Doctrina
Studia Społeczno-Polityczne 15/2018
PL ISSN 1730-0274

Beata Gałek
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Humanistyczny
ORCID 0000-0002-6923-7036

Nowe instrumenty współczesnych operacji pozainformacyjnych

New instruments of contemporary covert actions

Abstrakt: Wraz z profesjonalizacją służb wywiadowczych decydenci polityczni zyskali potężne instrumentarium umożliwiające uprawianie aktywnej polityki międzynarodowej. W warunkach szczególnego splotu globalizacji i rewolucji informacyjnej powstała rzeczywistość stwarzająca nowe okoliczności dla konstruowania wielopoziomowych strategii wpływania na kierunki i dynamikę procesów społecznych oraz politycznych. Strategii, w których operacje pozainformacyjne służb wywiadowczych mają istotne znaczenie.
Słowa kluczowe: wywiad, operacje pozainformacyjne, media społecznościowe

Abstract: With the professionalization of intelligence services, political decision-makers have gained powerful instruments to play a very active role in international politics. An interlacement of globalization and the information revolution, have made a new reality and new circumstances for the construction of multi-level strategies influencing the directions and dynamics of social and political processes. Strategies in which covert actions of intelligence services take an important place. The article is an attempt to capture a number of factors defining contemporary covert actions.
Keywords: intelligence, covert actions, social media

Wraz z profesjonalizacją służb wywiadowczych decydenci polityczni zyskali potężne instrumentarium umożliwiające uprawianie aktywnej polityki międzynarodowej, zorientowanej na realizację krótko- i długoterminowych celów w pozadyplomatyczny i niejawny

sposób. W warunkach szczególnego splotu globalizacji i rewolucji informacyjnej powstała rzeczywistość stwarzająca nowe okoliczności dla konstruowania wielopoziomowych strategii wpływania na kierunki i dynamikę procesów społecznych i politycznych. Przyjęte metody badawcze, w oparciu o obserwację i analizę literatury przedmiotu, syntezę pozwalającą na zestawienie faktów z badaniami, a także wnioskowanie, pozwoliły na wskazanie szerokiego kontekstu, aczkolwiek nie do końca szczegółowego z racji charakteru publikacji.

Zakres badanego pojęcia jest stosunkowo szeroki. Amerykańska szkoła posługuje się pojęciem „tajna operacja" (covert action). Loch K. Johnson definiuje je jako „trzecią opcję, pomiędzy dyplomacją a działaniami wojennymi"[1], a Roy Godson uważa, że tajna operacja to „wysiłki rządu zmierzające do wpływania na wydarzenia w innym państwie lub na innym terytorium bez ujawnienia swego zaangażowania"[2]. Natomiast w dokumentach Centralnej Agencji Wywiadowczej tajna akcja to „operacja zaplanowana w celu wpływania na rządy, wydarzenia, organizacje lub osoby w celu wspierania polityki w sposób, który niekoniecznie charakteryzuje politykę państwa sponsorującego takie działania"[3].

Stosunkowo wyraźnie zarysowane są granice definicyjne tajnych operacji w prawie amerykańskim, w Ustawie o bezpieczeństwie narodowym (National Security Act) z 1947 roku[4] oraz Rozporządzeniu wykonawczym nr 12 333 z 1981 roku. W wydanym przez Ronalda Reagana rozporządzeniu *covert action* określa się jako specjalne działania (special activities) „(...) oznaczające działania prowadzone w ramach wsparcia celów polityki zagranicznej państwa realizowanej za granicą, które są planowane i realizowane w taki sposób, że rola rządu Stanów Zjednoczonych nie jest widoczna lub potwierdzana publicznie, a także funkcje wspierające takie działania, nie

[1] L.K. Johnson, *America's secret power. The CIA in a Democratic Society*, New York 1989, s. 17.
[2] R. Godson, *Dirty Tricks or Trump Cards. US Covert Action & Counterintelligence*, New Brunswick 2004.
[3] Cyt. za: DCAF Intelligence Working Group, *Intelligence Practice and Democratic Oversight – a Practicioner's View*, „Occasional Paper" 2003, nr 3, s. 17.
[4] *National Security Act of 1947*; http://intelligence.senate.gov/nsaact1947.pdf (dostęp: 20.09.2018).

wpływające na proces polityczny, opinię publiczną, działalność polityczną i media w Stanach Zjednoczonych, nie dotyczące działań dyplomatycznych, zbierania i wytwarzania informacji wywiadowczych oraz wspierania procesu wywiadowczego"[5]. Eksperci RAND Corporation posługują się również pojęciem „operacje wpływu", co wydaje się oddawać szeroki zakres aktywności państwa i skupia się na jej celach[6].

W terminologii rosyjskiej najpowszechniej używa się terminu aktywne środki (przedsięwzięcia) (aktiwnyje mieroprijatija)[7]. Były archiwista KGB, Wasilij Mitrochin, pisze o: „działaniach agenturalno-operacyjnych skierowanych na wywieranie wpływu na politykę zagraniczną i wewnętrzną sytuację polityczną państw, będących obiektem tych działań, w interesie Związku Radzieckiego i innych krajów socjalistycznych, światowego komunizmu i ruchów narodowowyzwoleńczych; osłabianie politycznej, wojskowej, gospodarczej i ideologicznej pozycji kapitalizmu; torpedowanie jego agresywnych planów w celu stworzenia sprzyjających warunków pomyślnej realizacji polityki zagranicznej Związku Radzieckiego oraz zapewnienia pokoju i postępu społecznego"[8]. Współcześnie używa się również terminów takich jak „środki wsparcia" czy „specjalne środki wpływu". Pojawiły się one już w Doktrynie wojennej i Doktrynie bezpieczeństwa informacyjnego z 2000 roku, w ostatniej wersji Doktryny wojennej z grudnia 2014 roku wprowadzono dodatkowo pojęcie technologie informacyjne. Zostało ono przeniesione także do nowej redakcji Doktryny

[5] *Executive Order 12333 – United States intelligence activities*, http://www.archives.gov/federal-register/codification/executive-order/12333.html (dostęp: 20.09.2018).
[6] E.V. Larson, R.E. Darilek, D. Gibran, B. Nichiporuk, A. Richardson, L.H. Schwartz, C. Quantic Thurston, *Foundations of Effective Influence Operations A Framework for Enhancing Army Capabilities*, Santa Monica 2009, https://www.rand.org/pubs/monographs/MG654.html (dostęp: 10.11.2018).
[7] *Sowietskije aktiwnyje mieroprijatija. Dokład ob aktywnych mieroprijatijach i propagandie 1986–87*, http://okpz.freeservers.com/mashkov/activities/index.html (dostęp: 1.10.2018); *Aktiwnyje mieroprijatija spiecsłużb ot Trockogo do Jandarbijewa*, http://www.newsru.com/background/28jun2006/killbill.html (dostęp: 10.09.2018); *Active Measures: A Report on the Substance and Process of Anti-U.S. Disinformation and Propaganda Campaigns,* August 1986, http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20Substance%20and%20Process%20of%20Anti-US%20Disinformation%20August%201986.pdf (dostęp: 12.10.2018).
[8] W. Mitrochin, *KGB Lexicon: The Soviet Intelligence Officer's Handbook*, London 2002, s. 13.

bezpieczeństwa informacyjnego z grudnia 2016 roku[9]. Brytyjczycy natomiast posługują się terminem „specjalna akcja polityczna"[10]. Ciekawe rozstrzygnięcie terminologiczne proponuje Mirosław Minkina, używając pojęcia tajne operacje pozainformacyjne w odniesieniu do „cichej metody stosowanej w procesie zarządzania państwem, która ma przynieść określone cele w relacjach z innym podmiotem"[11]. Wydaje się, że jest to udana próba podkreślenia tajności działań państw i ich przedmiotu.

Tajne operacje wywiadu są faktem, a decydenci polityczni stosują je wtedy, kiedy inne metody oddziaływania mogą wywołać negatywne konsekwencje, niewspółmierne do uzyskanych efektów. Sięga się do nich, gdy użycie sił zbrojnych z pewnych względów nie jest możliwe, działania dyplomatyczne nie są skuteczne, a tylko tajne wpływanie uprawdopodobnia osiągnięcie celów. W tego typu akcjach decydenci polityczni używają służb wywiadowczych do kreowania procesów społecznych, politycznych i ekonomicznych korzystnych z punktu widzenia interesu państwa, konsekwentnie wypierając się podejmowania jakiejkolwiek aktywności w tym zakresie. W przeciwieństwie do działań wywiadowczych, których celem jest zbieranie i analizowanie informacji, tajne działania są aktywnym instrumentem osiągania celów polityki zagranicznej. Jennifer D. Kibbe wyodrębnia trzy główne kategorie ukrytych działań, obejmują one: propagandę, działania polityczne i działania paramilitarne[12]. Spektrum narzędzi uzupełnia aktywność w sferze gospodarczej, która ma destabilizować gospodarkę państwa będącego przedmiotem wpływu.

Dostrzegając wielowymiarowość aktywności państwa, która nie mieści się w ramach instrumentarium dyplomatycznego i militarnego, można wskazać, że obejmuje ona: tajne wspieranie zaprzyjaźnionego państwa, wpływanie na postrzeganie i ocenę przez

---

[9] J. Darczewska, *Środki aktywne jako rosyjska agresja hybrydowa w retrospekcji. Wybrane problemy*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 18 (10), s. 48.

[10] P.H.J. Davies, *From special operations to special political action: The 'rump SOE' and SIS post-war covert action capability 1945–1977,* "Journal of Intelligence and National Security" 2000, Volume 15, Issue 3, https://www.tandfonline.com/doi/ abs/10.1080 /02684520008432617 (dostęp: 16.10.2018).

[11] M. Minkina, *Sztuka wywiadu w świecie współczesnym*, Warszawa 2014, s. 214.

[12] J.D. Kibbe, *Covert Action*, Oxford Research Encyclopedia of International Studies, Mar 2010, oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626. 001.0001/acrefore-9780190846626-e-135?print=pdf (dostęp: 24.11.2018).

państwo zainteresowania wywiadowczego, wspieranie ruchów politycznych reprezentujących pożądane wartości i cele zbieżne celami polityki zagranicznej, wpływanie na wydarzenia z wykorzystaniem przemocy w sposób bezpośredni, włącznie z fizyczną eliminacją wroga (direct action)[13].

Badania dotyczące tajnych operacji wywiadowczych koncentrują się na analizie poszczególnych działań i oparte są na metodzie *case study*. Wskazuje się przyczyny podjętych działań i implikacje dla środowiska bezpieczeństwa, określa uwarunkowania prawne i instytucjonalne, poszukuje prawidłowości, a także nakreśla metodologię działania. W literaturze przedmiotu podejmuje się próby docierania do źródeł sukcesu lub porażki poszczególnych operacji, analizuje się koszty materialne i niematerialne prowadzonych działań. Ważnym obszarem badań są kwestie etyczne, nadzoru nad tajnymi operacjami, a także ich wpływ na kondycję demokracji.

Elementem, który stanowi o specyfice tajnych operacji i wyróżnia je od innych działań rządu, jest wiarygodne zaprzeczenie, czyli zdolność władz do zaprzeczania wiedzy lub odpowiedzialności za wszelkie działania prowadzone przez ich służby, często obejmujące oferowanie alternatywnej wersji odpowiedzialności[14]. Podkreślić należy, że tajne operacje należą do najbardziej strzeżonych tajemnic współczesnych państw. Wykorzystywane metody naruszają prawo nie tylko państwa, przeciwko któremu lub na którego terytorium prowadzona jest operacja, ale często są niezgodne z prawem państwa, którego obywatelami są ich wykonawcy. Tworzy to sprzyjające warunki do otaczania tajnych operacji wywiadowczych legendą, wzmacnianą i utrwalaną przez literaturę i kinematografię. Nie zwalnia to jednak od naukowej refleksji nad tym z definicji nieprzejrzystym polu badawczym.

W świecie wywiadu, w którym niezmiennie sięga się do starych, wypróbowanych metod, znanych i z powodzeniem stosowanych od wieków, obserwujemy obecnie wiele jakościowych zmian.

---

[13] M. Minkina, B. Gałek, *Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015, s. 36-54.

[14] M. Stout, *Covert Action in the Age of Social Media,* "Georgetown Journal of International Affairs" 2017, Volume 18, No. 2, https://www.georgetownjournal ofinternationalaffairs. org/online-edition/2017/12/22/ (dostęp: 15.11.2018).

Zniknęły ograniczenia w zakresie rozprzestrzeniania informacji[15], które pozwalały na prowadzenie działań na stosunkowo niewielką skalę, co sprowadzało je do wymiaru taktycznego, a wykluczało operacyjny czy strategiczny. Współczesne środowisko informacyjne przeniosło tajne operacje wywiadu w inny wymiar, a „geopolityczni alchemicy"[16] otrzymali nowe mikstury i tworzą adekwatne do wektorów zmian receptury. Naiwnością byłoby sądzić, że wywiad nie wykorzysta nowej broni, którą Witold Sokala nazywa BMM – bronią masowej manipulacji[17].

Rozwój technologiczny, a przede wszystkim Internet i dynamiczny rozwój mediów, tzw. „nowych mediów"[18], oraz „nowych, nowych mediów"[19] stworzyły olbrzymie możliwości oddziaływania, dzięki którym łatwiej niż kiedykolwiek przedtem można modyfikować postawy i zachowania szerokich warstw populacji, tym samym wpływać na procesy polityczne i społeczne, a finalnie wywierać presję na rządy innych państw. Nie ulega bowiem wątpliwości, iż uzyskanie możliwości ingerowania w treści przetwarzane przez miliony użytkowników może przynieść wymierne korzyści. Jak wynika z badań przeprowadzonych przez zespół naukowców Microsoft Research oraz Uniwersytetu Cambridge, nawet prosta analiza kliknięć w ikonę typu „Lubię to!" (Facebook) pozwala ze znacznym prawdopodobieństwem (rzędu 80-95%) określić takie cechy użytkowników, jak: rasa, wiek, preferencje polityczne, a nawet orientacja seksualna[20]. Dzięki zaa-

---

[15] Do głównych ograniczeń w zakresie rozprzestrzeniania się informacji zalicza się uwarunkowania techniczne i demograficzne, tj. niską przeciętną gęstość zaludnienia, ograniczoną mobilność oraz jej zniekształcenia przy przekazywaniu metodą „z ust do ust". H. Królikowski, *Historia działań specjalnych. Od wojny trojańskiej do II wojny światowej*, Warszawa 2004.

[16] Określenie Johna le Carré (wł. David John Moore Cornwell) w odniesieniu do służb wywiadowczych, przywołane przez Wojciecha Chudego. W. Chudy, *Społeczeństwo zakłamane. Esej o społeczeństwie i kłamstwie*, t. 2, Warszawa 2007, s. 395.

[17] W. Sokala, *Strategie medialne w konfliktach asymetrycznych*, [w:] *Terroryzm w medialnym obrazie świata,* red. K. Liedel, S. Mocek, Warszawa 2010, s. 45.

[18] T. Goban-Klas, *Media i komunikowanie masowe – teoria i analizy prasy, radia, telewizji i Internetu*, Warszawa 2004.

[19] Pojęcie nowych, nowych mediów wprowadza Paul Levinson w odniesieniu do szczególnie dynamicznych mediów społecznościowych kolejnej generacji; P. Levinson, *Nowe media. Rewolucja w komunikacji*, Warszawa 2010.

[20] M. Kosiński, D. Stillwell, T. Graepel, *Private traits and attributes are predictable from digital records of human behawior*, s. 1-4, http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf (dostęp: 23.10.2018).

wansowanym technologiom badania Internetu współczesne środowisko informacyjne oferuje szczegółowy obraz sieci, aktorów i powiązań komunikacyjnych. A to stanowi solidną podstawę do rozpracowania operacyjnego opinii publicznej.

W świecie bez Facebooka, Tweetera i blogosfery organizacja podstępu i dezinformacji była trudniejsza, droższa i miała znacznie bardziej ograniczony zasięg. Podczas II wojny światowej alianci włożyli wiele wysiłku w podważanie morale ludności niemieckiej, począwszy od nadawania audycji radiowych i kolportowania fałszowanych niemieckich znaczków pocztowych, kpiących z Hitlera, po bombardowania lotnicze[21]. Wysiłki te miały niewielki wpływ, ponieważ wpływanie na poglądy polityczne i preferencje milionów ludzi jednocześnie nie było wówczas możliwe. W czasach zimnej wojny sukcesem wywiadu był pojedynczy artykuł zamieszczony w popularnym tytule prasowym czy przejęcie kontroli nad gazetą lub czasopismem, często o niewielkim nakładzie. Wysiłki KGB, aby wpłynąć na zachodnie środki masowego przekazu, wiązały się z dużymi kosztami finansowymi i organizacyjnymi, a jednocześnie przynosiły niewielkie korzyści. Dostęp do w mediów masowych głównego nurtu był bardzo utrudniony[22].

Współczesne służby wywiadowcze są w stanie wpływać na duże populacje, angażując w tego rodzaju przedsięwzięcia stosunkowo niewiele zasobów. Dzieje się tak w dużej mierze dlatego, że zainteresowani polityką obywatele preferują informacje zgodne z ich światopoglądem. Uwzględniając tę tendencję natury ludzkiej, wyrafinowany aktor może wzmocnić lub nawet stworzyć realia, wpływając tym samym na polityczne postawy szerokich mas ludności[23]. Obok misternych intryg szpiegowskich pojawiły się boty i trolle[24]. Boty,

---

[21] M. Minkina, B. Gałek, *Kłamstwo i podstęp…*, s. 70-71.

[22] A. Weisburd, J.M. Berger, C. Watts, *Trolling for Trump: How Russia is Trying to Destroy our Democracy*, https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/, (dostęp: 27.11.2018).

[23] Ibidem.

[24] Według NATO StratCom (CoE) państwem o największym zinstytucjonalizowanym i profesjonalnie zarządzanym potencjale hybrydowych trolli jest Rosja. Co więcej, nowoczesne podejście Moskwy do działań w mediach społecznościowych zostało zintegrowane z jej doktrynami i strategiami państwa obejmującymi aktywność różnych instytucji; *Robotrolling: Trump, NATO, and Russian Trolls*, https://www.stratcomcoe.org/robotrolling-trump-nato-and-russian-trolls, "Robotrolling" 2018, Issue 3; J. Darczewska, *Rosyjskie siły zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*, „Prace

czyli konta fikcyjnych internautów generujące aktywność w sieci, okazały się skutecznym instrumentem dystrybucji informacji. Dzięki zdolności do masowego rozprzestrzeniania treści tworzą przydatne złudzenie masowości. W efekcie czego można nadawać przekazom wymiar powszechności, a odbiorcy zwracają uwagę na rzeczy, które są bardziej popularne. Znacząco ułatwia to konstruowanie i dystrybuowanie spreparowanej treści, czyniąc je bardziej wiarygodnymi z psychologicznego punktu widzenia[25]. Podczas gdy tysiące botów mogą być wykorzystywane do rozpowszechniania treści dowolnego rodzaju, armie trolli internetowych mogą kontrolować cały proces. Towarzyszy temu zjawisko bańki filtrującej[26], zmieniające środowisko informacyjne w zatomizowaną przestrzeń, w której ludzie żyją w hermetycznie zamkniętych realiach politycznych i społecznych. Otwarci tylko na informacje zgodne z ich poglądami, które są im podsuwane przez algorytm zbudowany na podstawie historii coraz bardziej spersonalizowanych doświadczeń internetowych. Najczęściej konsumujemy treści polityczne podobne do naszych poglądów. Większość publicznego dyskursu dotyczącego mediów społecznościowych sugeruje przekonanie, że tzw. internetowe ideologiczne komory echa, zwane także cyfrowymi wyspami izolacji, są głęboko problematyczne dla demokracji, ale dają wyjątkowe możliwości modyfikowania postaw i zachowań w ramach szeroko pojętej walki informacyjnej. Mamy do czynienia ze znaczącym ułatwieniem uderzenia operacyjnego na łatwiejszy do określenia cel, który odcina się od innych źródeł informacji. Istnieje możliwość błyskawicznego upowszechniania spreparowanych treści, wycinania treści niepożądanych, narzucania preferowanej interpretacji, zapewniając przy tym anonimowość nadawcy i dostęp do odbiorcy bez pośredników.

OSW" 2016, nr 57, https://www.osw.waw.pl/pl/publikacje/prace-osw/2016-06-27/rosyjskie-silyzbrojne-na-froncie-walki-informacyjnej-dokumenty (dostęp: 11.11.2018).

[25] C. Paul, M. Matthews, *The Russian Firehose of Falsehood PE-198 – OSD (2016)*, https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf (dostęp:14.09.2018).

[26] Bańka filtrująca (ang. filter bubble) – sytuacja powstała w wyniku działania określonego algorytmu, gdzie osoba korzystająca z sieci otrzymała informacje wyselekcjonowane, które dobrane zostały na podstawie informacji dostępnych na temat użytkownika, np. lokalizacja lub historia wyszukiwania. Powoduje to, że użytkownik zamknięty jest w samonapędzającym się cyklu opinii, a szukający nie zostaje nigdy skierowany na odmienne tematy lub punkty widzenia; E. Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, New York 2012.

Zapewnia też możliwości „wybielania" dezinformacji: odbiorca, który zada sobie trud zweryfikowania podsuniętej mu informacji, otrzyma potwierdzenie z kilku innych dezinformujących źródeł[27].

Zarówno praktycy, jak i teoretycy wywiadu wskazują na szerokie możliwości związane z poszukiwaniem informacji w publikatorach otwartych, zwłaszcza portale społecznościowe są postrzegane jako cenne źródła danych dla tzw. „białego wywiadu" (OpenSource Intelligence – OSiNT). Posługujemy się dziś osobną kategorią działań wywiadowczych, której nadano nazwę SoCMiNT (Social Media Intelligence)[28]. Szczegółowe zastosowania, szanse i zagrożenia związane z prowadzeniem SoCMiNT-u wciąż pozostają tematem stosunkowo mało eksplorowanym, ale zainteresowania śledzeniem zawartości portalów społecznościowych nie kryją służby specjalne i organy ścigania współczesnych państw[29]. Szczególnie istotne dla tego wymiaru aktywności wywiadu jest tworzenie map relacji społecznych oraz ustalanie linii podziałów politycznych w kraju będącym przedmiotem zainteresowania wywiadowczego[30].

To co sprawia, że media społecznościowe są szczególnie interesujące w kontekście wywiadu, to możliwość prowadzenia działań z dala od terenu konfliktu i gromadzenia danych w czasie rzeczywistym – w zależności od szybkości oprogramowania monitorującego i analizującego. Znacząco ułatwia to prowadzenie działań, kiedy dostęp do obszaru operacyjnego jest utrudniony lub nawet niemożliwy ze względu na brak mandatu politycznego i brak spełnienia kryteriów „zasady zaangażowania" (RoE)[31] lub z innych względów bezpieczeń-

---

[27] J. Darczewska, *Środki aktywne jako rosyjska agresja…*, s. 40-65.

[28] D. Omand, *Introducing Social Media Intelligence (SOCMINT)*, "Journal of Intelligence and National Security" 2012, Volume 27, Issue 6, s. 801-823.

[29] Dziennik „Kommiersant" 27 sierpnia 2012 roku poinformował, że Służba Wywiadu Zagranicznego Federacji Rosyjskiej (SWR) ogłosiła trzy przetargi na zaprojektowanie i wdrożenie kompleksowego systemu monitorowania sieci społecznościowych „Dysput", „Monitor" i „Sztorm" na łączną sumę 30 mln rubli.

[30] H. Farrell, *Five key questions – and answers – about Iran's social media influence*, "The Washington Post", 17 grudnia 2013, http://www.washingtonpost.com/blogs/monkey-cage/wp/2013/12/17/five-key-questionsand-answers-about-irans-social-media-influence/ (dostęp: 30.10.2018).

[31] Zasady podejmowania działań przy użyciu siły obejmują reguły, przeznaczone dla dowódców i pojedynczych żołnierzy, określające warunki użycia siły – kiedy, gdzie i jaka siła może zostać wykorzystana – bądź do osiągnięcia celu operacji, bądź w ramach

stwa. Zasadniczo, możliwość funkcjonowania w sferze online oznacza obecność w teatrze działań wojennych, podczas gdy nawet nie działa się za jego kulisami, tylko można wygodnie zasiąść w loży.

Odrębnym zagadnieniem badawczym jest problem wykorzystania przez wywiad cyberprzestępczości. Jest oczywiste, że wykorzystanie prawdziwych danych ułatwia tworzenie strategii oddziaływania na procesy decyzyjne, w oparciu o co wpływa na uprawdopodobnienie koncepcji prowadzonych działań i wiarygodne zaprzeczenie. Cyberprzestępczość może generować ogromne ilości prawdziwych danych w krótkim czasie, o wiele więcej niż można było „ukraść" w erze przed Internetem. Jako przykład użyteczności cyberprzestępców dla służb specjalnych wskazuje się wykorzystanie przez rosyjski wywiad Guccifera 2.0, DCLeaks.com i WikiLeaks[32]. Sukcesy APT28 (FANCY BEAR) i APT29 (COZY BEAR) potwierdzają, że Rosja jest liderem w dziedzinie cyberprzestępczości i umiejętnie wykorzystuje ten najbardziej produktywny sposób generowania prawdziwych lub możliwych do modyfikacji treści[33]. Nie jest również trudne – choć pracochłonne – manipulowanie skradzionymi danymi lub fałszowanie danych, jeśli istnieją prawdziwe do wykorzystania jako model[34].

Kolejnym czynnikiem, ułatwiającym konstruowanie i prowadzenie operacji przez takich uczestników systemu międzynarodowego jak Rosja i państwa o podobnych zdolnościach, jest brak ko-

samoobrony; B. Janusz-Pawletta, *Zasady użycia siły (ang. Rules of Engagement) – wybrane problemy prawne*, „Wiedza Obronna. Zeszyt problemowy" 2011, nr 2 (66).

[32] Department of Homeland Security, *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security*, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national; *Threat Group-4127 Targets Hillary Clinton Presidential Campaign*, https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign; *FANCY BEAR Has an (IT) Itch They Can't Scratch*, https://www.threatconnect.com/blog/fancy-bear-it-itch-they-cant-scratch/ (dostęp: 15.11.2018).

[33] *APT28: At the Center of the Storm: Russia Strategically Evolves Its Cyber Operations*, Special Report 2017, https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html?utm_source=FEcom&utm_campaign=intel-apt28&utm_medium=blog (dostęp: 14.10.2018).

[34] W listopadzie 2016 roku FBI prowadziło dochodzenie w sprawie fałszywych dokumentów, które skierowane były przeciwko Hilary Clinton i które znalazły się w mediach społecznościowych. M. Hosenball, *FBI Examining Fake Documents Targeting Clinton Campaign*, http://www.reuters.com/article/us-usa-election-documents-idUSKBN12Y2WY/ (dostęp: 11.11.2018).

nieczności przesadnego dbania o spójność podejmowanych działań[35]. Dziś wiemy, że odbiorcy przekazu szukają informacji zgodnych z ich z góry przyjętymi założeniami i odrzucają wszystkie przekazy i kanały niegodne z tym, czego już się spodziewają i oczekują. Wystarczy więc, że wywiad dostarczy pożądaną narrację, zaproponuje adekwatne ramy analityczne oparte na tzw. *fake news*[36]. Ten zaledwie naszkicowany obraz współczesnych operacji pozainformacyjnych może stworzyć wrażenie, że wraz z nowymi technologiami informacyjnymi ukształtował się system oparty na omnipotencji służb specjalnych w zakresie ingerowania w sprawy wewnętrzne innych państw. Rzeczywiście, instrumenty informacyjne zyskały dziś status środka bojowego, ale na tym obrazie, który ze względu na stan badań znajduje się w fazie *in statu nascendi*, widnieją poważne rysy.

Należy zwrócić uwagę na to, że oddziaływanie mediów społecznościowych nie jest prostym odwzorowaniem procesu komunikowania masowego z użyciem jako kanału przekazu tzw. tradycyjnych mediów. Generują one zwiększony poziom niepewności i ryzyka. Należy uwzględnić nieprzewidywalność i szybkość informacji pojawiających się za pośrednictwem mediów społecznościowych, które mogą zniekształcić sposób postrzegania działań aktywnych i obronnych na poziomie politycznym i publicznym w sposób szkodliwy dla strategicznych celów państwa. Kolejnym aspektem, który podnosi stopień niepewności przebiegu i skutków operacji, jest nieprzewidywalność i anonimowość zarówno odbiorców, jak i autorów przekazu w mediach społecznościowych. Uważa się, że stwarzają one znaczne ryzyko dla bezpieczeństwa operacji obronnych, w szczególności pod względem bezpieczeństwa operacyjnego i życia personelu wojskowego[37].

Poważnym problemem dla planowanych działań operacyjnych jest utrudnienie lub brak możliwości wiarygodnego zaprzeczenia. Z jednej strony wywiad zyskał nowy arsenał instrumentów,

---

[35] C. Paul, M. Matthews, *The Russian…*, op. cit.

[36] *Fake news* – fałszywa wiadomość, często o charakterze sensacyjnym, publikowana w mediach z intencją wprowadzenia odbiorcy w błąd w celu osiągnięcia korzyści finansowych, politycznych lub prestiżowych; *Mały leksykon postprawdy*, Warszawa 2018, s. 28.

[37] T.E. Nissen, *The Weaponization Of Social Media Characteristics of Contemporary Conflicts*, Royal Danish Defence College, Copenhagen, March 2015, s. 12.

z drugiej powszechny dostęp do technologii informacyjnych i komunikacyjnych (ICT) stał się kluczowym czynnikiem podnoszącym ryzyko utraty tajnego charakteru działań[38]. Michael F. Joseph, Michael Poznansky przewidują koniec tajnych działań, w dużej mierze dlatego, że zwiększona ekspozycja, spowodowana zmianami w mediach i technologiach komunikacyjnych, powoduje erozję wiarygodnego zaprzeczenia[39]. Natomiast Rory Cormac i Richard J. Aldrich formułują tezę, że przywódcy państw znacznie ostrożniej podejmują decyzję o tajnych operacjach, gdy potencjalny cel ma gęstą sieć ICT. Uważają, że tajne działania w stylu zimnowojennym mogą być już przeszłością w epoce, w której technologie komunikacyjne i medialne rozprzestrzeniły się w najdalszych zakątkach globu[40]. Niemniej jednak w świetle wskazanych wyżej korzyści, wynikających z funkcjonowania w erze globalnej informacji, państwa pragnące użyć siły spotykają się z silnymi zachętami do podjęcia działań tajnych. Skutecznie przeprowadzona tajna operacja może znacząco zmniejszyć prawdopodobieństwo niechcianej eskalacji konfliktu z silnym rywalem i pomóc decydentom ukryć niepopularne działania zarówno przed własnymi obywatelami, jak i obywatelami państw będących obiektem działań. Pokusę wzmacnia niski koszt operacji, podczas gdy koszty działań wojennych stale rosną.

Na tle problemu erozji „wiarygodnego zaprzeczenia" warto przyjrzeć się sprawie ostentacyjnego mordu saudyjskiego dziennikarza Dżamala Chaszodżdżiego[41], a także próbie otrucia Siergieja i Julii Skripal[42]. W obydwu przypadkach mamy do czynienia z sytuacją,

[38] Problemem dla zachowania tajności operacji wywiadowczych jest działalność dziennikarzy śledczych, którzy specjalizują się w badaniach *open source* i mediach społecznościowych, portali śledczych, tj. Bellingcat, który m.in. wraz z rosyjskim portalem „The Insider" zdemaskowali agentów GRU zamieszanych w próbę zabójstwa Skripalów, https://www.bellingcat.com/tag/skripal/ (dostęp: 4.10.2018).

[39] M.F. Joseph, M. Poznansky, *Media technology, covert action, and the politics of exposure,* "Journal of Peace Research" 2017, No. 55 (3), s. 320-335.

[40] R. Cormac, R.J. Aldrich, *Grey is the new black: covert action and implausible deniability*, "International Affairs" 2018, Volume 94, Issue 3, s. 477-494.

[41] *CIA finds Saudi crown prince ordered Jamal Khashoggi killing – report*, "The Guardian", https://www.theguardian.com/world/2018/nov/16/cia-determines-saudi-crown-prince-ordered-journalists-killing-washington-post (dostęp: 18.12.2018).

[42] M. Wilgocki, *Otrucie Siergieja Skripala. USA, Francja, Niemcy i Kanada potępiają Rosję za atak nowiczokiem*, „Gazeta Wyborcza", 6 września 2018, http://wyborcza.pl/7,75399,23871453,otrucie-siergieja-skripala-usa-francja-niemcy-i-kanada-potepiaja.html (dostęp: 20.12.2018).

w której tajne służby działają coraz bardziej otwarcie, zarzucając tradycyjną dbałość o zachowanie tajemnicy. Wolfgang Krieger w wypowiedzi dla „Deutsche Welle" potwierdza, że „staranne maskowanie tajnych operacji jak gdyby wyszło z mody, a służby coraz częściej działają z otwartą przyłbicą; przestały się kryć"[43]. Sprawa Skripalów stanowi swoistą ilustrację starej metody działania służb specjalnych. Zdrajca, który przeszedł na stronę wroga, musi liczyć się z najwyższym wymiarem kary. Różnica polega na tym, że dawniej operowano w ścisłej tajemnicy, starając się upozorować zabójstwo na samobójstwo albo zwykły wypadek. Dżamal Choszodżdżi nie był funkcjonariuszem wywiadu, był dziennikarzem, ale jego brutalne zabójstwo łączy się ze sprawami Litwinienki i Skripalów. W obu przypadkach akcja służb specjalnych miała stanowić komunikat dla ewentualnych naśladowców, a więc nie mogła pozostać tajna.

Chociaż omawiana problematyka jest skrajnie nietransparentna, prezentowane wyniki badań wydają się potwierdzać, że wiodącym praktykiem tych działań jest Federacja Rosyjska[44]. Ze względu na swoją wielkość, umiejętności techniczne oraz kulturę polityczną i wywiadowczą jest dobrze przygotowana do wykorzystania możliwości jakie oferuje infosfera. Chiny również z powodzeniem odnalazły się w nowej rzeczywistości[45]. Stany Zjednoczone wraz z sojusznikami także stosowały w przeszłości i dziś wykorzystują możliwości. Powstają liczne analizy, dowodzące, że mamy do czynienia z próbami podważenia wartości porządku liberalnego na świecie, destabilizowania systemów politycznych zgodnie z celami strategicznymi Rosji na obszarze euroatlantyckim. Najczęściej wskazuje się na wysiłki podejmowane przez rosyjskie służby specjalne w celu wpłynięcia na nastroje społeczne i decyzje wyborcze podczas kampanii

[43] N. Oberhäuser, *Tajne służby. Rośnie zapotrzebowanie na skrytobójców*, „Deutche Welle", 21 października 2018, https://www.dw.com/pl/tajne-s%C5%82u%C5%B Cbyro%C5%9Bnie-zapotrzebowanie-na-skrytob%C3%B3jc%C3%B3w/a-45971400 (dostęp: 24.11.2018).

[44] *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, ODNI, Assessing Russian Intentions and Activities, 6 January 2017, https://www.dni.gov/files/ documents/ICA_2017_01.pdf (dostęp: 10.12.2018).

[45] A. Grace, *China's Influence Operations Are Pinpointing America's Weaknesses*, "Foreign Policy", October 4 2018, https://foreignpolicy.com/2018/10/04/chinas-influence-operations-are-pinpointing-americas-weaknesses/ (dostęp: 10.11.2018).

prezydenckiej w Stanach Zjednoczonych, a także w Szwecji[46], Francji[47] i Niemczech[48].

Warto posłużyć się parafrazą słów Vladimira Volkoffa, że z tajnymi operacjami pozainformacyjnymi jest tak jak z gazami bojowymi – stosuje się je wówczas, gdy wieją przychylne wiatry[49]. Niewątpliwie zmiany w środowisku informacyjnym są kluczowe dla zrozumienia ewolucji i natury współczesnych tajnych działań służb wywiadowczych. Rzeczywistości online i offline przenikają się. Zatem aby uniknąć mispercepcji, konieczne jest jednoczesne uwzględnienie obydwu sfer. Nowe narzędzia komunikacji przeniosły wysiłki służb wywiadowczych na inny poziom. Media społecznościowe stały się cennym narzędziem określania i profilowania celów rozpracowania operacyjnego. Do bogatego już arsenału narzędzi walki, używanych przez państwa i organizacje niepaństwowe, włączane są operacje z udziałem tzw. trolli i trudno jest nie dostrzec korelacji ich aktywności z aktywnością wybranych państw czy organizacji w wymiarze politycznym, militarnym i gospodarczym.

Bibliografia

Active Measures: A Report on the Substance and Process of Anti-U.S. Disinformation and Propaganda Campaigns, August 1986, http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20Substance20and%20Process%20of%20AntiUS%20Disinformation%20August%201986.pdf.

Aktiwnyje mieroprijatija spiecsłużb ot Trockogo do Jandarbijewa, http://www.newsru.com/ background/28jun2006/killbill.html.

Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution,

[46] M. Kragh, S. Åsberg, *Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case*, "Journal of Strategic Studies" 2017, 40 (6) 30, s. 1-44, (dostęp: 25.10.2018).

[47] E. Ferrara, *Disinformation and Social bot operations in the run up to the 2017 French presidential election*, "First Monday" 2017, 22 (8), https://arxiv.org/ ftp/arxiv/papers/1707/1707.00086.pdf (dostęp: 26.11.2018).

[48] C. Copley, *Spy Chief Adds to Warnings of Russian Cyber Attacks on Germany*, http://www.reuters.com/article/us-germany-election-russia-idUSKBN13O133 (dostęp: 17.10.2018).

[49] V. Volkoff, *Dezinformacja. Oręż wojny*, Warszawa 1991, s. 9.

ODNI, Assessing Russian Intentions and Activities, 6 January 2017.

Copley C., *Spy Chief Adds to Warnings of Russian Cyber Attacks on Germany*, http://www.reuters.com/article/us-germany-election-russia-idUSKBN13O133.

Cormac R., Aldrich R. J., *Grey is the new black: covert action and implausible deniability*, "International Affairs", Volume 94, Issue 3, 1 May 2018.

Darczewska J., *Rosyjskie Siły Zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*, „Prace OSW" 2016, nr 57, https://www.osw.waw.pl/pl/publikacje/prace-osw/2016-06-27/rosyjskie-silyzbrojne-na-froncie-walki-informacyjnej-dokumenty.

Darczewska J., *Środki aktywne jako rosyjska agresja hybrydowa w retrospekcji. Wybrane problemy*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 18 (10).

DCAF Intelligence Working Group, *Intelligence Practice and Democratic Oversight – a Practicioner's View*, "Occasional Paper" 2003, nr 3.

Davies P.H.J., *From special operations to special political action: The 'rump SOE' and SIS post-war covert action capability 1945–1977*, "Journal Intelligence and National Security" 2000, Volume 15, Issue 3, https://www.tandfonline.com/doi/abs/10.1080/02684520008432617.

Department of Homeland Security, *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security*, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

Executive Order 12333-United States intelligence activities, Part 3 par. 3.4, p. H.

FANCY BEAR Has an (IT) Itch They Can't Scratch, https://www.threatconnect.com/blog/fancy-bear-it-itch-they-cant-scratch/.

Farrell H., *Five key questions – and answers – about Iran's social media influence*, "The Washington Post", 17 grudnia 2013, http://www.washingtonpost.com/blogs/monkey-cage/wp/2013/12/17/five-key-questionsand-answers-about-irans-social-media-influence.

Ferrara E., *Disinformation and Social bot operations in the run up to the 2017 French presidential election*, "First Monday" 2017, 22 (8), https://arxiv.org/ftp/arxiv/papers/1707/1707.00086.pdf.

FireEye, *APT28: At the Center of the Storm: Russia Strategically Evolves Its Cyber Operations, Special Report*, 2017.

Goban-Klas T., *Media i komunikowanie masowe – teoria i analizy prasy, radia, telewizji i Internetu*, Warszawa 2004.

Grace A., *China's Influence Operations Are Pinpointing America's Weaknesses*, "Foreign Policy", October 4 2018, https://foreignpolicy.com/2018/10/04/chinas-influence-operations-are-pinpointing-americas-weaknesses.

Godson R., *Dirty Tricks or Trump Cards. US Covert Action & Counterintelligence*, New Brunswick 2004.

Hosenball M., *FBI Examining Fake Documents Targeting Clinton Campaign*, http://www.reuters.com/article/us-usa-election-documents-idUSKBN12Y2WY/ .

Joseph M.F., Poznansky M., *Media technology, covert action, and the politics of exposure*, "Journal of Peace Research" 2017, 55 (3).

Johnson L. K., *America's secret power. The CIA in a Democratic Society*, New York 1989.

Kibbe J.D., *Covert Action*, Oxford Research Encyclopedia of International Studies, Mar 2010, xfordre.com/internationalstudies/view/ 10.1093/acrefore/9780190846626.001.0001/acrefore-9780 190846626-e-135?print=pdf.

Kosiński M., Stillwell D., Graepel T., *Private traits and attributes are predictable from digital records of human behawior*, http://www.pnas. org/content/early/2013/03/06/12187721 10.full.pdf .

Kragh M., Åsberg S., *Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case*, "Journal of Strategic Studies" 2017, 40(6)30.

Levinson P., *Nowe nowe media. Rewolucja w komunikacji*, Warszawa 2010.

Larson E.V., Darilek R. E., Gibran D., Nichiporuk B., Richardson A., Schwartz L. H., Thurston C. Quantic, *Foundations of Effective Influence Operations A Framework for Enhancing Army Capabilities*, Santa Monica 2009, https://www.rand.org/pubs/monographs/MG654.html.

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

Minkina M., Gałek B., *Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015.

Mitrochin W., *KGB Lexicon: The Soviet Intelligence Officer's Handbook*, London 2002.

National Security Act of 1947 (approved July 26, 1947) Sec. 104A (d) (4).

Nissen T.E., *The Weaponization Of Social Media Characteristics of Contemporary Conflicts*, Royal Danish Defence College, Copenhagen, March 2015.

Oberhäuser N., *Tajne służby. Rośnie zapotrzebowanie na skrytobójców*, „Deutche Welle", 21 października 2018.

Omand D., *Introducing Social Media Intelligence (SOCMINT)*, "Journal Intelligence and National Security" 2012, Volume 27, Issue 6.

Pariser E., *The Filter Bubble: What The Internet Is Hiding From You*, New York 2012.

Paul C., Matthews M., *The Russian 'Firehose of Falsehood PE-198 - OSD (2016)*, https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.

Robotrolling: Trump, NATO, and Russian Trolls, https://www.stratcomcoe.org/robotrolling-trump-nato-and-russian-trolls, "Robotrolling" 2018, Issue 3.

Sokala W., *Strategie medialne w konfliktach asymetrycznych*, [w:] *Terroryzm w medialnym obrazie świata*, K. Liedel, S. Mocek (red.), Warszawa 2010.

Sowietskije aktiwnyje mieroprijatija. Dokład ob aktywnych mieroprijatijach i propagandzie 1986–87, http://okpz.freeservers.com/mashkov/activities/index.html.

Stout M., *Covert Action in the Age of Social Media*, "Georgetown Journal of International Affairs" 2017, Volume 18, No. 2. https://www.georgetownjournalofinternationalaffairs.org/online-edition/2017/12/22.

Threat Group-4127 Targets Hillary Clinton Presidential Campaign, https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign.

Weisburd A., Berger J.M., Watts C., *Trolling for Trump: How Russia is Trying to Destroy our Democracy*, https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy.

Wilgocki M., *Otrucie Siergieja Skripala. USA, Francja, Niemcy i Kanada potępiają Rosję za atak nowiczokiem*, „Gazeta Wyborcza", 6 września 2018.

Volkoff V., *Dezinformacja. Oręż wojny*, Warszawa 1991.