaterialnemu.

127 cf. ibid., p. 154.
128 v. A. Andrzejuk, *Tomasz z Akwinu jako psycholog*, Wydawnictwo von Borowiecky, Warszawa 2020, p. 76.
129 cf. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 194-201.
130 cf. J. Kossecki*, PSC 9A. Człowiek jako proces autonomiczny - wykład (HD)*, https://www.youtube.com/watch?v=7P1wIZNv6dM, wykład online, dostęp na 04.08.2021.

W przypadku podejmowania decyzji możliwe jest, że już potencjał receptorowy będzie na tyle silny, że spowoduje decyzję. Z drugiej strony możliwe jest też, że decyzja zostanie podjęta po wielu emocjach korelatora oddziałujących na homeostat i wielu refleksjach homeostatu oddziałującego na korelator. Dodatkowo w pracy przyjęto, że możliwości oddziaływania homeostatu na korelator nie są nieograniczone (a więc refleksja nie może być dowolnie silna). Przyjmuje się zatem, że $V_f \in <0;V_{f_{max}}>$ i $V_s \in <0;V_{s_{max}}>$. Istnieje zatem maksymalny potencjał fizykalny jaki może być przyłożony do korelatora. Podobnie siła woli (potencjał swobodny) jest ograniczona. Na podstawie rozważań filozoficznych z zakresu antropologii (neo)tomistycznej wydaje się, że $V_{s_{max}}$ może się zwiększać lub zmniejszać w czasie po świadomych działaniach jednostki. Taka forma zapisu posiada również tę zaletę, że można nią opisać dowolny system autonomiczny, a przy niektórych z nich (jak e.g. rośliny, zwierzęta, czy bardziej zaawansowane maszyny) ustalić, że $V_{s_{max}}=0$.



Rys. 20: Korelator i homeostat

źródło: opracowanie własne na podstawie: M. Mazur, *Cybernetyka i charakter...*, op. cit., p. 199, 222; J. Kossecki*, PSC 9A...* op. cit.

Istotny dla działania homeostatu jest również akumulator (związany z przetwarzaniem mocy fizjologicznej systemu), który przeciąża lub odciąża homeostat, a sam jest sprężany lub odprężany[131]. Jako jeden z parametrów związanych z akumulatorem Mazur wyróżnia dynamizm charakteru (D), który związany jest ze współczynnikiem rozbudowy systemu C (odzwierciedlający szybkość przyrostu ilości tworzywa, z którego zbudowany jest system) i ze współczynnikiem starzenia się tworzywa A (a więc zmianą jakości każdej jednostki tworzywa, z której zbudowany jest system). Dynamizm charakteru określa się jako $D=\log\frac{C}{A}$[132]. Na podstawie logarytmu stosunku współczynnika rozbudowy do

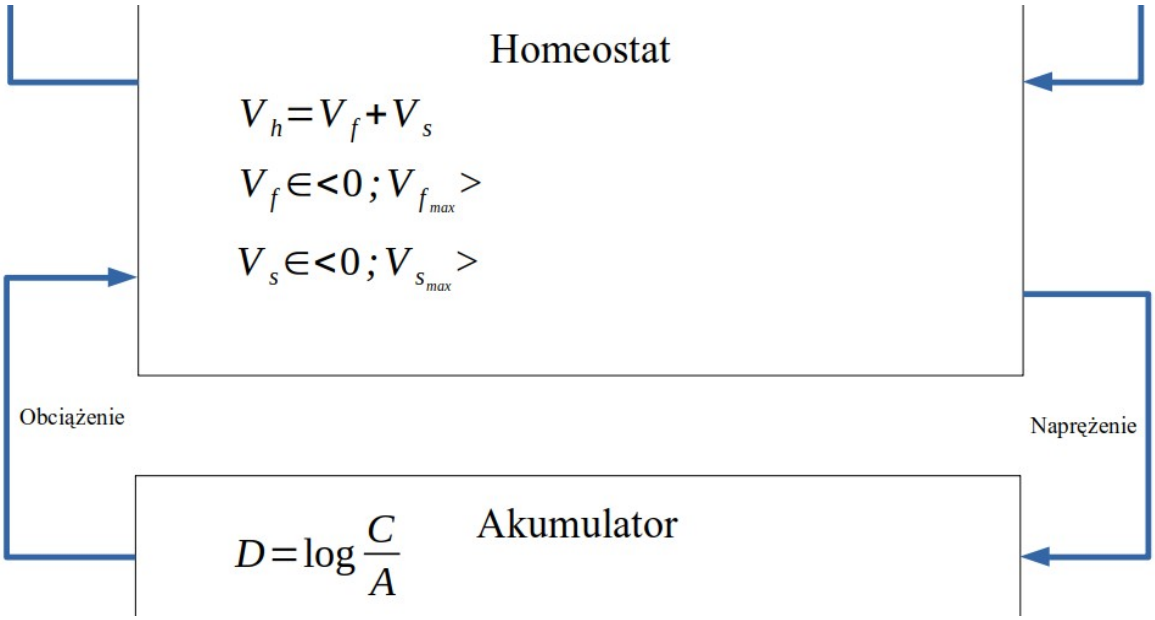
131 cf. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 225-226.
132 cf. ibid., p. 227-231, 290-291.

współczynnika starzenia się można umownie wyróżnić następujące typy dynamizmu charakteru[133]:

- egzodynamik – wyraźny, dodatni dynamizm charakteru,
- egzostatyk – dość wyraźny, dodatni dynamizm charakteru,
- statyk – dynamizm charakteru jest bliski zeru,
- endostatyk – dość wyraźny, ujemy dynamizm charakteru,
- endodynamik – wyraźny, ujemny dynamizm charakteru.

Dynamizm charakteru przejawia się w działaniu systemu tym, że egzodynamicy rozpraszają energomaterię, statycy tyle rozpraszają co gromadzą, a endodynamicy więcej gromadzą, niż rozpraszają. Wynika z tego, że egzodynamicy częściej reagują, ich reakcje są szybsze i silniejsze. Ta tendencja zmniejsza się wraz z dynamizmem charakteru, aż do endodynamizmu, którego przedstawiciele reagują rzadko, a jeśli dochodzi do ich reakcji, to są one słabe[134]. Relację homeostatu i akumulatora można przedstawić poniższym schematem:

133 cf. ibid., 293-295.
134 cf. ibid., p. 298.



Rys. 21: Homeostat i akumulator

źródło: opracowanie własne na podstawie: M. Mazur, *Cybernetyka i charakter...*, op. cit., p. 224.

Mazur wyróżnił również szerokość charakteru systemu (L), która jest sumą tolerancji (T) i podatności (M), czyli $L = T + M$. Tolerancja jest związana z pojęciem aprobaty, a więc ze wzrastaniem potencjału homeostatycznego w ramach refleksji. Tolerancja jest długością między dwoma dynamizmami granicznymi, a więc dwoma bodźcami, mniejszymi i większymi od dynamizmu charakteru, które jeszcze wywołują decyzję w danym systemie. Z kolei podatność jest zakresem między takimi bodźcami, które są wywoływane pod przymusem, a na które system jeszcze reaguje[135]. Zatem jednostka o dużej tolerancji działa nawet jeśli dana sytuacja (bodziec) jest bardzo niezgodna z jej dynamizmem (ale w zakresie tolerancji), natomiast przy niskiej tolerancji zakres działania niezgodnego z dynamizmem charakteru jest niewielki. Podatność określa jak bardzo dana jednostka może zostać przymuszona do działania – im wyższa podatność, tym wyższa możliwość przymuszenia danej jednostki. Dla przykładu osoba egzodynamiczna, która ma tendencję do rozpraszania energii, może wysiedzieć długi czas w bibliotece, gdzie trzeba zachować ciszę, tylko jeśli posiada wysoką

135 cf. ibid., p. 195, 366-368.

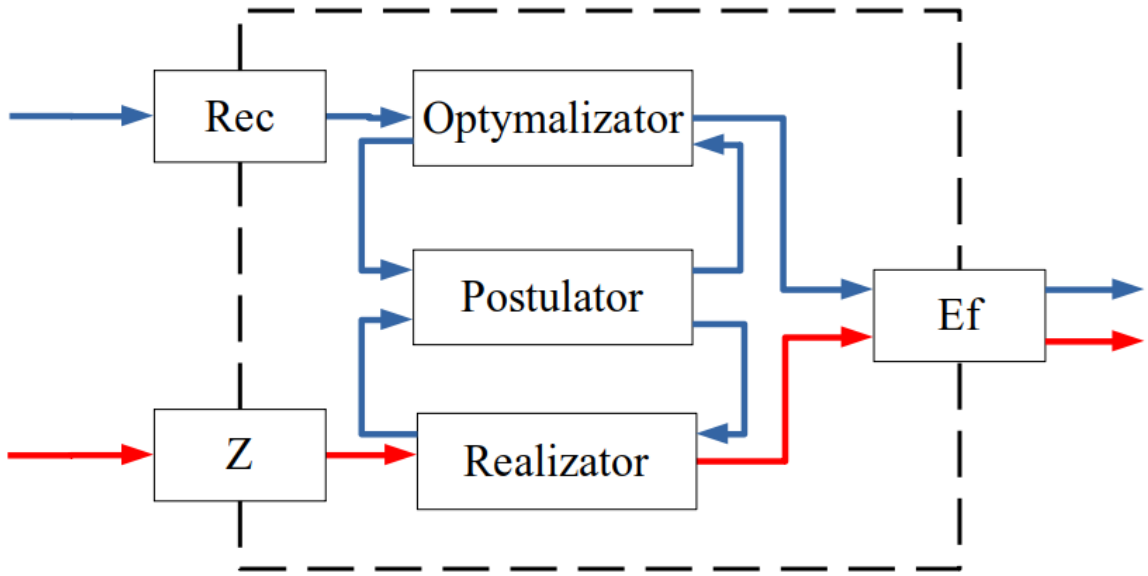
tolerancję lub wysoką podatność (zakładając, że została przymuszona do tej czynności). Podobnie rzecz się ma z próbą nakłonienia endodynamika na spotkanie towarzyskie, gdzie będzie miał do czynienia z dużą liczbą bardzo towarzyskich osób. Tylko przy wysokiej tolerancji lub wysokiej podatności możliwe jest, aby endodynamik zgodził się na taką inicjatywę.

W ramach podejmowania decyzji należy rozwiązać problemy decyzyjne. Mazur dowodzi, że istnieją trzy i tylko trzy problemy decyzyjne[136]:

- postulacja – odpowiadający na pytania „Co osiągnąć? Jaki system osiągnąć?”,
- optymalizacja – odpowiadająca na pytania „Jak osiągnąć zadany system? Jaką transformacją?”,
- realizacja – odpowiadająca na pytanie „Z czego osiągnąć dany system?”.

Możliwe jest zestawienie problemu postulacji z działalnością homeostatu, który miałby określać cel działania. Działanie korelatora odpowiednie jest problemowi optymalizacji, a więc poszukiwaniu najlepszej transformacji dla danego systemu. Z kolei realizator spełnia funkcję wydatkowania energii w celu realizacji postawionego zadania przez postulator za pomocą sposobu opracowanego przez optymalizator[137].

136 cf. M. Mazur, *Pojęcie systemu...*, op. cit., p. 7.
137 cf. ibid.



Rys. 22: Problemy decyzyjne a system autonomiczny

źródło: opracowanie własne na podstawie: M. Mazur, *Pojęcie systemu...*, op. cit., p. 8.

Z kolei proces decyzyjny u Akwinaty wygląda następująco:

Tabela 1: Proces decyzyjny według św. Tomasza z Akwinu

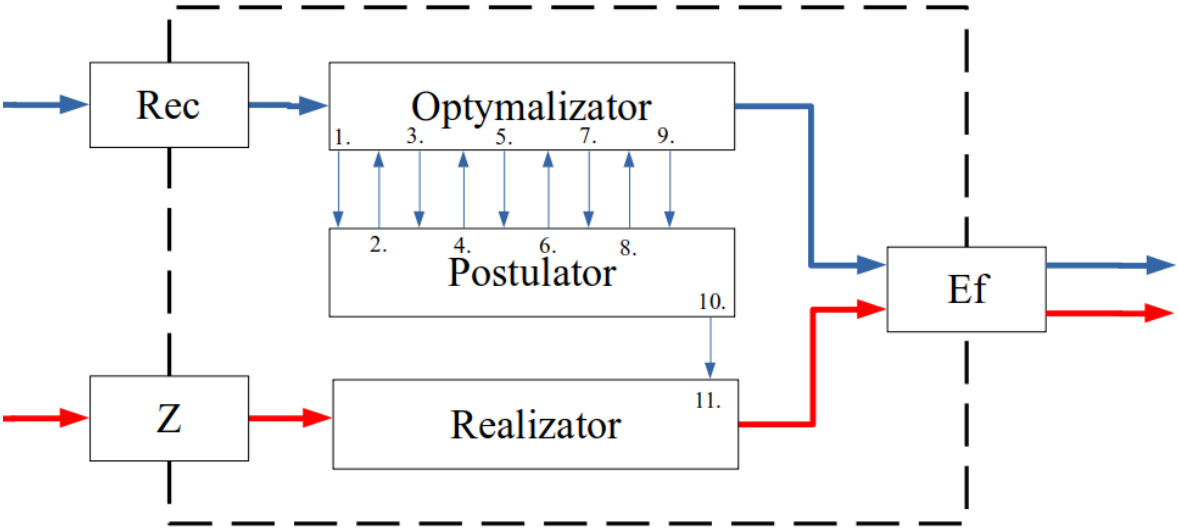
źródło: opracowanie własne na podstawie: T. Stępień, op. cit., p. 117.

L.p.	etap	nazwa aktu	opis	odpowiedzialna władza
1.		pomysł	myśl o przedmiocie jako dobrym	rozum
2.		upodobanie	uznanie przedmiotu jako dobry	wola
3.	zamierzenie	zamysł	myśl o przedmiocie jako celu	rozum
4.		zamiar	uznanie przedmiotu za cel	wola
5.		namysł	rozważenie środków do osiągnięcia celu	rozum
6.		przyzwolenie	odrzucenie niektórych środków	wola
7.		rozmysł	rozsądzenie między środkami	rozum
8.		wybór	wybór jednego ze środków	wola

L.p.	etap	nazwa aktu	opis	odpowiedzialna władza
9.	wykonanie	rozkaz	postanowienie czynu	rozum
10.		wykonanie czynne	wykonanie woli	wola
11.		wykonanie bierne	wykonanie przez inne władze	inne władze
12.		zadowolenie	zadowolenie z osiągniętego czynu	wola
13.		osąd	myśl o procesie osiągnięcia celu	rozum

Uznając, że rozum wykonuje zadanie optymalizacji, wola postulatora, a inne władze odpowiadają za realizację można powyższy proces nanieść na schemat systemu autonomicznego, w którym uwzględniono problemy decyzyjne. Warto dodać, że 12. i 13. akt nie jest umieszczony, gdyż wynika on z obserwacji skutków swoich działań, a więc jest związany z odrębnym procesem poznawczym. Strzałki z numerem fazy procesu decyzyjnego nie oznaczają różnych torów informacyjnych, ale oddzielono je dla przejrzystości odwzorowania procesu decyzyjnego. Oczywiście w trakcie procesu mogą pojawiać się w korelatorze nowe informacje z receptora lub mogą być odczytywane już zapamiętane przez kierowanie mocy korelacyjnej przez rejestraty, co może spowodować e.g. dodanie w fazie rozmysłu (7.) dodatkowego środka i cofnięcie się do namysłu (5.). Ewentualnie pewne nowe informacje mogą poddać w wątpliwość czy cel jest godny wysiłku, co cofa proces decyzyjny do zamysłu (3.). W każdym razie czyn będący już w akcie wykonania biernego (11.) wyzwala reakcję efektora, która już oddziałuje na rzeczywistość, a więc nie da się jej cofnąć. Pojawia się pytanie jak rozkaz (9.) i wykonanie czynne (10.) i bierne (11.) mają się do przełamania potencjału decyzyjnego (V_d) w korelatorze. Być może w akcie rozkazu (9.) poza oddziaływaniem emocją (potencjałem perturbacyjnym V_p) na homeostat (postulator) również dochodzi do wytworzenia decyzji (przekroczenia potencjałem efektorowym V_e potencjału decyzyjnego V_d). Pozwoliłoby to uniesprzecznić

obydwa ujęcia. Kwestia ta wymaga bardziej szczegółowych badań na linii psychocybernetyki i (neo)tomistycznej antropologii filozoficznej.



Rys. 23: Proces decyzyjny św. Tomasza z Akwinu w systemie autonomicznym

źródło: opracowanie własne na podstawie: M. Mazur, *Pojęcie systemu...*, op. cit., p. 8; T. Stępień, op. cit., p. 117.

Kossecki wyróżnia bodźce motywacyjne, które w nadsystemie jakim jest grupa nazywane są normami społecznymi. Do bodźców motywacyjnych należą[138]:

- bodźce witalne – dotyczą bodźców związanych z reprodukcją, przyjemnościami, pozycją w grupie i pozycją grupy na tle innych grup (odwołują się do ilości i jakości tworzywa systemu), jak i posłuszeństwa wobec władzy[139],
- bodźce ekonomiczne – odnoszące się do zysku i straty (odwołują się do toru energetycznego w grupie),
- bodźce konstytutywne – związane ze strukturą grupy:
  - odnoszące się do celu grupy:

138 cf. J. Kossecki, *Tajniki...*, op. cit., p. 76-78.
139 v. J. Kossecki, *Metacybernetyka*, op. cit., p. 184.

        - normy ideologiczne – związane ze zgodnością lub jej brakiem z wiodącym systemem ideologicznym w danej grupie (mogą dotyczyć e.g. patriotyzmu, katolicyzmu, komunizmu etc.),
    - odnoszące się do metod osiągnięcia celu przez grupę:
        - bodźce etyczne – oddziaływania tylko informacyjne związane z metodami osiągania celów (e.g. wyrzuty sumienia, infamia etc.),
        - bodźce prawne – podobnie jak bodźce etyczne, ale poza oddziaływaniem informacyjnym możliwe są również represje energetyczne (e.g. więzienie, przymus fizyczny, kara śmierci etc.).
- bodźce poznawcze – związane z prawdą i fałszem.

Każda jednostka posiada pewne motywacje, a więc reaguje w sposób szczególny (aprobatą) na rodzaj bodźców zgodny z daną motywacją. A więc osoba, która kieruje się motywacjami ekonomicznymi będzie bardziej skora do działania, jeśli w ramach próby sterowania nią używać się będzie bodźców ekonomicznych takich jak obiecanie wysokiego zysku, albo zagrożenie stratą. Innym przykładem może być osoba, która kieruje się bodźcami poznawczymi, a więc która szczególnie będzie zainteresowana zgłębianiem rzeczywistości i dojściem do Prawdy. Oddziaływanie na osobę o dominujących bodźcach poznawczych e.g. bodźcami ekonomicznymi (próba przekupienia) lub bodźcami witalnymi (oferowanie dostępu do różnych przyjemności, zaszczytów etc.) może okazać się wielce nieskuteczna.

Podczas procesu podejmowania decyzji biorą udział również emocje[140] (oddziaływania korelatora na homeostat), które są stricte związane z celem (a więc dążeniem do dobra lub unikaniem zła). Należą do nich uczucia władzy pożądliwej[141] i uczucia władzy gniewliwej[142]. Nie jest jednak jasne czy uczucia w (neo)tomizmie są tym samym co emocje w psychocybernetyce Mazura, gdyż

140 Jako, że nie istnieje jedna definicja *emocji* i *uczuć*, a praca nie wymaga szczegółowej analizy tego zagadnienia, to obydwa terminy będą traktowane zamiennie, aczkolwiek z naciskiem na używanie terminu *emocja* ze względu na, to iż Mazur tak nazwał oddziaływanie korelatora na homeostat.
141 cf. T. Stępień, op. cit., p. 101.
142 cf. ibid., p. 104.

skoro uczucia są nakierunkowane na cel, to wydaje się, że powinny bezpośrednio dotyczyć homeostatu (ze względu na problem postulacji) i składać się na potencjał fizykalny, a nie być tylko potencjałem oddziałującym na homeostat. Dodatkowo różni się sposób działania władz intelektualnych wobec emocji. Wola kieruje uczuciami jak władca niewolnikami (w sposób absolutny), a rozum po królewsku (przedstawiając pewne argumenty, racje do rozważenia), a więc człowiek za pomocą władzy rozumu stara się przedstawiać sobie takie racje, aby uspokoić emocje lub nakierować je w pożądany przez siebie sposób[143]. I tak stan korelatora (władze poznawcze) odpowiada za ewentualne powstanie emocji. Efekt potencjału perturbacyjnego (odpowiedzialny za powstanie emocji) może być już w samym homeostacie zmniejszony potencjałem swobodnym (siłą woli), który jest częścią potencjału homeostatycznego.

Podstawowe emocje według tomizmu związane z konkretnymi władzami wyglądają następująco:

Tabela 2: Uczucia władzy pożądliwej zorientowane na dobro

źródło: opracowanie własne na podstawie: T. Stępień, op. cit., p. 101.

emocja	**opis**
miłość	źródło dążenia do dobra
pożądanie	proste dążenie do dobra
przyjemność	zjednoczenie z dobrem

Tabela 3: Uczucia władzy pożądliwej zorientowane na zło

źródło: opracowanie własne na podstawie: T. Stępień, op. cit., p. 101.

emocja	**opis**
niechęć	źródło unikania zła
wstręt	proste unikanie zła
ból	zjednoczenie ze złem

143 cf. ibid., p. 95-96.

Tabela 4: Uczucia władzy gniewliwej

źródło: opracowanie własne na podstawie: T. Stępień, op. cit., p. 104-105.

cel	**oddalanie/ przybliżanie**	**emocja**	**opis**
dobro	przybliżanie	nadzieja	dążenie do trudnego dobra, któremu towarzyszy trud
dobro	oddalanie	rozpacz	rezygnacja z trudnego dobra z powodu przeszkód
zło	przybliżanie	odwaga	konfrontacja z trudnym do uniknięcia złem
zło	oddalanie	bojaźń	wycofanie się w celu uniknięcia zła
zło	brak możliwości uniknięcia konfrontacji	gniew	próba przezwyciężenia obecnego zła (realnego lub wyobrażonego), niemożliwego do uniknięcia, przez zaatakowanie go

Emocje władzy pożądliwej dotyczą dążenia do dobra i unikania zła. Dla przykładu, jeśli jakiś byt posiadający emocje miłuje (w znaczeniu lubi, ale nie w znaczeniu miłości rozumianej jako chęci dobra dla drugiej osoby, gdyż takie nastawienie wynika z władz intelektualnych, a nie z emocji) inny byt. E.g. gdy człowiek miłuje pieniądze, to gdy zidentyfikuje swoimi władzami zysk, to może odczuć pożądanie, które będzie motywowało go do zjednoczenia się z tym rodzajem dobra. Jeśli dążenie się uda, to dana osoba odczuje radość. W przypadku odwrotnym – gdy dana osoba nienawidzi e.g. swojego przełożonego, to będzie odczuwała wstręt, który motywuje daną osobę do jego unikania. Jeśli unikanie będzie nieskuteczne i dojdzie do spotkania z osobą, której się nienawidzi, to osoba nienawidząca odczuje pewien ból.

Emocje władzy gniewliwej pojawiają się, gdy osoba napotka przeszkody w dążeniu do swojego celu (osiągnięcia pewnego dobra lub uniknięcia pewnego zła). Jeśli osoba odczuje, że przybliża się do pożądanego dobra, to odczuje nadzieję, a jeśli dla osoby pożądane dobro się oddala, to odczuje ona rozpacz lub smutek. Pozostałe emocje władzy gniewliwej wyzwalane są w przypadku napotkania zła w dążeniu do celu. Jeśli osoba czuje, że sprosta przeszkodzie, to

odczuje odwagę, a jeśli czuje, że nie ma odpowiednich zasobów do tego, to odczuje bojaźń. Jeśli jednostka skonfrontuje się ze złem przed którym nie może uciec, to odczuje gniew, który będzie motywował daną osobę do ataku na to zło.

3.1.3. Aktualizacja wzorca psychocybernetycznego Mazura

Wzorzec teoretyczny dotyczący odbierania bodźców, rejestracji i derejestracji jest problematyczny i wydaje się, że wymaga uzupełnienia. Autor nie będzie zatem wykorzystywał zależności wynikających ze szczegółowych wzorów w ramach tych wzorców z trzech powodów. Po pierwsze szczegółowe pomiary potencjałów w mózgu są zagadnieniami stricte neuronauk[144], czym autor się nie zajmuje, po drugie intencją autora nie jest badanie zależności ilościowych (na skalach przedziałowej i stosunkowej), ale jakościowych (szczególnie porządkowych) ze względu na założony poziom ogólności analizy. Mimo to wykorzystanie psychocybernetycznego wzorca teoretycznego Mazura wiąże się z ogromnym zyskiem diagnostycznym ze względu na wyróżnienie zależności potencjałów homeostatycznego, receptorowego, perturbacyjnego i efektorowego od siebie oraz ich związek z przewodnością korelacyjną.

Mazur zaznaczył, że na zachowanie człowieka wpływają następujące czynniki[145]:

- Informacyjne (na podstawie zależności $K = G * (V_r + V_h)$):
  - S – aktualne bodźce, które wywołują potencjał receptorowy V_r,
  - V_h – potencjał homeostatyczny (w rozumieniu Mazura jest tożsamy z potencjałem fizykalnym – V_f wyróżnionym przez Kosseckiego),
  - G – przewodność korelacyjna, która może być interpretowana jako aktualna pamięć systemu.
- Energetyczne (na podstawie zależności $P = P_0 + P_d = P_0 + P_r + P_s$):
  - P_0 – moc jałowa wykorzystywana do utrzymania systemu w istnieniu,

144 Co więcej, co zostało już zaznaczone w pracy, nie każde środowisko korelacyjne ma charakter materialny.
145 v. M. Mazur, *Cybernetyka i charakter*, op. cit., p. 251-252.

- P_r – moc robocza, która jest zużywana na sterowanie otoczeniem w celu zdobycia mocy jałowej,
- P_s – moc swobodna, która jest do dyspozycji systemu.

Z drugiej strony możliwe jest przeanalizowanie reakcji systemu autonomicznego na bodziec przez uwzględnienie reaktywności każdego z podsystemów, z których składa się system autonomiczny. Można to wyrazić wzorem:

$$R = r\left(r_{Rec}, r_{Kor}, r_{Hom}, r_{Ef}, r_{Ak}, r_{Zas}\right) * S$$, gdzie

- R – reakcja systemu,
- S – bodziec,
- funkcja r – reaktywność systemu autonomicznego,
- r_{Rec} – reaktywność receptora lub receptorów zgodnych z bodźcem S,
- r_{Kor}– reaktywność korelatora,
- r_{Hom} – reaktywność homeostatu,
- r_{Ef} – reaktywność efektorów,
- r_{Ak} – reaktywność akumulatora,
- r_{Zas} – reaktywność zasilacza zgodna z bodźcem S.

Co więcej system nie działa na bodźcu zewnętrznym, ale na pewnym jego wyobrażeniu, czyli na potencjale receptorowym V_r, który oddziałuje na wejście korelatora. Zakładając, że tor sterowniczy między receptorami a korelatorem nie zmienia potencjału, albo czyni to w sposób pomijalny, można wyliczyć V_r w następujący sposób:

$$V_r = S * r_{Rec}$$

Dzięki takiemu zabiegowi możliwe jest skorygowanie Mazura, gdyż reakcja na bodziec może być niezależna od siły bodźca dla jednego systemu, jeśli receptory nie potrafią odbierać danego bodźca ($r_{Rec} = 0$, dla e.g. osoby niewidomej, na którą oddziałuje się światłem lub w przypadku systemu bez dostępu do radia lub innego odbiornika fali radiowej, na który oddziałuje się właśnie falą radiową).

W podobny sposób można potraktować reaktywność zasilacza (r_{Zas}) i bodźce energomaterialne. Nie umniejszy to samej jakości analizy, gdyż, za Mazurem, będzie uwzględniona moc systemu ($P=\frac{E}{t}$), w której już zawarta jest energia, którą system operuje, a która została wcześniej przetworzona przez zasilacz. Reaktywność akumulatora (r_{Ak}) zależy nie tylko od aktualnej energii systemu, ale również od dynamizmu charakteru (D), podatności (M) i tolerancji (T). To czy akumulator zadziała na homeostat zwiększając V_f zależy od tego, czy postrzegane lub planowane działanie jest zgodne z dynamizmem charakteru, a więc mieści się w przedziale $<D-\frac{T}{2}-\frac{M}{2};D+\frac{T}{2}+\frac{M}{2}>$. Moc systemu jest również zależna od jakości materiału (a), z którego składa się system, jednakże ten czynnik został przez Mazura ujęty w dynamizmie charakteru[146].

W przypadku korelatora poza potencjałem receptorowym V_r (ściśle powiązanym z bodźcem S), przewodnością korelacyjną G i potencjałem homeostatycznym V_h na reaktywność tego podsystemu wpływają zdolności do przetwarzania informacji, a więc intelekt, na który składają się inteligencja (Int), pojemność (Poj) i talent (Tal). Na potencjał homeostatyczny, jak już wcześniej nadmieniono, składa się potencjał fizykalny V_f i potencjał swobodny V_s. Kolejnym istotnym czynnikiem związanym z pracą homeostatu jest motywacja na dany rodzaj bodźców (Mot), który oddziałuje na wejście lub został wzbudzony potencjałem swobodnym. Jednostka silnie zmotywowana pewnym rodzajem bodźców może działać, nawet jeśli potencjał receptorowy w korelatorze jest relatywnie niski. Wyróżnienie jednocześnie potencjału swobodnego i motywacji pozwoli na opisanie zjawiska, w którym dana jednostka posiada ogromne zasoby samokontroli, a jednak nie chce robić danych czynności albo może mieć ogromne chęci (motywację), ale niewielki zasób samokontroli, a jednak ani w jednym, ani w drugim przypadku nie dochodzi do reakcji systemu. Co więcej efektory systemu

146 cf. ibid., p. 289. Jakość materiału jest powiązana z mocą systemu przez współczynnik starzenia i początkową jakość materiału.

mogą nawet w znaczny sposób wzmacniać lub osłabiać reakcję R powstałą pod wpływem decyzji (jeśli V_e przekroczył V_d). Zagadnienie to jest szczególnie istotne, gdy jednostka korzysta z pewnych zewnętrznych zasobów, które mogą przekroczyć naturalne ograniczenia człowieka. Reaktywność efektora jest dodatkowo zależna od akumulatora.

Podsumowując powyższe rozważania można uszczegółowić wzór reakcji systemu autonomicznego do następującej postaci (V_f zostało pominięte, gdyż jest to wypadkowa oddziaływań akumulatora i korelatora na homeostat, które zostały uwzględnione we wzorze):

$$R = r\left(r_{Rec}, r_{Kor}, r_{Hom}, r_{Ef}, r_{Ak}, r_{Zas}\right) * S = \left(r_{Rec}, r_{Zas}, V_s, Mot, P, D, T, M, \mathrm{Int}, Poj, Tal, G, r_{Ef}\right) * S$$

Kolejnym zagadnieniem jest kwestia rozdzielenia procesów poznawczego i decyzyjnego. Wydawać by się mogło, że taki podział jest zasadny, chociażby ze względu na fakt, że obydwa te procesy zostały oddzielnie opisane w ramach tego rozdziału. Z drugiej strony sytuacja, w której system tylko podejmuje decyzję, przy jednoczesnym braku bodźców jest sytuacją idealną, gdyż człowiek zawsze ma do czynienia z informacją ($I = \frac{K}{G} = V_r + V_h$[147]) w korelatorze. Przypadek oddziaływania na system, który nie prowadzi do jego reakcji, ale prowadzi do zmian w korelatorze (proces poznawczy) też nie wymaga zmiany powyższego wzoru, gdyż iloczyn reaktywności systemu autonomicznego i bodźca będzie w takim przypadku wynosił 0, co nie zmienia faktu, że w czasie tego procesu może dojść do zmiany G w korelatorze, a więc do rejestracji lub derejestracji konkretnych informacji. Możliwym jest scenariusz, w którym oddziałuje się na system tylko i jedynie w celu zmiany rejestratów, aby przygotować ten system do reakcji dopiero w pewnej perspektywie czasowej. Podsumowując te rozważania wydaje się, że bliższym rzeczywistości jest stan, w którym zarówno proces decyzyjny, jak i poznawczy występują razem.

147 cf. ibid., p. 179; 193. Informacja przez Mazura została w tym kontekście opisana jako sam potencjał receptorowy bodźca, który się pojawił na wejściu systemu autonomicznego. z drugiej strony potencjał homeostatyczny również oddziałuje na rejestraty w korelatorze, a więc może zostać uznany za informację.

Możliwe jest oszacowanie wpływu poziomów wymienionych czynników systemu autonomicznego na siłę i prawdopodobieństwo reakcji:

- im większy iloczyn siły bodźca i reaktywności receptora tym większy potencjał receptorowy, który wiąże się z przepływem większej mocy korelacyjnej przez rejestraty i powstaniem silniejszych emocji (potencjał perturbacyjny) lub silniejszej decyzji (potencjał efektorowy),
- im większy potencjał swobodny (siła woli), tym wyższe prawdopodobieństwo reakcji systemu na rodzaj bodźców zgodnych z motywacją systemu i tym silniejsza ewentualna reakcja,
- im większy potencjał swobodny (siła woli), tym mniejsze prawdopodobieństwo reakcji systemu na rodzaj bodźców niezgodnych z motywacją systemu i tym słabsza ewentualna reakcja,
- im większa motywacja na dany rodzaj bodźców tym większe prawdopodobieństwo na reakcję systemu i tym silniejsza ewentualna reakcja,
- im wyższy dynamizm charakteru tym większe prawdopodobieństwo na reakcję systemu i tym silniejsza ewentualna reakcja,
- im szerszy charakter (suma podatności i tolerancji) tym większe prawdopodobieństwo na reakcję systemu,
- im wyższa przewodność korelacyjna związana z danym rodzajem bodźca tym większe prawdopodobieństwo na reakcję systemu i tym ewentualna silniejsza reakcja,
- im większy iloczyn siły bodźca i reaktywności zasilacza (która może być traktowana jako sprawność tego podsystemu) tym większa moc systemu,
- im większa moc systemu tym większe prawdopodobieństwo na reakcję systemu i tym silniejsza ewentualna reakcja,
- im większa reaktywność efektorów tym silniejsza reakcja systemu,
- czynniki takie jak inteligencja, podatność i talent opisują optymalny dla danej jednostki sposób przetwarzania informacji w korelatorze (jak dużo

informacji może jednostka przetwarzać, jak szybko i jakie informacje preferuje).

Na podstawie powyższych rozróżnień możliwa jest analiza ryzyka szczegółowego przypadku oddziaływania na jednostkę w zależności od tego czy daną reakcję uznaje się za odpowiednią w danych okolicznościach czy nie. Podobnie wprowadzanie pewnych rejestratów do korelatora może składać się na zwiększone prawdopodobieństwo przyszłych reakcji, a więc być traktowane jako czynnik ryzyka powodujący określone straty (zmniejszanie poziomu bezpieczeństwa systemu) tym większe im nieadekwatna reakcja jest silniejsza.

3.2. Systemy addycyjne w cyberprzestrzeni

W poniższym podrozdziale wykorzystano właściwości podsystemów systemu autonomicznego w celu klasyfikacji zasobów pod kątem ich wspierania jednostki. Dodatkowo opracowano wzorzec komunikacji między systemami wyróżniając źródło zakłóceń i odbiornik ulotu, jak i opisano oddziaływanie jednostki na zasób. W drugiej części podrozdziału opisano grupy z punktu widzenia cybernetyki i neotomizmu, wyróżniono relacje osobowe między jednostkami w danej grupie, rodzaje sprawiedliwości, cnoty społeczne i cnoty związane z cnotą roztropności. Rozdział zamknął opis relacji podsystemu sterującego i podsystemu sterowanego z punktu widzenia PSC.

3.2.1. Zasób i jego relacje

Biorąc pod uwagę fakt, że aby człowiek mógł korzystać z zasobu związanego z oddziaływaniem informacyjnym musi wprowadzić do niego komunikaty (a więc i informacje, co wymusza posiadanie przez te zasoby receptorów). Co więcej człowiek musi mieć dostęp do tych komunikatów (informacji), więc tego typu zasoby muszą również posiadać efektory. Na podstawie receptorów i efektorów można już rozważać systemy (układy) zorganizowane. W warunkach współpracy nie byłoby potrzeby rozważać systemów zorganizowanych, gdyż byłyby po prostu

częścią innych systemów. Inaczej sprawa się ma w warunkach konkurencji czy wręcz walki (kooperacji negatywnej), gdyż nawet system zorganizowany w postaci kabla lub powietrza, przez które przenosi się dźwięk i fale radiowe jest miejscem spornym. Kontrolowanie przez systemy różnych stron konfliktu mediów komunikacyjnych jest procesem dynamicznym, mogącym ulegać zmianom (nawet częstym). Dlatego w ramach analizy będą uwzględniane systemy zorganizowane. Od tego, które wejścia i wyjścia systemów zorganizowanych są kontrolowane przez którą stronę konfliktu wynikają konkretne zagrożenia, co zostanie opisane w dalszej części pracy.

Poza systemami zorganizowanymi zasób może przetwarzać informacje przez przetwarzanie komunikatów. Sprawia to potrzebę posiadania przez dany zasób korelatora, który będzie komunikaty zapisywał (kodował), przechowywał, wydobywał i przetwarzał. Pojawia się problem w jaki sposób opisać te systemy. Operacje na informacjach nie zawsze wymagają ciągłego użycia energii. Przykładem może być zapisanie danych na pendrive'ie lub zapisanie kartki papieru. Z drugiej strony pamięć RAM jest pamięcią ulotną, a więc wymaga ciągłego udziału energii w celu samego przechowywania danych. Również problematyczne wydaje się użycie wzorca systemu samosterownego, gdyż komputer posiada homeostat, chociażby dlatego, że w razie niskiego poziomu baterii może się zahibernować. Wydaje się, że istnieją dwa rozwiązania tego problemu. Pierwszy polega na wypisaniu różnych rodzajów zasobów i szczegółowo opisania w nich tych i tylko tych podsystemów, które są istotne dla rozważanych systemów. Drugie rozwiązanie, przyjęte w tej pracy, polega na uznaniu wszystkich systemów (poza systemami zorganizowanymi) jako systemów autonomicznych i opisania części ich podsystemów jako nieaktywnych, czyli takich, których reaktywność homeostatu wynosi 0, a innych podsystemów 1. Pozwoli to na wyprowadzenie w prostszy sposób ogólnych zależności między zasobami a człowiekiem.

Co więcej nawet, jeśli dane systemy nie wymagają przetwarzania energii do spełniania swojej funkcji, to ich moc jałowa nigdy nie będzie równa 0, gdyż

materia, z której składają się te systemy (a w pracy rozważane są tylko byty złożone z materii), posiada swoją jakość, która spada z czasem, aż do momentu unicestwienia (utraty jedności addycyjnej, którą można też nazwać przejściem do stanu $<0,0,0>$) danego systemu.

Znając zależność jakości w czasie możliwe jest prognozowanie uszkodzenia danego elementu w procesie jego eksploatacji. Co więcej możliwe jest ingerowanie w zasób, aby go uszkodzić (zmniejszając jego jakość), aby został unicestwiony dopiero po pewnym czasie. Odpowiednie uszkodzenie może prowadzić do utraty gotowości przez zasób, czyli przejścia w stan $<1,0,0>$, z którego można przejść w stan gotowości ($<1,1,0>$) po naprawie, a w przypadku znacznego uszkodzenia zasób jest unicestwiony, a więc przechodzi nieodwracalnie w stan $<0,0,0>$, gdyż dalsza naprawa jest nieopłacalna lub wręcz niemożliwa[148]. Zatem nawet w systemach, które nie potrzebują dodatkowej energii na spełnianie swojej funkcji występuje moc jałowa i dynamiczne procesy w ramach ich struktury. Z punktu widzenia celu pracy są to zjawiska pomijalne, a więc zostanie przyjęte, że dla systemów, które nie potrzebują dodatkowej energii do działania $P_0 \approx 0$. Dla przykładu zapisana kartka papieru nie potrzebuje dodatkowej energii, aby być nośnikiem danych, ale z czasem może ulec zniszczeniu ze względu na spadek jakości papieru do pewnej granicznej wartości.

Na podstawie powyższych rozważań można podzielić zasoby ze względu na rodzaj systemu i na podsystemy człowieka, które wspiera.

Rodzaje systemów wśród zasobów wyglądają następująco:

- system zorganizowany (medium komunikacyjne, kanał komunikacyjny),
- system autonomiczny:
  - z nieaktywnym homeostatem – o maksymalnym potencjale fizycznym homeostatu $V_{f_{max}} = 0$[149] – e.g. nośnik pamięci flash,

148 v. J. Konieczny, *op. cit.*, p. 56-57.
149 Warto podkreślić, że w zasobach maksymalny potencjał swobody homeostatu wynosi zawsze zero.

- z nieaktywnym zasilaczem, akumulatorem ($P_0 \approx 0$) i homeostatem – e.g. książka napisana alfabetem Braille'a,
- z aktywnymi wszystkimi podsystemami – e.g. komputer.

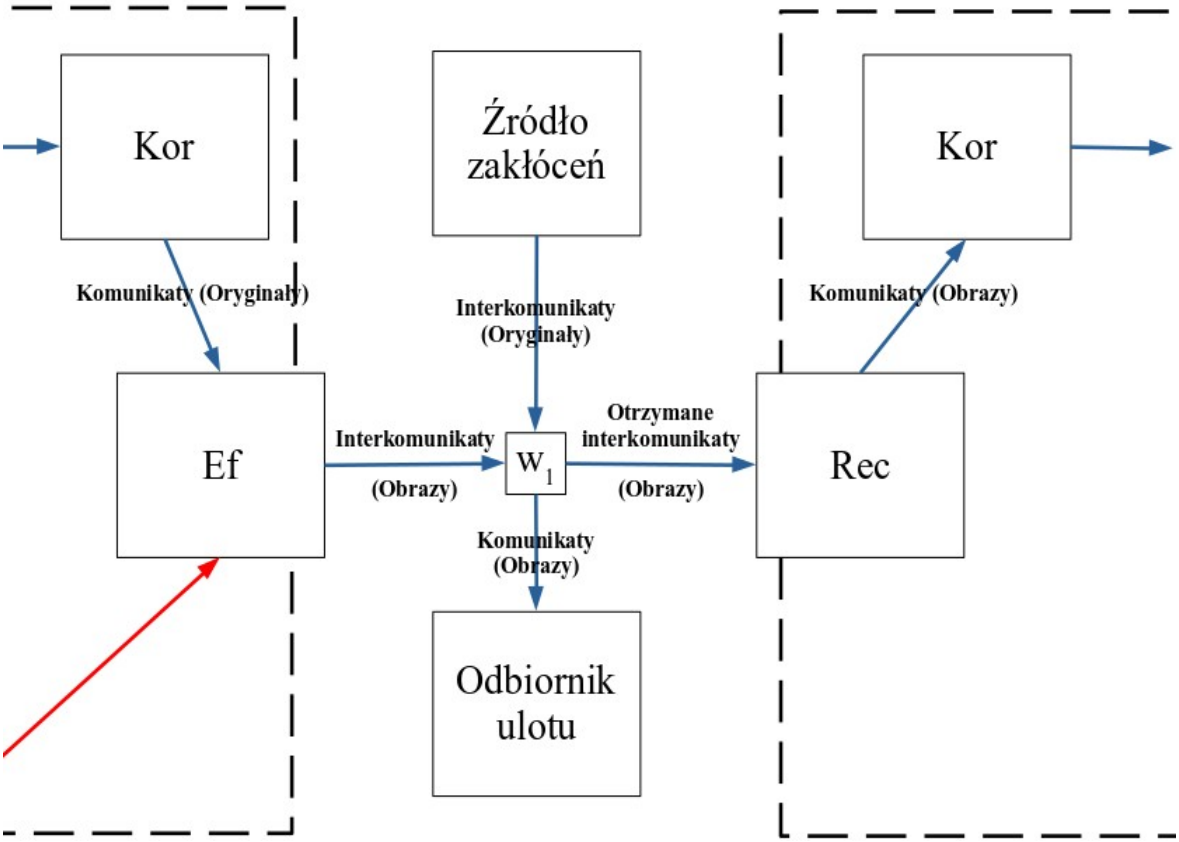
Podział ze względu na wspierane podsystemy człowieka wraz z ich funkcjami:

- wspieranie receptorów człowieka w zbieraniu informacji (spostrzeganiu).
- wspieranie korelatora człowieka w przechowywaniu i przetwarzaniu informacji.
- wspieraniu efektorów człowieka w wyrażaniu informacji.

Istotne jest, aby zaznaczyć, iż nawet, jeśli e.g. dany zasób odpowiada za wspieranie człowieka tylko w przechowywaniu informacji, to i tak musi te informacje wcześniej zebrać (przez swoje receptory), zakodować, przechować, a następnie wydobyć (w swoim korelatorze) i wyrazić (swoimi efektorami). W przypadku zasobów procesy kodowania i wydobywania informacji są tak projektowane, aby wydobywanie było odwrotnością kodowania i vice versa. Jednak procesy te mogą w rzeczywistości się różnić, chociażby z powodu eksploatacji urządzenia (zmniejszenia jakości materiału danego zasobu), która może prowadzić do wadliwego działania całego zasobu. Należy również nadmienić, iż wspieranie może oznaczać zarówno zwiększanie reaktywności danego podsystemu, jak i jego zmniejszanie (e.g. zwiększanie reaktywności receptora jakim jest wzrok przez okulary korekcyjne, dzięki czemu poprawia się jakość widzenia jednostki, albo zmniejszenie reaktywności tego receptora przez okulary przeciwsłoneczne chroniąc jednostkę przed przeciążeniem wzroku).

Jak już stwierdzono, zarówno zasoby (poza systemami zorganizowanymi), jak i jednostki traktowane będą jako systemy autonomiczne. Informacje przesyłane są między systemami przez systemy zorganizowane. Niezależnie czy przesyłanie informacji odbywa się przez idealną próżnię, kabel, powietrze, wodę czy inne medium komunikacyjne, to wszystkie te systemy uznawane są za systemy zorganizowane, które posiadają pewne receptory (wejścia) i efektory (wyjścia).

W ramach matematycznej teorii komunikacji wyróżniono, poza źródłem informacji, transmiterem, odbiornikiem i celem, również i źródło zakłóceń. Źródło zakłóceń może wpływać na medium komunikacyjne (system zorganizowany) tylko i jedynie dlatego, iż posiada dostęp do części jego receptorów. Nie jest dla przykładu możliwe zakłócanie sygnału w dobrze wyizolowanym kablu biegnącym pod ziemią, jeśli się do niego nie dostanie fizycznie. Z drugiej strony fala radiowa rozchodzi się w powietrzu, do którego ma dostęp każda osoba, a wpływać na samą falę radiową o danych parametrach może każda osoba posiadająca odpowiedni transmiter. Może pojawić się analogiczna sytuacja w przypadku, gdy inne systemy mają dostęp do efektorów (wyjścia) danego systemu zorganizowanego. Te systemy nazywane będą odbiornikami ulotu. O ile problematyczne jest odbieranie (podsłuchiwanie) sygnałów biegnących w kablu, to nie sprawia większego problemu podsłuchiwanie transmisji radiowej, jeśli tylko posiada się odpowiedni odbiornik. Oczywiście granica między celem, a odbiornikiem ulotu jest zależna od nadawcy, gdyż w przypadku komunikacji radiowej używanej w służbach mundurowych liczba odbiorców jest ściśle określona (w odpowiednich dokumentach opisujących kierunki lub sieci radiowe), a każda inna osoba, która będzie chciała się zaznajomić z informacją przesyłaną przez radio jest do tego nieuprawniona. Z drugiej strony stacja radiowa emitująca treści rozrywkowe lub programy informacyjne będzie chciała, aby dotrzeć do jak największej liczby osób, a odbiornikiem ulotu będzie po prostu każdy byt, który nie jest osobą. Podobnie rzecz się ma z źródłem zakłóceń. Może być to działanie zarówno niepożądane (gdyż utrudnia lub uniemożliwia komunikację) lub pożądane (gdy ma na celu zamaskować przekaz przed przeciwnikiem). Jeśli źródła zakłóceń nie pochodzą od jednostek, zasobów lub grup, to przyjmuje się, że są generowane przez otoczenie. Podobnie odbiornikiem ulotu, który nie jest jednostką, zasobem lub grupą jest również otoczenie. Powyższą sytuację można zobrazować następującym schematem, gdzie w_1 jest węzłem komunikacyjnym, czyli systemem zorganizowanym (medium komunikacyjnym):



Rys. 24: Wzorzec komunikacji między systemami

źródło: opracowanie własne

W ramach wzorca komunikacji między systemami wykorzystano również jakościową teorię informacji Mazura. Źródło zakłóceń polega na niczym innym, jak dodawaniu komunikatów do przekazu, które mogą prowadzić do dezinformacji symulacyjnej lub pseudoinformowania symulacyjnego. Z drugiej strony odbiornik ulotu przechwytuje część przekazu lub prowadzi do dezinformacji dysymulacyjnej. Co więcej w rzeczywistości wydaje się, że nie występują media komunikacyjne, w których ulot lub zakłócenie może dotyczyć tylko i jedynie pojedynczego punktu takiego medium. Dla przykładu w kablu lub powietrzu zarówno zakłócenie, jak i ulot mogą nastąpić w każdym miejscu kabla lub przestrzeni, w której znajduje się powietrze. Zatem ulot może nastąpić przed, w trakcie lub po zakłóceniu. Co więcej zakłócenie nie musi być pojedyncze, co jeszcze bardziej komplikuje sytuację. W opisach szczegółowych scenariuszy jedno medium komunikacyjne może zostać

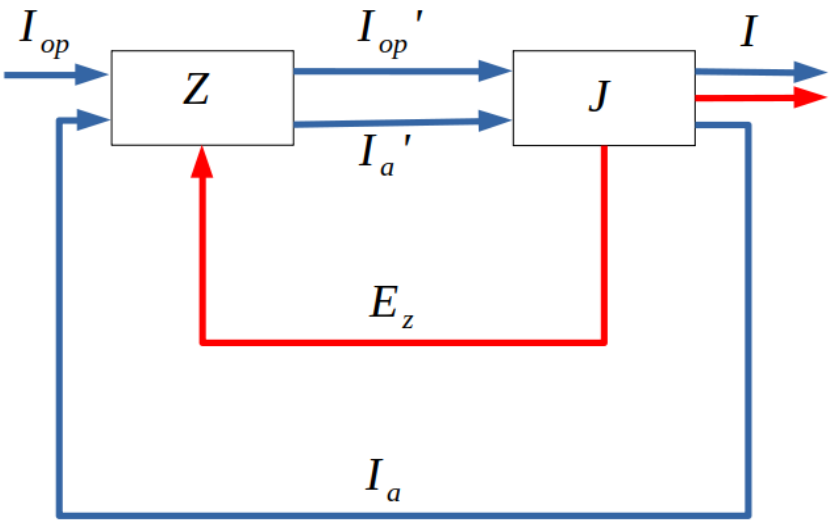
rozbite na wiele połączonych szeregowo węzłów komunikacyjnych wedle potrzeb analityka, aby móc jak najdokładniej odwzorować rzeczywistą sytuację.

Jeśli system jako jedyny może nadawać (przesyłać komunikaty) przez dany węzeł komunikacyjny, to ma kontrolę nad wejściem danego węzła komunikacyjnego (kontroluje receptory węzła komunikacyjnego). W takim przypadku nie występują źródła zakłóceń. Jeśli system odbiera komunikaty ze wszystkich efektorów danego węzła komunikacyjnego, to znaczy, że kontroluje wyjście (efektory) danego węzła komunikacyjnego. Nie występują wtedy odbiorniki ulotu. Oczywiście są to sytuacje idealne, a w rzeczywistości można mówić o większym lub mniejszym poziomie kontroli nad danym węzłem komunikacyjnym (jego wejściem i wyjściem), w zależności od tego jaki jest stosunek kontrolowanych wejść (lub wyjść) do wszystkich wejść (lub wyjść) danego węzła komunikacyjnego. W tym kluczu kontrola systemu nad węzłem komunikacyjnym w przypadku kabla będzie raczej wysoka, a w przypadku systemu nadającym za pomocą fal radiowych – raczej niska.

Według założenia tejże pracy zasoby pełnią funkcję tylko i jedynie służebną dla jednostek. Aby móc wykorzystywać zasoby jednostka musi albo odbierać bodźce od zasobu (w postaci komunikatów), albo przekazywać zasobowi bodźce ze swoich efektorów (aby zostały odpowiednio wykorzystane przez bodziec). Dla przykładu okulary odbierają bodźce z otoczenia, odpowiednio je przetwarzają i swoimi efektorami oddziałują na noszącą je jednostkę. Z kolei legendarny czerwony przycisk uruchamiający kaskadę zdarzeń prowadzącą do wystrzelenia rakiet z głowicami jądrowymi będzie przekazywał dalej bodźce z efektora jednostki jakim jest jej palec. Informacje (zestawy komunikatów) zarówno odbierane, jak i generowane przez zasoby, które dotyczą funkcji, którą mają pełnić, będą nazywane informacjami operacyjnymi (I_{op}).

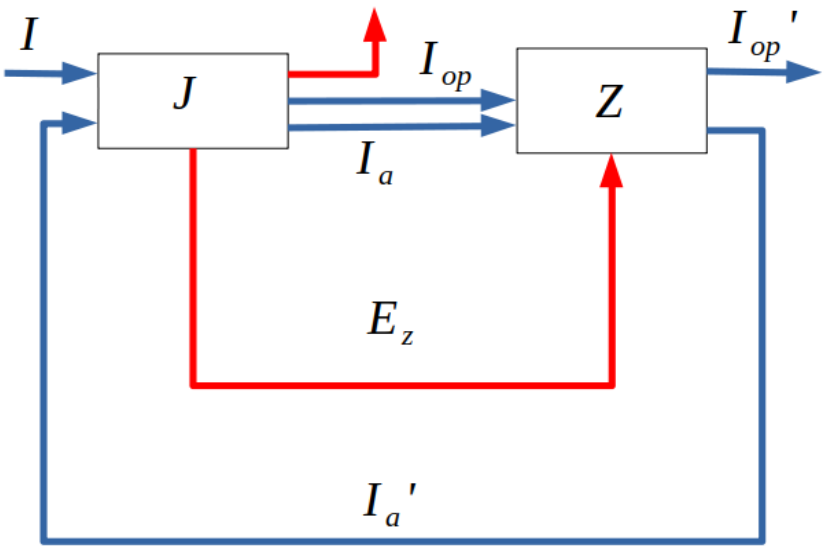
Poza zjawiskiem informacji operacyjnych system może (a wręcz powinien) oddziaływać na inne sposoby na zasób. Z jednej strony powinien, o ile jest to wymagane, zapewniać mu zasilanie (E_z). Z drugiej strony zasoby muszą być odpowiednio zarządzane, aby skutecznie wypełniać swoje zadanie. Wymaga to,

aby działały również sprzężenia administracyjne z jednostki do zasobu i z zasobu do jednostki. System dzięki takiemu obiegowi administracyjnemu może zarządzać zasobem. Przykładowo może go wyłączyć lub włączyć, zmienić jego konfigurację (poprawić położenie okularów, zmienić plik konfiguracyjny programu, uruchomić odpowiednie tryby pracy przez wciśnięcie przycisków etc.), naprawić lub przetestować, czyli zmienić jego stan. Aby móc zaobserwować skuteczność swojego działania zasób generuje informację zwrotną sprzężeniem od zasobu do jednostki. Informacje w obiegu administracyjnym będą nazywane informacjami administracyjnymi (I_a oraz informacją administracyjną zwrotną I_a'). Niekiedy informacja operacyjna i informacja administracyjna poruszają się tym samym torem sterowniczym. Dla przykładu skuteczność poprawienia położenia okularów jest widoczna w ten sam sposób, w jaki odbywa się normalne widzenie, a więc zmysłem wzroku. Powyższe rozważania opisano poniższymi schematami, gdzie J oznacza jednostkę, a Z - zasób, I_{op}' informację operacyjną na wyjściu zasobu, a I_{op} informację operacyjną na wejściu zasobu:



Rys. 25: Oddziaływanie zasobu na jednostkę

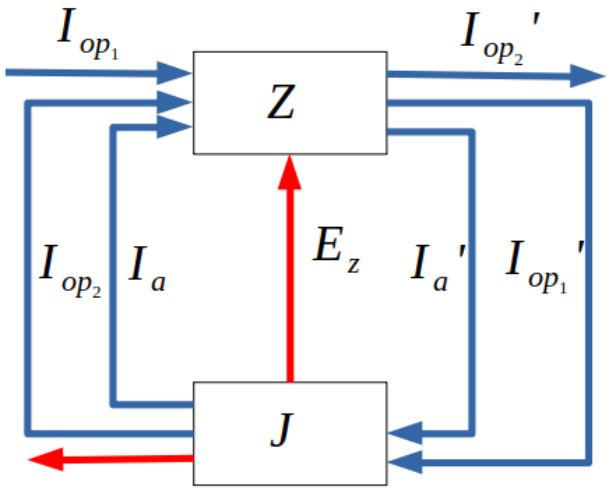
źródło: opracowanie własne



Rys. 26: Oddziaływanie jednostki na zasób

źródło: opracowanie własne

Niektóre zasoby do poprawnego funkcjonowania wymagają zarówno oddziaływania na wejście, jak i wyjście jednostki. Przykładem może być komputer, który odbiera bodźce (e.g. przez klawiaturę), przetwarza je i przedstawia je jednostce (e.g. przez monitor). Następnie bodźce generowane przez jednostkę odbiera, przetwarza i przesyła dalej.



Rys. 27: Oddziaływanie zasobu na wejście i wyjście jednostki

źródło: opracowanie własne

Zatem zasób może nie oddziaływać na jednostkę wcale lub oddziaływać na jej wejście, na wyjście lub na wejście i wyjście jednocześnie. Zasoby powiązane relacjami mogą tworzyć nadsystemy, które też są zasobami. Relacje mogą dotyczyć zarówno sfery fizycznej, czyli, w przypadku, gdy e.g. podzespół komputera jest połączony do innego podzespołu lub sfery logicznej, gdy pewne oprogramowanie oddziałuje na inne oprogramowanie. Jeśli węzły komunikacyjne (ich wejścia i wyjścia) wewnątrz takiego nadsystemu są kontrolowane przez jednostkę wykorzystującą powiązane zasoby, to można dany nadsystem traktować w analizie jako jeden system. Jeśli takiej kontroli nie ma, to istotne jest, aby dane zasoby wyróżnić, aby móc ocenić ryzyko związane z zakłóceniem lub ulotem informacji (zarówno administracyjnej, jak i operacyjnej) między każdym z elementów. Każdy węzeł komunikacyjny wiąże się z potencjalnym ryzykiem. Z drugiej strony szczegółowość podziału elementów zależy od badacza lub analityka. Można jako jeden zasób traktować po prostu komputer, oddzielnie hardware i software, rozróżniać konkretne programy i system operacyjny, analizować oddzielnie każdy podzespół, aby analizować ulot magnetyczny każdego z nich etc. Analiza ryzyka każdego z tych podziałów wykaże inne

zagrożenia i podatności. Co do zasady sam cybernetyczny wzorzec teoretyczny wygląda tak jak opisano.

Jeśli jednostka kontroluje zasób lub zasoby (w zależności od szczegółowości analizy), to może tworzyć z nimi jeden nadsystem, który wchodzi w interakcje z otoczeniem jako samodzielny byt. I tak człowiek uzbrojony w okulary, termowizję lub noktowizję (wspomaganie receptorów) tworzy nadsystem takiej klasy. Podobnie rzecz się ma z analitykiem korzystającym z komputera, kartek, ołówka, pinezek i tablicy korkowej do wspomagania przechowywania i przetwarzania informacji. Dzięki takiemu zabiegowi możliwa jest prostsza analiza oddziaływań informacyjnych przy minimalnym uproszczeniu rzeczywistości. Tylko i jedynie jednostki podejmują decyzje, a więc z punktu widzenia analizy połączenie zasobów i jednostki nic w tej materii nie zmienia. Jednostka jest traktowana tak jak wcześniej z tą zmianą, że jej możliwości są poszerzone. Nie sprawia to jednak, że można zrezygnować z analizy zasobów jako takich, gdyż istnieją pewne zasoby sporne, czyli takie, które nie są kontrolowane (a przynajmniej kontrolowane w dużej mierze) przez żaden z systemów. Dla przykładu wystawienie panelu do logowania do usługi sieciowej do internetu sprawia, że właściciel tej usługi niekoniecznie już ją kontroluje[150], a więc dana usługa niekoniecznie może być traktowana jako wsparcie podsystemów tego użytkownika, a przynajmniej ta sytuacja może się zmienić.

Korzystanie z zasobów nie posiada samych zalet. Aby móc z nich korzystać jednostka musi posiadać moc swobodną (P_s), która zostanie wykorzystana na obsługę zasobu, czyli na pewną moc roboczą (P_{r_x}), gdzie x oznacza indeks zasobu. Musi się składać na nią:

- zasilanie zasobu (o ile jest takie potrzebne), czyli zagospodarowanie mocy zasilającej (P_{z_x}),
- administracja zasobem, czyli zagospodarowanie mocy administracyjnej (P_{a_x}),

150 Właściciel może kontrolować samą usługę i panel logowania, ale z pewnością nie kontroluje wejścia i wyjścia węzła komunikacyjnego jakim jest sieć internet.

- operowanie zasobem, czyli zagospodarowanie mocy operacyjnej (P_{op_x}).

Operowanie zasobem i utrzymywanie go (administrowanie nim) wymaga odpowiednich umiejętności i wiedzy ze strony jednostki. Zarówno moc administracyjna, jak i operacyjna może się zmniejszać z czasem jak jednostka wyrobi przyzwyczajenia w obsłudze danego zasobu (czyli odpowiednią przewodność korelacyjną). Dzieje się tak, ponieważ na początku wykonywania nowej czynności wykorzystywany jest potencjał swobodny, a z czasem czynność staje się czynnością automatyczną, co zwalnia zasoby umysłu (woli, uwagi, myślenia etc.). Wykorzystywanie danego zasobu, nawet pomimo zwiększenia mocy roboczej na poczet jego obsługi, może (a wręcz powinno) zmniejszyć całkowitą moc roboczą jednostki na rzecz mocy swobodnej. Możliwe jest, że początkowy bilans mocy (przed osiągnięciem odpowiednich przyzwyczajeń) będzie niekorzystny, ale opłaci się wraz z osiągnięciem pewnej wprawy. Również jest możliwe, że do pewnych zadań używa się zasobów, których obsługa więcej kosztuje i zużywa czasu i energii, niż osiąga się korzyści.

3.2.2 Grupa i jej relacje

Z punktu widzenia cybernetyki grupa może być traktowana jako system. Jeśli system składa się z podsystemów, które są systemami autonomicznymi, to można go również zaklasyfikować jako system autonomiczny, który może jednak mieć interes rozbieżny z interesem pojedynczych systemów autonomicznych, które wchodzą w jego skład[151]. Z drugiej strony system autonomiczny zakłada zdolność do sterowania samym sobą i zdolność do zachowania tej sterowności w czasie. Zakładając, iż do grupy należą jednostki (a więc systemy autonomiczne) należałoby uznać, że i same grupy są bezwzględnie systemami autonomicznymi. Tak jednak nie musi być, gdyż jedna grupa może być kontrolowana przez inną grupę lub jednostkę i wykonywać ślepo ich polecenia. Odpowiedni dla takiego stanu rzeczy byłby schemat systemu samosterownego. Jednak, aby uprościć zapis, każda grupa będzie traktowana jako system autonomiczny, ale,

151 v. J. Kossecki, *Metacybernetyka*, op. cit., p. 93.

analogicznie do założeń przyjętych w przypadku zasobów, maksymalny potencjał swobodny lub fizykalny niektórych grup będzie równy lub bliski 0, gdyż sterowanie korelatorem i akumulatorem będzie odbywało się przez zewnętrznego organizatora (przez tor informacyjny związany z receptorem). Co więcej, jak wykazana wyżej, jednostka może korzystać z zasobów rozszerzając swoje możliwości reagowania na otoczenie, zatem również te używane zasoby będą częścią grup ze względu, że służą jednostkom, które do tych grup należą. Zaznaczyć trzeba, że należenie zasobów do grup zależy tylko i jedynie od ich relacji z jednostką z danej grupy (e.g. relacji posiadania, korzystania, zasilania lub administrowania). Jeśli takiej relacji zasób nie posiada, to nie można zaklasyfikować go do żadnej z grup. Również jeśli dany zasób związany jest relacjami z jednostkami z różnych grup, to można uznać, że nie należy bezwzględnie do żadnej z nich, ale jest mniej lub bardziej przez nie kontrolowany.

Uznanie grupy za system autonomiczny ma swoje konsekwencje w tym, iż grupa będzie posiadała wszystkie właściwości systemu autonomicznego. Zatem będzie można rozważać inteligencję grupy, jej pojętność, dynamizm charakteru etc. Właściwości grupy będą ściśle zależne od właściwości jednostek ją tworzących, jak i relacji między tymi jednostkami. Zatem jednostki, których działalność wiąże się z pracą korelatora (związanego z przechowywaniem i przetwarzaniem informacji) posiadają wysoką inteligencję (pojemność korelatora) i dodatkowo ją wzmacniają przez korzystanie z różnych zasobów do tego przeznaczonych (e.g. komputerów lub systemu archiwów), to można uznać, iż cały korelator posiada wysoką inteligencję. Co istotne również motywacje (poznawcze, ideologiczne, etyczne, prawne, ekonomiczne i witalne) dotyczą grupy, ale nazywane są nie motywacjami, a normami społecznymi, które związane są z dominującymi motywacjami pojedynczych jednostek, z których składa się grupa. Socjocybernetyczna koncepcja norm społecznych jest uogólnieniem teorii cywilizacji Konecznego[152]. Od norm społecznych w danym społeczeństwie zależą znaczenia słów prawda i fałsz, obraz świata, kryteria wyboru oryginałów (z punktu

152 v. J. Kossecki, *Metacybernetyka*, op. cit., p. 151-152.

widzenia jakościowej teorii informacji) i zasady oceniania i przetwarzania informacji. W przypadku, jeśli nie dominuje żadna cywilizacja, to może dochodzić do konfliktów między zwolennikami konkretnych norm społecznych[153].

Systemowe ujęcie grupy koresponduje z neotomistycznym rozumieniem wspólnoty jako „zespołu osób powiązanych relacjami zarówno realnymi, jak i myślnymi"[154]. Do relacji realnych wchodzą relacje osobowe, które są oparte o ogólne właściwości bytu, czyli relacje miłości (serdeczności), wiary (zaufania) i nadziei (dążenie do trwania w wierze i miłości), które budują wspólnoty takie jak rodzina lub Naród. Obok relacji realnych można wyróżnić relacje myślne oparte tylko i jedynie na pewnej konwencji, opinii lub umowie, z którymi związane są państwa, związki zawodowe, instytucje handlowe etc. Relacje myślne powodują, że wspólnoty zaczynają się różnić między sobą[155]. Wynika z tego, że rodzaj grupy (wspólnoty) zależy tylko i jedynie od relacji między jednostkami ją tworzącymi (konkretnymi osobami).

Życie we wspólnocie związane jest z cnotą sprawiedliwości, która polega na stałej i trwałej chęci oddawania każdemu tego to co mu się słusznie należy[156]. Sprawiedliwość ma na celu wprowadzanie ładu w życie społeczne[157]. Święty Tomasz z Akwinu wyróżnia trzy rodzaje sprawiedliwości[158]:

- sprawiedliwość prawną – związaną z relacją jednostka-grupa, która polega na obowiązkach osoby wobec wspólnoty,
- sprawiedliwość rozdzielczą – związaną z relacją grupa-jednostka, która polega na obowiązkach wspólnoty wobec osoby,
- sprawiedliwość wymienną – związaną z relacją jednostka-jednostka, która polega na obowiązkach osoby do osoby.

153 v. ibid., p. 181-182.
154 v. M. Gogacz, *Wprowadzenie do etyki chronienia osób*, NAVO, Warszawa 1998, p. 73.
155 v. ibid., p. 74.
156 v. A. Andrzejuk, *Tomasz…*, op. cit., p. 103.
157 v. ibid., p. 102.
158 v. ibid., p. 104-106.

Obok rodzajów sprawiedliwości można za Akwinatą wyróżnić również katalog cnót społecznych, które regulują strukturę nadsystemu jakim jest grupa[159]:

- religijność (łac. religio) – objawiająca się szacunkiem do Boga, który jest Stworzycielem,
- szacunek do przodków, rodziców i Ojczyzny (łac. pietas) – ze względu na otrzymane od rodziców życie i wychowanie od Ojczyzny,
- poważanie osób piastujących istotne funkcje społeczne (łac. observantia) – dotycząca każdego kto piastuje wyższe stanowisko,
- posłuszeństwo (łac. oboedientia) – dotycząca posłuchu przełożonym w dziedzinie ich kompetencji ściśle związanych z osiągnięciem założonego celu (e.g. dążeniem do ładu w społeczeństwie, wygrania wojny etc.),
- wdzięczność (łac. gratia) – odnosząca się do dobroczyńców,
- karanie przewin, odzyskiwanie długów (łac. vindicatio) – odnosząca się do karania w celu osiągnięcia dobra (skazanego lub społeczeństwa),
- prawdomówność (łac. veracitas) – odnosząca się do mówienia prawdy w celu uzyskania pewnego dobra (związanego z dobrym celem),
- uprzejmość (łac. affabilitas) – polegająca na traktowaniu każdego człowieka po przyjacielsku,
- życzliwość (łac. benevolentia) – odnosząca się do osób niżej w hierarchii, młodszych,
- hojność (łac. liberalitas) – polegająca na osiągnięciu złotego środka w gospodarowaniu własnymi pieniędzmi, czyli unikaniu zarówno rozrzutności, jak i chciwości,
- epikeia (gr. ἐπιείκεια) – cnota polegająca na działaniu zgodnie z duchem prawa (czasem wbrew literalnemu zapisowi).

Z drugiej strony również cnoty związane z roztropnością posiadają swój wymiar społeczny. Aby móc zastosować odpowiednie środki do osiągnięcia celu należy posiadać pamięć (łac. memoria) praktyczną o rzeczach przeszłych, która

159 v. ibid., p. 106-111.

skutkuje posiadaniem doświadczenia. Zagadnienie teraźniejszości – jej adekwatne zidentyfikowanie i ujęcie intelektualne wymaga cnoty inteligencji (łac. intelligentia). Nadmiar szczegółów, które składają się na rzeczywistość jest niemożliwy do zgłębienia przez jednego człowieka, więc w pewnej części należy swoje poznanie świata oprzeć na radach innych osób. Korzystanie z wiedzy innych nazywane jest cnotą pouczalności (łac. docilitas), a przekazywanie takowej wiedzy – cnotą doradzania (gr. εὐβουλία)[160].

Z punktu widzenia cybernetyki społecznej zagadnienie hierarchii w danej wspólnocie można opisać za pomocą dwóch podsystemów – podsystemu sterującego (ośrodka władzy, kierownictwa) i podsystemu sterowanego (wykonawczego), które są w sprężeniu zwrotnym. Z jednej strony podsystem sterujący wysyła do systemu sterowanego wytyczne do wykonania, a podsystem sterowany je wykonuje (o ile posiada odpowiednie kwalifikacje (korelator), chęć (homeostat) i środki (akumulator)), o czym informowane jest kierownictwo. Skutek wydawanych poleceń, jak i informacji zwrotnych zależą od jakości kanałów komunikacyjnych, czyli tego jaki jest ubytek komunikatów przy przesyłaniu[161].

160 v. ibid., p. 98-99.
161 cf. J. Kossecki, *Cybernetyka społeczna*, Państwowe Wydawnictwo Naukowe, Warszawa 1975, p. 197-200.

Rozdział IV.
BEZPIECZEŃSTWO SYSTEMÓW I KOMUNIKATÓW W CYBERPRZESTRZENI

„Zatem jeśli coś jest zwrócone do zewnętrznego celu, tak jak okręt do portu, obowiązkiem rządzącego jest nie tylko zachować tę rzecz bez szwanku, ale ponadto doprowadzić ją do celu."

św. Tomasz z Akwinu

Poniższy rozdział dotyczy aspektów bezpieczeństwa zarówno systemów substancjalnych, addycyjnych, jak i komunikatów. W pierwszym podrozdziale opisano ogólne ujęcie bezpieczeństwa, na które składa się zarówno bezpieczeństwo obiektywne, jak i bezpieczeństwo subiektywne (odczuwane przez jednostkę). Na podstawie teorii Freia wyróżniono cztery stany bezpieczeństwa (stan bezpieczeństwa, fałszywego bezpieczeństwa, obsesji i braku bezpieczeństwa), które są wypadkową bezpieczeństwa obiektywnego i subiektywnego. Ze względu na fakt, iż o obiektywnym stanie bezpieczeństwa orzekają ludzie (zarówno eksperci, jak i laicy), którzy również mają wobec niego pewne odczucia i sposób zachowania (powstały na podstawie e.g. procedur bezpieczeństwa lub doświadczenia życiowego), to zagadnienie zarówno bezpieczeństwa obiektywnego i subiektywnego dotyczy wszystkich ludzi.

Ujęcie bezpieczeństwa obiektywnego opracowano na podstawie propozycji św. Tomasza z Akwinu, wedle której bezpieczeństwo obejmuje zarówno aspekty człowieka, które ma wspólne z wszystkim co istnieje, z tym co ma wspólne z innymi istotami żyjącymi oraz tym co jest typowo ludzkie (związane z rozumnością). Przy opisie bezpieczeństwa subiektywnego zostały użyte teoria emocji Akwinaty, jak i koncepcje psychologiczne związane z wagami decyzyjnymi mało lub bardzo prawdopodobnych wydarzeń, czy stosunkiem do ryzyka jednostki. Bezpieczeństwo zasobów i grup ściśle powiązano z bezpieczeństwem jednostki.

Podrozdział dotyczący bezpieczeństwa komunikatów opracowano głównie przez przywołanie modelu Intrusion kill chain opisującego fazy ataków na system teleinformatyczny i kostkę bezpieczeństwa McCumbera dzielącego bezpieczeństwo informacyjne na trzy wymiary (stany informacji, właściwości informacji, środki bezpieczeństwa). Dodatkowo opisano powyższe modele w języku cybernetyki wraz z procesem szyfrowania, steganografii i zagłuszania. Podrozdział został zakończony wzorcami teoretycznymi związanymi z oddziaływaniem na wejścia i wyjścia systemu atakowanego.

4.1. Ogólne ujęcie bezpieczeństwa

Bezpieczeństwo nie posiada jednej definicji. Co więcej może dotyczyć wielu podmiotów (e.g. jednostki, grupy, państwa, regionu[162]) na licznych płaszczyznach (e.g. bezpieczeństwo wojskowe, polityczne, społeczne, ekonomiczne, ekologiczne, kulturowe[163]). Dodatkowo może być analizowane pod kątem tego jaki jest obiektywny stan rzeczywistości, ale również tego jak odbierana jest aktualna sytuacja pod kątem samego poczucia bezpieczeństwa. Wychodząc z takiego podziału Frei wyróżnił cztery stany bezpieczeństwa jako wypadkowej postrzeganych zagrożeń (bezpieczeństwa subiektywnego) i faktycznego stanu rzeczy (bezpieczeństwa obiektywnego), które przedstawia poniższa tabela:

Tabela 5: Stany bezpieczeństwa według Freia

źródło: opracowanie własne na podstawie: J. Stańczyk, Współczesne..., op. cit., p. 17.

Bezpieczeństwo obiektywne	Bezpieczeństwo subiektywne	Nazwa stanu
Poważne zagrożenie	Postrzeganie zagrożenia jako poważne	Stan braku bezpieczeństwa
Brak zagrożenia	Postrzeganie zagrożenia jako niewielkie	Stan bezpieczeństwa
Poważne zagrożenie	Postrzeganie zagrożenia	Stan fałszywego bezpieczeństwa

162 v. J. Stańczyk, *Istota współczesnego pojmowania bezpieczeństwa – zasadnicze tendencje*, in: *Rocznik Bezpieczeństwa Międzynarodowego*, 5 (2010), p. 18.
163 v. ibid., p. 19.

	jako niewielkie	
Brak zagrożenia	Postrzeganie zagrożenia jako poważne	Stan obsesji

Stańczyk twierdzi, że subiektywne postrzeganie bezpieczeństwa jest, do pewnego stopnia, zjawiskiem obiektywnym, a czynniki uważane jako subiektywne mogą być ważniejsze od swoich obiektywnych odpowiedników[164]. Postrzeganie bezpieczeństwa może kształtować jego stan obiektywny przez zachowanie jednostek. Dla przykładu, jeśli grupa ludzi postrzega pewne wydarzenia jako niebezpieczne, to może to spowodować masowy wybuch paniki, który z pewnością przełoży się na bezpieczeństwo obiektywne danej wspólnoty niezależnie czy wydarzenia początkowe było realnym zagrożeniem (stan braku bezpieczeństwa), czy nie (stan obsesji).

Należy zwrócić uwagę, iż zawsze sądy dotyczące bezpieczeństwa są wydawane przez pewną jednostkę, która poza władzami poznawczymi posiada również władze pożądawcze (szczególnie emocje), które mogą zaburzać i postrzeganie rzeczywistości, jak i proces podejmowania decyzji. Wydaje się zatem, iż obydwie domeny bezpieczeństwa – bezpieczeństwo obiektywne i bezpieczeństwo subiektywne w różnym natężeniu dotyczą każdego pojedynczego człowieka.

Konsekwencją takiego ujmowania bezpieczeństwa jest uznanie, że o bezpieczeństwie obiektywnym orzekają nie tylko eksperci, ale każdy człowiek w różnym zakresie. Jest to zgodne z pojmowaniem relacji jednostka-grupa przez św. Tomasza z Akwinu. Akwinata rozważając postacie cnoty roztropności (związaną z wybieraniem odpowiednich środków do osiągnięcia celu) wyróżnia roztropność osobistą (dotyczącą kierowaniem własnym działaniem) i roztropność związaną z kierowaniem zbiorowościami (na którą się składają roztropność wojskowa, roztropność rodzinna i roztropność polityczna). Roztropność polityczna jest sprawnością związaną z kierowaniem państwem, ale nie dotyczy tylko

164 cf. J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Instytut Studiów Politycznych Polskiej Akademii Nauk, Warszawa 1996, p. 28.

i jedynie rządzących, ale, w różnym zakresie, też obywateli[165]. Zatem bezpieczeństwem grupy (niekoniecznie państwa) interesować się powinny również osoby, które nie są decydentami, z tą różnicą, iż osoby zawodowo zajmujące się bezpieczeństwem powinny szczególnie wypracować cnotę inteligencji (rozpoznania rzeczywistości) i doradzania w dziedzinie bezpieczeństwa, natomiast osoby, które w obowiązkach zawodowych nie mają zadań związanych z bezpieczeństwem szczególnie powinny pracować nad cnotą przyjmowania rad (pouczalności) z zakresu bezpieczeństwa. Również zachowania związane z bezpieczeństwem mogą być różne w zależności od piastowanego stanowiska danej jednostki.

Jedną z możliwości ujęcia bezpieczeństwa obiektywnego jest rozumienie tego fenomenu za Stańczykiem jako „obiektywnej pewności gwarancji nienaruszalnego przetrwania i swobód rozwojowych”[166]. W przypadku jednostki definicja bezpieczeństwa może być uszczegółowiona, jeśli zostanie odniesiona do tomistycznej antropologii filozoficznej. Świniarski i Chojnacki wydzielając elementy definicji bezpieczeństwa odwołują się do zaproponowanego przez Akwinatę porządku przykazań prawa naturalnego, które wynikają z naturalnych skłonności człowieka ku dobru, a do których należą[167]:

- trwanie – utrzymanie człowieka w istnieniu – wspólne wszystkiemu co jest,
- prolongowanie – skłonność ku temu co człowiek ma wspólnego ze zwierzętami (prokreacja, wychowanie dzieci etc.),
- przetrwanie – dążenie do dóbr odpowiadających rozumnej naturze człowieka (e.g. poznawanie Boga i życie w społeczności).

W tym ujęciu bezpieczeństwo rozumiane jest jako „naturalna skłonność do trwania wspólnie z całym światem, prolongowania tego trwania wśród świata organicznego i przetrwania w świecie społecznym – świecie poszanowania prawdy, przyjaźni i wzajemnego szacunku”[168]. Z kolei Gogacz identyfikuje na

165 v. A. Andrzejuk, *Tomasz…*, op. cit., p. 99.
166 v. J. Stańczyk, *Współczesne…*, op. cit., p. 20.
167 v. J. Świniarski, W. Chojnacki, *Filozofia bezpieczeństwa. Podręcznik akademicki*, ZUMS BN, Warszawa 2004, p. 56-57. cf. Tomasz z Akwinu, *Summa Theologiae,* I-II, q. 94, r.
168 cf. ibid. p. 57.

podstawie struktury bytowej człowieka następujące dobra osób, które powinny podlegać chronieniu[169] [170]:

- istnienie,
- życie (zespół relacji osobowych i działań cielesnych i duchowych człowieka),
- usprawnienie intelektu w wiedzy i mądrości (umiejętność ujmowania zarówno prawdy, jak i dobra),
- usprawnienie woli w wolności i prawości (stała wierność dobru wskazanemu przez intelekt),
- odpowiednie kształtowania wyobrażeń i uczuć,
- zdrowie (harmonijne i prawidłowo wyzwalane działania przez organy cielesne),
- pozostawanie we wspólnocie z osobami (relacje wiary, nadziei i miłości):
  - humanizm (udział w życiu innych ludzi),
  - religia (udział w życiu Boga),
- kultura:
  - podmiotowa – zgodna z rzeczywistością wiedza i uzyskiwana na jej podstawie mądrość,
  - przedmiotowa – wytwory człowieka.

W swoim traktacie O władzy Doktor Anielski opisuje, że warunkiem dobrego życia jednostki jest życie cnotliwe i dostatek. W przypadku społeczności (grupy) obok życia cnotliwego i dostatku Akwinata dodaje jeszcze pokój[171]. Triadę pokój, dobro i dostatek uznaje się zatem za warunek bezpiecznego życia[172]. Jednak celem jednostki, jak i całego społeczeństwa, jest według św. Tomasza z Akwinu zbawienie, a zabieganie o dobre życie jest tylko i jedynie środkiem do tego celu[173]. Nie jest możliwe działanie cnotliwe, jeśli wybierane przez człowieka dobro nie

169 v. M. Gogacz, *Wprowadzenie…*, op. cit., p. 12-13.
170 v. M. Gogacz, *Mądrość…*, op. cit., p. 51-52.
171 v. Tomasz z Akwinu, *O władzy*, op. cit., 152-154.
172 v. J. Świniarski, W. Chojnacki, *Filozofia…*, op. cit., p. 58.
173 v. Tomasz z Akwinu, *O władzy*, op. cit., 152-154.

będzie faktycznie dobre, dlatego też do dobrego działania potrzebna jest mądrość, która pozwala dążyć do dobra uwzględniając prawdę[174]. Pomimo, że zagadnienie zbawienia dotyczy stricte teologii, to w naukach społecznych istnieją podejścia uznające istnienie Boga (a więc i możliwość realnego zbawienia), które e.g. w ramach psychologii religii określane są jako podejścia włączające transcendencję. Oczywiście istnieją również ujęcia, które wyłączają transcendencję i uznają, że wszystkie obiekty religijne są tylko i jedynie procesami wewnętrznymi konkretnych osób[175]. Co więcej dążenie do zbawienia jako celu dla pojedynczych osób, jak i całych społeczeństw może być odrzucane ze względu na kult ciała, który jest obecny w postmodernistycznych społeczeństwach, w którym to pomija się problem śmierci, a co za tym idzie – również zagadnień związanych z rzeczami ostatecznymi człowieka (eschatologią), które po niej następują. Innym powodem, który może spowodować odrzucenie zbawienia jako celu ostatecznego jest przejmowanie prerogatyw religii przez państwo, które może próbować zapewnić człowiekowi sens życia, spełnienie i szczęście[176]. W przypadku marksizmu również widoczne jest zastępowanie przez państwo religii, co objawia się w zastąpieniu eschatologii chrześcijańskiej przez tak jakby eschatologię świecką, która postuluje jako ostateczny cel każdego człowieka budowanie raju na ziemi, co sprowadza się do parodiowania religii i samego Boga[177]. Z formalnego punktu widzenia zarówno eschatologia chrześcijańska postulująca dążenie do zbawienia, jak i dążenie do budowania raju na ziemi należą do norm ideologicznych, czyli pewnego systemu teoretycznego, z którego wynika pewien cel zarówno dla jednostki (w przypadku motywacji ideologicznych), jak i grupy (w przypadku norm ideologicznych). Różnica tych norm wynika z ich treści, jak i ich wpływu na bezpieczeństwo jednostki i grupy – co zostanie opisane w podrozdziale 5.2, w którym przedstawiono wzorzec bezpieczeństwa

174 v. A. Andrzejuk, *Tomasz…*, op. cit., p. 93.
175 v. D. Wulff, *Psychologia religii. Klasyczna i współczesna*, Wydawnictwo Szkolne i Pedagogiczne, Warszawa 1999, p. 531-532.
176 v. C. Smuniewski, *Between Eternal Life, Politics And Peace: Thoughts on Contemporary Challenges for Eschatology*, in: *Path*, 18(2019), p. 480-482.
177 v. ibid., p. 482-485.

cyberprzestrzeni wobec operacji informacyjnych i w podrozdziale 5.4, gdzie porównano model dywersji ideologicznej KGB z powyższym wzorcem.

Warto pochylić się nad zagadnieniem szczęścia, gdyż również związane jest z celem człowieka. Według Akwinaty szczęście, rozumiane jako trwała satysfakcja z życia i z tego, co się w nim robi, można osiągnąć przez działania, które wynikają z rozumnej natury ludzkiej, a więc z przyjaźni z innymi i cnotliwego życia[178]. Zatem aspekt bezpieczeństwa związany z przetrwaniem jest jednocześnie powodem szczęścia.

Według Akwinaty zabezpieczenie danej społeczności przez rządzących może się odbyć przez wprowadzenie odpowiedniego prawa, dbanie o wysoki poziom moralności, edukację następców decydentów i obronę granic[179]. Na podstawie powyższych rozważań należy uznać, że propozycja Tomaszowego społeczeństwa opiera się na budowaniu społeczeństwa o wysokich normach ideologicznych (dążenie do zbawienia), etycznych (prowadzenie cnotliwego życia) i poznawczych (szukanie mądrości i wiedzy) przy jednoczesnym niezaniedbywaniu norm prawnych (jako zabezpieczenie dobrego życia jednostek), ekonomicznych (zapewnienie dobrobytu obywatelom) i witalnych (zachowanie zdrowia). Postulat dbania przez władcę o rozwój swojego społeczeństwa[180] świadczy o dynamicznym charakterze systemu sterowania społecznego[181] proponowanego przez Akwinatę.

Z punktu widzenia dominujących norm w propozycji Doktora Anielskiego i jej dynamicznego charakteru można określić tę wizję społeczeństwa jako system dynamiczno-informacyjny z przewagą motywacji etyczno-ideologicznych. Ten rodzaj systemu sterowania społecznego cechuje się wysoką zdolnością do homeostazy i jest odporny na zakłócenia związane z sytuacją ekonomiczną, zagrożeniami militarnymi i wymuszeniami prawnymi, a z drugiej strony jest podatny na indyferentyzm ideologiczny, osłabianie etyki społeczeństwa, jak i programowanie społeczeństwa w innej ideologii. Dominującym typem sterowania

178 v. ibid., p. 73-75.
179 v. J. Świniarski, W. Chojnacki, *Filozofia…*, op. cit., p. 58-59.
180 v. Tomasz z Akwinu, *O władzy*, op. cit., 154.
181 cf. J. Kossecki, *Cybernetyka kultury*, Państwowy Instytut Wydawniczy, Warszawa 1974, p. 152-153.

jest sterowanie pośrednie przez wychowanie, a sam proces sterowania zużywa niewiele energii przez niski udział zarówno represji, jak i kontroli. Przykładem takiego systemu sterowania społecznego jest starożytny Rzym (szczególnie w okresie republiki)[182]. Zagrożenia wynikające z programowania inną ideologią, czy wręcz próby zastąpienia systemu sterowania o dominujących bodźcach ideologiczno-etycznych jakimś innym systemem sterowania (e.g. o dominujących bodźcach witalnych lub ekonomicznych) związane są z brakiem pokoju w danym społeczeństwie. Akwinata definiował zgodę jako „zejście się w jedno" w jakiejś sprawie. Jeśli zgoda obejmuje wszystkie sprawy zasadnicze, to dopiero wtedy można mówić o pokoju[183]. Zatem niezgoda w kwestiach najistotniejszych (cel społeczeństwa i wykorzystywane środki do jego osiągnięcia) uniemożliwia pokój, a więc jest pewnym niebezpieczeństwem. Potwierdza to również Koneczny (którego teoria cywilizacji jest podstawą uogólnienia teorii norm społecznych Kosseckiego[184]), który twierdzi, iż „nie można być cywilizowanym na dwa sposoby"[185], a więc różne systemy sterowania społecznego w tym samym społeczeństwie są oznaką jego rozpadu[186]. Należy podkreślić, iż Kossecki stwierdza, że nie jest zasadne tworzenie jednego, uniwersalnego układu norm społecznych dla wszystkich ludzi, gdyż każdy posiada wady i zalety w określonych okolicznościach[187], co stoi w sprzeczności z ujęciem (neo)tomistycznym. Z drugiej strony przyjęcie kryterium szczęścia jako istotnego elementu bezpieczeństwa jednostki i jej głównego celu ogranicza liczbę optymalnych systemów sterowania społecznego (e.g. wszystkich systemów sterowania społecznego, w których normy etyczne zgodne z normami poznawczymi nie są dominujące, gdyż szczęście rodzi się z wypracowywania cnót). Podobnie założenie o istnieniu celu społeczeństwa (zbawieniu) zakłada dominację norm ideologicznych w postulowanym społeczeństwie, co dodatkowo ogranicza pulę optymalnych systemów sterowania społecznego.

182 v. J. Kossecki, *Cybernetyka społeczna*, op. cit., p. 363-368.
183 v. A. Andrzejuk, *Tomasz…*, op. cit., p. 111-112.
184 v. J. Kossecki, *Metacybernetyka*, op. cit., p. 152
185 v. ibid., p. 210.
186 v. ibid., p. 210-211.
187 v. ibid.

Tomistyczne postulaty można odnieść do systemu autonomicznego. W przypadku korelatora jednostki powstałe rejestraty powinny wspomagać podejmowanie optymalnych decyzji (na podstawie posiadanej mądrości) dla systemu (dążenie do Dobra i Prawdy). W przypadku człowieka optymalna decyzja (dążenie do zbawienia przez cnotliwe życie) może być niezgodna z energomaterialnym interesem jednostki, ale może być wzmacniana przez wykorzystanie potencjału swobodnego w homeostacie (związanego z cnotami – dobrym życiem). Aby jednak dowolna inicjatywa mogła zostać podjęta przez system musi on posiadać moc swobodną (dobrobyt). W skrajnych przypadkach akcja może być podjęta kosztem energii roboczej co może prowadzić do unicestwienia systemu, jednakże w postulowanej przez Doktora Anielskiego wizji społeczeństwa każdy powinien posiadać odpowiednią ilość dóbr materialnych, które powinno pozwolić na godne i dobre życie, które doprowadzi do równowagi funkcjonalnej systemu.

Św. Tomasz z Akwinu definiuje poczucie bezpieczeństwa (łac. securitas) jako „skutek opanowania strachu”[188]. Jak zostało przedstawione w poprzednim rozdziale, według Doktora Anielskiego jednostka odczuwa strach, jeśli czuje, iż nie jest w stanie poradzić sobie ze złem, które napotyka na swojej drodze. Strach może być opanowany, jeśli dana osoba posiada odpowiednio wyćwiczoną wolę (związaną z potencjałem swobodnym) w ramach cnoty jaką jest męstwo. To co jest postrzegane przez jednostkę jako dobre lub złe zależy od dominujących motywacji danej jednostki. Dla przykładu, jeśli jednostka posiada wysokie motywacje ekonomiczne (związane z zyskiem lub stratą), to strach może zostać wywołany przez bodziec zawierający informację e.g. o nadchodzącej stracie pieniężnej (lub jej prawdopodobieństwu). Jeśli dana jednostka opanowała strach, to można mówić, o tym, że czuje się bezpieczna. Gogacz dodaje, że poczucie bezpieczeństwa związane jest z trwaniem jednostki w przyjaźni, dzięki której jednostka może zawsze uzyskać potrzebną jej pomoc[189], jak i związana jest

188 v. A. Andrzejuk, *Tomasz*…, op. cit., p. 113.
189 v. M. Gogacz, *Wprowadzenie*…, op. cit., p. 70.

z Ojczyzną, którą należy rozumieć jako odniesienie do tego, co wprowadza osoby w stan szczęścia, a więc jest pośrednio związana z poczuciem bezpieczeństwa[190].

Szczególnie istotne jest podejście człowieka do wydarzeń (związanych z potencjalnym zyskiem lub potencjalną stratą), które jednostka uważa, że najprawdopodobniej zajdą (prawdopodobieństwo bliskie, ale nierówne 1), jak i w przypadku wydarzeń, które w mniemaniu jednostki raczej nie zajdą (prawdopodobieństwo bliskie, ale nierówne 0). Ludzka psychika nie reaguje na przewidywane wydarzenia w sposób proporcjonalny do prawdopodobieństwa jego wystąpienia. Kahneman i Amos przeprowadzili badanie, w którym przyporządkowali wagi decyzji (od 0 do 100) nadawane decyzjom związanym z zakładami hazardowymi do prawdopodobieństwa wygranej lub przegranej w tych zakładach[191]. Wyniki badania przedstawia poniższa tabela.

Tabela 6: Prawdopodobieństwo wydarzenia a jego waga decyzyjna

źródło: opracowanie własne na podstawie: D. Kahneman, Pułapki..., op. cit., p. 417.

Prawdopodobieństwo	0	0,01	0,02	0,05	0,1	0,2	0,5	0,8	0,9	0,95	0,98	0,99	1
Waga decyzji	0	5,5	8,1	13,2	18,6	26,1	42,1	60.1	71,2	79,3	87,1	91,2	100

Można zauważyć, iż e.g. zmiana prawdopodobieństwa z 0 do 0,01 wiąże się z większą zmianą wagi decyzji, niż e.g. zmiana prawdopodobieństwa wydarzenia z 0,05 do 0,1. Podobnie zmiana prawdopodobieństwa z 0,99 do 1 zmienia wagę decyzyjną o 8,8, czyli o więcej, niż przy zmianie prawdopodobieństwa z 0,9 na 0,95. Warto również zauważyć, że przedziałowi prawdopodobieństw od 0,05 do 0,95 odpowiada węższy przedział wag decyzyjnych (od 13,2 do 79,3, czyli około 2/3 wszystkich wartości)[192]. Efekt zmiany prawdopodobieństwa z 0 na 0,05 został nazwany efektem możliwości, natomiast efekt związany ze zmianą prawdopodobieństwa z 0,95 na 1 efektem pewności[193]. Wynik badania sugeruje, że jednostki przeceniają wydarzenia mało prawdopodobne (nadają im

190 v. ibid., p. 76.
191 v. D. Kahneman, *Pułapki…*, op. cit., p. 417-420.
192 cf. ibid.,, p. 418.
193 v. ibid., p. 412-413.

nieproporcjonalnie wysoką wagę decyzyjną wobec ich prawdopodobieństwa), ale i nie doceniają wydarzeń prawie pewnych (nadają im nieproporcjonalnie niską wagę w stosunku do ich prawdopodobieństwa). W przypadku wydarzeń o skrajnie niskim lub skrajnie wysokim prawdopodobieństwie, jednostka je zupełnie ignoruje (waga decyzyjna równa 0), a jeśli zaczyna je brać pod uwagę, to przypisuje im nieproporcjonalną do prawdopodobieństwa wagę decyzyjną[194]. Wynika to z heurystyki dostępności, która polega na tym, iż osoba w swojej ocenie rzeczywistości (ocenianiu częstości wydarzeń lub istotności idei) nie kieruje się całością swojej wiedzy i bieżących informacji wynikającymi z poznania, ale tylko tymi aspektami, które są łatwo wydobywane z umysłu lub łatwo z nimi kojarzone[195].

Ludzka reakcja na bodziec jest uzależniona również od tego czy przewidywane wydarzenie wiąże się ze stratą (pewnym złem), czy z zyskiem (pewnym dobrem). Według badań psychologicznych człowiek niechętnie podchodzi do sytuacji, która może spowodować stratę[196]. Wydaje się zatem, iż łatwiej wywołać w człowieku te emocje władzy gniewliwej, które odnoszą się do zła (odwagę, strach lub gniew), niż te, które odnoszą się do dobra (nadzieję, smutek). Zatem informacja o potencjalnej stracie (e.g. pewnej kwoty pieniędzy) wywoła większą reakcję jednostki od informacji o potencjalnym zysku takiej samej kwoty. Odnosząc się jednocześnie do zjawiska odczuwanej straty i zysku oraz efektu pewności i możliwości możliwe jest opisanie czterech wariantów stosunku do ryzyka. Jeśli dana osoba ma perspektywę dużego zysku i może wybrać między ryzykiem i możliwością zarobienia większej kwoty (przy minimalnym prawdopodobieństwie nie wygrania niczego), a pewnością wygrania mniejszej kwoty, to najprawdopodobniej wybierze kwotę pewną. Jeśli wysokie prawdopodobieństwo dotyczy straty, to prawdopodobnie jednostka odrzuci korzystną (z punktu widzenia wartości oczekiwanej) ugodę, aby zaryzykować uniknięcia strat w ogóle. W przypadku niskiego prawdopodobieństwa zdarzenia, to

194 v. ibid., p. 418-419.
195 cf. ibid., p. 116, 193.
196 v. ibid., p. 376-378.

w przypadku zysków jednostki będą prawdopodobnie chętnie ryzykować, aby osiągnąć duży zysk nawet przy pomijalnym prawdopodobieństwie wygranej, a w przypadku potencjalnych strat jednostka zastosuje nieproporcjonalnie wysokie koszty zabezpieczenia się przed wydarzeniem przynoszącym straty, którego prawdopodobieństwo wystąpienia jest niskie[197].

Tabela 7: Warianty stosunku do ryzyka

źródło: opracowanie własne na podstawie: D. Kahneman, Pułapki..., op. cit., p. 420-423.

	Zyski	Straty
Wysokie prawdopodobieństwo (efekt pewności)	Niechęć do ryzyka Lęk przed rozczarowaniem	Skłonność do ryzyka Nadzieja uniknięcia starty
Niskie prawdopodobieństwo (efekt możliwości)	Skłonność do ryzyka Nadzieja na dużą wygraną	Niechęć do ryzyka Lęk przed dużą stratą

Odnosząc się do bezpieczeństwa grup i zasobów, należy uznać, iż na podstawie przyjętych założeń metafizycznych bezpieczeństwo jednostki jest punktem odniesienia do bezpieczeństwa zarówno grup, jak i zasobów. Zasoby są wykorzystywane przez jednostki zarówno do poznawania, jak i działania, a więc zasadność zachowania pewnych zasobów w istnieniu i gotowości do działania (utrzymywanie stanu $<1,1,0>$ zasobu), aby jednostka mogła go wykorzystać w momencie, kiedy będzie tego chciała i działania (stan $<1,1,1>$) w momencie, kiedy jednostka chce, aby dany zasób był aktywny. Z drugiej strony grupa jest nierozerwalnie związana z jednostkami. Zbiór osób, które są powiązane relacjami określają grupę i jej właściwości, a zatem zmiana właściwości (stanu) jednostki zmienia również samą grupę.

4.2. Bezpieczeństwo informacyjne

Dążenie do dobrobytu, dobrego życia i pokoju wymaga działania, które zawsze musi opierać się na pewnych informacjach w korelatorze. Zatem na

197 v. ibid., 420-423.

bezpieczeństwo jednostki, z którego wynika bezpieczeństwo grupy i zasobów, wyróżnić należy również aspekt bezpieczeństwa komunikatów. Informacja jest rozumiana jako relacja między dwoma komunikatami, a więc chroniąc komunikaty chroni się jednocześnie informacje z nich wynikające. Do zgłębiania zagadnienia bezpieczeństwa komunikatów (bezpieczeństwa informacyjnego) użyto i uogólniono model kostki cyberbezpieczeństwa (ang. cybersecurity cube) i model kill chain.

Na potrzeby opisu ataków na sieć komputerową i prób jej podsłuchiwania został opracowany model Intrusion kill chain, na który składają się następujące fazy[198]:

1 Faza rekonesansu (ang. reconnaissance) – zdobycie informacji o systemie, na który ma zostać przeprowadzony atak.
2 Faza uzbrajania (ang. weaponization) – opracowanie narzędzi (exploitów) do przeprowadzenia ataku.
3 Faza dostarczania (ang. delivery) – dostarczenie uzbrojonego oprogramowania.
4 Faza eksploatacji (ang. exploitation) – przełamanie zabezpieczeń.
5 Faza instalacji (ang. installation) – instalowanie złośliwego oprogramowania.
6 Faza sterowania (ang. command and control) – zdalne łączenie się atakującego do zainfekowanego środowiska w celu sterowania nim.
7 Faza działania (ang. action on objectives) – wykonanie zamierzonego celu (naruszenie poufności, integralności lub dostępności danych).

Powyższy model można opisać w kategoriach cybernetycznych. Rekonesans polega na wykorzystaniu kanału komunikacyjnego do rozpoznawanego systemu, aby za pomocą receptorów odbierać komunikaty z jego efektorów. Można tu wyróżnić dwa rodzaje rozpoznania: pasywne (tylko odbieranie komunikatów)

198 E. Hutchins, M. Cloppert, R. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, in: *Leading Issues in Information Warfare and Security Research*, vol. 1, J. Ryan (red.), Academic Publishing International Limited, Reading 2011, p. 87-88.

i aktywne (odbieranie komunikatów po uprzedniej ingerencji w receptory rozpoznawanego systemu, co pozwala sprawdzić reaktywność systemu na dany bodziec). Nie zawsze jest jednak możliwość, aby stwierdzić, że dany komunikat na pewno pochodzi od danego systemu, albo że jest powiązany akurat z danym bodźcem. Faza uzbrajania polega na opracowaniu takiego komunikatu, który w fazie eksploatacji wywoła taki potencjał receptorowy atakowanego systemu, w wyniku którego (w fazie instalacji) w jego korelatorze powstaną rejestraty, które będą wykorzystywane na potrzeby dalszych etapów ataku. Faza dostarczania polega na znalezienie kanału komunikacyjnego do atakowanego systemu, aby dostarczyć nim komunikat (bodziec) do receptorów tegoż systemu (faza instalacji). Faza sterowania polega na tym, iż dzięki powstałym rejestratom zostaje zestawiony kanał komunikacyjny (możliwość przesyłania danych zainfekowanemu systemowi przez jego receptory przy jednoczesnej możliwości odbierania informacji o skuteczności tych poczynań przez jego efektory) z atakowanego systemu do atakującego, dzięki któremu ten może generować kolejne komunikaty sterując zainfekowanym systemem przez wytworzone w fazie instalacji rejestraty. W wyniku takiego sterowania zostaje wypełniony cel atakującego – niszczenie rejestratów w atakowanym systemie (atak na integralność lub dostępność informacji, utrata aktywności, gotowości lub unicestwienie systemu), kradzież informacji (atak na poufność), wymuszenie pewnej reakcji systemu (aktywacja systemu) lub przygotowanie środowiska korelacyjnego na przyszłe ataki (na przykład przez utrzymanie kanału komunikacyjnego do zainfekowanego systemu tworzeniem trudno usuwalnych i wykrywalnych rejestratów).

Przełożenie modelu Intrusion kill chain na język cybernetyki pozwala również go uogólnić, aby nie dotyczył tylko cyberprzestrzeni i zasobów, ale również jednostek i grup w przestrzeni sterowania jako takiej. Rekonesans jednostki polega na analizowaniu jej reakcji, która została wymuszona przez atakującego (rekonesans aktywny) lub niewymuszona (rekonesans pasywny). Faza uzbrojenia dotyczy opracowania komunikatu (przekazu e.g. perswazyjnego), który po procesie informowania (faza dostarczania), zwraca uwagę danej jednostki (faza

eksploatacji), aby odcisnął się w jej umyśle jako rejestrat (faza instalacji). Tak powstałe rejestraty mogą zwiększać reaktywność całego systemu na niektóre bodźce (inne rejestraty pochodzące z następnych przekazów – z fazy sterowania), które się odwołują do tych rejestratów, co może zwiększyć prawdopodobieństwo na reakcję systemu (jednostki) zgodnie z wolą atakującego (faza działania).

McCumber podzielił zagadnienia związane z cyberbezpieczeństwem na trzy domeny, w których każda z nich zawiera trzy elementy[199]:

- właściwości informacji:
  - poufność – polegająca na tym, iż dostęp do wiadomości posiadają tylko i jedynie osoby do tego uprawnione,
  - integralność – zwana również jakością informacji, czyli tym jak bardzo informacja odpowiada rzeczywistości (czy jest trafna, kompletna lub wiarygodna),
  - dostępność – dotycząca tego czy informacja jest dostępna, wtedy kiedy powinna być dostępna.
- stany informacji:
  - informacja przechowywana,
  - informacja przesyłana,
  - informacja przetwarzana,
- środki bezpieczeństwa:
  - środki dotyczące personelu – obejmują treningi czujności i szkolenia – dotyczą pojedynczych jednostek (osób),
  - polityki, dobre praktyki i procedury – organizacyjne sposoby zapewniania bezpieczeństwa informacyjnego – dotyczą relacji myślnych między osobami, a więc właściwości grupy,
  - środki techniczne – techniczne sposoby (przez sprzęt i oprogramowanie) na zapewnienie bezpieczeństwa informacyjnego – dotyczą zasobów.

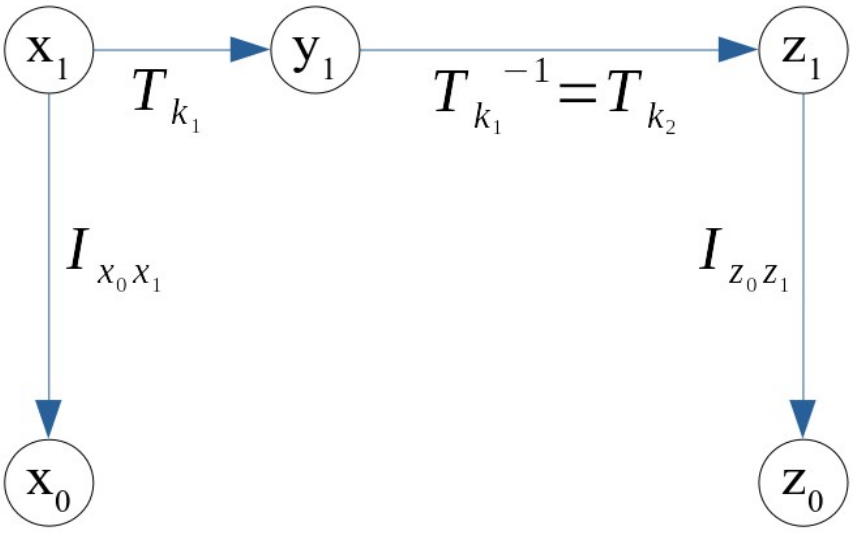
199 v. J. McCumber, *Assessing and Managing Security Risk in IT Systems. A Structured Methodology*, Auerbach Publications, Nowy York 2004, p. 99-107.

Możliwe jest analizowanie wycinka bezpieczeństwa informacyjnego cyberprzestrzeni przez dobranie jednego elementu z każdego wymiaru. Dla przykładu można analizować poufność informacji w czasie ich przesyłania pod kątem polityk i procedur bezpieczeństwa. Pełna analiza bezpieczeństwa, według powyższego modelu, będzie dotyczyła wszystkich dwudziestu siedmiu możliwości.

Próbując powyższy model osadzić w jakościowej teorii informacji Mazura należy ustalić jaki charakter informowania posiadają procesy związane z przesyłaniem i przechowywaniem informacji. Niezależnie czy informacja ma na celu szkodzenie przeciwnikowi, czy działanie na korzyść sił własnych lub sprzymierzonych, musi ona dostać się do odbiorcy w niezmienionej formie, aby wywołać odpowiednie zmiany w korelatorze pod wpływem których może dojść do przewidzianej przez nadawcę reakcji. Zatem niezależnie od celu nadawcy, informowanie powinno mieć charakter transinformowania (informowania wiernego). W przypadku przesyłania komunikatów do osoby, która jest uprawniona do ich otrzymania pożądane jest paratransinformowanie, w którym komunikaty, które odebrał odbiorca wchodzą w relację z już istniejącymi komunikatami (rejestratami) w jego korelatorze. Rejestraty odbiorcy dotyczą chociażby języka, którym się dana osoba posługuje, ale mogą również obejmować pewne sposoby, procedury działania, wcześniej ustalone kody, dzięki którym powstanie pożądana informacja, którą chciał przesłać nadawca. W przypadku przechwycenia informacji przez osobę nieuprawnioną pożądany jest efekt paradezinformowania, czyli uzyskania u niepożądanego odbiorcy informacji, które są rozbieżne z informacjami, jakie chciał przesłać nadawca do uprawnionej osoby. Może się tak stać, jeśli nieuprawniony odbiorca nie zna języka nadawcy lub kodu w kluczu którego można wiadomość odpowiednio zrozumieć, czyli w korelatorze odbiorcy nie występują rejestraty (komunikaty), które pozwalają na powstanie odpowiedniej informacji.

Paradezinformowanie osób nieuprawnionych do informacji przy równoczesnym paratransinformowaniu osób, które są do niej uprawnione może być przeprowadzone przez szyfrowanie lub korzystanie ze steganografii (sztuki

ukrywania przekazu). Współczesna kryptografia oferuje dwa rodzaje szyfrowania – z wykorzystaniem kluczy symetrycznych i asymetrycznych. Szyfrowanie kluczem symetrycznym polega na wykorzystaniu tego samego klucza kryptograficznego w procesie szyfrowania i odszyfrowywania. W przypadku klucza asymetrycznego wyróżnia się dla każdej ze stron (nadawcy i odbiorcy) parę kluczy, na którą się składa klucz prywatny (k_2 strony, do której się wysyła zaszyfrowaną wiadomość) i publiczny (k_1 strony, do której wysyła się zaszyfrowaną wiadomość). Szyfrowanie w jakościowej teorii informacji można przedstawić w następujący sposób:



Rys. 28: Szyfrowanie w jakościowej teorii informacji

źródło: opracowanie własne.

Gdzie:

- k_1i k_2 są kluczami kryptograficznymi (w szyfrach symetrycznych $k_1 = k_2$, a przy asymetrycznych $k_1 \neq k_2$ i obydwa klucze należą do odbiorcy),
- T_{k_1} – szyfrowanie (kodowanie) pierwszym kluczem,
- $T_{k_2} = T_{k_1}^{-1}$ – deszyfrowanie drugim kluczem. Funkcja deszyfrująca jest odwrotnością funkcji szyfrującej takiej, że $T_{k_2}\left(T_{k_1}(x_1)\right) = z_1$,

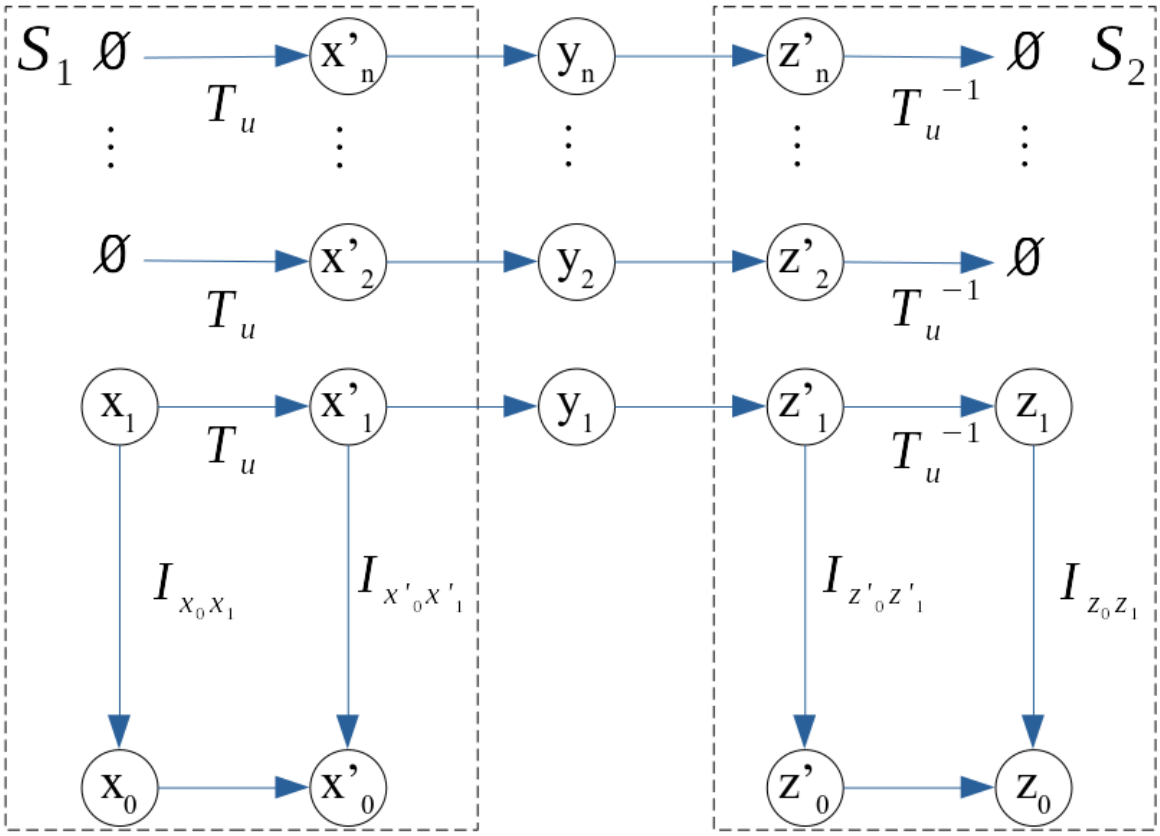
- x_1, z_1 – tekst jawny,
- y_1 – szyfrogram (zaszyfrowany interkomunikat),

W przypadku jakościowej teorii informacji transformacja oznacza tylko i jedynie konkretną operację (e.g. dodawanie wartości 5, ale już nie dodawanie)[200]. Zatem szyfrowanie (transformacja T_{k_1}) nie oznacza szyfrowania jako takiego, a nawet szyfrowania konkretnym szyfrem, ale szyfrowanie konkretnym szyfrem (operacja) przy wykorzystaniu konkretnego klucza (parametr operacji)[201]. Dodatkowo, aby możliwe było paratransinformowanie ($I_{x_0x_1}=I_{z_0z_1}$) w korelatorze zarówno nadawcy, jak i odbiorcy muszą występować rejestraty x_0 i z_0, takie że $x_0=z_0$. Należy nadmienić, iż jeśli przeciwnik przechwycił komunikat i posiada rejestrat a_0, taki że $a_0=x_0=z_0$, to $I_{a_0y_1}\neq I_{x_0x_1}$ i $I_{a_0y_1}\neq I_{z_0z_1}$, a więc wystąpi zjawisko paradezinformowania. Według zasady Kerckhoffsa bezpieczeństwo szyfrów powinno opierać się tylko i jedynie na poufności klucza kryptograficznego[202]. Zatem w przypadku szyfrów symetrycznych klucz nie może zostać ujawniony jednostkom i zasobom nieuprawnionym, a w przypadku szyfrów asymetrycznych – należy chronić poufność klucza prywatnego, gdyż obliczenie funkcji odwrotnej do funkcji szyfrującej, jak i funkcji odwrotnej do funkcji deszyfrującej, jest niemożliwe, nawet przy dużych możliwościach obliczeniowych atakującego, w czasie, po którym informacja wynikająca z odszyfrowanego komunikatu będzie jeszcze przedstawiała jakąkolwiek wartość sterowniczą[203].

Z kolei steganografia polega na wytworzeniu lub wykorzystaniu wielu torów sterowniczych (dezinformowaniu symulacyjnym) do ukrycia w nich komunikatów istotnych z punktu widzenia nadawcy (zwanych dalej istotnymi komunikatami, które tworzą informację istotną). Nadprogramowa ilość komunikatów może nie posiadać żadnej właściwości sterowniczej lub nawet być szkodliwa dla

200 cf. M. Mazur, *Jakościowa…*, op. cit., p. 45-46.
201 cf. ibid.
202 cf. J. Szmidt, M. Misztal, *Wstęp do kryptologii*, Wyższa Szkoła Informatyki Stosowanej i Zarządzania, Warszawa 2004, p. 28.
203 cf. ibid., p. 37, 155.

podsłuchującego, jeśli nie uświadamia sobie, że dodatkowe komunikaty pełnią tylko rolę szumu. Bezpieczeństwo tak ukrytego przekazu polega na niemożności przetworzenia wszystkich możliwości przez korelator jednostki nieuprawnionej do otrzymania informacji. Odbiorca uprawniony musi znać sposób (transformację) w jaki istotne komunikaty zostały ukryte, aby móc usunąć komunikaty nieistotne (dezinformacja dysymulacyjna). Steganografię można zobrazować następującymi schematem:



Rys. 29: Steganografia w jakościowej teorii informacji

źródło: opracowanie własne.

Gdzie:

- S_1 – system pierwszy (nadawca),
- S_2 – system drugi (odbiorca),
- $\varnothing$ – brak komunikatu,
- x_1 – komunikat istotny,

- x'_n – komunikaty po procesie ukrycia przekazu,
- T_u – transformacja ukrywająca przekaz,
- z'_n – komunikaty przed procesem odkrywania przekazu,
- T_u^{-1} – transformacja odkrywająca przekaz,
- $x_1 = x'_1$ i $z_1 = z'_1$, gdyż transformacja ukrywająca lub odkrywająca prowadzi do dezinformacji komunikatów odpowiadających za tworzenie szumu informacyjnego, ale nie narusza istotnych komunikatów,
- $I_{x_0 x_1} = I_{x'_0 x'_1} = I_{z'_0 z'_1} = I_{z_0 z_1}$ – istotna informacja, która miała zostać przekazana.

Jak można zauważyć, jeśli osoba nie zna transformacji odkrywającej, to w celu zrozumienia wiadomości musi przeanalizować znacznie więcej informacji, niż osoba, która przeprowadzi transformację odkrywania przekazu. Przy założeniu, że osoba nieuprawniona posiada w korelatorze rejestraty $a_0 = x_0 = z_0$, to musi przeanalizować wiadomości $I_{a_0 y_0}$ do $I_{a_0 y_n}$, aby zrozumieć przekaz. Jeżeli komunikaty obejmują pojedyncze litery lub nawet bity, które muszą być odczytywane w określonym, ściśle ustalonym porządku, to zwiększa się liczba możliwości odczytywania przekazu, czyniąc go trudnym lub wręcz niemożliwym do wychwycenia. Istnieje prawdopodobieństwo, iż osoba nieuprawniona nawet nie zauważy, że w danych torach sterowniczych są przesyłane komunikaty z wykorzystaniem steganografii. Analizę ukrytego przekazu można dodatkowo skomplikować przez wcześniejsze zaszyfrowanie komunikatu. Co więcej, powyższy schemat może być wykorzystany do generowania szumu. Generowanie dodatkowych komunikatów w torach sterowania (dezinformowanie) transformacją ukrywającą (przez źródło zakłóceń) może doprowadzić do sytuacji, w której odbiorca komunikatów nie będzie w stanie odczytać pierwotnego komunikatu, gdyż nie będzie znał transformacji odkrywającej przekaz. Co istotne strona generująca szum również nie musi znać transformacji odkrywającej.

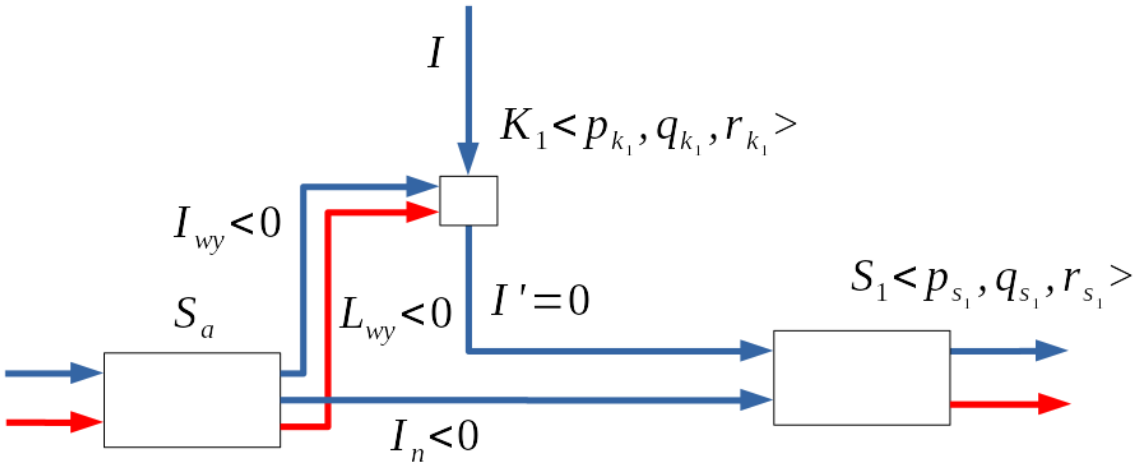
Szyfrowanie i steganografia mogą być użyteczne do zapewnienie poufności informacji w stanie przenoszenia i przechowywania informacji głównie za pomocą

środków technicznych. Korzystanie z szyfrów wymusza wprowadzenie dodatkowych środków organizacyjnych i osobowych ze względu na potrzebę administracji urządzeń, na których odbywa się szyfrowanie (zarówno zdalną, jak i bezpośrednio w pomieszczeniach, w których fizycznie znajdują się dane maszyny) i zarządzanie kluczami kryptograficznymi (szczególnie w przypadku szyfrów asymetrycznych).

Kolejną możliwością chronienia poufności danych jest kontrola wejść (torów wchodzących do receptorów) i wyjść (torów wychodzących z efektorów) kanałów komunikacyjnych (według rysunku 23.). Jeśli część wyjść efektorów nie jest kontrolowana (a więc występuje odbiornik ulotu), to może to doprowadzić do podsłuchiwania komunikatów, z tym, że ich odczytanie może zostać udaremnione opisanymi powyżej szyfrowaniem i steganografią. Z drugiej strony niekontrolowanie wszystkich wejść może doprowadzić do wprowadzania przez przeciwnika dodatkowych komunikatów zakłócających planowany przekaz (przez źródło zakłóceń), co jest naruszeniem zarówno integralności (przy zaburzeniu części przekazu, gdy część komunikatów nie dociera do docelowych receptorów) lub dostępności (gdy wszystkie komunikaty są niedostępne).

Zagadnienie kontrolowania wejść i wyjść atakowanego systemu obrazują poniższe rysunki. Zastosowano w nich następującą konwencję nazwową:

- I – informacja,
- $I<0$ – informacja niszcząca (prowadząca do wytworzenia się dalekiej od optymalnej reakcji systemu lub wprowadzenia rejestratów do korelatora przeciwnika, które taką reakcję mogą łatwiej sprowokować w przyszłości),
- L – energomateria niebędąca informacją,
- S – system,
- K – kanał komunikacyjny,
- $S<p,q,r>$ – stan systemu S (w tym kanału komunikacyjnego).



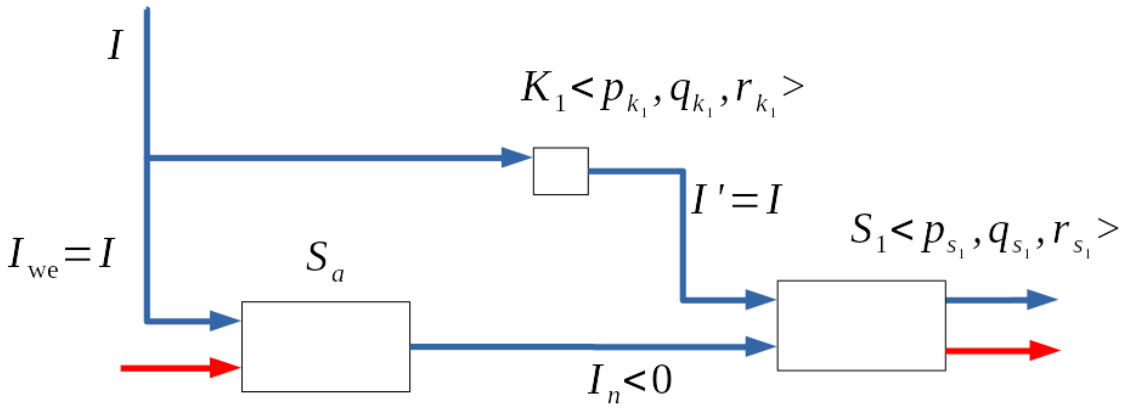
Rys. 30: Oddziaływanie na system i kanał komunikacyjny z otoczenia

źródło: opracowanie własne.

System atakujący (S_a) oddziałuje jednocześnie informacją niszczącą (I_n<0) na system S_1 i informacją niszczącą (I_{wy}<0) wraz z energomaterią (L_{wy}<0) na kanał komunikacyjny K_1. Należy podkreślić, iż w podanym scenariuszu system atakujący nie zna informacji z otoczenia (I). Sterowanie kanałem komunikacyjnym może doprowadzić do zmiany jego stanu tak, że system K_1 utraci aktywność (przestanie przesyłać informację potencjalnie użyteczną sterowniczo[204] I), utraci gotowość do przesyłania informacji (dojdzie do uszkodzenia kanału informacją lub energomaterią) lub zostanie trwale unicestwiony. Jeśli system atakujący przewiduje, iż informacja pochodząca z otoczenia jest nieużyteczna bądź szkodliwa, to może oddziaływać na kanał komunikacyjny w taki sposób, iż uzyska on aktywność do przesyłania informacji lub w przypadku jego uszkodzenia – zostanie on naprawiony (uzyska stan gotowości). Możliwy jest również scenariusz, w którym atakujący wprowadzi do kanału komunikacyjnego szum, który zagłuszy informację I sprawiając, że do systemu atakowanego dojdzie bezużyteczny ciąg komunikatów
(I'=0). Oddziaływanie informacji I' i I_n mają na celu sterowanie systemem atakowanym tak, aby zmieniać jego stan zgodnie z wolą systemu atakującego –

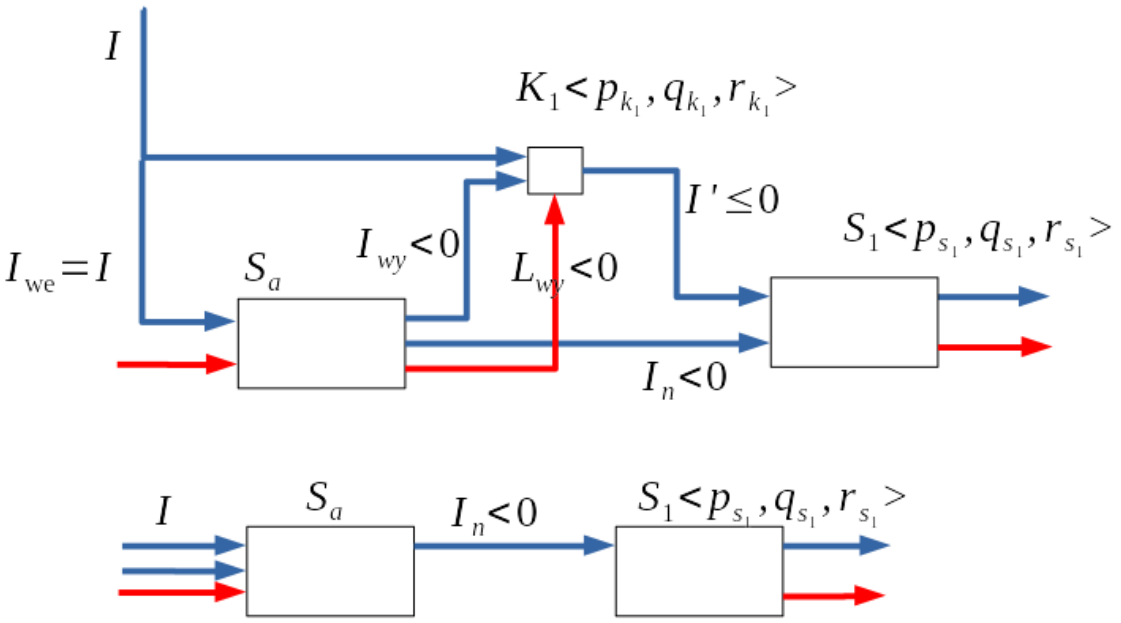
204 v. M. Mazur, *Jakościowa*…, op. cit., p. 188: „Informacja użyteczna jest to informacja spośród najmniejszej możliwej liczby informacji zawartych w danym łańcuchu informacyjnym, niezbędnych w danym procesie sterowniczym."

aktywowanie i uzyskiwanie gotowości, gdy reakcja S_1 jest pożądana lub dążenie do utraty aktywności lub gotowości S_1 lub unicestwienie tegoż systemu, gdy reakcja tego systemu jest niepożądana.



Rys. 31: Oddziaływanie na system i podsłuchiwanie informacji z otoczenia
źródło: opracowanie własne.

System atakujący S_a podsłuchuje informację z otoczenia I. Oddziaływanie dotyczy tylko i jedynie systemu S_1, ale dzięki komunikatom pochodzącym z otoczenia atakujący może odpowiednio dostosować informację niszczącą, aby odniosła zamierzony skutek w systemie atakowanym.

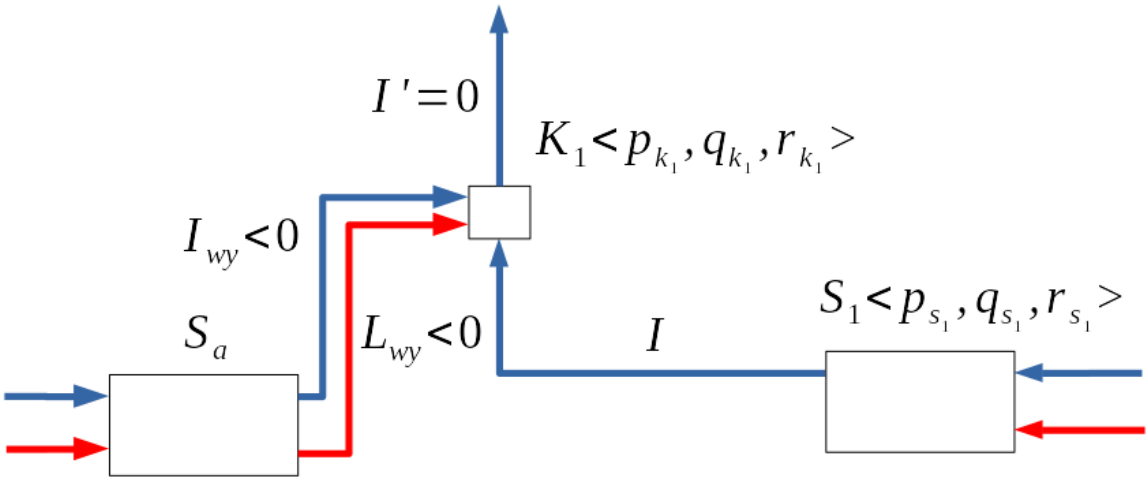


Rys. 32: Oddziaływanie na system przy pełnym kontrolowaniu wejścia

źródło: opracowanie własne.

Jeśli jednocześnie zachodzi podsłuchiwanie informacji z otoczenia przez system atakujący, jak i oddziaływanie na kanał komunikacyjny K_1 w taki sposób, iż atakujący może oddziaływać na każdą informację pochodzącą z otoczenia, to dochodzi do pełnej kontroli nad wejściem systemu atakowanego S_1. Atakujący może odpowiednio preparować informacje z otoczenia (fałszując nawet ich autorstwo), zagłuszać je, a przez podsłuchiwanie – odpowiednio dobierać przyszły przekaz. System atakowany nie ma możliwości, aby zweryfikować przychodzące informacje, gdyż nie posiada żadnych kanałów komunikacyjnych, które pochodzą z otoczenia, a nie są kontrolowane przez system atakujący. Wyjątek stanowi sytuacja, w której przeciwnik nie jest w stanie powtórzyć typowego zachowania osoby pod którą się podszywa (gdyż go nie zna lub nie ma do tego odpowiednich środków technicznych) lub nie ma tej samej wiedzy (rejestratów w korelatorze odnośnie wspólnych kodów etc.) e.g. przeciwnik nie jest w stanie zaszyfrować kluczem prywatnym jednostki, pod którą się podszywa, gdyż takiego klucza nie posiada, a zatem system atakowany może zauważyć, że doszło do zmiany

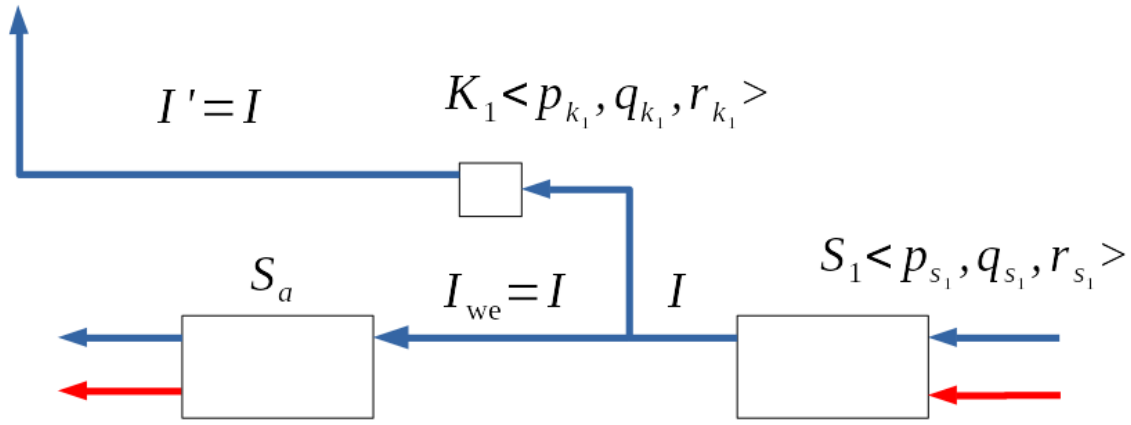
zachowania u jednostki, która przeważnie szyfrowała swoje wiadomości, a tym razem tego nie zrobiła.



Rys. 33: Oddziaływanie na kanał komunikacyjny do otoczenia

źródło: opracowanie własne.

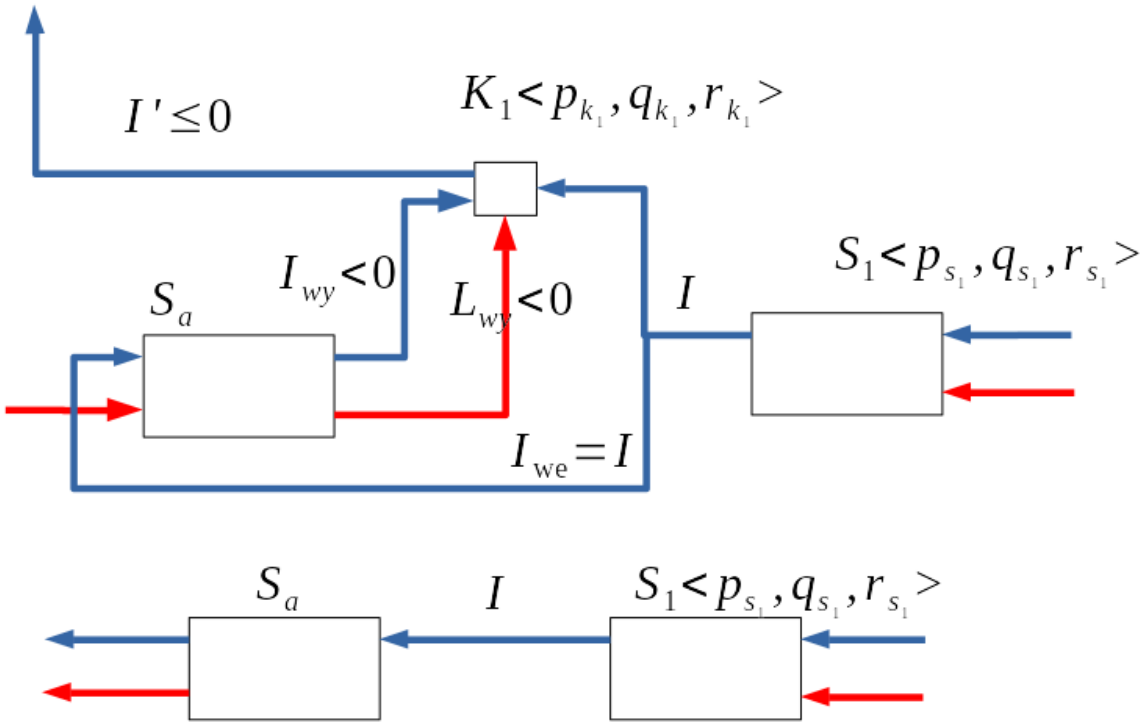
W przypadku oddziaływania na wyjście systemu możliwe jest wykorzystanie informacji niszczącej I_{wy} i energomaterii L_{wy} do wpływania na kanał komunikacyjny do otoczenia K_1 analogicznie jak w przypadku oddziaływania na kanał komunikacyjny z otoczenia. Informacja I generowana przez system atakowany może być zmieniana (zagłuszana), a sam kanał komunikacyjny uszkadzany (utrata gotowości), wyłączany (utrata aktywności) lub unicestwiany, jeśli atakujący przewiduje, że oddziaływanie na otoczenie informacją I przyniesie korzyść atakowanemu (lub zaszkodzi atakującemu). W przypadku przewidywania, że oddziaływanie informacją I na otoczenie będzie niekorzystne dla atakowanego, a korzystne dla atakującego, to S_a może aktywować K_1, a czasem nawet go naprawiać (przywracać stan gotowości).



Rys. 34: Podsłuchiwanie wyjścia systemu

źródło: opracowanie własne.

Podsłuchiwanie wyjścia systemu S_1 przez system S_a może zapewnić w przyszłości przewagę informacyjną (w zależności od podsłuchanych danych) atakującemu ze względu na rozpoznanie pasywne. Uzyskane informacje mogą być pomocne w przygotowaniu odpowiedniego przekazu w przyszłości (faza uzbrajania) w celu ataku na S_1 lub lepszego oddziaływania na otoczenie przez S_a.



Rys. 35: Pełne kontrolowanie wyjścia systemu

źródło: opracowanie własne.

W przypadku podsłuchiwania informacji z wyjścia S_1 i jednoczesnego oddziaływania na kanał komunikacyjny K_1 dochodzi do pełnej kontroli wejścia S_1. Atakujący wie jakie informacje generuje system atakowany, a co więcej może je dowolnie modyfikować, zagłuszać, przesyłać lub fabrykować własne.

W przypadku pełnej kontroli zarówno wejść, jak i wyjść system atakujący przy odpowiednich metodach sterowania może kontrolować system atakowany, w taki sposób, że będzie on otrzymywał tylko te informacje, na które zgodzi się atakujący, jak i tylko te informacje, które są zgodne z jego wolą będą wysyłane do otoczenia. Schemat ten może dotyczyć e.g. społeczeństwa w państwie totalitarnym (gdzie podsystem sterujący jest systemem atakującym, a podsystem wykonawczy systemem atakowanym) lub kontrolowanego zasobu (podsystemem sterujący jest operator, a podsystemem atakowanym zasób). Kontrolowanie wejść i wyjść systemu jest pożądane z punktu widzenia bezpieczeństwa informacyjnego danego systemu, gdyż uniemożliwia się ingerencję przeciwnika w dany system.

Jest to jednak przykład idealny, a więc wydaje się, że kontrola nad wejściami i wyjściami może być jedynie zbliżona do pełnej kontroli, chociażby przez fakt, że nie można w pełni kontrolować operatorów zasobów (przez posiadanie przez nich potencjału swobodnego w homeostacie).

Zapewnianie integralności informacji może zostać zapewnione przez obliczanie funkcji skrótu wiadomości i dołączania jej do wiadomości pierwotnej. Funkcja skrótu jest pseudoinformowaniem dysymulacyjnym, w którym komunikaty w wiadomości oryginalnej zostają przekształcone do wiadomości (skrótu lub hashu) o ustalonej z góry dla danego algorytmu funkcji skrótu długości przy utracie informacji z tekstu pierwotnego. Istotnymi cechami funkcji skrótu są niemożliwość (ze względu na niewystarczalne zasoby obliczeniowe i czasowe systemu atakującego) znalezienia wiadomości pierwotnej na podstawie skrótu, niemożliwość obliczeniowa znalezienia dowolnej wiadomości, która daje taki sam skrót jak wiadomość pierwotna, jak i niemożliwość obliczeniowa znalezienia dwóch, dowolnych wiadomości dających ten sam skrót[205].

205 J. Szmidt, M. Misztal, *Wstęp...*, op. cit., p. 125.

Rozdział V.
WZORZEC TEORETYCZNY ODDZIAŁYWANIA OPERACJI INFORMACYJNYCH NA BEZPIECZEŃSTWO JEDNOSTEK I GRUP

„Wynika z tego, że marksizm-leninizm jako utopijne uszczęśliwienie ludzkości jest skazany na ostateczne niepowodzenie. Kiedy i jak to się ma stać, zależy nie od gołosłownych stwierdzeń tych, którzy posiadają nieporównywalnie lepszą broń duchową, ale od ich woli, by stale stawiać czoła wyzwaniu marksizmu-leninizmu i nastawić swoje myśli i działania na nieustanną walkę z nim. Jest to sprawa sumienia."

J. Bocheński

Rozdział piąty składa się z czterech podrozdziałów. Pierwszy z nich dotyczy operacji informacyjnych opisanych zgodnie z dokumentami doktrynalnymi Sił Zbrojnych Rzeczypospolitej Polskiej DD 3.10 (A) o operacjach informacyjnych wraz z DD 3.20 o operacjach w cyberprzestrzeni. Wyróżnione w dokumentach przedmioty oddziaływań (zrozumienie sytuacji, wola działania i zdolności do działania) powiązano z wcześniej opisanym procesem decyzyjnym według psychocybernetyki Mazura i (neo)tomistycznej antropologii filozoficznej. Dodatkowo opisano miejsce operacji informacyjnych w ramach komunikacji strategicznej i koordynowane w ramach operacji informacyjnych zdolności i techniki.

Drugi podrozdział zawiera wzorzec bezpieczeństwa cyberprzestrzeni wobec operacji informacyjnych, na który składają się zagadnienia bezpieczeństwa jednostek, grup, zasobów i komunikatów. Opisano kryteria bezpieczeństwa poszczególnych systemów w cyberprzestrzeni ze szczególnym uwzględnieniem bezpieczeństwa jednostek. Wyodrębniono również sposób określania trendów bezpieczeństwa jednostek i grup w kontekście operacji informacyjnych. Trzeci podrozdział dotyczy porównania wzorca z teorią metod pokojowych i wojennych.

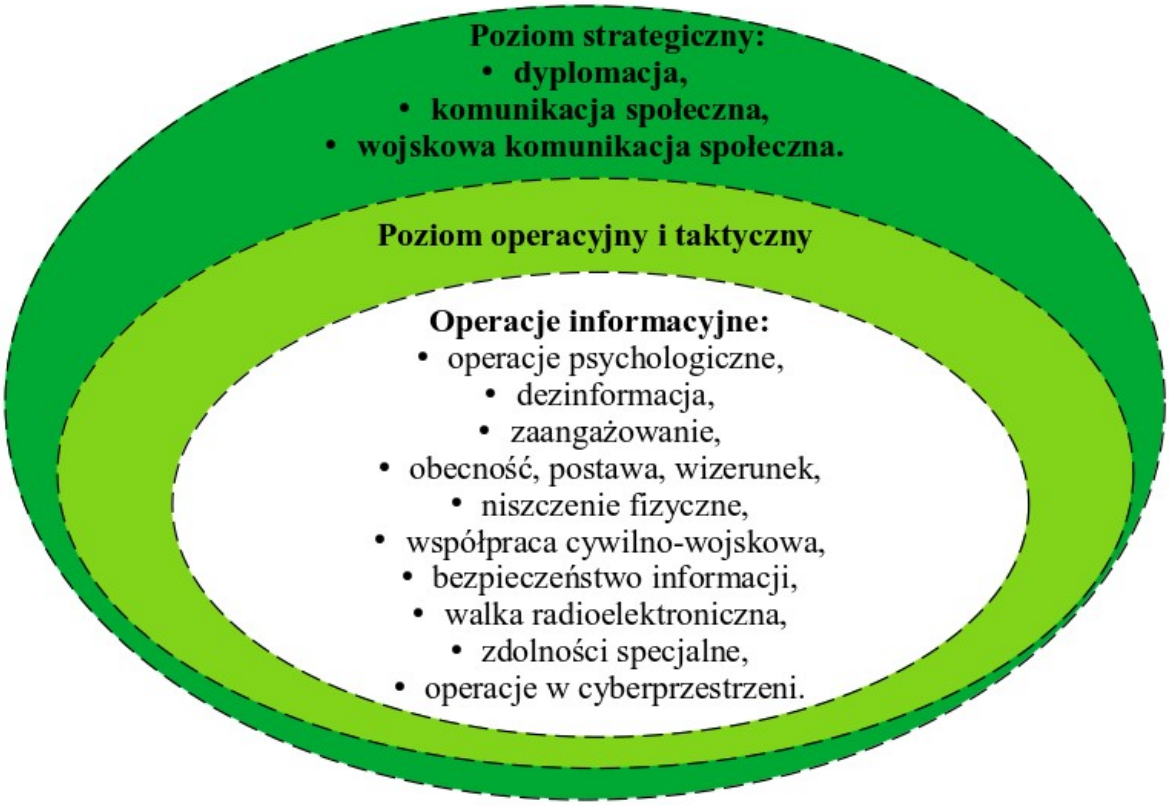
Czwarty podrozdział dotyczy porównania wzorca z drugiego podrozdziału do modelu dywersji ideologicznej KGB opisanej przez Bezmienowa. Model składa się z czterech faz – fazy demoralizacji, destabilizacji, kryzysu i normalizacji. Faza demoralizacji dotyczy wpływania na idee (religię, edukację, media i kulturę), strukturę (prawo i porządek, stosunki społeczne, bezpieczeństwo, politykę wewnętrzną i zewnętrzną) i życie (rodzinę i społeczeństwo, zdrowie, rasę, populację i pracę). Faza destabilizacji odnosi się do biurokratyzacji i centralizacji państwa, powszechnego niezadowolenia i oczekiwania przez ludzi charyzmatycznego przywódcy. Faza kryzysu polega na przejęciu władzy przez dywersanta przez wojnę domową lub zewnętrzną interwencję. Celem fazy normalizacji jest unormowanie stosunków społecznych w nowym systemie sterowania społecznego.

5.1. Operacje informacyjne

Według dokumentu doktrynalnego Wojska Polskiego DD 3.10 (A) (dotyczącego operacji informacyjnego) operacje informacyjne są częścią komunikacja strategicznej[206], która jest rozumiana jako „zamierzona koordynacja procesów komunikacyjnych realizowanych na wszystkich poziomach kierowania i dowodzenia, również w ramach operacji wspierających realizację celów resortu obrony narodowej na płaszczyźnie narodowej, sojuszniczej i koalicyjnej”[207].

Relacje między komunikacją strategiczną (na poziomie strategicznym, operacyjnym i taktycznym) a operacjami informacyjnymi przedstawia poniższy schemat:

206 v. *Operacje Informacyjne DD-3.10(A)*, MON CDiSSZ, Bydgoszcz 2017, p. 11, 36.
207 v. ibid., p. 11.



Rys. 36: Komunikacja strategiczna

źródło: opracowanie własne na podstawie: *Operacje Informacyjne...*, op. cit., p. 36.

Według dokumentu doktrynalnego operację informacyjną można ująć jako „przedsięwzięcia koordynowane przez komórkę sztabu polegające na analizowaniu środowiska informacyjnego, planowaniu, integrowaniu i ocenie działań informacyjnych w celu uzyskania oczekiwanych efektów oddziaływania na wolę działania, zrozumienie sytuacji i posiadane zdolności przeciwnika (potencjalnego przeciwnika) i inne zatwierdzone obiekty oddziaływania dla wsparcia osiągania zakładanych celów operacji, a także celów komunikacji strategicznej”[208]. Z kolei działania informacyjne zostały zdefiniowane jako „czynności mające wpływ na obiekty oddziaływania, informacje i systemy informacyjne przy zastosowaniu odpowiednich zdolności oraz narzędzi. Mogą być

208 v. ibid., p.15.

one realizowane przez któregokolwiek z uczestników działań z uwzględnieniem środków prewencyjnych ograniczających oddziaływanie na własne informacje i systemy informacyjne”[209].

Dokument wskazuje również na istotę operacji informacyjnych, jaką jest uzyskanie przewagi informacyjnej nad przeciwnikiem lub potencjalnym przeciwnikiem[210]. Przewaga informacyjna może zostać uzyskana przez oddziaływanie na wolę działania, zrozumienie sytuacji i zdolność prowadzenia operacji[211] zarówno przeciwnika, potencjalnego przeciwnika, sił własnych, sojuszniczych, jak i neutralnych[212]. Oddziaływanie docelowo dotyczy jednostek, ale można na nie wpływać poprzez działanie na zasoby. Zmiana woli działania, zrozumienia sytuacji i zdolności do działania jednostek zmienia również grupy, do których dana jednostka należy.

Powiązanie trzech przedmiotów oddziaływania w ramach operacji informacyjnych z podsystemami systemu autonomicznego pozwala również bezpośrednio odnieść zagadnienie InfoOpsu do opisanego w pracy procesu decyzyjnego. Homeostat (związany z wolą działania) pełni funkcję postulatora w systemie autonomicznym, korelator (związany ze zrozumieniem sytuacji wraz z receptorem) – optymalizatora, a akumulator (odpowiadający za zdolności do działania obok zasilacza i efektora) – realizatora. Odwołując się do procesu decyzyjnego według Akwinaty można dokonać następującego przyporządkowania aktów procesu decyzyjnego na wolę do działania, zrozumienie sytuacji i zdolności do działania:

- zrozumienie sytuacji (w ramach korelatora pełniącego rolę optymalizatora) związane jest z pomysłem (myśleniem o przedmiocie jako dobrym), zamysłem (propozycją dążenia do przedmiotu jako celu), namysłem (rozważaniem środków do osiągnięcia wyznaczonego celu), rozmysłem (przeanalizowaniem środków do osiągnięcia celu), rozkazem

209 v. ibid.
210 v. ibid., p. 16.
211 v. ibid., p. 17-18.
212 v. ibid., p. 15.

(postanowieniem czynu) i osądem (przeanalizowaniem procesu dążenia do celu),

- wola do działania (w ramach homeostatu pełniącego rolę postulatora) związana jest z upodobaniem (uznaniem pewnego przedmiotu za dobry), zamiarem (akceptacją przedmiotu jako celu), przyzwoleniem (odrzuceniem części środków), wyborem (wyborem jednego ze środków do osiągnięcia celu), wykonaniem czynnym (wykonaniem rozkazu przez wolę) i zadowoleniem (zadowoleniem z osiągniętego celu),
- zdolność do działania (w ramach akumulatora pełniącego rolę realizatora) związany jest z wykonaniem biernym rozkazu rozumu (optymalizatora), który został zaakceptowany przez wolę (postulatora).

Propozycja Doktora Anielskiego jest na tyle ogólna, iż jako przedmiot dążenia można uznać e.g. pojedynczy, fizyczny przedmiot, jak i cel operacyjny lub taktyczny. Środkami do celu mogą być konkretne scenariusze, warianty działania etc.

W ramach zdolności i technik informacyjnych, które są koordynowane i integrowane w ramach operacji informacyjnych wymienia się[213]:

- operacje psychologiczne (ang. psychological operation – PsyOps) – oddziaływanie w celu zmiany percepcji, postaw i zachowań,
- walka radioelektroniczna (ang. electronic warfare – EW) – działania wojskowe wykorzystujące energię elektromagnetyczną,
- współpraca cywilno-wojskowa (ang. civil-military cooperation – CIMIC) – nawiązywanie i utrzymywanie dobrych relacji między podmiotami wojskowymi, cywilnymi i ludnością lokalną,
- operacje w cyberprzestrzeni – wykorzystanie potencjału cyberprzestrzeni (rozumianej jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne”[214]) do wspierania operacji informacyjnych,
- obecność, postawa i wizerunek (ang. presence, posture and profile – PPP):

213 v. ibid., p. 23-33.
214 v. *Operacje w cyberprzestrzeni DD-3.20*, MON CDiSSZ, Bydgoszcz 2020, p. 9.

- obecność sił (wojsk),
- postawa – związana z zachowaniem wojsk,
- wizerunek – wizerunek sił własnych (w tym dowódców).

- dezinformacja – działania, które mają na celu wprowadzenie przeciwnika w błąd,
- bezpieczeństwo operacji (ang. operations security – OPSEC) – działania mające na celu ukrycie przed przeciwnikiem zamiarów i możliwości sił własnych,
- zdolności specjalne – dotyczą „określonych, często ściśle tajnych zdolności narodowych, które posiada dane państwo lub które zostały wydzielone do realizacji danej misji”[215],
- zaangażowanie:
  - zaangażowanie kluczowych przywódców (ang. key leader engagement – KLE) – analiza wpływu kluczowych przywódców (wojskowych i cywilnych) na środowisko informacyjne,
  - zaangażowanie na poziomie taktycznym (ang. soldier-level engagement – SLE) – analiza wpływu personelu militarnego na środowisko cywilne.
- niszczenie fizyczne – wykorzystanie oddziaływania kinetycznego (energomaterialnego) na środowisko informacyjne,
- wojskowa komunikacja społeczna (ang. military public affairs – MPA) – planowanie i realizacja współpracy z mediami, współpraca ze społeczeństwem i komunikacja wewnętrzna w celu promowania zadań i celów Sił Zbrojnych RP.

Powyższa lista nie jest zamknięta, a jedynymi ograniczeniami do wykorzystania innych metod i technik są uwarunkowania polityczne i normy prawne[216]. Odwołując się do podziałów systemów zaproponowanych w pracy możliwe jest podzielenie działań informacyjnych na te, które mają na celu oddziaływanie na same zasoby (operacje w cyberprzestrzeni, walka

215 v. *Operacje Informacyjne...*, op, cit., p. 30.
216 v. ibid. p. 23.

radioelektroniczna, niszczenie fizyczne), jak i na jednostki wraz z grupami (PsyOps, KLE, SLE, PPP, dezinformacja, CIMIC, niszczenie fizyczne, OPSEC, socjotechnika w ramach operacji w cyberprzestrzeni). Powyższe inicjatywy w różnym zakresie uwzględniają oddziaływanie na zasoby, jednostki i grupy zarówno w zależności od tego czy są to systemy własne, sojusznicze, neutralne lub należące do przeciwnika, jak i tego jak wysoko w hierarchii się znajdują lub czy są systemami wojskowymi albo cywilnymi. Szczególną uwagę należy zwrócić na niszczenie fizyczne, które z jednej strony może dotyczyć niszczenia jednostek i zasobów[217], ale również wywoływania efektu psychologicznego na jednostki i grupy przez użycie broni[218]. Jednak nie jest konieczne używanie posiadanych środków niszczących do wywołania efektu psychologicznego, gdyż zwiększenie morale sił własnych może nastąpić nawet przez sam fakt posiadania odpowiedniej broni[219], a co więcej może prowadzić do obniżenia morale u przeciwnika, które w odpowiednich warunkach może skutkować nawet jego poddaniem się[220].

5.2. Wzorzec bezpieczeństwa cyberprzestrzeni wobec operacji informacyjnych

Na podstawie powyższych rozważań możliwe jest opisanie wzorca bezpieczeństwa cyberprzestrzeni wobec operacji informacyjnych, który składa się z czterech zagadnień:

- bezpieczeństwa jednostek wobec operacji informacyjnych,
- bezpieczeństwa grup wobec operacji informacyjnych,
- bezpieczeństwa zasobów wobec operacji informacyjnych,
- bezpieczeństwa komunikatów wobec operacji informacyjnych.

Jak zaznaczono w pracy, centralnym zagadnieniem, które jest punktem odniesienia do wszystkich innych, jest bezpieczeństwo jednostki (osoby), które zostanie opisane na początku.

217 v. ibid., p. 32-33.
218 v. ibid. p. 20, 32.
219 v. L. Murray, *Psychologia wojny. Strach i odwaga na polu bitwy*, Wydawnictwo RM, Warszawa 2014, p. 144-147.
220 v. ibid., p. 160-161.

Jednostkę można uznać za bezpieczną o ile prowadzi dobre życie, czyli żyje życiem cnotliwym i posiada odpowiednią ilość dóbr materialnych, które zapewniają dobrobyt. Co więcej w grupie (nadsystemie), do którego należy jednostka musi panować pokój. Deficyty w ramach cnotliwego życia, dobrobytu i pokoju prowadzą do stanu obiektywnego braku bezpieczeństwa. Odwołując się do dóbr osoby wyróżnionych przez Gogacza można powyższe kryteria bezpieczeństwa uszczegółowić jednocześnie umiejscawiając je w teorii systemów autonomicznych Mazura. Podstawą działania jednostki jest fakt, że istnieje i żyje, a zatem należy zabiegać, aby system autonomiczny (a więc wszystkie jego podsystemy) jakim jest jednostka trwał w czasie i był gotowy do działania, a więc był zdrowy. Cnotliwe życie może zostać uzyskane przez dobre działanie, co związane jest z działaniem homeostatu (wola i uczucia pożądliwe i gniewliwe) i korelatora (intelekt, wyobraźnia, pamięć). W odniesieniu do jednostki dobrze działający homeostat, to taki, na który składa się wola usprawniona w cnoty męstwa, umiarkowania, sprawiedliwości i roztropności oraz uczucia (związane z władzą gniewliwą i pożądliwą), które działają zgodnie z rozumem (podnosząc potencjał fizykalny homeostatu dla czynów dobrych moralnie, a obniżając dla złych moralnie). Z kolei dobrze działający korelator, to taki, którego rejestraty zmysłowe (związane z pamięcią i wyobraźnią) i rejestraty intelektualne (związane z intelektem czynnym i biernym) prowadzą do dobrego moralnie działania (czyli pozwalają przekraczać potencjał efektorowy, w taki sposób, iż wyzwalana jest reakcja, którą można ocenić jako dobrą moralnie).

Posiadanie odpowiednich wytworów pozwala zaspakajać potrzeby związane z zasilaniem systemu (w ramach zasilacza, akumulatora i efektora). Moc całkowita systemu musi wystarczyć przynajmniej na zaspokojenie mocy jałowej i mocy roboczej systemu. Z drugiej strony brak mocy swobodnej (czyli moc całkowita idealnie pokrywa tylko i jedynie moc jałową i roboczą) jest stanem niepożądanym, gdyż jest równoznaczny z niewolnictwem (współczynnik swobody $s=0$), ale też moc robocza, nie może wynosić zero, gdyż taki stan nie daje motywacji do

rozwoju. Optymalną wartością współczynnika swobody jest wartość znajdująca się pomiędzy 0, a 1, ale nie będąca zbliżona do tych wartości.

Odnosząc się do nadsystemu jakim jest grupa, to dobra osób można zidentyfikować jako relacje między jednostkami (podsystemami grupy) w postaci relacji osobowych wiary, nadziei i miłości, jak i odpowiedni zestaw norm społecznych (kultura), który opiera się na prawdziwej wiedzy (normy poznawcze), która prowadzi do mądrości, a która z kolei wskazuje na dobry cel życia (normy ideologiczne) i środki do jego osiągnięcia za pomocą cnoty roztropności (normy etyczne). Zatem bezpieczna jednostka, to jednostka, która jako system spełnia następujące kryteria:

- istnieje – system jest w stanie innym, niż $<0,0,0>$ (istnieje i żyje),
- posiada wszystkie podsystemy w stanie gotowości ($<1,1,0>$) lub aktywności ($<1,1,1>$) (jest zdrowa),
- posiada odpowiednie rejestraty w ramach zmysłowego środowiska korelacyjnego (wyobraźnia i pamięć ukształtowana tak, aby łatwiej wypełniać dobre moralnie czyny),
- posiada odpowiednie rejestraty w ramach intelektualnego środowiska korelacyjnego (intelekt usprawniony w wiedzy i mądrości),
- posiada odpowiedni potencjał fizykalny dla danych bodźców (uczucia władz gniewliwych i pożądliwych wywołują potencjał fizykalny wzmacniający potencjał decyzyjny dla decyzji podejmowanych władzą rozumu),
- posiada odpowiedni potencjał swobodny (wolną wolę usprawnioną w cnoty),
- posiada moc swobodną (wolne zasilanie do działania),
- ma możliwość przetwarzania informacji zgodnie z właściwościami swojego korelatora (inteligencją, pojętnością i talentem),
- ma możliwość przetwarzania energomaterii zgodnie z właściwościami swojego akumulatora (dynamizmem charakteru, tolerancją i podatnością),
- posiada możliwość korzystania z zasobów rozszerzających możliwości jej podsystemów (wytworów ludzkich),

- w strukturze nadsystemu, do którego należy dominuje jeden układ norm społecznych (dominacja jednego układu norm społecznych zapewnia pokój),
- w strukturze nadsystemu, do którego należy dominują normy informacyjne, które nie są w sprzeczności z normami energomaterialnymi (taki układ norm zapewnia wychowanie jednostek w Dobru i Prawdzie, o ile normy ideologiczne i etyczne są zgodne z normami poznawczymi, przy jednoczesnym zabieganiu o dobrobyt, zdrowie, reprodukcję i poszanowanie prawa i hierarchii),
- w strukturze nadsystemu, do którego należy, jednostki są powiązane wieloma wiążącymi je ze sobą relacjami (relacje osobowe wiary, nadziei i miłości zapewniają trwałość struktury przez wiązanie elementów systemu ze sobą niezależnie od relacji myślnych takich jak podległość etc.),
- wejścia i wyjścia zarówno jednostki, jak i nadsystemu, do którego należy, muszą w niezakłócony sposób (zapewnienie dostępności, poufności i integralności informacji) dawać dostęp do informacji użytecznych sterowniczo, jak i umożliwiać oddziaływanie takimi informacjami na otoczenie.

W ramach bezpieczeństwa jednostki zawarte są również elementy związane z bezpieczeństwem zasobów, jak i grup, od których zależy bezpieczeństwo jednostek. Brak bezpieczeństwa zasobów, czyli ich brak (nieistnienie) lub niedziałanie (brak stanu gotowości lub żywotności – w wyniku e.g. uszkodzenia) może wpłynąć negatywnie na bezpieczeństwo jednostki, gdyż może wpłynąć na jej zdrowie (uszkodzenie rozrusznika serca), uniemożliwić kształtowania odpowiednich wyobrażeń i uczuć (e.g. brak dostępu do sztuki wywołującej rejestraty ułatwiające dobre moralnie czyny), uniemożliwić zgłębianie wiedzy i mądrości (e.g. brak dostępu do wartościowych książek), zmniejszyć moc systemu (e.g. brak narzędzi do pracy zarobkowej) i uniemożliwić przebywanie z innymi osobami (e.g. brak możliwości komunikacji w celu umówienia spotkania,

brak środków transportu). Bezpieczeństwo grup jest ściśle związane z dominującym układem norm informacyjnych (takich, że normy ideologiczne i etyczne są zgodne z normami poznawczymi) w społeczeństwie i trwałością relacji między jednostkami. Oczywiście istnieją grupy, które są trwałe ze względu na przykład na przymus energomaterialny ze strony podsystemu kierowniczego, ale nie cechują się dominacją norm informacyjnych, ale na podstawie powyższych rozważań nie można ich uznać za bezpieczne, gdyż jednostkom w tej grupie systemowo brakuje bezpieczeństwa (chociażby ze względu na brak kultury kształtującej ku Dobru i Prawdzie lub jej marginalny charakter w danej społeczności).

Na bezpieczeństwo jednostki wpływa również stan jej wejścia i wyjścia. Informacje docierające do receptorów systemu mogą wpływać na bezpieczeństwo jednostki na kilka sposobów. Z jednej strony mogą być to informacje nieużyteczne sterowniczo z punktu widzenia czynów dobrych moralnie. W ramach operacji informacyjnych przeciwnik będzie dążył, aby kanały informacyjne, w których przesyłane są informacje nieużyteczne sterowniczo były w ciągłym stanie aktywności lub gotowości, a więc jeśli są uszkodzone, to w interesie przeciwnika jest, aby zostały naprawione. Warto zauważyć, że przeciwnik nie musi być odpowiedzialny za tworzenie treści w ramach tych kanałów, ale wystarczy, że nie będzie w nie ingerował. Jeśli kanał informacyjny przesyła informacje użyteczne sterowniczo, to w interesie przeciwnika jest je uszkodzić, aby nie były ani w stanie aktywności, ani nawet w stanie gotowości, a najlepiej jakby zostały nieodwracalnie uszkodzone za pomocą oddziaływania informacyjnego lub energomaterialnego.

W ramach kanału komunikacyjnego prowadzącego do receptorów jednostki możliwe jest podsłuchiwanie w ramach wyróżnionego już w pracy odbiornika ulotu, ale również wprowadzanie informacji w ramach źródła zakłóceń. Przeciwnik może podsłuchiwać informacje z kanału informacyjnego, aby móc dostosować linię retoryczną do swojej propagandy. W ramach źródła zakłóceń możliwe jest atakowanie ilościowe i jakościowe. Z punktu widzenia ataku ilościowego przeciwnik może wprowadzić tyle komunikatów, iż korelator jednostki nie jest

w stanie ich zmagazynować i przetworzyć, gdyż wykracza to poza jego inteligencję. Z drugiej strony informacje mogą być niemożliwe do przetworzeniu, gdyż jest ich zbyt wiele w danej jednostce czasu, a co jest związane z przekroczeniem pojętności korelatora jednostki. Kolejnym aspektem ataku może być przesyłanie jednostce informacji, które nie są dla niej interesujące, czyli są niezgodne z talentem jej korelatora. Z punktu widzenia jakościowego informacje, które są źródłem zakłóceń mogą być nieużyteczne sterowniczo, a więc zaznajamianie się z nimi przez jednostkę jest stratą czasu i energii (a więc mocy swobodnej), a może wręcz wytworzyć rejestraty w korelatorze, które w przyszłości doprowadzą do złego moralnie działania.

Efektem działań na wejście korelatora jest brak odpowiednich informacji użytecznych sterowniczo (które można nazwać również informacjami niskiej jakości – o niskiej integralności), które mogą zaburzyć proces decyzyjny jednostki. Nieodpowiednie rejestraty w korelatorze wiążą się z błędnym zrozumieniem sytuacji, przez który powstają emocje (w znaczeniu psychocybernetyki Mazura), które wywołują wolę do działania w przypadku reakcji złych, a osłabiają wolę do działania w przypadku reakcji dobrych. Również siły i środki w ramach zdolności do działania mogą być nieodpowiednio używane, czyli może być ich użytych zbyt mało, za dużo lub zostaną wykorzystane do złej reakcji. Proces podejmowania decyzji w przypadku grup jest analogiczny, ale dotyczy większej skali, a więc z punktu widzenia cybernetyki jest to tylko i jedynie różnica ilościowa. Efekt braku odpowiednich informacji użytecznych sterowniczo w korelatorze może być krótkotrwały, a więc zostać wywołany doraźnie, tak jak e.g. wystąpienia ludności przeciwko władzy, albo długotrwały, który stopniowo zmniejsza motywacje jednostki lub normy społeczne z informacyjnych do energomaterialnych lub programuje jednostki i grupy w normach ideologicznych i etycznych niezgodnych z normami poznawczymi, a co doprowadzi do większej podatności na oddziaływania psychologiczne (w ramach operacji informacyjnych) i przymus fizyczny.

Efekt krótkotrwały można uzyskać e.g. przez wprowadzenie do korelatora jednostki informacji dotyczących pewnego zagrożenia, który wywoła uczucie strachu (związanego z zagrożeniem dóbr jednostki, takich jak zdrowie, życie, mienie) i potrzebę zabezpieczenia się za wszelką cenę, nawet pomimo pomijalnie małego prawdopodobieństwa wystąpienia zdarzenia (czyli wystąpi efekt możliwości) co może wprowadzić jednostkę do stanu obsesji (postrzegania bezpiecznej obiektywnie rzeczywistości jako zagrażającej, niebezpiecznej). Powyższy efekt może zostać zniwelowany przez przyłożenie do korelatora potencjału homeostatycznego (dodatkowo zwiększonego potencjałem swobodnym dzięki cnotom – szczególnie cnocie męstwa), który może nie dopuścić do wyzwolenia nieracjonalnej reakcji. Dodatkowo efekt takiego ataku może złagodzić cnota inteligencji (dotycząca adekwatnego rozpoznania rzeczywistości), jak i cnota pouczalności (przyjmowania rad), ale tylko o ile jednostka ma dostęp do rad osób kompetentnych w danej dziedzinie. Alternatywnym przykładem ataku krótkotrwałego jest zapewnianie jednostkom, iż ma do czynienia ze stanem bezpieczeństwa, pomimo tego, iż obiektywnie rzeczywistość jest zagrażająca. Wprowadza to jednostkę w stan fałszywego bezpieczeństwa, który może być użyteczny dla przeciwnika w celu zaskoczenia jednostki swoimi przyszłymi działaniami. Również i ten rodzaj ataku może zostać złagodzony przez cnoty – szczególnie cnotę inteligencji i pouczalności. Odpowiednio przygotowane przez przeciwnika społeczeństwo pod kątem rejestratów jego jednostek będzie z jednej strony bardziej podatne na krótkotrwałe oddziaływania, a z drugiej, bardziej oddalone od prawdziwej wiedzy, mniej uzdolnione w cnotach i z niewykształconą odpowiednio pamięcią i wyobraźnią.

Poza wprowadzaniem niepożądanych rejestratów do korelatora jednostek i całych społeczeństw efektem oddziaływań przeciwnika na wejście może być rozbijanie relacji między jednostkami w ramach danej grupy. Tworzenie i programowanie w społeczeństwie stereotypów może osłabić zaufanie (osłabienie relacji wiary) i sympatię (osłabienie relacji miłości) jednostki do pozostałych jednostek, a wręcz doprowadzić do sytuacji, gdy jednostka takich relacji nie szuka

(osłabienie relacji nadziei). Szczególnym przypadkiem uderzenia w relacje międzyjednostkowe jest zaburzenie relacji między podsystemem kierowniczym i podsystemem wykonawczym grupy, które to działanie może doprowadzić do dezintegracji dobrego działania całej grupy. Próby takich ataków mogą zostać złagodzone, jeżeli jednostka cechuje się cnotami związanymi z cnotą sprawiedliwości, czyli cnotami życzliwości (dotyczących osób niżej w hierarchii), poważania (wobec osób wyżej w hierarchii), posłuszeństwa (dotycząca posłuchu wobec przełożonych w ramach dziedziny ich autorytetu), uprzejmości (traktowanie każdego człowieka po przyjacielsku), cnotą pietas (szacunek do przodków, rodziców i Ojczyzny) i religijności (szacunek do Boga). Zaburzenie działania grupy możliwe jest również w przypadku podsłuchania informacji przeznaczonych tylko i jedynie dla ograniczonej liczby jednostek piastujących odpowiednie stanowiska. Naruszenie poufności informacji może być szansą dla przeciwnika na przygotowanie lepszego działania uderzającego w grupę, z której niejawne informacje udało się pozyskać.

Obniżenie bezpieczeństwa jednostki przez oddziaływanie na wejście systemu może się również odbyć pośrednio przez oddziaływanie na zasoby, których jednostka używa. Przeprowadzenie odpowiedniego ataku cybernetycznego (zgodnie z modelem intrusion kill chain) w przypadku komputerów i innych urządzeń przyłączonych do sieci może uniemożliwić wykorzystanie tych zasobów, a więc zmniejszyć bezpieczeństwo jednostki przez sam brak tych zasobów lub przez użycie ich w celu wyłączenia lub uszkodzenia kolejnych zasobów i zmniejszenia mocy swobodnej jednostki (e.g. przez kradzież pieniędzy z konta bankowego). Uniemożliwienie wykorzystania zasobu może również się odbyć przez operacje informacyjne związane z walką radioelektroniczną lub ich niszczeniem fizycznym. Brak zasobów związanych z receptorami może ograniczyć dostępność użytecznych sterowniczo informacji, a więc uniemożliwić dobre działanie przez brak odpowiedniego zrozumienia sytuacji.

W przypadku efektorów jednostki również może dochodzić do zjawiska podsłuchiwania (w ramach odbiornika ulotu, który może być w pewnej mierze

kontrolowany przez przeciwnika), jak i dodawania komunikatów z źródła zakłóceń. Ewentualne sukcesy w podsłuchiwaniu mogą być wykorzystane w procesie planowania przyszłych ataków (przez profilowanie przyszłej ofiary). Podsłuchiwanie wejścia lub wyjścia systemu może zostać zmniejszone lub zupełnie zniwelowane przez wykorzystanie środków technicznych jakimi są szyfrowanie i steganografia. Z kolei dodawanie dodatkowych komunikatów może zmniejszyć efektywność wpływania na otoczenie przez system, a wręcz doprowadzić do negatywnych skutków jak e.g. utrata zaufania drugiego systemu, co jest związane z osłabianiem relacji osobowych (przykładem takiego ataku może być opracowanie deep fake'a zawierającego sfabrykowaną przemowę przywódcy danej grupy, która stawia w niekorzystnym świetle całą wspólnotę). Zmiana informacji na wejściu lub wyjściu może zostać wykryta przez zastosowanie środków technicznych takich jak szyfrowanie lub wykorzystywanie algorytmów sprawdzających integralność danych (e.g. funkcje skrótu).

Kontrolowanie wejścia i wyjścia jednostki i grupy, do której należy, przez przeciwnika daje możliwość kontrolowania tej jednostki lub grupy. Jest to szczególny przypadek, w którym przeciwnik może jednocześnie podsłuchiwać i wpływać na kanały komunikacyjne na wejściu i wyjściu systemu jakim jest jednostka i grupa. Kontrolowany system nie może efektywnie oddziaływać na otoczenie, gdyż jego reakcje wyzwalające informacje są znane i modyfikowane przez przeciwnika. Należy jednak zaznaczyć, że jednostki posiadają potencjał swobodny (wolną wolę) i pomimo kontroli mogą działać wbrew napływającym bodźcom. Podobnie informacje, które docierają do kontrolowanego systemu są modyfikowane i znane przeciwnikowi. Taką sytuację można zauważyć e.g. w sektach i państwach totalitarnych, gdzie dostęp do informacji i sposób ich wyrażania do otoczenia jest ściśle ograniczany i filtrowany w ramach norm społecznych dominujących w systemie atakującym, które są inne, niż normy informacyjne zgodne z normami poznawczymi. Można zauważyć, że może wystąpić scenariusz, kiedy system (jednostka lub grupa) ma w pełni kontrolowane wejścia i wyjścia, ale informacje wchodzące i wychodzące z systemu są

modyfikowane i cenzurowane (niekoniecznie w sposób pełny) przez inny system według norm informacyjnych zgodnych z normami poznawczymi, co wydaje się sytuacją pożądaną w niektórych przypadkach. Przykładami takich sytuacji mogą być e.g. zakonnicy z zakonów kontemplacyjnych (za modyfikację wejścia i wyjścia odpowiadają ich przełożeni), wychowywane dzieci (za kontrolowanie wejść i wyjść odpowiadają rodzice lub inni prawni opiekunowie) lub więźniowie w zakładach karnych (podobnie jak w przypadku zakonów – za modyfikacje informacji na wejściu i wyjściu odpowiadają przełożeni). Ze względu na dostęp do informacji zgodnych z normami informacyjnymi zgodnymi z normami poznawczymi te systemy można zaklasyfikować jako bezpieczniejsze od systemów kontrolowanych przez przeciwnika, które ograniczają dostęp do takich informacyjnych.

Operacje informacyjne przeprowadzane przez własne siły mogą wzmacniać poziom bezpieczeństwa jednostek, a więc i zasobów i grup, na kilka sposób. Z jednej strony, w przypadku krótkotrwałej próby wpływu, nie wystarczy zapewnić obiektywnego bezpieczeństwa danej jednostce, ale operacje psychologiczne muszą doprowadzić do tego, aby jednostka dodatkowo była przekonana o tym, że jest bezpieczna wraz ze swoim otoczeniem. Zatem należy zabiegać, aby jednostka nie była w stanie obsesji, ale w stanie bezpieczeństwa. Wspomóc mogą to operacje psychologiczne, obecność, postawa i wizerunek wojsk własnych, jak i zaangażowanie kluczowych przywódców (e.g. lokalnej grupy, którzy mogą uspokajać swoich podopiecznych), zaangażowanie na poziomie taktycznym (wpływ personelu wojskowego na daną grupę), wojskowa komunikacja społeczna, jak i CIMIC. Dodatkowo w momentach intensywnych operacji informacyjnych przeciwnika, gdy zadaniem trudnym jest rozróżnienie prawdy od fałszu mogą być pomocne kanały oparte na zaufaniu, czyli, wyżej wymieni, lokalni przywódcy, zaufane osoby, które mogą być dodatkowo informowane wiarygodnymi kanałami (e.g. szyfrowanymi środkami komunikacji zapewniających możliwość potwierdzenia źródła informacji, pocztą lub bezpośrednimi spotkaniami z innymi jednostkami) przez wyższe władze lub służby publiczne.

Przed długotrwałym wpływem propagandy przeciwnika może uchronić dbanie o bezpieczeństwo jednostki, a szczególnie dostarczanie jej zgodnej z rzeczywistością wiedzy, promowania w społeczeństwie norm informacyjnych zgodnych z normami poznawczymi i zapewnianie możliwości zdobywania przez jednostkę mocy swobodnej, aby mogła wolną moc wykorzystać do pogłębiania motywacji informacyjnych zgodnych z motywacjami poznawczymi. System dynamiczno-informacyjny z przewagą motywacji ideologiczno-etycznych jest podatny na obniżanie norm etycznych, indyferentyzm ideologiczny i próby programowania społeczeństwa w innych normach ideologicznych, które niekoniecznie są zgodne z normami poznawczymi, natomiast jest odporny na kryzysy militarne, katastrofy naturalne, ekonomiczne i wymuszenia prawne, gdyż wydarzenia te związane są z tymi motywacjami i normami (witalnymi, ekonomicznymi i prawnymi), które nie są dominujące w danej grupie.

Na podstawie powyższego wzorca można również przewidywać trendy zmian bezpieczeństwa jednostek i grup na podstawie zachowań jednostek w danej grupie. Tendencja zmniejszania się bezpieczeństwa jednostki jest możliwa do zaobserwowania w przypadku, gdy jednostka:

- jest coraz rzadziej w stanie aktywności (co może świadczyć o pewnym zastoju i być może pewnych problemów natury psychicznej lub fizycznej),
- coraz częściej poszukuje bodźców nieodpowiednio kształtujących wyobraźnię i pamięć,
- coraz częściej poszukuje wiedzy niezgodnej z normami poznawczymi,
- stawia wyżej bodźce energomaterialne (związane z normami witalnymi, energetycznymi i prawnymi) nad informacyjne (związane z normami ideologicznymi, etycznymi i poznawczymi),
- izoluje się od innych jednostek (zmniejszanie ilości i pogorszenie jakości relacji osobowych jednostki wobec innych jednostek),
- jej współczynnik swobody dąży do 0 (jednostka nie posiada mocy swobodnej) lub osiągnął wartość 1 lub wartość zbliżoną do 1 (jednostka jest w stanie się utrzymać, ale nie pracuje, co powoduje zastój i brak rozwoju),

Użyte powyżej terminy takie jak coraz częściej, stawia wyżej, współczynnik dąży do są terminami nieostrymi, dlatego w celu zobiektywizowania ocen należy użyć e.g. testów statystycznych na wynikach odpowiednio przygotowanych narzędzi, aby wykazać czy zmiany są istotne statystycznie. Implikuje to potrzebę wytworzenia narzędzi pomiarowych dla wyżej wymienionych współczynników. W przypadku bezpieczeństwa grup należy rozważyć dodatkowo (obok coraz rzadszej aktywności, kultury oferującej bodźce niezgodne z normami informacyjnymi zgodnymi z normami poznawczymi, zaniku relacji osobowych jednostek danej grupy (szczególnie należących do podsystemu kierowniczego) do jednostek spoza grupy lub jednostek grupy własnej, współczynnika swobody zbliżonego do 0 albo 1) wymienić pojawianie się paru grup o różnym wobec siebie układzie norm, co prowadzi do podziałów i dezintegracji społeczeństwa.

5.3. Porównanie wzorca bezpieczeństwa cyberprzestrzeni wobec operacji informacyjnych do metody pokojowej i wojennej

Rozróżnienie związanych z bezpieczeństwem metod na metody pokojowe, wojenne, nie-pokojowe i nie-wojenne ma swoje źródło z jednej strony w myśli Empedoklesa, który uważał, że podstawową zasadą istnienia rzeczywistości jest miłość, która łączy elementy (żywioły), jak i nienawiść, która je rozdziela. Świniarski podobne elementy odnajduje w myśli psychoanalitycznej Freuda, który postulował, że człowiek jest popychany do działania przez dwie siły – Thanatos, związany z niszczeniem i Eros, który odpowiada za życie, jak i w podziale czynów przez Kotarbińskiego na czyny zmieniające jakiś stan rzeczy (permutacyjne), do których zaliczył działania destrukcyjne i konstrukcyjne, jak i czynów dążących do braku zmiany w rzeczywistości, na które składają się działania konserwatywne (zapewnienie, że dany byt nie utraci pewnej cechy) i działania profilaktyczne (zapewniające, że dany byt nie uzyska pewnej cechy). Na podstawie powyższego wyprowadzono metody pokojowe, które są konstrukcyjno-profilaktyczne i metody wojenne, które są destrukcyjno-konserwacyjne. Z kolei połączenie destrukcyjno-

profilaktyczne zostało nazwane metodą nie-wojenną, a konstrukcyjno-konserwacyjne – metodą nie-pokojową[221].

Z drugiej strony Kotarbiński twierdzi, że zarówno czyny konstrukcyjne i destrukcyjne, jak i profilaktyczne i konserwacyjne mogą być używane zamiennie. Obrazuje to zagadnienie przez podanie przykładu wybicia szyby, która może, z jednej strony, uzyskać cechę dziurowatości, a więc czyn wybicia szyby będzie czynem konstrukcyjnym, a z drugiej, utracić cechę całości, co zakwalifikuje wybicie szyby jako czyn destrukcyjny[222]. Zatem każdy czyn może być określany jako należący do metody wojennej, pokojowej, nie-wojennej lub nie-pokojowej. Z drugiej strony podział wojen i pokojów Świniarskiego i Chojnackiego na etyczne i nieetyczne zakotwicza cel czynów prostych w ramach obiektywnych, gdyż konstrukcję, dekonstrukcję, konserwację i profilaktykę odnosi do dobra i zła moralnego. Według tego podziału[223]:

- pokojem etycznym jest pokój, który konstruuje dobro i zachowuje zło (nie pozwalając mu wzrastać),
- pokojem nieetycznym jest pokój, który konstruuje zło i zachowuje dobro (nie pozwalając mu wzrastać),
- wojna etyczna jest wojną, w której konserwuje się dobro (nie pozwalając, aby się zmniejszyło) i dekonstruuje zło,
- wojna nieetyczna jest wojną, w której konserwuje się zło (nie pozwalając, aby się zmniejszyło) i dekonstruuje dobro,

Jednak z punktu widzenia (neo)tomizmu nawet ten podział nie rozwiązuje powyższej aporii, gdyż Doktor Anielski twierdził (za św. Augustynem), że zło jest brakiem dobra[224], a więc dekonstrukcja zła jest konstrukcją dobra i vice versa.

---

221 cf. J. Świniarski, K. Kawalerski, *Drogi i bezdroża securitologii*, Wojskowa Akademia Techniczna, Warszawa 2019, p. 39-41.
222 v. T. Kotarbiński, *Traktat o dobrej robocie*, Zakład Narodowy Imienia Ossolińskich, Wrocław 1958, p. 40.
223 v. J. Świniarski, W. Chojnacki, *Etyka bezpieczeństwa*, Akademia Obrony Narodowej, Warszawa 2004, p. 145.
224 Tomasz z Akwinu, *Przekład: Tomasz z Akwinu – Czy zło jest czymś? (Kwestie dyskutowane o złu, q. 1, a. 1)*, in: *Edukacja Filozoficzna*, (2001), q. 1, a. 1, r.

Analogicznie wygląda sytuacja czynów konserwacyjnych i czynów profilaktycznych. Zabieganie o niezwiększanie się zła (czyn profilaktyczny) prowadzi jednocześnie do niezmniejszania się dobra (czyn konserwacyjny). Można zauważyć na poziomie samych fundamentów, że teoria metod pokojowych i wojennych znacząco różni się od podejścia (neo)tomistycznego, a więc i samego wzorca teoretycznego zaproponowanego w pracy.

Odchodząc od ogólnych rozważać można odwołać się do konkretnych przykładów użycia metody pokojowej i metody wojennej, które zostały wymienione przez jej autora. Metoda pokojowa wiąże się ze stabilnym życiem i unikaniem zabijania, natomiast metoda wojenna z zadawaniem śmierci i prowadzeniem walki zbrojnej[225]. W ujęciu teorii metod pokojowych i wojennych bezpieczeństwo określa się jako cnotę, która polega na zachowaniu umiaru między wykorzystywaniem metody pokojowej, jak i metody wojennej[226]. Również w tej kwestii można napotkać różnice, gdyż optymalnym stanem dla człowieka jest pokój (zgoda w kwestiach istotnych), dobre życie (zgodnie z normami etycznymi i normami ideologicznymi zgodnymi z normami poznawczymi), jak i dobrobyt. Z drugiej strony w ramach cnoty sprawiedliwości Akwinata wyróżnia cnotę pietas, która polega na oddawaniu Ojczyźnie tego co jej się słusznie należy, do czego zalicza się również służbę wojskową i wykorzystywanie przemocy w jej obronie. Wydaje się zatem, że dla św. Tomasza z Akwinu złoty środek w wykorzystywaniu powyższych metod jest znacząco bliżej metod pokojowych, aczkolwiek przy uwzględnieniu możliwości wykorzystania metod wojennych.

Z punktu widzenia operacji informacyjnych akcent na metody pokojowe przesuwa się jeszcze bardziej, gdyż jednostka o wysokich motywacjach etycznych i ideologicznych (w ramach ideologii zgodnej z normami poznawczymi), która ma liczne rejestraty, które ułatwiają jej dobre etycznie czyny jest bardziej odporna na manipulacje[227]. Zatem samo uznanie, że dana jednostka jest bezpieczna (według kryteriów wymienionych w ramach wzorca teoretycznego opracowanego

225 v. J. Świniarski, W. Chojnacki, *Etyka…*, op. cit., p. 114-115.
226 v. ibid., p, 142.
227 v. A. Andrzejuk, *Tomasz…,* op. cit., p. 97.

w ramach tej pracy) sprawia, że jest bardziej odporna na negatywne skutki operacji informacyjnych przeciwnika. Z drugiej strony taki profil jednostki sprawia, że jest ona szczęśliwa. Zatem operacje informacyjne dążące do zwiększenia bezpieczeństwa jednostki z punktu widzenia operacji informacyjnych jednocześnie zapewniają, że efekt będzie trwały.

5.4. Porównanie wzorca bezpieczeństwa cyberprzestrzeni wobec operacji informacyjnych do modelu dywersji ideologicznej

Bezmienow (pod nazwiskiem Schuman) opisał model dywersji ideologicznej, którą stosowało KGB, dla którego pracował przed ucieczką do Kanady ze Związku Socjalistycznych Republik Radzieckich. Celem dywersji ideologicznej miał być „ostateczny bój o zwycięstwo komunizmu”[228]. Sam proces dywersji obliczony jest na długi czas, aby zamaskować powolne zmiany. Co więcej nie istnieje potrzeba inicjowania przez prowodyrów dywersji wszystkich destrukcyjnych procesów społecznych, gdyż część z aktualnie dziejących się przemian na poziomie społeczeństwa może być odpowiednio wykorzystana, skanalizowana i wzmocniona, aby zwiększyć ich negatywny charakter. Możliwe jest również wykorzystywanie pewnych tendencji do zapoczątkowania procesów związanych z dywersją[229]. Proces dywersji ideologicznej dzieli się na cztery fazy[230]:

1 Demoralizacji.
2 Destabilizacji.
3 Kryzysu.
4 Normalizacji.

Pierwszy etap – demoralizacji, trwa od około 15 do 20 lat. Celem jest wychowanie jednego pokolenia, które zostanie pozbawione zasad moralnych i aktualnej ideologii narodowej, która obowiązuje w danej społeczności. Brak

228 v. T. Schuman, *Agentura wpływu. Tajniki działalności wywrotowej KGB*, Wydawnictwo AA, Kraków 2020, p. 17-31.
229 v. ibid., p. 50-52.
230 v. ibid., p. 50.

wiodącej ideologii ułatwia proces demoralizacji. Tak wykształcone pokolenie z czasem staje się decydentami przez obejmowanie funkcji państwowych, pracowanie w mediach, służbach mundurowych, czy przez prowadzenie firmy. Przyjmuje się, że w większości przypadków demoralizacja, przynajmniej na przestrzeni jednego pokolenia, jest nieodwracalna[231]. Według Bezmienowa demoralizacja dzieli się na trzy poziomy: poziom idei, struktur i życia[232].

Pierwszy z nich, poziom idei dotyczy szczególnie religii, edukacji, mediów i kultury. Jednym z elementów działalności jest zastąpienie wartości związanych z dziedzictwem judeochrześcijańskim marksizmem-leninizmem. Osłabianie religii przeprowadza się głównie przez jej upolitycznienie, skomercjalizowanie i nastawienie na rozrywkę. Upolitycznienie religii polega na wykorzystaniu autorytetu danej religii do upowszechniania niemoralnych zasad i idei przez wspólnotę państwową. Komercjalizacja prowadzi do konkurencji między różnymi grupami religijnymi, której miernikiem są wpływy pieniężne dla wspólnoty. Uzależnia to daną denominację od charyzmatycznych liderów, którzy zapewniają największe zyski (przy niekoniecznie najwyższych standardach moralnych), a dodatkowo odciąga wiernego od osobistego, fizycznego kultu. Dywersant może wykorzystać taką sytuację przez porównywanie w mediach religii jako kolejnego elementu wyzysku. Nastawienie na rozrywkę otwiera dywersantowi możliwość wykorzystania braku krytycyzmu w wyborze e.g. zespołów muzycznych podczas wydarzenia religijnego przez religijnych przedstawicieli danej wspólnoty religijnej. Przykładem może być promowanie przez muzyków idei sprawiedliwości społecznej lub innych aspektów związanych z marksizmem. Innymi metodami uderzającymi w religię jest promowanie i tworzenie innych wyznań i sekt, szerzenie relatywizmu moralnego, usuwanie religii z życia publicznego (e.g. ze szkół) lub promowanie kultu jednostki w ramach danej wspólnoty religijnej stawiając jej lidera w miejsce Boga. Wynikiem walki z religią jest powolny upadek danej cywilizacji, które Bezmienow nazwał, za Szafariewiczem, pragnieniem

231 v. ibid., p. 55-62.
232 v. ibid., p. 63.

śmierci[233]. Przykładem upolitycznienia religii jest aktualna sytuacja Rosyjskiego Kościoła Prawosławnego, który jest narzędziem w rękach władzy państwowej Federacji Rosyjskiej wykorzystywanym do jej politycznych celów, takich jak wspieranie we wprowadzaniu polityki społecznej państwa lub sankcjonowania wojny rosyjsko-ukraińskiej[234]. Elementy religijne, czy wręcz mistyczne, które pojawiają się w retoryce Putina wykorzystywane są na potrzebny wewnętrznej, rosyjskiej propagandy w sposób instrumentalny, prawdopodobnie, aby wzmocnić legitymację jego władzy[235].

Z punktu widzenia wypracowanego wzorca bezpieczeństwa cyberprzestrzeni wobec operacji informacyjnych można w powyższych fragmencie zidentyfikować atak informacyjny na normy ideologiczne (religia) i etyczne w atakowanej grupie. Można wyróżnić następujące zależności związane z atakiem:

- tworzenie i promowanie sekt i innych wyznań prowadzi do zastępowaniu norm ideologicznych zgodnych z normami poznawczymi normami ideologicznymi, które są niezgodne z normami poznawczymi,
- szerzenie relatywizmu moralnego służy obniżeniu motywacji i norm etycznych,
- skomercjalizowanie prowadzi do promowania motywacji ekonomicznych, które będą odrzucone przez osoby wierzące (kierujące się motywacjami informacyjnymi, zgodnymi z motywacjami poznawczymi) i może doprowadzić do ich odejścia z danej wspólnoty,
- upolitycznienie prowadzi do zmniejszenia motywacji informacyjnych przywódców religijnych na rzecz motywacji witalnych, w których zawiera się ślepe posłuszeństwo w ramach hierarchii grupy (w tym przypadku władzy państwowej),

233 v. ibid., p. 63-70.
234 v. M. Składanowski, C. Smuniewski, *The Secularism of Putin's Russia and Patriarch Kirill's Church: The Russian Model of State–Church Relations and Its Social Reception*, in: *Religions*, 14 (2023), p. 3.
235 v. M. Składanowski, C. Smuniewski, *From Desecularization to Sacralization of the Political Language: Religion and Historiosophy in Vladimir Putin's Preparations for War*, in: *Verbum Vitae*, 40 (2022), p. 870.

- promowanie kultu jednostki-kapłana wśród wiernych wyrabia motywacje witalne u szeregowych wyznawców,
- nastawienie na rozrywkę otwiera religię na wpływy obcej propagandy, czyli pozwala kontrolować wejście systemu grupy przez efektory przeciwnika,
- usuwanie religii z życia publicznego zmniejsza dostęp jednostek do odpowiedniej wiedzy, na podstawie której można budować mądrość, jak i ogranicza możliwości programowania jednostek w ramach norm ideologicznych i etycznych zgodnych z motywacjami poznawczymi.

W przypadku edukacji dywersant będzie promował masowy charakter edukacji, który zastępuje indywidualne rozwijanie talentów i umiejętności danej osoby. Wadą takiego rozwiązania jest podporządkowanie się systemu szkolnictwa politycznej dyktaturze, możliwość rozpowszechniania propagandy wśród uczniów, zanikanie indywidualnej inicjatywy u absolwentów i opóźnienia w rozwoju zarówno techniki, jak i nauki. Do metod demoralizacji systemu edukacyjnego należą e.g. wymiany studenckie (w czasach Bezmienowa e.g. do Moskwy), promowanie w księgarniach marksistowskiej literatury, międzynarodowe seminaria i konferencje, na których promuje się ideologię dywersanta, przenikanie lewicowych działaczy i aktywistów do szkół i uniwersytetów, zakładanie czasopism, gazet, kół naukowych i grup badawczych mających na celu promocję ideologii komunistycznej. Efektem działań dywersanta w dziedzinie edukacji jest brak wiedzy w społeczeństwie i negatywne nastawienie do własnego Narodu[236].

W ramach działania dywersanta na edukację można wymienić następujące zależności:

- masowe szkolnictwo zwiększa dostęp państwa do wejścia jednostek (dzieci i młodzieży) co może być wykorzystane do promowania norm ideologicznych narzuconych przez kierownictwo grupy, a więc służyć

236 v. T. Schuman, op. cit., p. 71-73. Bezmienow opisuje, iż jednym z efektów działalności przeciw systemowi edukacji będzie *antyamerykanizm*, gdyż książka została zaadresowana do Amerykanów, natomiast wydaje się, iż wniosek można uogólnić na Naród jako taki.

jednostce zapewniając jej bezpieczeństwo lub je ograniczając przez promowanie nieodpowiednich norm,

- treści promujące normy ideologiczne niezgodne z normami poznawczymi prowadzą bezpośrednio do niszczenia norm poznawczych i wypracowywania niewłaściwych rejestratów w korelatorze (niezgodnej z rzeczywistością wiedzy),
- masowy charakter utrudnia pracę z uczniem, czyli uniemożliwia, aby proces nauczania był zgodny z rejestratami w korelatorze ucznia, a więc z jego wiedzą, wyobrażeniami i przyzwyczajeniami oraz z jego pojętnością, inteligencją i talentem, co może prowadzić do nieefektywnego nauczania i skutków opisanych przez Bezmienowa.

Kolejnym aspektem na poziomie idei są media. Bezmienow wyróżnia dwie główne działalności mediów w dziedzinie demoralizacji. Pierwszą z nich jest ignorowanie lub wręcz dyskredytowanie osób, które przekazują wiedzę o zjawiskach związanych z dywersją ideologiczną i tych, które prezentują dowody na zbrodniczy charakter komunistycznej ideologii. Drugą jest angażowanie społeczeństwa w różne pseudoproblemy, czyli takie zagadnienia, które dotyczą tylko i jedynie wąskiej liczby ludzi, a ich ewentualne rozwiązanie wiąże się z poważnymi konsekwencjami dla całej populacji danej społeczności. Jako przykład takiego pseudoproblemu Bezmienow podaje walkę o prawa homoseksualistów. Efektem takiej działalności jest przekierowanie uwagi, energii, czasu i pieniędzy społeczeństwa na kwestie nieistotne[237].

W zakresie oddziaływania dywersanta na media wyróżnia się:

- niszczenie przez jednostki pracujące w mediach relacji osobowych (wiary, nadziei i miłości) jednostek w grupie do jednostek nieprzychylnych dywersantowi, gdyż promują one zgodną z rzeczywistością wiedzę o dywersancie, co może uodpornić innych na ataki z jego strony,

237 v. ibid., p. 74-77.

- drugi aspekt dotyczy zmniejszania mocy swobodnej jednostek (pieniędzy, czasu, sił) przez zużywanie jej na czynności bez znaczenia sterowniczego.

Aspekt oddziaływania na kulturę polega na promowaniu, a czasem i opłacaniu, przez dywersanta różnych artystów, dziennikarzy, czasopism, intelektualistów etc., którzy w swoim działaniu upowszechniają treści niemoralne, osłabiają autorytety, dyscyplinę i buntują dzieci. Celem jest stworzenie pokolenia, które nie potrafi nad sobą panować i przez to jest łatwe w kontroli[238].

Oddziaływanie dywersanta na kulturę dotyczy:

- osłabiania w społeczeństwie norm etycznych,
- kształtowanie złych wyobrażeń, pamięci i nieprzydatnej lub szkodliwej wiedzy pod kątem sterowniczym,
- kształtowania nieodpowiednich emocji, które prowadzą do nieadekwatnej reakcji (decyzji) homeostatu,
- niszczenia relacji osobowych wobec autorytetów, zniechęcanie do wypracowywania w ramach potencjału swobodnego cnoty posłuszeństwa (związanej z autorytetami), ale też i innych cnót jak męstwa i umiarkowania,
- zaburzają proces programowania (przez wychowanie) według norm informacyjnych zgodnych z normami poznawczymi.

Poziom struktur obejmuje prawo i porządek (system prawny i organy ścigania), stosunki społeczne (organizacje i instytucje zajmujące się relacjami pomiędzy jednostkami i grupami), bezpieczeństwo (organizacje odpowiadające za obronę), politykę wewnętrzną (partie i inne grupy polityczne) i politykę zagraniczną (rządowe i pozarządowe organizacje kształtujące politykę zagraniczną). Oddziałując na strukturę związaną z prawem i porządkiem dywersant będzie dążył do tego, aby prawo dominowało nad moralnością. Może to doprowadzić do sytuacji, w której przestępca staje się ofiarą, a poszkodowany obywatel czuje się bezbronny. Efektem takiego działania jest brak zaufania obywateli do systemu

238 v. ibid., p. 78-81.

prawnego i organów ścigania. Również mogą pojawić się postulaty surowszych kar i zwiększenia kontroli nad obywatelem, co jest pożądane przez dywersanta. W aspekcie życia społecznego dywersant będzie zabiegał, aby w społeczeństwie przedkładano prawa nad obowiązki co ma doprowadzić do wytworzenia społeczeństwa nieodpowiedzialnych jednostek i być przyczynkiem do tyranii. Odnośnie do bezpieczeństwa działania dywersyjne polegają na osłabieniu autorytetu służb mundurowych i specjalnych przez kampanie podkreślające przewiny jednostek z którejś z tych służb przy jednoczesnym wybielaniu strony przeciwnej (grupy dywersanta), czego efektem jest bezbronność danego społeczeństwa. Szczególnie istotne są działania przeciwko służbom kontrwywiadowczym, które powodują wywołanie złej opinii o danej służbie w grupie, za czym mogą iść rozwiązania prawne, które uniemożliwiają skuteczną walkę z dywersją ideologiczną. Podziały i antagonizmy wśród różnych grup politycznych prowadzą do braku jedności. Z kolei błędy w polityce zagranicznej, jak na przykład próby negocjowania z ZSRR i innymi państwami komunistycznymi kończyły się według Bezmienowa spadkiem zaufania różnych krajów (e.g. Wietnamu) do USA co finalnie może prowadzić do całkowitej izolacji danej społeczności na arenie miedzynarodowej[239].

W oddziaływaniu atakującego na strukturę możliwe jest wyróżnienie:

- w zakresie prawa i porządku:
  - promowania norm prawnych kosztem norm etycznych (przechodzenie jednostki z motywacji informacyjnych do energomaterialnych),
  - wzmacniania norm prawnych i związanych z nimi represji energomaterialnych (zabieganie o surowsze kary),
  - promowania norm witalnych (większej kontroli obywatela przez państwo),
- w zakresie życia społecznego dochodzi do niszczenia norm etycznych (związanych z powinnościami), niepromowaniu cnót, a szczególnie cnoty sprawiedliwości i cnót z nią związanych (odpowiedzialnych za relacje

239 v. ibid., p. 53, 82-90.

społeczne) na rzecz promowania norm witalnych (przyjemności) i ekonomicznych (zysk),

- w zakresie bezpieczeństwa:
  - tworzenia negatywnych stereotypów przeciwko własnym służbom (czyli kształtowania złych emocji i wiedzy niezgodnej z normami poznawczymi) co prowadzi do niszczenia relacji osobowych (szczególnie wiary) jednostek z grupy wobec jednostek własnych służb,
  - uważania przez jednostki informacji od własnego kontrwywiadu za nieprawdziwych uniemożliwia uzyskanie wiedzy użytecznej sterowniczo, jak i niweluje skuteczność operacji informacyjnych sił własnych w celu zapobieganiu skutkom działań atakującego,
  - promowania w grupie norm prawnych niezgodnych z pozostałymi normami (szkodzących grupie),
- w zakresie polityki wewnętrznej podziały partyjne niszczą relacje osobowe między jednostkami w grupie zmniejszając jej trwałość,
- w zakresie polityki zewnętrznej układy z atakującym niszczą relacje osobowe jednostek z grupy (szczególnie z podsystemu kierowniczego), która negocjowała niekorzystne układy z grupą dywersanta do jednostek spoza tej grupy, co może prowadzić do izolacji.

Poziom życia dotyczy rodziny i społeczeństwa, zdrowia, rasy, populacji i pracy. W zakresie rodziny i społeczeństwa dywersant będzie wykorzystywał lub dążył do rozpadu rodzin, aby nie wytworzyła się u dziecka wychowującego się w rozbitej rodzinie lojalność wobec niej. Według Bezmienowa brak lojalność wobec własnej rodziny spowoduje, że danej osobie będzie trudno nauczyć się lojalności wobec własnego Narodu. Z drugiej strony dywersant będzie zabiegał, aby przenieść (u osób lojalnych wobec własnego Narodu) lub wypracować od podstaw (u osób, które nie wypracowały lojalności wobec własnego Narodu) lojalność do państwa opiekuńczego, które będzie władne, aby zaspakajać potrzeby danej osoby, jak i odebrać jej wolność osobistą. W zakresie zdrowia dywersant będzie

promował takie rozwiązania, które doprowadzą do fizycznego osłabienia społeczeństwa. Według Bezmienowa może się to objawić przez promowanie publicznej służby zdrowia, (która jest nieefektywna), zawodowego sportu (oglądania sportu zamiast uprawiania go) i złego jedzenia. Dywersant w celu przekonania do tych rozwiązań będzie pokazywał rzekome udane ich aplikacje, jak e.g. skutecznych sportowców sowieckich (którzy byli ewenementem na tle biednego i słabego fizycznie społeczeństwa sowieckiego) lub działające ośrodki medyczne w ZSRR (które były utrzymywane głównie na potrzeby zagranicznych delegacji). W zakresie rasy dywersant będzie dążył do stworzenia nowych podziałów i pogłębienia już istniejących. Może temu posłużyć powoływanie się na istniejące nierówności, które mogą być względnie niewielkie w porównaniu do innych państw, aby zwiększyć zakres ingerencji państwa w życie obywateli (pod pretekstem walki z rasizmem) i zwiększyć podziały i nienawiść między ludźmi. Problem populacji sprowadza się do wątku posiadania ziemi i urbanizacji, która według Bezmienowa należy do jednej z bardzo istotnych aspektów w kontekście demoralizacji. Rolnicy – osoby przywiązane do ziemi są często bardziej przywiązane do swojej Ojczyzny, niż osoba z miasta, zatem promocja przez dywersanta odbierania prywatnych gruntów jest uderzeniem właśnie w najbardziej patriotyczny element społeczeństwa. Odnośnie do pracy Bezmienow wymienia zagrożenia związane ze związkami zawodowymi, które są infiltrowane przez komunistów w celu promowania strajków. Osoby strajkujące mogą opuszczać, niekoniecznie z racjonalnych powodów, swoje obowiązki, do których może należeć e.g. opiekowanie się chorymi. Problemem są oddolne represje wobec osób, które nie chcą brać udziału w takich inicjatywach[240].

W zakresie poziomu życia można wyróżnić następujące działania dywersanta:

- w zakresie rodziny:
  - niszczenie relacji osobowych w rodzinie,

240 v. ibid., p. 54, 91-99.

    - zamiast promowania cnoty pietas dywersant propaguje motywacje witalne (posłuszeństwo wobec państwa opiekuńczego), jak i ekonomiczne (zysk),
- w zakresie zdrowia dochodzi do osłabienia zdrowia jednostki (osłabienia jakości jej podsystemów),
- w zakresie rasy:
    - promowanie rozwiązań prawnych zamiast etycznych,
    - niszczenie relacji osobowych między jednostkami w grupie,
    - promowanie norm witalnych (zwiększona kontrola państwa),
- w zakresie populacji zmniejszanie mocy całkowitej przez odbieranie gruntów osobom z potencjalnie większą cnotą pietas,
- w zakresie pracy zmniejszanie norm etycznych kosztem norm energomaterialnych.

Drugim etapem dywersji ideologicznej jest destabilizacja, która w zależności od kondycji i stawianego oporu przez społeczeństwo trwa od około 2 do 5 lat. Pierwszą oznaką braku stabilności jest chęć w społeczeństwie, aby zaczął rządzić charyzmatyczny przywódca, który zapewni więcej świadczeń społecznych, przepisów dotyczących pewności zatrudnienia, darmową opiekę medyczną i inne doraźne pomoce. Ludzie dążąc do łatwych rozwiązań i widząc niewydolność tradycyjnych struktur mogą skłonić się ku rozwiązaniom socjalistycznym. Bezmienow twierdzi, iż zaczną w takich warunkach powstawać komitety obywatelskie, które zdobywać będą coraz większe wpływy polityczne. W przepływie towarów coraz bardziej będzie uczestniczyło państwo. Wystąpi centralizowanie gospodarki i centralne jej planowanie. W miejsce władz wykonawczej, ustawodawczej i sądowniczej pojawi się biurokracja w rządzie, biurokracja w pracy i biurokracja w gospodarce. W przypadku sytuacji międzynarodowej państwo będzie coraz głębiej izolowane i coraz bardziej bezradne[241].

241 v. ibid., p. 100-103.

W przypadku etapu destabilizacji można wyróżnić następujące zjawiska:

- dominacja w społeczeństwie norm witalnych (chęć podporządkowania się państwu) i ekonomicznych (chęć świadczeń socjalnych),
- oczekiwanie wysokiego współczynnika swobody (zbliżonego do wartości 1, gdyż nie trzeba wtedy wykonywać żadnej pracy),
- tworzenie się alternatywnych grup wobec atakowanej grupy,
- zwiększenie się norm prawnych (przez wprowadzanie rozbudowanej biurokracji) niezgodnych z normami ekonomicznymi (ograniczanie oddolnej przedsiębiorczości kosztem centralizacji gospodarki),
- pogłębione niszczenie relacji osobowych jednostek (szczególnie z podsystemu kierowniczego) z grupy atakowanej wobec jednostek z innych grup.

Trzecim etapem dywersji ideologicznej jest etap kryzysu, który trwa od 2 do 6 miesięcy. Uśpieni agenci dostają wytyczne, aby przejąć władzę w danym kraju jak szybko się da, przy wykorzystaniu nawet najbardziej bezwzględnych metod. Szybkość działania może spowodować nawet zadowolenie pewnej części społeczeństwa z powodu silnego rządu. Objęcie władzy może odbyć się przez wojnę domową, rewolucję lub zewnętrzną interwencję. Możliwy jest również scenariusz, iż władza zostanie wybrana w demokratycznych wyborach i uzyska czasowe, nadzwyczajne uprawnienia. W zakresie gospodarki zostaną znacjonalizowane najważniejsze gałęzie przemysł i ograniczona do minimum własność prywatna. Rząd zacznie przeprowadzać redystrybucję dóbr i kampanię uzasadniającą reformy[242].

Ostatni etap dywersji – normalizacja. Bezmienow użył terminu normalizacja za Breżniewem, który wykorzystał ten zwrot w kontekście inwazji Układu Warszawskiego na Czechosłowację. W trakcie etapu normalizacji zostanie wprowadzona cenzura, obozy koncentracyjne i represje osób, które nie zgadzają się na aktualny stan rzeczy. Działacze lewicowi i aktywiści, którzy wcześniej brali

242 v. ibid., p. 49, 104-105.

udział w fazach demoralizacji i destabilizacji zostaną zamknięci w więzieniach, obozach lub zamordowani, gdyż nie są już potrzebni ze względu na destabilizujący charakter ich wcześniejszej działalności. Państwo będzie potrzebowało nowej moralności i stabilizacji. Zostaną wprowadzone zbrojne patrole na ulicach i cenzura prasy[243]. Z punktu widzenia operacji informacyjnych w etapach kryzysu i normalizacji dochodzi do pogłębionych procesów związanych z normami z etapu destabilizacji (umocnienie norm energomaterialnych) wraz z ograniczaniem przez cenzurę wiedzy użytecznej sterowniczo (zgodnej z rzeczywistością i prowadzącej do mądrości), jak i niszczenie relacji osobowych jednostek w atakowanej grupie. W ramach norm informacyjnych system w stanie normalizacji promuje jedynie normy ideologiczno-etyczne (marksizm) niezgodne z normami poznawczymi w celu wprowadzenia nowego pokoju (stabilizacji) w społeczeństwie.

Powyższe rozważania można odnieść do współczesnej Federacji Rosyjskiej. W retoryce Putina od 2007 roku pojawiają się nawiązania do takich norm ideologicznych jak twierdzenie o pewnym zwrocie konserwatywnym w Rosji, jej historycznej misji, potrzebie zjednoczenia historycznej Rusi, której tylko i jedynie Rosja jest kontynuatorem, podkreślanie osamotnienia aksjologicznego Rosji i tego, iż miałaby ona być oddzielną cywilizacją. Dodatkowo dochodzi do cenzurowania historii e.g. przez zakazywanie rozpowszechniania informacji o sojuszu III Rzeszy z ZSRR przed 1941 rokiem[244]. Powyższy sposób programowania społeczeństwa wpisuje się w zachowania związane z fazą normalizacji (rozpowszechnianie norm ideologicznych niezgodnych z normami poznawczymi i ograniczanie rozpowszechniania innych norm ideologicznych za pomocą cenzury). Istotne jest, aby podkreślić, że w retoryce Putina widać pewien sentyment do ZSRR oparty na rzekomej jedności Związku Sowieckiego, która się skończyła po jego rozpadzie doprowadzając do społecznego kryzysu. Dodatkowo według Putina wartości budowniczych komunizmu były kopiami uproszczonych wartości wynikających z Ewangelii. Z drugiej strony Putin potępiał totalitaryzm

243 v. ibid., p. 105-109.
244 v. M. Składanowski, C. Smuniewski, *From Desecularization...*, op. cit., p. 869, 873-874.

czasów komunizmu[245]. W fazie normalizacji w przypadku niepotrzebnych jednostek, z punktu widzenia atakującego, następuje nawet ich fizyczne wyeliminowanie, czyli wykorzystanie oddziaływań kinetycznych w celu wywarcia efektu psychologicznego na innych jednostkach przez odwołanie się do norm witalnych. Wydaje się, że w przypadku współczesnej Federacji Rosyjskiej ciągle można mówić o utrzymywaniu się stanu normalizacji, ale przy pewnych zmianach w wiodących normach ideologicznych, co jednak nie zmienia formalnej charakterystyki fazy normalizacji, która została wyprowadzona za pomocą wzorca teoretycznego bezpieczeństwa jednostek i grup wobec operacji informacyjnych.

Podsumowując, porównanie modelu dywersji ideologicznej z wzorcem bezpieczeństwa cyberprzestrzeni wobec operacji informacyjnych wskazuje na wysoką zbieżność obydwu ujęć. Elementy bezpieczeństwa jednostki wyróżnione w ramach wzorca pokryły się (od oddziaływania dywersanta na zdrowie, zmysłowe środowisko korelacyjne, intelektualne środowisko korelacyjne, potencjał swobodny, współczynnik swobody, moc swobodną, układ norm w nadsystemie, relacje osobowe między jednostkami), a co więcej model KGB zakłada oddziaływanie na atakowanego w sposób uwzględniony w ramach wzorca. Wskazuje to na użyteczność wzorca, gdyż jest zgodny z modelem, który był używany z powodzeniem w praktyce. Co więcej ze względu na ogólny charakter wzorzec może opisywać ataki nie tylko związane z marksizmem-leninizmem, ale też innymi normami ideologicznymi niezgodnymi z normami poznawczymi, ale również oddziaływania techniczne na zasoby.

245 v. ibid., p. 874-876.

ZAKOŃCZENIE

Założone cele pracy wymusiły na autorze wprowadzenie dodatkowych rozróżnień i aktualizacji wzorców, które nie występowały wcześniej w ramach Polskiej Szkoły Cybernetyki. Wprowadzano rozróżnienie na systemy substancjalne (istniejące same z siebie, takie które posiadają w sobie swoją zasadę tożsamości) i addycyjne (konwencjonalne, istniejące tylko w ludzkiej myśli, a będące w rzeczywistości tylko złożeniami innych systemów substancjalnych). Dodano koncepcję stanów systemu do rozważań nad systemem autonomicznym i systemem zorganizowanym. Opracowano zbiór możliwości systemów w cyberprzestrzeni (rozumianej jako przestrzeń sterowania) pod kątem operacji informacyjnych. Podzielono zasoby pod kątem ich użyteczności we wspieraniu jednostki, jak i zaproponowano sposób ich opisu i analizy jako systemów autonomicznych posiadających ograniczenia pewnych parametrów jego podsystemów. Umiejscowiono proces poznawczy i decyzyjny według tomizmu i neotomizmu w ramach parametrów systemu autonomicznego. Dodano do rozważań nad procesem decyzyjnym w systemie autonomicznym potencjał swobodny wyróżniony przez Kosseckiego. Rozszerzono rozważania nad reaktywnością systemu autonomicznego przez odniesienie go do wszystkich podsystemów systemu autonomicznego, jak i uwzględniając potencjał swobodny. Opracowano wzorzec komunikacji między systemami zgodnie z jakościową teorią informacji uwzględniający źródła zakłóceń i odbiorniki ulotu. Przeanalizowano relacje jednostki do zasobu uwzględniając wejście i wyjście zarówno jednostki, jak i zasobu, jak również problem administracji i korzystania z zasobów. Uzgodniono zagadnienie grupy (nadsystemu składającego się z jednostek i relacji między nimi) z ujęciem tomistycznym i neotomistycznym. Korzystając z jakościowej teorii informacji opisano szyfrowanie symetryczne, asymetryczne, steganografię, funkcje skrótu i zagłuszanie. Przełożono metodologię kostki cyberbezpieczeństwa McCumbera i modelu kill chain na język Polskiej Szkoły Cybernetyki. Przeanalizowano wpływ informacji niszczącej na wejścia i wyjścia systemów jako takich. Opisano i uogólniono w języku polskiej cybernetyki istotę operacji

informacyjnych i wykorzystywane w ramach nich techniki i zdolności według DD 3-10(A) i DD-3.20. Opracowano kryteria bezpieczeństwa jednostki, grupy, zasobów i informacji w języku PSC przy wykorzystaniu ujęć tomistycznych i neotomistycznych.

W ramach pracy udało się wypełnić założony cel główny – opracowanie wzorca teoretycznego oddziaływania operacji informacyjnych na bezpieczeństwo jednostek i grup w cyberprzestrzeni. Do tego celu zidentyfikowano systemy w cyberprzestrzeni, ustalono ich właściwości, elementy tych systemów i relacje między nimi, co wypełnia założone cele poznawcze. Wzorzec został potwierdzony przez porównanie do modelu dywersji ideologicznej KGB opisanej przez Bezmienowa.

Wzorzec opracowano na podstawie analizy i krytyki piśmiennictwa i analizy systemowej przy pomocniczym wykorzystaniu analizy ryzyka. Co więcej przy wykorzystaniu wzorca możliwe jest przeprowadzanie pogłębionej analizy ryzyka, jeśli zostaną wykorzystane dodatkowe narzędzia mierzące wyróżnione w ramach pracy właściwości systemów wpływające na bezpieczeństwo jednostek i grup. Wyróżnione kryteria bezpieczeństwa jednostek, a więc i grup są jednocześnie katalogiem zagrożeń. Zmniejszenie bezpieczeństwa jednostek można uzyskać przez oddziaływanie na wybrane kryterium jej bezpieczeństwa. Wymienione kryteria mogą jednocześnie służyć ocenie bezpieczeństwa systemu i przewidzieć trendy jego zmian na poziomie ogólnym i jakościowym. Aby uszczegółowić wzorzec potrzeba badań empirycznych w celu jego sparametryzowania, co jest aktualnym jego ograniczeniem. Na podstawie powyższego stwierdza się wypełnienie celów utylitarnych.

Biorąc pod uwagę powyższe rozważania uznaje się, że hipotezy dotyczące właściwości diagnostycznych i prognostycznych wzorca w zakresie bezpieczeństwa jednostek i grup wobec operacji informacyjnych zostały zweryfikowane pozytywnie na zadanym poziomie ogólności.

W trakcie pracy wykazano rozbieżności między teoriami tworzonymi w ramach PSC a filozofią (neo)tomistyczną w postaci:

- niejasnego statusu uczuć w tomizmie w kontekście psychocybernetyki Mazura, czyli czy władze gniewliwe i pożądliwe należą ściśle do homeostatu, czy są tylko oddziaływaniem korelatora na homeostat,
- zagadnienia uniwersalnego, optymalnego układu norm społecznych, który według Kosseckiego jest niemożliwy do opracowania, natomiast kryteria bezpieczeństwa wyróżnione na podstawie antropologii (neo)tomistycznej i teorii bezpieczeństwa Świniarskiego i Chojnackiego wskazują na jeden układ norm (dominacja norm ideologiczno-etycznych zgodnych z pozostałymi normami, a szczególnie z normami poznawczymi),
- materialnego charakteru komunikatów, a więc i informacji, według Mazura, co jest niezgodne z intelektualnym charakterem poznania w ramach władzy intelektu człowieka (postulat o materialnym charakterze informacji jest zgodny jedynie ze zmysłowymi władzami poznawczymi),
- procesów decyzyjnych rozkazu, wykonania czynnego i biernego w kontekście przełamywania potencjału decyzyjnego, gdyż rozkaz (dotyczący optymalizacji, a więc korelatora) według Akwinaty wpływa na wolę (związaną z homeostatem), ale już nie na władze wykonujące rozkaz (efektory), co jest sprzeczne z koncepcją Mazura,

Powyższe rozbieżności nie wpływają na sam wzorzec bezpieczeństwa i grup wobec oddziaływań operacji informacyjnych, ale wymagają dalszych badań w dziedzinie porównań (neo)tomizmu z PSC. Największą rozbieżnością jest hipoteza Kosseckiego, iż nie jest możliwa uniwersalna, optymalna konfiguracja norm dla wszystkich ludzi. Być może wynikała ona z braku bardziej szczegółowych kryteriów dobroci danych konfiguracji norm w socjocybernetyce, które są osiągalne dopiero przez uszczegółowienie wzorców z PSC o teorie z zakresu (neo)tomistycznej antropologii filozoficznej.

Możliwe jest dalsze rozwijanie tematyki na paru płaszczyznach. Pierwszą z nich jest kontynuowanie badań nad bezpieczeństwem jednostek i grup, ale w kontekście toru energomaterialnego (zasileniowego), które może obejmować

takie bezpieczeństwa przedmiotowe jak e.g. bezpieczeństwo energetyczne, wojskowe, ekonomiczne i prawne, czyli aspekty bezpieczeństwa związane z normami witalnymi, ekonomicznymi i prawnymi. Interesującym problemem wydaje się opracowanie relacji cnoty umiarkowania do wykorzystywania toru energomaterialnego (związanego z zasilaczem, akumulatorem i efektorami), jak i relacji tej cnoty wobec dynamizmu charakteru, który jest właściwością akumulatora. Kolejną płaszczyzną jest możliwość operacjonalizacji kryteriów bezpieczeństwa wyróżnionych w ramach wzorca, aby móc ocenić stan bezpieczeństwa na skalach ilościowych. Następną możliwością pogłębiania wzorca jest rozszerzenie rozważań związanych z już użytymi monoscyplinami takimi jak kryptologia, cyberbezpieczeństwo i antropologia filozoficzna. Dodatkowo możliwe są badania nad rozszerzeniem i zweryfikowaniem wzorca w ramach innych monodyscyplin dotyczących zasobów, jednostek, grup i informacji jak e.g. medycyna, biologia czy nauki o kulturze.

BIBLIOGRAFIA

Pozycje książkowe:

1 Andrzejuk A., *Tomasz z Akwinu jako psycholog*, Wydawnictwo von Borowiecky, Warszawa 2020.
2 Bocheński J., *Ku filozoficznemu myśleniu,* Instytut Wydawniczy PAX, Warszawa 1986.
3 Bocheński J., *Współczesne metody myślenia*, W drodze, Poznań 1992.
4 Carr N., *The Shallows. What the Internet is doing to our brains*, W.W. Norton & Company, Nowy York, Londyn 2010.
5 Cumming J., *Listy świętych do grzeszników*, Instytut Wydawniczy PAX, Warszawa 2003.
6 Ferguson G., Takane Y., *Analiza statystyczna w psychologii i pedagogice*, Wydawnictwo Naukowe PWN, Warszawa 2003.
7 Gogacz M., *Mądrość buduje państwo*, Wydawnictwo Ojców Franciszkanów, Niepokalanów 1993.
8 Gogacz M., *Wprowadzenie do etyki chronienia osób*, NAVO, Warszawa 1998.
9 Kahneman D., *Pułapki myślenia. o myśleniu szybkim i wolnym*, Media Rodzina, Poznań 2012.
10 Kalat J., *Biologiczne podstawy psychologii*, Wydawnictwo Naukowe PWN, Warszawa 2006.
11 Konieczny J., *Cybernetyka walki*, Wydawnictwo Naukowe PWN, Warszawa 1970.
12 Kossecki J., *Cybernetyka kultury*, Państwowy Instytut Wydawniczy, Warszawa 1974.
13 Kossecki J., *Cybernetyka społeczna*, Państwowe Wydawnictwo Naukowe, Warszawa 1975.
14 Kossecki J., *Metacybernetyka*, Narodowa Akademia Informacyjna, Warszawa 2015.
15 Kossecki J., *Tajniki Sterowania Ludźmi*, Krajowa Agencja Wydawnicza, Warszawa 1984.
16 Kotarbiński T., *Traktat o dobrej robocie*, Zakład Narodowy Imienia Ossolińskich, Wrocław 1958.
17 Krąpiec M., *Metafizyka*, Redakcja Wydawnictw Katolickiego Uniwersytetu Lubelskiego, Lublin 1995.
18 Kuhn T., *Struktura rewolucji naukowych,* Państwowe Wydawnictwo Naukowe, Warszawa 1968.
19 Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012.
20 Mazur M., *Cybernetyka a zarządzanie*, Ministerstwo Spraw Wewnętrznych Departament Szkolenia i Wydawnictw, Warszawa 1969.
21 Mazur M., *Cybernetyka i charakter*, Państwowy Instytut Wydawniczy, Warszawa 1976.
22 Mazur M., *Cybernetyczna teoria układów samodzielnych*, Państwowe Wydawnictwo Naukowe, Warszawa 1966.

23 Mazur M., *Jakościowa teoria informacji*, Wydawnictwo Naukowo Techniczne, Warszawa 1970.
24 McCumber J., *Assessing and Managing Security Risk in IT Systems. A Structured Methodology*, Auerbach Publications, Nowy York 2004.
25 Murray L., *Psychologia wojny. Strach i odwaga na polu bitwy*, Wydawnictwo RM, Warszawa 2014.
26 *Operacje Informacyjne DD-3.10(A)*, MON CDiSSZ, Bydgoszcz 2017.
27 *Operacje w cyberprzestrzeni DD-3.20*, MON CDiSSZ, Bydgoszcz 2020.
28 Shannon C., Weaver W., *The mathematical theory of communication*, The University of Illnois Press, Urbana 1964.
29 Sienkiewicz P., *Analiza systemowa. Podstawy i zastosowania*, Wydawnictwo Bellona, Warszawa 1994.
30 Sienkiewicz P., *Poszukiwanie golema*, Krajowa Agencja Wydawnicza, Warszawa 1988.
31 Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Instytut Studiów Politycznych Polskiej Akademii Nauk, Warszawa 1996.
32 Stępień A., *Elementy filozofii*, Redakcja Wydawnictw KUL, Lublin 1982.
33 Stępień T., *Wprowadzenie do antropologii filozoficznej św. Tomasza z Akwinu*, Warszawskie Towarzystwo Teologiczne, Warszawa 2013.
34 Swieżawski S., *Święty Tomasz na nowo odczytany*, W drodze, Poznań 1995.
35 Szmidt J., Misztal M., *Wstęp do kryptologii*, Wyższa Szkoła Informatyki Stosowanej i Zarządzania, Warszawa 2004.
36 Świniarski J., Chojnacki W., Etyka bezpieczeństwa, Akademia Obrony Narodowej, Warszawa 2004.
37 Świniarski J., Chojnacki W., *Filozofia bezpieczeństwa. Podręcznik akademicki*, ZUMS BN, Warszawa 2004.
38 Świniarski J., Kawalerski K., *Drogi i bezdroża securitologii*, Wojskowa Akademia Techniczna, Warszawa 2019.
39 Trankwillus G., *Żywoty cezarów*, Zakład Narodowy im. Ossolińskich, Wrocław 1960.
40 Tomasz z Akwinu, *Summa contra gentiles. Prawda wiary chrześcijańskiej w dyskusji z poganami, innowiercami i błądzącymi*, vol. 1, W drodze, Poznań 2003.
41 Tomasz z Akwinu, *Summa Theologiae*, vol. 13, Katolicki Ośrodek Wydawniczy „Veritas", Londyn 1986.
42 Trentowski B., *Stosunek filozofii do cybernetyki*, PWN, Warszawa 2014.
43 Watson G., Mason A., Ackroyd R., *Social Engineering Penetration Testing. Executing Social Engineering Pen Tests, Assesments and Defense*, Syngress, Coppell 2020.
44 Wiener N., *Cybernetyka, czyli sterowanie i komunikacja w zwierzęciu i maszynie*, Państwowe Wydawnictwo Naukowe, Warszawa 1971.
45 Wittgenstein L., *Tractatus logico-philosophicus*, Wydwanictwo Naukowe PWN, Warszawa 2012.
46 Wulff D., *Psychologia religii. Klasyczna i współczesna*, Wydawnictwo Szkolne i Pedagogiczne, Warszawa 1999.

Artykuły:

47 Andrzejuk A., Zembrzuski M., *Mieczysław Gogacz jako twórca tomizmu konsekwentnego*, in: *Opera philosophorum Medii Aevi*, 11 (2012).
48 Grobler A., Koczanowicz L., *Elementy filozofii dla psychologów*, in: *Psychologia podręcznik akademicki*, vol. 1, J. Strelau, D. Doliński (red.), Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2008.
49 Hutchins E., Cloppert M., Amin R., *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, in: *Leading Issues in Information Warfare and Security Research*, vol. 1, J. Ryan (red.), Academic Publishing International Limited, Reading 2011.
50 Kossecki J., *O pewnych stereotypach wykorzystywanych do działań dezinformacyjnych i dezintegracyjnych*, in: *Socjotechnika w polityce - wczoraj i dziś*, vol. 2, A. Kasińska-Metryka, A. Kasowska-Pedrycz (red.), Wydawnictwo Uniwersytetu Humanistyczno-Przyrodniczego Jana Kochanowskiego, Kielce 2009.
51 Łuczewski M., Bednarz-Łuczewska P., *Analiza dokumentów zastanych*, in: *Badania jakościowe. Metody i narzędzia*, vol. 2, D. Jemielniak (red.), Wydawnictwo Naukowe PWN, Warszawa 2012.
52 Schuman T., *Agentura wpływu. Tajniki działalności wywrotowej KGB*, Wydawnictwo AA, Kraków 2020.
53 Sienkiewicz P., *Ontologia cyberprzestrzeni*, in: *Zeszyty Naukowe WWSI*, 13 (2015).
54 Składanowski M., Smuniewski C., *From Desecularization to Sacralization of the Political Language: Religion and Historiosophy in Vladimir Putin's Preparations for War*, in: *Verbum Vitae*, 40 (2022).
55 Składanowski M., Smuniewski C., *The Secularism of Putin's Russia and Patriarch Kirill's Church: The Russian Model of State–Church Relations and Its Social Reception*, in: *Religions*, 14 (2023).
56 Sławecki B., *Znaczenie paradygmatów w badaniach jakościowych,* in: *Badania jakościowe. Podejścia i teorie*, vol. 1, D. Jemielniak (red.), Wydawnictwo Naukowe PWN, Warszawa 2012.
57 Smuniewski C., *Between Eternal Life, Politics And Peace: Thoughts on Contemporary Challenges for Eschatology*, in: *Path*, 18(2019).
58 Stańczyk J., *Istota współczesnego pojmowania bezpieczeństwa – zasadnicze tendencje*, in: *Rocznik Bezpieczeństwa Międzynarodowego*, 5 (2010).
59 Sun Tzu, *Sztuka wojny*, in: *Sztuka wojny*, B. Oczko (red.), Helion, Gliwice 2014.
60 Tomasz z Akwinu, *O władzy*, in: *Św. Tomasz z Akwinu. Dzieła wybrane*, W drodze, Poznań 1984.
61 Tomasz z Akwinu, *Przekład: Tomasz z Akwinu – Czy zło jest czymś? (Kwestie dyskutowane o złu, q. 1, a. 1)*, in: *Edukacja Filozoficzna*, (2001).
62 Zembrzuski Z., *Problem mind-body w świetle Tomaszowej koncepcji hylemorfizmu*, in: *Rocznik tomistyczny*, 7 (2018).

Źródła internetowe:

63 Gogacz M., *Elementarz metafizyki*, https://www.katedra.uksw.edu.pl/gogacz/ksiazki/elementarz_metafizyki.pdf, dostęp na 25.09.2022.
64 Kossecki J.*, PSC 9A. Człowiek jako proces autonomiczny - wykład (HD)*, https://www.youtube.com/watch?v=7P1wlZNv6dM, wykład online, dostęp na: 04.08.2021.
65 Mazur M., *Pojęcie systemu i rygory jego stosowania*, http://autonom.edu.pl/publikacje/mazur_marian/pojecie_systemu_i_rygory_jego_stosowania-ocr.pdf, dostęp na: 29.07.2021.

SPIS RYSUNKÓW

SPIS TABEL