Joanna Kwiecień
Szymon Chojnowski

NOWE SFERY BEZPIECZEŃSTWA MIĘDZYNARODOWEGO

Wprowadzenie

Poniższe opracowanie przedstawia problematykę komunikowania i mediów elektronicznych w kontekście bezpieczeństwa międzynarodowego. Współcześnie obserwuje się rosnącą rolę mediów elektronicznych w dziedzinie polityki międzynarodowej i bezpieczeństwa. Serwisy informacyjne wiodących stacji telewizyjnych, portale informacyjne, największe agencje prasowe, a także media społecznościowe oddziałują w różny sposób na opinię publiczną zarówno w skali regionalnej, jak i globalnej. Wymienione elementy komunikowania mogą być wykorzystywane jako narzędzia perswazji i prowadzenia polityki informacyjnej przez partie polityczne, rządy, liderów politycznych, korporacje czy organizacje międzynarodowe.

1. Komunikowanie i media elektroniczne

Definicja bezpieczeństwa międzynarodowego ewoluuje zgodnie z kierunkiem zmian powodowanych szeroko rozumianą globalizacją. Następuje odejście od klasycznej definicji „twardego bezpieczeństwa" realistów, w której główny nacisk kładzie się na siłę militarną (Carl von Clausewitz). Obecnie, z powodu ekspansji zagrożeń, w centrum uwagi ekspertów do spraw bezpieczeństwa leżą „miękkie", pozamilitarne aspekty – takie, jak siła ekonomiczna, walka z globalnym ociepleniem czy właśnie komunikowanie międzynarodowe[1].

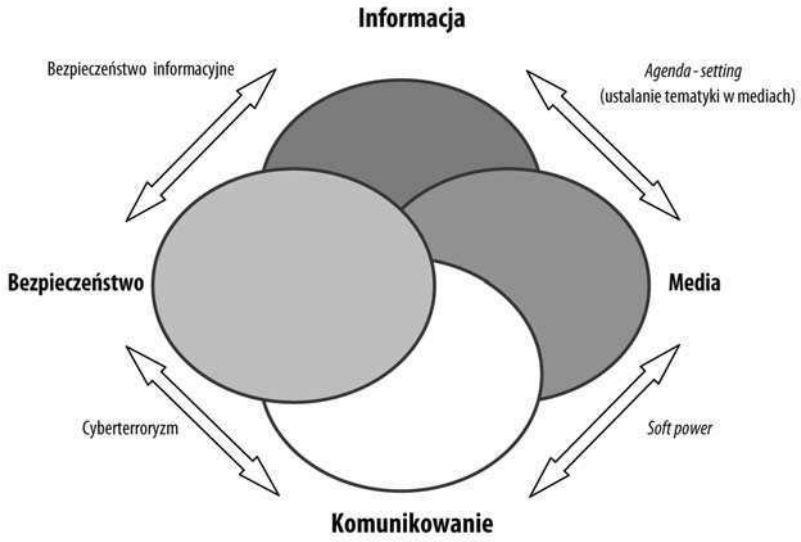
Omawiając problematykę komunikacji społecznej, należy zwrócić uwagę na szerokie znaczenie pojęcia *soft power* (inteligentnej władzy i siły). Termin ukuty przez

[1] Por. D.V.J. Bell, *Global Communications and Culture: Implications for International Security*, Centre for International and Strategic Studies, York University, „YCISS Working Paper" 1991, no 10.

amerykańskiego politologa Josepha Nye'a odnosi się nie tylko do bezpieczeństwa i stosunków międzynarodowych, lecz także do innych aspektów – kultury, przepływu wiedzy i modeli spędzania wolnego czasu. Wymiana komunikatów, wartości życiowych i idei powoduje homogenizację społeczeństw, czyli ich wzajemne upodabnianie się do siebie. Sfery te analizował właśnie Nye, rozpatrując *soft power* w kategoriach wpływów cywilizacyjnych i kulturowych Stanów Zjednoczonych.

Głównym celem opracowania jest udowodnienie tezy, że współczesne aspekty komunikowania, stymulując rozwój rządowych polityk informacyjnych, technik komunikacyjnych i mediów elektronicznych, wpływają na bezpieczeństwo międzynarodowe. Ze względu na złożoność tematu, poniższe studium wykorzystuje podejście interdyscyplinarne, łącząc zagadnienia z zakresu stosunków międzynarodowych i nauki o komunikowaniu. Badanie dokumentów oraz charakterystyka porównawcza odmiennych tradycji i koncepcji w przedmiotowej tematyce stanowią próbę wzmocnienia tej tezy.

Czy komunikowanie międzynarodowe może być obecnie uznane za element systemu bezpieczeństwa międzynarodowego? W celu uzyskania odpowiedzi na to pytanie należy wyjaśnić rolę mediów i przepływu informacji w stosunkach międzynarodowych na początku XXI wieku. Ważne jest w tym przypadku omówienie również takich zagadnień, jak bezpieczeństwo informacyjne i informatyczne.



Rysunek 1. Części składowe systemu bezpieczeństwa opartego na komunikowaniu międzynarodowym

Źródło: opracowanie własne.

Prezentowana analiza opiera się na relacji między kluczowymi pojęciami w badaniu komunikowania międzynarodowego w odniesieniu do współczesnych zagrożeń bezpieczeństwa: **informacja–media–komunikowanie–bezpieczeństwo**. Informacja jest treścią; media stanowią narzędzie, nośnik treści; komunikowanie jest procesem, natomiast bezpieczeństwo stanowi szerszy system, w którym komunikowanie odgrywa kluczową rolę. Wymienione części składowe występują w różnej konfiguracji i w różny sposób na siebie oddziałują. Informacja jest podstawowym odniesieniem względem pozostałych komponentów. Relacje między składowymi modelu dotyczą ważnych zjawisk i pojęć, które zostaną szczegółowo wyjaśnione w dalszej części tekstu: *agenda-setting* (ustalanie tematyki w mediach), *soft power*, bezpieczeństwo informacyjne i cyberterroryzm.

Komunikowanie międzynarodowe jest dziedziną rozwijającą się w bardzo dynamiczny sposób. W ubiegłym stuleciu, do końca zimnej wojny formą tego komunikowania była przede wszystkim propaganda wojenna. Źródła szeroko rozumianego komunikowania sięgają XIX wieku, gdy rozwijało się na gruncie wiedzy o komunikowaniu medialnym[2]. Wtedy to pojawiły się społeczności masowe i media masowe. W powszechnie dostępnych gazetach wykształciły się działy zagraniczne, dzięki którym obywatele otrzymali dostęp do bieżących informacji ze świata. W XX wieku zwiększył się udział mediów w integrowaniu narodowym ze względu na tragiczne doświadczenia obu wojen światowych. W miarę upływu czasu uwarunkowania polityczne i ekonomiczne doprowadziły do komunikacyjnej nierówności w skali międzynarodowej – rozwinięte kraje Północy zyskały przewagę nad zapóźnionym rozwojowo Południem. Dziś wyraźnie widać wpływy największych na świecie telewizji i periodyków, których zasięg jest geograficznie nieograniczony (np. CNN, BBC, Washington Post, Financial Times).

Komunikowanie międzynarodowe w wymiarze politycznym funkcjonuje jako pole oddziaływania państw w ramach polityki zagranicznej. Wyróżnia się jego cztery główne nurty: dyplomację publiczną, media międzynarodowe, zagraniczną politykę kulturalną oraz międzynarodowe public relations[3]. Ze względu na problematykę niniejszego opracowania omówione zostaną dwa pierwsze nurty.

Proces mediatyzacji polityki ciągle przybiera na sile. Media nie bez przyczyny nazywa się czwartą władzą, bo nie tylko zbierają i prezentują informacje, lecz także decydują o ich doborze, oceniają, interpretują wydarzenia, czasem tworząc pseudowydarzenia (*agenda-setting*). Związek płaszczyzny medialnej i politycznej jest dziś

[2] J. Mikułowski Pomorski, *Jak narody porozumiewają się ze sobą w komunikacji międzykulturowej i komunikowaniu medialnym*, Universitas, Kraków 2006, s. 65.

[3] Podział elementów komunikowania międzynarodowego zaproponowany przez S. Michalczyka w: *Komunikowanie polityczne. Teoretyczne aspekty procesu*, Wydawnictwo „Śląsk", Katowice 2005.

nierozerwalny, czego dalsze konsekwencje trudno przewidzieć. W kwestii wzajemnej relacji tych płaszczyzn dominują dwie teorie[4]. Pierwsza to koncepcja zależności polityki od mediów masowych. Zgodnie z jej założeniami, istnieje wysoka autonomia instytucji politycznych, a media pełnią wobec tych instytucji służebną rolę oraz stanowią zwierciadło opinii publicznej. Druga teoria opiera się na przeciwstawnym twierdzeniu, że to media zależne są od polityki. Według niej, większa jest rola autonomii mediów masowych, które wyrażają interesy społeczne, racjonalnie kształtują opinie społeczeństwa i pełnią funkcję kontrolną.

1.1. *Soft power*

Doktryna *soft power* (inteligentnej siły i władzy) wpisuje się w problematykę nowych sfer bezpieczeństwa międzynarodowego, ponieważ kładzie nacisk na różne przejawy działań pozamilitarnych w dobie globalizacji. Od czasów starożytnych głównym narzędziem rywalizacji państw była siła wojskowa, uzależniona od potencjału gospodarczego i ludnościowego. Są to właśnie atrybuty państwa zaliczane do tzw. *hard power*. Współcześnie państwa mają do dyspozycji zdywersyfikowane środki oddziaływania zewnętrznego, wśród których szczególnego znaczenia nabiera *soft power*. A. Blinken definiuje *soft power* jako uzyskiwanie od innych chęci zdobycia tych samych celów, których my chcemy i które wymagają zrozumienia sposobu oraz celu przekazywanych przez nas wiadomości i komunikatów[5].

Do najważniejszych elementów *soft power* należy informacja, dyplomacja publiczna, dyplomacja ekonomiczna oraz polityka kulturalna. Państwa były inicjatorami tworzenia instrumentów strategii komunikacyjnych między sobą, jednak wraz z rozwojem stosunków międzynarodowych, *soft power* stała się skutecznym narzędziem wykorzystywanym przez organizacje międzynarodowe, partie polityczne, a w ostatnich latach przez korporacje o zasięgu globalnym oraz lobbystów. Znawcy zagadnienia wskazują, że w odniesieniu do państw *soft power* różni się od *hard power* skalą oddziaływania na zewnątrz, która jest znacznie szersza w przypadku tej pierwszej siły. O ile bowiem konflikt zbrojny oraz interwencja ekonomiczna (np. sankcje gospodarcze wobec wrogiego państwa) działają niemal natychmiastowo, o tyle takie instrumenty *soft power*, jak np. dyplomacja publiczna

[4] W. Schulz, *Komunikacja polityczna, Koncepcje teoretyczne i wyniki badań empirycznych na temat mediów masowych w polityce*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006., s. 11.

[5] A.J. Blinken, *Winning the Word of Ideas*, w: A.T.J. Lennon, *The Battle for Hearts and Minds: Using the Soft Power to Undermine Terrorist Network*, MIT Press, Cambrige 2003, s. 289.

lub strategia informacyjna, w celu zbudowania pozytywnego wizerunku, przynoszą rezultaty w dłuższej perspektywie czasowej[6].

Największy wpływ na wzrost znaczenia *soft power* miały dwie wojny światowe XX wieku. Stany Zjednoczone, dzięki militarnemu zaangażowaniu, wyrosły po I wojnie światowej na mocarstwo globalne. Począwszy od prezydenta Woodrowa Wilsona kolejni przywódcy USA zarówno wzmacniali politykę propagandy ideologicznej, kulturowej oraz gospodarczej, jak i sprawnie wykorzystywali dyplomację publiczną w celu wzmocnienia swojej pozycji międzynarodowej oraz budowania sojuszy o zasięgu regionalnym i globalnym. W roku 1917 prezydent W. Wilson utworzył Komitet Informacji Publicznej (*Committee on Public Information*), którego głównym zadaniem było promowanie gospodarki i polityki amerykańskiej. Wraz z rozwojem telekomunikacji i radiofonii kolejne rządy tworzyły rozgłośnie radiowe szerzące propagandę i nieraz dezinformujące potencjalnych wrogów, nie tylko w swoich krajach, lecz także wśród innych narodów. W roku 1922 w Wielkiej Brytanii utworzono rozgłośnię BBC, która pod koniec lat dwudziestych nadawała już w większości języków europejskich, a nawet w języku arabskim. Do dziś BBC pozostaje jednym z najbardziej wpływowych mediów na świecie.

W XXI wieku głównym kanałem komunikacji i źródłem informacji jest internet – ze względu na niskie koszty obsługi i nieograniczony zasięg. Przejął on rolę, jaką wcześniej odgrywały największe gazety, stacje radiowe i telewizyjne. Jednak w odróżnieniu od Głosu Ameryki czy Radia Wolna Europa nie można stwierdzić, że jest jednoznacznie nacechowany ideologicznie. Internet jest nośnikiem idei, obrazem zmieniającego się świata, dzięki czemu użytkownicy mogą śledzić wydarzenia z odległych miejsc. Poszerza horyzonty, pokazuje różne modele życia i oddziałuje na różne sfery (rola kobiet, zmiany w świadomości).

Istotnym elementem *soft power* jest dyplomacja publiczna, na którą składają się trzy różne wymiary[7]. Pierwszym jest codzienna komunikacja, która odbywa się za pośrednictwem konferencji prasowych, komunikatów prasowych oraz wystąpień telewizyjnych (orędzia, przemówienia), a skierowana jest zarówno do obywateli, jak i do podmiotów zagranicznych. Dotyczy również polityki zagranicznej. Drugim składnikiem dyplomacji publicznej jest komunikacja strategiczna, do której należy informowanie o najważniejszych planach i agendach państwa oraz dezinformacja wrogich krajów i ugrupowań, w celu oddalenia rozmaitych zagrożeń i zabezpieczenia jego żywotnych interesów. Ponadto, w komunikacji strategicznej znaczącą rolę odgrywają kampanie reklamowe państw w zagranicznych środkach

[6] J.S. Nye, *Soft power: The Means to Success in Word Politics,* Public Affairs, New York, 2004, s. 2.
[7] Ibidem, s. 8–13.

masowego przekazu, dotyczące zwłaszcza walorów turystycznych, gospodarczych i inwestycyjnych. Ostatnią, ale nie mniej ważną niż dwie pierwsze, częścią składową dyplomacji publicznej jest rozwijanie trwałych i wieloletnich stosunków z kluczowymi podmiotami przez prowadzenie polityki wobec studentów czy biznesmenów zagranicznych. Wszystko to w celu budowania pozytywnego wizerunku państwa zapraszającego.

Reasumując, pojęcia inteligentnej siły, komunikacji społecznej i dyplomacji publicznej w pewnym zakresie nakładają się na siebie, a *soft power* w centrum zainteresowania decydentów politycznych stawia działania o charakterze pozamilitarnym, w znacznym stopniu opierające się na komunikowaniu międzynarodowym.

1.2. Odmienne tradycje komunikowania na przykładzie Unii Europejskiej i Chin

W zależności od regionu świata, ustrojów politycznych i tradycji – występują różne formy komunikowania. Polityka informacyjna i komunikacyjna państw europejskich i Unii Europejskiej kształtuje się w sposób zdecydowanie odmienny niż na przykład w Azji. Zgodnie z klasyfikacją instytucjonalistów, Chiny trudno skategoryzować jako ustrój demokratyczny (niedostatki w pluralizmie politycznym i prawach człowieka) czy pełnowartościowy system kapitalistyczno-wolnorynkowy (szeroki zakres kontroli państwa nad gospodarką). Z różnych tradycji i kultur wynika charakterystyczne dla danego państwa podejście do komunikacji społecznej – zarówno wewnętrznej, jak i międzynarodowej.

Przepływ informacji w krajach autorytarnych i *quasi*-demokratycznych jest zdecydowanie bardziej ograniczony niż w krajach demokratycznych. Wskazują na to takie czynniki, jak ograniczony dostęp do zagranicznych stacji telewizyjnych, internetu (w tym komunikatorów internetowych), jak i telefonów komórkowych. Przykładów cenzurowania audycji telewizyjnych i stron internetowych w Chinach jest bardzo wiele. Skutkują one ograniczeniami w przepływie informacji i zaburzają komunikowanie międzynarodowe. W państwach demokratycznych ograniczenia w dostępie do informacji mają inny, z reguły wewnętrzny charakter i służą głównie ochronie danych wrażliwych (danych osobowych). Poniżej przedstawione zostało krótkie omówienie dwóch tradycji (form) komunikowania międzynarodowego – europejski i chiński – obrazujące skrajnie różne podejścia w omawianej problematyce.

Formuła komunikowania międzynarodowego w Europie została wypracowana w toku procesu integracji europejskiej. W UE polityka komunikacyjna ma charakter dialogu, opierającego się na wymianie przekazów między obywatelami,

instytucjami i innymi podmiotami. Polityka komunikacyjna obejmuje całość działań i zadań komunikacyjnych, podejmowanych przez instytucje publiczne[8]. Polegają one na zarządzaniu obiegiem informacji w celu kreowania wizerunku instytucji na zewnątrz i wewnątrz. Polityka komunikacyjna polega na zarządzaniu w aspektach: wizerunku, informacji i mediów. Instytucja kontroluje informacje, jakie od niej wychodzą, buduje odpowiednie kontakty z mediami oraz publicznością wewnętrzną i zewnętrzną. Swoją politykę w tych wymiarach kształtuje właśnie Unia Europejska.

Wyróżnia się trzy ogólne modele komunikowania z odbiorcami: propagandowy, dialogowy i marketingowy[9]. Ten drugi wydaje się korzystny z punktu widzenia interesów społecznych. Jego wartością nadrzędną jest możliwość budowania konsensu i optymalne realizowanie interesów społecznych. Propagandowy mniej liczy się z publicznością, podobnie jak marketingowy, który wykorzystuje marketing polityczny, nazywany niekiedy socjotechniką. W przypadku Unii Europejskiej zdecydowanie dominuje model dialogowy, który koncentruje się na debacie publicznej i racjonalnej wymianie argumentów.

Z kolei chińska polityka komunikacyjna i informacyjna stanowi swoisty paradoks oraz kontrapunkt wobec polityki UE w omawianym zakresie. Z jednej strony boom gospodarczy przyczynił się do potężnego rozwoju w dziedzinie technologii i narzędzi komunikacji (produkcja i eksport technologii). Zgodnie z danymi OECD, w 2007 r. eksport Chin w sektorze technologii informacyjnych i telekomunikacyjnych był wart 260 mld dol., czyli więcej niż łączy eksport UE–15 i Stanów Zjednoczonych[10]. Z drugiej strony, do dziś poważnym problemem Chin jest cenzura internetu i telewizji.

Komunistyczna Partia Chin (CPC) od wielu lat kontroluje obieg informacji w mediach tradycyjnych (prasa, radio, telewizja). Internet z reguły trudniej jest cenzurować, ale mimo to w znacznym stopniu się to udaje. Służby stanowiące cybercenzurę i cyberpolicję liczą dziesiątki tysięcy ludzi. Wśród organów władzy państwowej nadzorujących internet są m.in. Ministerstwo Bezpieczeństwa Państwowego oraz Ministerstwo Przemysłu i Technologii Informatycznych[11]. Wyszukiwarki internetowe, blogi, media społecznościowe, komunikatory czy zagraniczne serwisy podlegają urzędniczej akceptacji. Nadzoruje się zarówno serwery, jak i numery IP użytkowników. Wszelkie formy komunikacji elektronicznej (email, SMS, komunikatory)

[8] B. Dobek-Ostrowska, *Komunikowanie polityczne i publiczne*, WN PWN, Warszawa 2006, s. 355.

[9] Ibidem, s. 357–358.

[10] OECD Information Technology Outlook 2008, *Information and Communications Technologies* (Polish version), http://www.oecd.org/dataoecd/52/31/42206408.pdf, s. 4.

[11] Istnieją inne organy władzy różnego szczebla, które zajmują się kontrolą Internetu i przepływu informacji. Wszystkie wymienia raport organizacji Reporterzy bez Granic: *China, Journey to the hart of Internet Censorship*, Investigative report, 2007.

podlegają kontroli, a część informacji krajowych i zagranicznych w ogóle nie dociera do opinii publicznej.

Komunikowanie treści „wolnościowych", zwłaszcza w dziedzinie ochrony praw człowieka i wolności osobistych, uznawane jest przez komunistyczne władze Chin za zagrożenie. Stosuje się zarówno kary pieniężne, jak i dotkliwe kary pozbawienia wolności. Porównanie polityki komunikacyjnej Chin i Unii Europejskiej pokazuje zatem dwa bieguny w dziedzinie komunikowania międzynarodowego: otwartości i transparentności z jednej strony, a kontroli i filtrowania treści z drugiej.

1.3. Wpływ rewolucji informacyjnej na bezpieczeństwo międzynarodowe

Powszechny dostęp do internetu i zaawansowanych technologii w istotny sposób zmienił charakter stosunków międzynarodowych i przedefiniował problemy suwerenności i bezpieczeństwa[12]. Dzięki rewolucji informacyjnej zdecydowana większość obywateli państw rozwiniętych oraz duże grupy społeczne w państwach rozwijających się zyskały dostęp do internetu. Łatwość, powszechność i szybkość wymiany danych, listów czy dokumentów zmieniły świadomość społeczną.

Jakie znaczenie dla bezpieczeństwa międzynarodowego ma rewolucja informacyjna? Szczególnie duże w odniesieniu do dwóch typów podmiotów stosunków międzynarodowych:

1) reżimów autorytarnych, które czują się zagrożone swobodną wymianą komunikatów i danych;
2) przybierających na sile organizacji pozarządowych (NGO), których liczba w drugiej połowie XX wieku wzrosła z 38 do 275[13].

Jeśli chodzi o tę pierwszą grupę podmiotów, dobry przykład może stanowić wcześniej opisana polityka informacyjna Chińskiej Republiki Ludowej. Natomiast ilustracją doniosłej roli drugiej grupy podmiotów są próby globalnej instytucjonalizacji norm dotyczących praw człowieka, korupcji czy ekologii (Amnesty International, Human Rights Watch, Greenpeace). Wiele przedsięwzięć i projektów NGOs jest skutecznych właśnie ze względu na wykorzystywanie narzędzi komunikacji.

[12] Wielu ekspertów w tej dziedzinie uważa, że Internet stanowi wyzwanie dla tradycyjnie pojmowanej suwerenności państwa. Jednym z ciekawych i ważnych przejawów ideologii Internetu definiowanego jako nieskrępowana wspólnota jednostek, uwolnionych spod dominacji struktur władzy, jest znany dokument J.P. Barlowa z 1996 r. *Deklaracja Niepodległości Cyberprzestrzeni*. Tekst angielski dostępny na stronie: https://projects.eff.org/~barlow/Declaration-Final.html.

[13] Dane dotyczą lat 1950–1990. Za: L. Porębski, *Rewolucja informacyjna a suwerenność państwa. Lekcje dla Polski*, Biblioteka Główna AGH, Kraków 2003 (dokument elektroniczny).

Do tych skutecznych projektów można zaliczyć m.in. debatę nad globalnym ociepleniem w Kyoto (1997) czy organizację World Economic Forum w Davos.

Z rewolucją informacyjną wiążą się trzy aspekty informacji, które wyszczególnia J. Nye[14]:

1) wymiana takich danych, jak nowe wiadomości czy informacje statystyczne;
2) przewaga informacyjna w warunkach konkurencji;
3) informacja strategiczna, czyli wiedza o planach przeciwnika.

Wszystkie te aspekty dotyczą też sfery bezpieczeństwa. Na Zachodzie podstawowy problem polega na nadmiarze informacji lub inaczej chaosie informacyjnym, w którym trudno zhierarchizować wagę komunikatów i danych oraz zweryfikować wiarygodność źródeł. Ta wiarygodność ma zresztą zasadnicze znaczenie w kontekście *soft power*[15]. Siła państwa korzystającego z *soft power* polega na władzy ideologicznej i kulturalnej, którą buduje się na wartościach podzielanych przez ogół odbiorców, dostępie do różnorodnych kanałów komunikacji oraz wiarygodnym wizerunku w polityce wewnętrznej i zagranicznej.

1.4. Bezpieczeństwo informacyjne i informatyczne

Postępująca globalizacja, intensyfikacja kontaktów międzyludzkich oraz rozwój komunikowania umiędzynarodowiły sferę bezpieczeństwa wewnętrznego. W związku z tym coraz większy zakres tej sfery wychodzi poza domenę państwa[16]. Rodzi to określone konsekwencje dla przepływu informacji i ochrony pewnych typów danych. Informacja jest zasobem strategicznym w ujęciu globalnym i regionalnym, zarówno dla podmiotów prywatnych, jak i instytucji publicznych (cywilnych i wojskowych). Dlatego zabezpieczenie informacji, zwłaszcza tych o znaczeniu strategicznym, staje się we współczesnym świecie jednym z najbardziej żywotnych interesów wymienionych podmiotów[17]. Bezpieczeństwo informacyjne oznacza nie tylko troskę o przekazywanie prawdziwych danych między określonymi podmiotami, lecz także przeciwdziałanie zniekształceniom, modyfikacjom danych, zwłaszcza tych szczególnie wrażliwych oraz istotnych dla państwa, narodu czy też podmiotu gospodarczego. Bezpieczeństwo informacyjne jest warunkiem *sine qua non* bezpieczeństwa narodowego w szerokim rozumieniu tego pojęcia. Od tego zależy

[14] J.S. Nye, Jr., *The Information Revolution and American Soft Power*, „Asia-Pacific Review" 2002, vol. 9, no 1, s. 68.

[15] Ibidem, s. 69

[16] K. Żukrowska, *Bezpieczeństwo międzynarodowe. Teoria i praktyka*, SGH, Warszawa 2005, s.5.

[17] A. Wisz, *Bezpieczeństwo informacji w wojskowych sieciach teleinformatycznych*, Biuro Bezpieczeństwa Narodowego, www.bbn.gov.pl/download.php?s=1&id=1002, s.70 (dokument elektroniczny).

stabilny rozwój gospodarczy i społeczny oraz właściwe funkcjonowanie struktur państwowych.

Brak informacji, informacja nieprawdziwa, celowo zmieniona lub przechwycona przez podmioty niepożądane – wszystko to może grozić destabilizacją, kryzysem czy wręcz chaosem. Wystarczy wyobrazić sobie chaos na giełdzie papierów wartościowych o znaczeniu globalnym, wywołany atakiem hakerów na sieć informatyczną. Konsekwencje ekonomiczne takiego zdarzenia byłyby brzemienne w skutkach nie tylko w czasie paraliżu giełdy, ale miałyby zapewne charakter długofalowy i wielowymiarowy. Najbardziej zagrożona jest tzw. infrastruktura strategiczna państwa – urzędy, biurowce, dworce i lotniska, centra logistyczne, sieci teleinformatyczne, sektor energetyczny, ważne pomieszczenia i urządzenia cywilne i wojskowe. Natomiast w odniesieniu do bezpieczeństwa informacyjnego państwa punktami podwyższonego ryzyka są strony internetowe instytucji rządowych oraz systemy przekazywania informacji i danych opatrzonych klauzulami tajności.

Wraz z rozwojem form komunikowania, pojawiło się niezwykle poważne zagrożenie w postaci cyberterroryzmu (akt terroru dokonywany za pomocą technologii informacyjnej)[18]. Instytucje państwowe funkcjonują w coraz bardziej skomplikowanych, wielowymiarowych środowiskach o zasięgu lokalnym, regionalnym i globalnym, a co za tym idzie stają się posiadaczami coraz większej ilości danych. Stąd też zauważalny jest wzrost zapotrzebowania na nowe, bardziej wydajne i – co najważniejsze – bezpieczne systemy kumulacji, przetwarzania i przechowywania baz danych. I właśnie te systemy stały się przedmiotem ataków terrorystów.

Zgodnie z uznawaną przez fachowców definicją M. Pollita „cyberterroryzm to przemyślany, politycznie umotywowany atak, skierowany przeciw informacjom, systemom komputerowym, programom i danym, który prowadzi do oddziaływania na niemilitarne cele, przeprowadzony przez grupy narodowościowe lub przez tajnych agentów”[19]. Cyberterroryzm określany jest też jako wykorzystywanie sieci teleinformatycznych oraz globalnej sieci przez organizacje terrorystyczne lub ruchy narodowo-wyzwoleńcze (powstańcze) do takich zadań, jak: propaganda, rekrutacja *on-line*, komunikowanie się, mobilizacja sił, zbieranie informacji o potencjalnych celach ataku, planowanie i koordynacja akcji oraz szeroko pojęta dezinformacja

[18] Cyberterrorzym lat osiemdziesiątych ubiegłego stulecia dotknął głównie Stany Zjednoczone oraz Kanadę, o globalnym charakterze tego zjawiska można mówić od początku lat dziewięćdziesiątych XX wieku.

[19] M. Pollit, *Cyberterrorism, Fact or Fancy*?, Computer Fraud & Security, Waszyngton 1998, Issue 2, http://www.cs.georgetown.edu/~denning/infosec/pollitt.html.

i walka o charakterze psychologicznym. Cyberatak może stanowić część większej akcji polityczno-militarnej lub samodzielny, jedno- lub wielorazowy atak[20].

Z powyższej definicji wynika, że bezpieczeństwo teleinformatyczne jest żywotnym interesem każdego współczesnego państwa. Jak podkreślają znawcy problematyki, niepokojącym zjawiskiem jest lekceważenie przez rządy i służby odpowiedzialne za obronę państwa możliwości ataków cyberterrorystycznych, które w porównaniu z „tradycyjnym" (konwencjonalnym) terroryzmem bywają o wiele bardziej brzemienne w skutkach i – co więcej – są z reguły prostsze do przeprowadzenia[21]. Dzieje się tak ze względu na relatywnie niskie koszty działalności cyberterrorystów, otwarcie granic terytorialnych w różnych regionach świata, względną anonimowość internetu oraz stosunkowo niskie ryzyko zdemaskowania ataku.

Możliwość przeprowadzenia ataku terrorystycznego jest bardzo realna dla wielu państw rozwiniętych i rozwijających się. Eksperci przewidują, że w nieodległej przyszłości cyberterroryzm stanie się główną formą zagrożenia. W najnowszej historii doszło do kilku spektakularnych ataków. W roku 2000 celem cyberterrorystów z Bałkanów stała się infrastruktura teleinformatyczna państw NATO, co wywołało paraliż komunikacyjny między sojusznikami. Władze organizacji szybko wyciągnęły wnioski z tego zdarzenia. W roku 2002 na szczycie NATO w Pradze zainicjowano budowę Programu Obrony Cybernetycznej – *The Cyber Defense Program* i rozwoju Zdolności Reagowania na Incydenty Komputerowe – *The Computer Incident Response Capability.* Kolejne ataki miały miejsce w 2007 r. w Estonii, w 2008 r. na Litwie oraz w 2008 r. w Gruzji. Efektem ataków na państwa bałtyckie było podpisanie memorandum o utworzeniu w Tallinie Centrum Kompetencyjnego ds. Obrony Teleinformatycznej – *The Concept for Cooperative Cyber Defense Centre of Excellence* (CCDCOE). Mimo że CCDCOE nie jest jednostką operacyjną Sojuszu Północnoatlantyckiego, ma jego akredytację, ściśle współpracuje z agencjami rządowymi państw członkowskich i wspiera ich działania prewencyjno-obronne w obszarze zagrożeń cyberterrorystycznych[22].

Również Polska rozwija politykę bezpieczeństwa teleinformatycznego. W roku 2008 powstał rządowy program ochrony cyberprzestrzeni na lata 2009–2011, którego zadaniem jest identyfikacja oraz zapobieganie zagrożeniom cybernetycznym[23]. W kraju istnieje system bezpieczeństwa oparty na takich instytucjach, jak Mini-

[20] L. Lichocki, *Cyberterrorzym państwowy i niepaństwowy – początki, formy i skutki,* Uniwersytet Gdański, Gdańsk 2009, http://strona.aon.edu.pl/files/csikgw/publikacje/20090519_04.pdf.

[21] Ibidem.

[22] Portal Ministerstwa Spraw Zagranicznych RP, http://www.msz.gov.pl/Cyberterroryzm,30058.html.

[23] Założenia Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009–2011. źródło: http://www.cert.gov.pl/portal/cer/30/23/Rzadowy_program_ochrony_cyberprzestrzeni_RP_na_lata_20092011__zalozenia.html.

sterstwo Spraw Wewnętrznych i Administracji (MSWiA), Agencja Bezpieczeństwa Wewnętrznego (ABW), Ministerstwo Obrony Narodowej (MON) oraz Służba Kontrwywiadu Wojskowego (SKW)[24]. Współdziałają one w ramach specjalnych zespołów:
1) CERT.GOV.PL – ochraniający systemy instytucji rządowych;
2) Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe – działające pod nadzorem MON[25].

Współpracują one z podobnymi zespołami państw sojuszniczych NATO w wymiarze dwustronnym i wielostronnym. Państwowe instytucje współpracują również z podmiotami prywatnymi w celu zapewnienia większego bezpieczeństwa infrastrukturze krytycznej naszego kraju.

Powyższe rozważania pokazują znaczenie bezpieczeństwa informacyjnego i teleinformatycznego dla współczesnego państwa w erze globalizacji zagrożeń. Zapewnienie tego bezpieczeństwa gwarantuje stabilność wielu dziedzin życia w kraju, zwłaszcza gospodarki, obronności oraz administrowania państwem. Proces rozbudowy systemów ochrony informacji oraz innych danych nabiera tempa nie tylko w skali jednego państwa, ale również w wymiarze regionalnym oraz globalnym. Stanowi to emanację dynamiki rozwoju stosunków międzynarodowych oraz wzrost znaczenia organizacji międzynarodowych o różnym zasięgu geograficznym i profilu funkcjonowania (militarny, gospodarczy, społeczny, polityczny). Zapewnienie bezpieczeństwa wymaga współdziałania różnych instytucji na szczeblu krajowym oraz kooperacji między państwami na szczeblu międzynarodowym.

Podsumowanie

Zaprezentowana we wstępie struktura współzależności poszczególnych części składowych systemu bezpieczeństwa międzynarodowego, opartego na komunikowaniu, wydaje się mieć uzasadnienie w rzeczywistości (rys. 1). W omawianym kontekście komunikowanie międzynarodowe zarówno w ujęciu teoretycznym (*soft power*), jak i praktycznym (cyberterroryzm, media) wpływa w niebagatelny sposób na współczesny wymiar bezpieczeństwa międzynarodowego. *Soft power* Nye'a bezpośrednio odnosi się do roli komunikowania w budowaniu ładu i bezpieczeństwa międzynarodowego. Kładzie nacisk na pozamilitarne aspekty bezpieczeństwa, m.in. dyplomację publiczną uważaną za przejaw komunikowania międzynarodowego.

[24] Szczegóły struktury polskiego systemu bezpieczeństwa opisują M. Madej, M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa,* PISM, Warszawa 2009.

[25] Więcej informacji na stronie internetowej Zespołu: www.cert.gov.pl.

Porównanie odmiennych tradycji komunikowania na świecie dostarcza z kolei materiału do rozważań nad jego rolą w budowaniu bezpieczeństwa. Różnice w prowadzeniu polityki komunikacyjnej w Chinach i w Unii Europejskiej wskazują spektrum rozwiązań charakterystycznych dla systemów demokratycznych i autorytarnych. Mimo że trudno jednoznacznie zestawić politykę organizacji z polityką państwa, to widać dwa różne modele komunikacji instytucji/władz z publicznością wewnętrzną i zewnętrzną. W reżimach demokratycznych polityka otwartości i transparentności rodzi konsekwencje związane z niekontrolowanym obiegiem informacji i łatwością dostępu do różnych danych (nadmiar informacji). Z kolei w reżimach zamkniętych głównym problemem jest ograniczanie dostępu do informacji i naruszenie „wolności komunikacji" (niedosyt informacji).

Rozwój nowych, powszechnie dostępnych technologii, wpłynął z kolei na pojawienie się nieznanych wcześniej zagrożeń, takich jak cyberterroryzm. Trzeba jednak podkreślić, że i w tej newralgicznej dziedzinie państwa ze sobą współpracują, co niejako automatycznie ogranicza partykularne interesy i środki przeznaczane na obronę. Osobnym problemem jest natomiast brak międzynarodowej koordynacji między poszczególnymi sektorami bezpieczeństwa: ekonomicznym, militarnym, cybernetycznym itp. (brak spójności działań i środków).

2. Globalne systemy nawigacji satelitarnej

Od najdawniejszych czasów człowiek próbuje znaleźć sposób, by jak najdokładniej wyznaczyć położenie obiektów. Jednak dopiero przełom lat sześćdziesiątych i siedemdziesiątych ubiegłego stulecia przyniósł nowinkę technologiczną, która doprowadziła do stworzenia satelitarnego systemu wyznaczania pozycji, będącego najpełniejszym rozwiązaniem problemu lokalizacji oraz orientacji przestrzennej obiektów.

Celem opracowania jest zbadanie, w jaki sposób technologie nawigacji satelitarnej mogą wpłynąć na system bezpieczeństwa międzynarodowego. Rozwój coraz bardziej zaawansowanych technologii nawigacji satelitarnej doprowadził do wzrostu intensywności rywalizacji w przestrzeni kosmicznej. Kluczowe wydaje się znalezienie odpowiedzi na pytanie, którym krajom udało się rozwinąć system nawigacji satelitarnej na tyle, by być globalnym graczem w tej dziedzinie.

2.1. Co to jest GNSS?

Zgodnie z terminologią stosowaną przez UE, **GNSS** to akronim od nazwy *Global Navigation Satelite System*, co oznacza Globalny System Nawigacji Satelitarnej przeznaczony do szybkiego i dokładnego wyznaczania współrzędnych określających pozycję odbiornika w globalnym systemie odniesienia.

Pierwszym systemem GNSS był GNSS–1, który opierał się na amerykańskim GPS oraz rosyjskim GLONASS wspomaganych przez systemy cywilne EGNOS, WAAS oraz MSAS, zaprojektowane, by dostarczyć użytkownikowi wystarczająco niezależnego monitoringu całego systemu. Z kolei, pod nazwą GNSS–2 rozumie się obejmujący cały świat cywilny system nawigacji satelitarnej, kontrolowany i zarządzany międzynarodowo, który spełnia wymagania użytkowników wszystkich kategorii, dotyczące określenia pozycji, prędkości oraz czasu, a ponadto jest w stanie dostarczyć jedyne dane nawigacyjne dla pewnych aplikacji[26].

2.2. Zasady działania systemów nawigacji satelitarnej

Nawigacja satelitarna pozwala określić położenie zarówno nieruchomych punktów, jak i przemieszczających się obiektów (wraz z parametrami określającymi ich ruch) na powierzchni Ziemi, bez względu na pogodę oraz porę doby.

Metoda pomiaru i działanie nawigacji satelitarnej GNSS są zbliżone. Sygnały wysyłane przez satelity odbierane są przez odbiorniki na ziemi za pomocą miniaturowych anten płaskich, przez nieograniczoną liczbę użytkowników w jednym czasie. Struktura sygnału satelitarnego została skonstruowana w taki sposób, by odbierający sygnał odbiornik mógł wyznaczyć czas, jaki upłynął od momentu wysłania sygnału do momentu jego odbioru, i określić na tej podstawie odległość między użytkownikiem a satelitą. Jednocześnie dane nawigacyjne[27] wyznaczane przez naziemne centra monitorujące służą odbiornikowi do określenia położenia satelity w momencie nadawania sygnału. Mając odległość od satelitów oraz ich współrzędne, odbiornik może określić swoje położenie. Warunki atmosferyczne nie mają wpływu na funkcjonowanie urządzeń oraz dokładność wyznaczanej pozycji. Jedynym ograniczeniem dla

[26] *Komunikat Komisji do Rady i Parlamentu Europejskiego: Towards a Trans-European Positioning and Navigation Network: including A European Strategy for Global Navigation Satellite Systems (GNSS)*, COM(1998) 29 final, Brussels 21.01.1998, s. 39.

[27] Parametry satelitarnych skal czasu i parametry orbit satelitarnych przesyłane są na pokłady satelitów celem dalszej retransmisji do użytkowników systemu. Najnowsza generacja satelitów GPS – blok IIR, zaprojektowana została tak, by mogła przejąć część funkcji stacji naziemnych. Przewiduje się, iż w przyszłości konstelacja satelitów GPS będzie mogła funkcjonować autonomicznie przez okres kilku miesięcy bez istotnego pogorszenia jakości serwisu.

funkcjonowania systemów jest ukształtowanie terenu (góry, doliny, wąwozy, itp.) oraz jego naniesienia (budynki, różnego rodzaju konstrukcje itp.). Przeszkody tego rodzaju uniemożliwiają dotarcie sygnałów w linii prostej do odbiornika.

Każdy GNSS można podzielić na 3 segmenty: kosmiczny, kontrolny i użytkowników. Segment kosmiczny (zwany też orbitalnym) to konstelacja satelitów na określonych orbitach, transmitujących jeden lub kilka sygnałów nawigacyjnych, obejmujących swoim zasięgiem całą kulę ziemską. Każdy system posiada sobie właściwą konstelację satelitów, które różnią się od siebie wieloma parametrami, m.in. liczbą obiektów, typem kodowania, wysokością orbitalną, czasem obiegu orbity oraz naturalnie częstotliwością[28]. Porównując systemy (tab. 1), które osiągnęły już swoją operacyjność, oraz te, które w najbliższych latach mają ją osiągnąć, należy pamiętać, że niezbędnym minimum dla spełnienia wymogu bycia globalnym systemem nawigacji satelitarnej jest konstelacja co najmniej 24 satelitów.

Tabela 1. Globalne Systemy Nawigacji Satelitarnej na świcie

Nazwa	Kraj	Kodowanie	Wysokość orbitalna, czas okrążenia, nachylenie orbity	Liczba satelitów	Częstotliwość[a]	Status
GPS	USA	CDMA	20 200 km 11 h 58 min. 55°	24 (32)	Sygnał L1: 1.57542 GHz sygnał L2: 1.2276 GHz sygnał L5: 1.1765 GHz	Operacyjny
GLONASS	Rosja	FDMA/ CDMA	19 100 km 11 h 15 min. 64.8°	26 (w tym 2 zapasowe)[b]	Sygnał L1: 1.6020 – 1.6093 GHz (do 2005) i 1.5981 – 1.6054 GHz po 2005 sygnał L2: 1.2460 – 1.2561 GHz	Operacyjny z pewnymi ograniczeniami
Galileo	UE	CDMA	23 616 km 14 h 56°	Planowane - 30 (w tym 27 aktywnych, 3 zapasowe)	Pasma E5a i E5b 1.164–1.215 GHz pasmo E6 1.215–1.300 GHz pasmo E2-L1-E11 1.559–1.592 GHz	Przygotowania (2 testowe satelity na orbicie)
COMPASS[c]	Chiny	CDMA	21 000 km 12 h 55°	Planowane – 35	B1: 1.5591~1.5918 GHz B2: 1.1662~1.2174 GHz B3: 1.2506~1.2864 GHz	4 satelity osiągnęły operacyjność

[a] Na podstawie prezentacji Jarosława Bosy *Globalne Satelitarne Systemy Nawigacyjne GNSS*, Projekt „Wiosna w geodezji i kartografii", Poznań, 14 maja 2009 r.; [b] na podstawie oficjalnej strony Federalnej Agencji Kosmicznej: http://www.glonass-ianc.rsa.ru/pls/htmldb (14.09.2010 r.); [c] na podstawie strony www.astronautix.com/craft/beidou (1.09.2010 r.).

Źródło: opracowanie własne na podstawie: UN Office for Outer Space Affairs, *Current and planned global and regional navigation satellite systems*, New York 2010; J. Bosy *Globalne Satelitarne Systemy Nawigacyjne GNSS*, Projekt „Wiosna w geodezji i kartografii", Poznań, 14 maja 2009 r.

[28] Choć częstotliwości mogą się pokrywać – przypadek Chin i UE.

Przykładowo, segment kosmiczny **GPS** składa się z 24 (32) satelitów umieszczonych na sześciu płaszczyznach orbitalnych, po 4 (5) satelity w płaszczyźnie, na wysokości 20 200 km. Zwiększona liczba satelitów ujęta w nawiasach uwzględnia aktywne satelity rezerwowe, które pozwalają na szybkie zastąpienie w przypadku uszkodzenia, bądź awarii jednego z satelitów operacyjnych. Czas obiegu jednego satelity wokół Ziemi jest równy połowie doby gwiazdowej, czyli wynosi ok. 11 h 58 min. (dokładnie 11 h 57 min 58,3 s.). Stąd wynika, że w ciągu doby jeden satelita systemu GPS okrąża Ziemię dwukrotnie z prędkością ok. 3,87 km/s, tj. 13 932 km/h.[29]. Czas, jaki satelita pozostaje nad horyzontem nieprzemieszczającego się użytkownika, wynosi w przybliżeniu 5 godzin. **GLONASS** składa się z 24 obiektów rozmieszczonych na trzech płaszczyznach orbitalnych na wysokości ok. 19 100 km – po 8 satelitów na każdej. Na początku 1996 r. udało się skompletować pełny zestaw satelitów, który był dostępny tylko przez ok. 40 dni. Satelita obiega całą orbitę w ciągu 11 godzin i 15 minut. Oznacza to, że obserwator na Ziemi zaobserwuje tę samą konstelację satelitów co 5 dni[30]. W związku z tym, że ruch satelitów nie jest zsynchronizowany z okresem obrotu Ziemi, jak w przypadku **GPS**, ilość manewrów orbitalnych potrzebnych do utrzymania stałej konfiguracji jest mniejsza. Satelity GPS rozmieszczone są w taki sposób, by co najmniej 5 z nich było widocznych z każdego punktu na Ziemi w konfiguracji zapewniającej prawidłowe wyznaczenie pozycji.

Na segment kosmiczny systemu **COMPASS** składa się: 5 satelitów geostacjonarnych oraz 30 satelitów niegeostacjonarnych, umieszczonych na trzech płaszczyznach orbitalnych[31]. **Galileo** zakłada umieszczenie 30 satelitów w konstelacji (po 9 + 1 satelitów na każdej z trzech płaszczyzn orbitalnych)[32].

Segment kontrolny, zwany także naziemnym, stanowi sieć stacji naziemnych, zapewniających stałą kontrolę i łączność z satelitami. Segment ten odpowiada przede wszystkim za nadzór nad prawidłową pracą poszczególnych GNSS (w pewnych przypadkach może dokonywać odpowiednich korekt).

Przepływ informacji między satelitą a poszczególnymi stacjami segmentu kontrolnego (między dwoma wymienionymi wyżej segmentami) przypomina działanie swego rodzaju aktywnej sieci geodezyjnej. Zespół satelitów przesyła informacje o swoim położeniu do stacji śledzących, które odbierają te same sygnały, co użytkownicy wojskowi i cywilni. Następnie stacje śledzące przesyłają uzyskane dane do głównych stacji kontrolnych. Stacje główne, odpowiadając za korektę parametrów

[29] Strona internetowa: http://nawgeo.com/index.php?q=node/2 (16.09.2010 r.).
[30] Strony Federalnej Agencji Kosmicznej: http://www.glonass-ianc.rsa.ru/pls/htmldb (14.09.2010 r.).
[31] Strona Federalnej Agencji Kosmicznej: http://www.glonass-ianc.rsa.ru/pls/htmldb (14.09.2010 r.).
[32] Strona internetowa: http://ec.europa.eu/enterprise/policies/satnav/galileo/index_en.htm#h2–4 (17.09.2010 r.).

ruchu satelitów oraz ich zegarów, dokonują ewentualnych poprawek przy uwzględnieniu czynników działających na każdego satelitę. Transmisja przewidywanych poprawek parametrów orbit każdego satelity realizowana jest przez stacje nadawcze.

Ostatnim segmentem jest segment użytkownika, który obejmuje wszystkie odbiorniki satelitarne, za pomocą których ich użytkownicy mogą wyznaczyć swoją pozycję na podstawie pomiaru odległości w stosunku do przynajmniej 3 satelitów. W związku z wyodrębnieniem się dwóch grup użytkowników: militarnych oraz cywilnych, istnieją dwa poziomy dostępu – odpowiednio: precyzyjny serwis pozycyjny oraz standardowy serwis pozycyjny. Warto przypomnieć, że **GPS**, **GLONASS** oraz **COMPASS** (w początkowej fazie jako Beidou) były systemami stworzonymi przez wojsko i początkowo używanymi wyłącznie w celach militarnych (w przeciwieństwie do cywilnego projektu Galileo). Stopniowo jednak udostępniano sygnały także użytkownikom cywilnym. W przypadku **GPS** nastąpiło to w styczniu 1984 r. (system stał się operacyjny w 1978 r.), w przypadku **GLONASS** – dopiero w 2007 r.[33] System **COMPASS** przewiduje udostępnienie użytkownikom cywilnym sygnału już od momentu osiągnięcia operacyjności, nie podano jednak, na jakim poziomie: regionalnym czy globalnym. System **Galileo** z założenia jest projektem cywilnym, co oznacza, że uruchomienie systemu będzie tożsame z udostępnieniem sygnału użytkownikom cywilnym. Pierwotnie miało to nastąpić już w 2008 r., następnie przełożono uruchomienie systemu na 2010 r., a obecnie pełna zdolność operacyjna spodziewana jest w 2013 r.

Dlaczego podział na użytkowników cywilnych i wojskowych jest taki ważny? Obydwie grupy użytkowników otrzymują sygnały o różnych parametrach. Dla użytkowników wojskowych i innych grup uprzywilejowanych (tzw. autoryzowanych użytkowników) przeznaczony jest precyzyjny serwis pozycyjny o znacznie wyższej odporności na zakłócenia celowe i próby przekłamań oraz wyższej dokładności w stosunku do standardowego serwisu pozycyjnego. Standardowy serwis, dostępny dla wszystkich użytkowników, może być celowo ograniczany przez pogorszenie jakości sygnału. Na przykład standardowy serwis **GPS** aż do 2000 r. był zakłócany przez sztuczny błąd – system Selektywnej Dostępności (*Selective Availability* – SA), co dawało dokładność do 100 m. Po wyłączeniu systemu Selektywnej Dostępności cywilny użytkownik otrzymuje informacje z dokładnością do 20 m. W Rosji w przypadku precyzyjnego serwisu pozycyjnego systemu **GLONASS** nie stosuje się ani sztucznego błędu (SA), ani dodatkowego kodowania kanału precyzyjnego

[33] *Rosyjska nawigacja satelitarna kontra GPS,* „Gazeta Wyborcza", 16 listopada 2006 r., http://gospodarka.gazeta.pl/gospodarka/1,52981,3740319.html; *Rosja chce udostępnić swój GPS,* „Gazeta Wyborcza", 22 marca 2006 r., http://gospodarka.gazeta.pl/gospodarka/1,52981,3228793.html.

(*anti-spoofing*). Natomiast korzystanie z precyzyjnego serwisu pozycyjnego wymaga zezwolenia rosyjskiego Ministerstwa Obrony.

Przedstawione powyżej trzy segmenty są podobne pod względem budowy oraz pewnych funkcji w poszczególnych globalnych oraz regionalnych systemach nawigacji satelitarnej. Warto jednak dodać, że projekt systemu **Galileo** zawiera wiele rewolucyjnych rozwiązań. Na przykład transmitowane sygnały satelitarne zawierać będą również dane na temat pewności i wiarygodności tych sygnałów. Dla użytkownika będzie to oznaczało, że w ciągu 6 sekund otrzyma informacje o wykryciu błędów systemu. Ponadto, system Galileo ma oferować 5 rodzajów serwisów nawigacyjnych: Otwarty Serwis Pozycyjny (*Open Service*); Serwis Bezpieczeństwa Życia (*Safety of Life Service*); Serwis Komercyjny (*Commercial Service*); Serwis Kontrolowany Publicznie (*Public Regulated Service*); Serwis Poszukiwania i Ratownictwa (*Search and Rescue Service*)[34].

Jeżeli chodzi o to, kto kontroluje i zarządza GNSS, to w większości przypadków jest to rząd. System **GPS** jest zarządzany przez Połączone Biuro Programu GPS (*Joint Program Office* – JPO) powołane w lipcu 1973 r., które jest złożone z przedstawicieli poszczególnych rodzajów wojsk USA, państw NATO i Australii[35]. Operatorem i dysponentem NAVSTAR GPS jest Departament Obrony Stanów Zjednoczonych (*United States Department of Defense* – DoD)[36]. **GLONASS** jest zarządzany przez rząd Federacji Rosyjskiej poprzez Rosyjskie Siły Kosmiczne, a jego operatorem jest Centrum Koordynacji Naukowo-Informacyjnej (*Coordination Scientific Information Center* – KNITs) Ministerstwa Obrony. Mimo że **COMPASS** został zainicjowany przez rząd chiński, kontrolę nad badaniami, budową oraz zarządzaniem nim przejmie ostatnio ustanowione chińskie Centrum Projektu Nawigacji Satelitarnej[37]. **Galileo**, jako cywilny projekt, pozostaje w kompetencji Komisji Europejskiej.

2.3. Zastosowania nawigacji satelitarnej

Rynek produktów i usług opartych na GNSS wciąż się powiększa. Należy podkreślić, że najwięcej możliwości zastosowania oferuje system Galileo, choć nadal nie osiągnął pełnej operacyjności.

Podstawową dziedziną, która intuicyjnie nasuwa się na myśl, jest szeroko rozumiany **transport** (lotniczy, morski, drogowy, kolejowy oraz pieszy). Nawigacja

[34] Strona internetowa: http://ec.europa.eu/enterprise/policies/satnav/galileo/index_en.htm#h2–4 (17.09.2010 r.).

[35] Strona internetowa: http://nawgeo.com/index.php?q=node/2 (16.09.2010 r.).

[36] Ibidem.

[37] Strona internetowa: http://www.insidegnss.com/aboutcompass (20.09.2010 r.).

satelitarna może być wykorzystywana m.in. do identyfikacji przemieszczających się jednostek (samochody i statki), kontroli poszczególnych faz lotu samolotu (zwłaszcza w obszarach pozbawionych infrastruktury kontroli przestrzeni powietrznej)[38].

Tabela 2. Zastosowania usług nawigacyjnych

Obszar	Przykłady
Finanse, bankowość i ubezpieczenia	Certyfikowane znaczniki czasu w elektronicznym systemie przesyłania danych i dokonywania elektronicznych transakcji Archiwizowanie danych w jednorodnym i godnym zaufania systemie czasu Stałe monitorowanie cennych ładunków
Elektroniczne zestawy podręczne oraz telefony komórkowe	Dostarczanie aktualnych informacji Nadzór nad osobami przewlekle chorym i lub monitorowanie pracowników służb publicznych podczas pracy w sytuacjach zagrożenia, rekreacji (np. żeglarstwo) i turystyki
Ochrona cywilna oraz obserwacja	Śledzenie zasobów i siły roboczej Szybkie reagowanie w rozproszonych i odległych obszarach Monitorowanie ruchów organizacji humanitarnych
Energetyka	Optymalizacja przepływu prądu Szybkie przywrócenie sieci energetycznej do pracy po awarii Wydobycie ropy naftowej i gazu
Mapowanie i zarządzanie terenem	Geodezja
Synchronizacja sieci	Integracja odbiorników nawigacji satelitarnej z telefonami komórkowymi oraz innymi środkami komunikacji
Meteorologia oraz zapobieganie katastrofom naturalnym	Powodzie, trzęsienia Ziemi, pożary lasów
Rolnictwo precyzyjne oraz zarządzanie środowiskiem	Pomiar gruntów Optymalizacja plonów Ograniczenie wykorzystania nawozów i pestycydów Zapewnienie optymalnego wykorzystania gruntów i wody
Rybołóstwo	Systemy monitorowania, kontroli i nadzoru połowów
Logistyka	Monitorowanie ruchu towarów i ciężarówek
Kolej	Optymalne sterowanie trasami Ostrzeganie o potencjalnych niebezpieczeństwach i konieczności zmiany zaplanowanego toru i tempa jazdy
Transport miejski	Sterowanie sygnalizacją świetlną w zależności od natężenia ruchu
Transport drogowy	Automatyczna identyfikacja poruszających się jednostek
Transport morski	Wpływanie do portu i na teren wód objętych ograniczeniami Kontrola ruchów statków poza zasięgiem nabrzeżnych stacji audiokomunikacyjnych
Lotnictwo	Kontrola wszelkich faz lotu samolotu Szersze wykorzystanie istniejących lotnisk, nawet podczas niepogody

Źródło: opracowanie własne na podstawie: *Kierunki rozwoju systemów satelitarnych*, Raport I fazy Projektu Foresight, Polskie Biuro ds. Przestrzeni Kosmicznej, styczeń 2007.

[38] Space Foundation, *The Space Report 2010. The Authoritative Guide to Global Space Activity*, 2010, s. 34.

Kolejnym obszarem, w którym usługi GNSS sprawdzą się doskonale są **finanse, bankowość i ubezpieczenia**. Systemy nawigacji satelitarnej ze swymi certyfikowanymi znacznikami czasu będą mogły zapewnić autentyczność, integralność i bezpieczeństwo elektronicznego systemu przesyłania danych i dokonywania elektronicznych transakcji. Zmniejszy się prawdopodobieństwo nadużyć, a transakcje będą archiwizowane w jednorodnym systemie czasu. Rutynowa instalacja systemu w samochodach, pozwalająca monitorować cenne ładunki podczas ich przewożenia, stanie się najważniejszym podsystemem dla firm ubezpieczeniowych[39].

Podczas poszukiwań nowych aplikacji pojawiło się nowe określenie **„nawigacja osobista".** Jest to dziedzina charakteryzująca się najszerszym spektrum zastosowań: od pomocy w poruszaniu się w terenie i dostarczaniu aktualnej informacji, przez nadzór nad osobami przewlekle chorym, monitorowanie pracowników służb publicznych podczas sytuacji zagrożenia, do szeroko rozumianej turystyki (np. żeglarstwo).

Obecnie, kiedy kładzie się nacisk na mniejsze zużycie energii **efektywne zarządzanie przesyłaniem energii elektrycznej** staje się priorytetem. Precyzyjne znaczniki czasu otrzymywane z systemów nawigacji satelitarnej pozwolą na optymalizację przepływu prądu i szybkie przywrócenie sieci energetycznej do pracy po awarii. Nie można zapomnieć o **akcjach poszukiwawczych i ratunkowych**. Nadajniki określające i przekazujące swoją pozycję pozwolą na szybką lokalizację zaginionych samolotów, statków, pojazdów i osób. Wśród niezliczonych obszarów zastosowań główną dziedziną, w której GNSS od zawsze były obecne i praktycznie zaczerpnęły z niej początek, jest **bezpieczeństwo międzynarodowe**[40].

2.4. Bezpieczeństwo międzynarodowe

Jak już wspomniano, w przestrzeni kosmicznej pojawił się nowy globalny gracz – Chiny. Chińskie programy kosmiczne rozwijają się w błyskawicznym tempie, a ogromne środki finansowe sprzyjają realizacji dążeń Chińczyków. Obecnie Pekin pracuje nad projektem wysłania bezzałogowej misji na Księżyc w 2012 r.

Tak więc obraz rywalizacji w przestrzeni kosmicznej zmienił się z bipolarnego systemu, ukształtowanego przez zimnowojenną rzeczywistość, w trójstronny układ. Właściwie w globalnej grze istnieje czterech graczy, ale projekt UE – choć zakłada wprowadzenie największych rewolucji – nadal jest w fazie rozwoju, a kolejne daty

[39] *Kierunki rozwoju systemów satelitarnych*, Raport I fazy Projektu Foresight, Polskie Biuro ds. Przestrzeni Kosmicznej, styczeń 2007, s. 45.

[40] *Kierunki rozwoju systemów…*,op.cit., s. 45.

osiągnięcia pełnej operacyjności są coraz mniej optymistyczne. Stąd zasadne jest rozważanie układu trójstronnego.

Działalność kosmiczna utożsamiana jest zazwyczaj z lotami ludzi na Księżyc oraz dalszą eksploracją kosmosu. Tymczasem największe gospodarcze i społeczne znaczenie ma dziś przestrzeń okołoziemska, w której krążą satelity zapewniające łączność na obszarze całego globu, dostarczające obrazów jego powierzchni i oferujące precyzyjną informację o położeniu. Obecnie działalność kosmiczna to przede wszystkim rosnąca liczba produktów i usług komercyjnych opartych na możliwościach tych satelitów oraz na dostarczanych przez nie danych. Dopiero w dalszej kolejności działalność kosmiczna to rakiety kosmiczne, stacje orbitalne oraz misje naukowe. One także przynoszą wymierne korzyści, odgrywając rolę jednej z najważniejszych lokomotyw rozwoju nowych technologii i innowacyjnych rozwiązań, które po pewnym czasie znajdują zastosowanie w codziennym życiu.

Obecnie obserwuje się intensywne działania każdej z trzech stron w dziedzinie technologii pozwalających niszczyć obiekty orbitalne. Pomysł opracowania takiej technologii zrodził się z potrzeby usuwania starych nieaktywnych satelitów i innych obiektów z orbity, gdyż wraz z pojawianiem się nowych obiektów w kosmosie rośnie prawdopodobieństwo ich zderzenia. Według szacunków NASA wokół Ziemi orbituje ok. 13 000 obiektów większych niż 10 cm i ponad 600 tysięcy obiektów mierzących 1 cm. Każdy z obiektów, nad którym nie ma kontroli, stanowi ogromne zagrożenie dla satelitów i promów kosmicznych. W lutym 2008 r. niekontrolowany rosyjski satelita uderzył i doprowadził do zniszczenia amerykańskiego satelity telekomunikacyjnego[41].

Z drugiej jednak strony, rozwój technologii niszczących obiekty orbitalne ma poważne konsekwencje dla bezpieczeństwa międzynarodowego. Państwo, które nimi dysponuje, nie tylko jest w stanie bronić własnych satelitów, lecz także może niszczyć obiekty uznane przez siebie za wrogie. Jednym słowem, ma zdolność prowadzenia działań wojennych w kosmosie. Do państw o takich możliwościach należą USA, Rosja i Chiny. Amerykanie są najbardziej zaawansowani w tej dziedzinie i obecnie mogą usuwać obiekty z orbity za pomocą: naziemnych systemów wystrzeliwujących pociski SM–3, samolotów wystrzeliwujących rakiety na dużej wysokości lub broni laserowej[42]. Broń laserowa jest najskuteczniejsza, gdyż nie można się przed nią obronić. Amerykański Pentagon planował umieścić broń laserową na orbicie do 2012 r., jednak cięcia budżetowe odsunęły realizację tego projektu w czasie. Taki przebieg wydarzeń ucieszył Rosję i Chiny, które również podjęły wysiłki opracowania broni

[41] B. Bartoszek, *Zmagania o kosmos*, http://www.mojeopinie.pl/zmagania_o_kosmos,3,1257203471, (3.11.2009 r.).

[42] Ibidem.

laserowej, ale nie są tak zaawansowane jak Stany Zjednoczone. Warte odnotowania jest jednak to, że w sierpniu 2008 r. ogłoszono wznowienie radzieckiego programu, który przewidywał, że samoloty MIG–31 będą wystrzeliwały rakiety „antysatelitarne". Pomimo dominacji, USA o wiele bardziej zaniepokoiła wiadomość o zestrzeleniu przez Chiny starego satelity pogodowego w styczniu 2007 r. Była to swego rodzaju demonstracja siły, a także ostrzeżenie dla USA, że Chiny są zdolne do uderzenia w amerykańskie satelity w razie konfliktu z Tajwanem[43]. Wystarczyłoby uszkodzenie tylko kilku satelitów armii Stanów Zjednoczonych, a zdolność komunikowania się na duże odległości i satelitarnego namierzania celów byłaby skutecznie ograniczona. Świadomi takiego zagrożenia Amerykanie już w 2001 r. przeprowadzili pierwszą symulację konfliktu kosmicznego, umiejscawiając go w 2017 r. Pokazała ona, jak boleśnie Stany Zjednoczone odczułyby taki konflikt. W związku z tym powołano 527-ty Szwadron Kosmicznej Agresji (*527th Space Aggressor Squadron*), który ma przeprowadzać symulacje ataków na obiekty wojskowe i cywilne w przestrzeni kosmicznej. W razie pojawienia się kosmicznego konfliktu Szwadron ma brać w nim aktywny udział[44].

Jak wynika z powyższego, potencjalnymi rywalami w tym względzie są USA i Chiny. Już teraz wysuwają postulaty, którymi podkopują się nawzajem. Chiny nalegają na całkowitą demilitaryzację kosmosu. Stany Zjednoczone, wobec braku przepisów międzynarodowych czy organizacji, które czuwałyby nad bezpieczeństwem na orbicie, sugerują, że oni mogą pełnić funkcję „strażnika bezpieczeństwa kosmicznego". Stratedzy z Pentagonu są zdania, że umieszczenie broni na orbicie pozwoliłoby jeszcze lepiej chronić interesy USA oraz całego świata.

Chinom wtóruje Rosja. Oba państwa chciałyby opracowania nowego traktatu międzynarodowego, który zakazem umieszczania systemów obrony na orbicie objąłby wszystkie rodzaje broni, na co nie zgadzają się Stany Zjednoczone. Zakaz umieszczania systemów obrony na orbicie znacznie osłabiłby zdolność USA do obrony antyrakietowej. Poza tym, Amerykanie znacząco rozwinęli już ten rodzaj broni, choć mają problem z umieszczeniem go na orbicie. Wprowadzenie takiego zakazu byłoby jednostronnie krzywdzące, gdyż Moskwa i Pekin nadal mogłyby rozwijać technologie walki z satelitami z ziemi, ponieważ nowy traktat nie objąłby tego rodzaju broni.

Obecnie międzynarodowe prawo kosmiczne z 1967 r. zabrania umieszczania w kosmosie jedynie broni masowej zagłady. Od momentu rozpoczęcia rywalizacji na polu zdobywania kosmosu oraz rozwoju związanych z tym systemów nawigacji

[43] Ibidem.
[44] Ibidem.

satelitarnej w problematykę tą włączyła się Organizacja Narodów Zjednoczonych (ONZ)[45]. Od lat sześćdziesiątych ONZ zajmuje się promowaniem pokojowego eksplorowania kosmosu. W tym celu wydała pięć międzynarodowych porozumień, w których przede wszystkim chodzi o włączenie krajów rozwijających się, o udaremnienie zbrojenia się w przestrzeni kosmicznej, zakaz umieszczania broni atomowej, uregulowanie odpowiedzialności za szkody, rejestrowanie wszystkich startów i urządzeń wynoszonych w kosmos, ratowanie astronautów i pojazdów kosmicznych. Już w 1966 r. sformułowano *Outer Space Treaty*, który ratyfikowało 85, a podpisało tylko 26 krajów. Szczególnie zachowawczo postępują kraje, które dysponują zaawansowanymi programami kosmicznymi – jak USA, Chiny czy właśnie Rosja. Eksploracja kosmosu już przestała być wykorzystywana w celach pokojowych. Więc jeśli kiedyś faktycznie wybuchnie „wojna informacyjna", to satelity komunikacyjne będą w niej odgrywały zasadniczą rolę.

Moon Treaty z 1979 r. miał wypełnić lukę pozostawioną przez poprzedni dokument – zabronić zajmowania obszarów i surowców na Księżycu i innych ciałach niebieskich naszego systemu słonecznego, lecz spotkał się z jeszcze mniejszym zainteresowaniem państw. Ratyfikacji dokonało 9 państw, podpisało zaś tylko 5. Oznacza to, że prawa własności są nadal niedookreślone, co – wobec zintensyfikowanej eksploracji kosmosu – może prowadzić do konfliktów. Pod tym względem przestrzeń przypomina Dziki Zachód[46]. Wniosek jest jeden: tak jak wszędzie, możliwości zysków oraz władza stoi w sprzeczności z pokojową współpracą, wspólnym interesem oraz „dobrem publicznym".

Koncepcja nowego traktatu międzynarodowego dotyczącego przestrzeni kosmicznej, całkowicie zabraniającego umieszczania w niej broni, powinna być wsparta zakazem użycia broni naziemnej, przeznaczonej do niszczenia obiektów na orbicie okołoziemskiej. Pierwszy – miałby zatrzymać kosmiczny wyścig zbrojeń, natomiast, drugi – rozwój broni naziemnej[47]. Obecnie na orbicie nie umieszczono jeszcze żadnej broni. ONZ mogłoby zająć się utrzymaniem tego *status quo*, choć nie będzie to proste zadanie. Wobec negatywnej postawy Stanów Zjednoczonych wciąż nie ma postępów w pracach nad nowym traktatem. A brak międzynarodowych regulacji w tej dziedzinie może mieć dalekosiężne negatywne konsekwencje. Niekiedy nawet groźba potencjalnego użycia siły ma wielką moc. W odpowiedzi na amerykańskie zbrojenia kosmiczne, Chiny rozwijają własny program. Może to

[45] F. Rötzer, *Ist der Weltraum ein öffrntliches Gut?*, 21 lipca 1999 r.

[46] Pewna firma rozpoczęła przez Internet sprzedaż działek na wszystkich planetach.

[47] V. Vasiliev, *The draft treaty on the prevention of placement of weapons in outer space, the threat or use of force against outer space objects*, w: *Security in Space: The Next Generation-Conference Report*, 31 March–1 April 2008, United Nations Institute for Disarmament Research (UNIDIR), 2008, s.145–146.

wywołać reakcję łańcuchową – Indie zaczną rozwijać swoją broń kosmiczną, co wywoła reakcję Pakistanu, z kolei na to nie pozostanie obojętny Izrael, obawiający się przekazania technologii krajom arabskim przez Islamabad.

Podsumowanie

Przemysł nawigacji satelitarnych charakteryzuje się nieustannym dążeniem do innowacyjności i zmian. Stąd, pomimo ogromnego doświadczenia w dziedzinie GNSS, globalni gracze: Stany Zjednoczone, Rosja oraz Chin, nie pozostają obojętni wobec „groźby" fizycznego pojawienia się nowego-starego gracza – UE, którego dobrze znają i z którym współpracują.

Obecnie w najlepszej pozycji znajdują się Stany Zjednoczone, których system jest w pełni operacyjny i dlatego stanowi podstawę systemu światowej nawigacji. Pozycja dwóch kolejnych: Rosji i Chin jest podobna. Rosyjski GLONASS ma silną pozycje, ale obecny potencjał gospodarczo-społeczny ogranicza jgo znaczenie. Z kolei, chiński COMPASS, choć znajduje się w fazie rozwoju, ma mocne zaplecze finansowe, co daje możliwość przyspieszenia prac. W globalnej grze o dominację w dziedzinie usług nawigacyjnych regionalne znaczenie ma chiński Beidou oraz rozwijające się: japoński system QZSS oraz indyjski IRNSS.

Kwestią zasadniczą z punktu widzenia bezpieczeństwa międzynarodowego jest jednak prawne uregulowanie przestrzeni kosmicznej, zarówno tej bliższej, która w ostatnim czasie zyskała na znaczeniu za sprawą wymiernych korzyści płynących z GNSS, jak i tej dalszej – kojarzonej z eksploracją kosmosu. W przeciwnym razie możemy zetknąć się z nowym wymiarem wojny – wojny informacyjnej.

New spheres of international security

The first part of the article introduces the problematic **of communication and electronic media in the context of international security**. We observe today increasing role that electronic media play in international policy and security. News reports of major TV stations, news portals and largest news agencies as well as social media influence in different ways public opinion both on local and global scale. **The goal of the second part of the article is examination of the essence of the global positioning systems**. The key issue in this context is finding an answer to the question: which countries have managed to develop global

positioning system sufficiently enough to become world players in the field and which countries are important only in their region? Increasing rivalry in space leads to examination of the problem how global positioning technologies can influence international security.

De nouveaux domaines de la sécurité internationale

La première partie de l'article présente le problème de communication et des médias électroniques dans le contexte de la sécurité internationale. Aujourd'hui, le rôle des médias électroniques dans le domaine de la politique et de la sécurité internationale augmente. Les services d'information des principales chaînes de télévision, les portails d'information, les plus grandes agences de presse, ainsi que les médias sociaux influent de différentes manières sur l'opinion publique tant au niveau régional que mondial. L'objectif de la deuxième partie de l'article est d'examiner les systèmes de navigation par satellite. Dans cette situation, il est important de répondre à la question suivante: «Quels pays ont réussi à développer un système de navigation par satellite à un tel point d'être un acteur mondial dans ce domaine et quels pays jouent un rôle essentiel seulement dans leur région?». L'intensification de la concurrence dans l'espace tend à examiner la question de la façon dont les technologies satellitaires peuvent affecter le système de sécurité internationale.