Komentarza udziela
MARIUSZ RUKAT

POLITYKA INFORMACYJNA PAŃSTW W DOMENIE CYFROWEJ

Publikacja w ramach projektu Neptune fundacji Stratpoints.

NEPTUNE
PROJEKT • BEZPIECZEŃSTWO & ROZWÓJ

Komentarza udziela
MARIUSZ RUKAT

POLITYKA INFORMACYJNA PAŃSTW W DOMENIE CYFROWEJ

Jeśli cyberprzestrzeń jest domeną gdzie informacja może być tworzona, przechowywana, transmitowana i manipulowana, tak cyber siła jest procesem przetwarzania informacji na cele strategiczne.[1]

Rewolucja informacyjna jest jedną z zasadniczych cech naszej ery. Wielowymiarowy postęp w obszarze technologii informacyjnych wywiera silne skutki w środowiskach społecznych, strukturach bezpieczeństwa, agendach biznesu, i wpływa na legitymizację państwowej władzy w wielu, jeśli nie we wszystkich, regionach świata. Dziś szerokie ramy społeczne i rządowe, wartość produkcyjna gospodarki państw, a nawet atrybuty wewnętrzne, takie jak tożsamość, „hermetyka" religijna czy przekonania polityczne podlegają globalnym wpływom i zwrotnemu oddziaływaniu informacji, na wcześniej niespotykaną skalę.

Rewolucja informacyjna fundamentalnie zmienia lokalne społeczności, nasilając ich konwergencję na poziomie regionalnym i globalnym. Dramatyczny rozwój technologii komputerowych i komunikacyjnych wpływa na naturę rządów, wzmacniając rolę aktorów niepaństwowych (w tym jednostek i aktorów pozapaństwowych) i zwiększając wagę „soft power" w obszarze narodowej polityki zagranicznej. Zmiana w sposobie komunikacji wpływa również na proces i strukturę dystrybucji siły w społeczeństwie, jego ewolucję jako całości i oddziałuje na przekonania. W zależności od przyjmowanego punktu widzenia, szybkość i „uwolnienie" globalnej komunikacji, w pewnym zakresie, może doprowadzić do pożądanej (lub nie) uniwersalizacji, a w pewnych przypadkach, korozji tradycyjnych wartości. Jednocześnie, globalna, ponadgraniczna komunikacja online poddaje w wątpliwość atrybut suwerenności państwa

w systemie międzynarodowym, szczególnie w kategoriach efektywnego sprawowania władzy i zapewnienia bezpieczeństwa obywateli na terytorium kraju - w rzekomo wirtualnej domenie „cyberprzestrzeni".

Internet i media społecznościowe dostarczają dziś nowych sposobów konstruowania rzeczywistości. Oddziałują zarówno na aktorów międzynarodowych, widownię, jak i na same media. Zdolność do wywierania wpływu została dziś skutecznie „zdemokratyzowana", ponieważ każda jednostka, czy grupa posiada potencjał komunikowania się i wpływania na szerokie grupy odbiorców online, w sposób, który był wcześniej utrudniony, chociażby ze względu na koszty takiego procesu, w erze przed-internetowej. [1] Państwa w różny sposób starają się rozwijać spójne polityki narodowe i podstawy prawne służące swobodnemu przepływowi informacji w sieci. W określonych przypadkach, są to również mechanizmy polityczne (czy operacyjne) służące do kreowania obrazu i wywierania wpływu poprzez informację. Proces wpływania na społeczności przy zastosowaniu instrumentów online jest jednak utajniony, a użytkownicy „sieci" mogą być poddawani wpływom informacji dostarczanych przez anonimowe źródła, bez ich atrybucji geograficznej czy ideologicznej, i bez powiązanego z informacją czynnika odpowiedzialności.

Informacja w domenie cyfrowej:

Nie należy zgadzać się z twierdzeniem, że informacja jest towarem, którego wyróżniającą cechą jest to, że *udzielając jej jednym osobom, nie odbieramy jej innym*.[2] **Informacja** od zawsze była towarem szczególnie wrażliwym. Jej wartość polega na możliwości **ekskluzywnego wykorzystania do celów strategicznych** w wymiarze narodowego bezpieczeństwa, społecznym, politycznym lub handlowym. Z chwilą ujawnienia lub upublicznienia informacji jej wartość dramatycznie spada, a przy niefrasobliwym, czy nieumiejętnym wykorzystaniu może rodzić surowe konsekwencje, m.in. dla spójności struktur politycznych, bezpieczeństwa lub narodowych.

Wzmożona komunikatywność, jaką zapewnia dziś Internet, umożliwia przeniesienie siły społecznego oddziaływania z rządów i legitymizowanych agend państwowych na aktorów niepaństwowych i poza-państwowych, bez względu na ich geograficzne położenie. Internet pozwala dziś wzmocnić projekcję siły grup, którym wcześniej brakowało takiego medium oddziaływania. W tym przypadku interkomunikacyjność może wzmacniać system państwa, ale może także odwracać uwagę od tradycyjnych źródeł narodowej tożsamości, kierując ją w stronę rywalizujących wartości opartych na etniczności, religii czy ideologii.[3]

W kontekście skutków oddziaływania informacji zawartej w cyberprzestrzeni na proces polityczny należy zwrócić uwagę na cztery zasadnicze czynniki: *wszechobecność technologii informacyjnych*; *rosnącą „ilość" i zmniejszający się koszt informacji*; *zmieniający się (oparty na informacji) system wartości społeczeństw*, *skutki, jakie większa liczba informacji wywiera na struktury organizacyjne w środowisku wewnątrzkrajowym, jak i międzynarodowym*.[4] Elementy te zasadniczo determinują kierunki opinii społecznej w państwach demokratycznych - legitymizując słuszność rządowych działań, a w państwach o strukturze niedemokratycznej - narażają reżim na krytykę obywatelską, perspektywę liberalizacji poglądów i ewentualny sprzeciw wobec podejmowanych decyzji.

Cytowana na wstępie **cyber siła** przyczynia się więc do dystrybucji siły, co ma dziś miejsce w polityce międzynarodowej, i wzmacnia jednostki, organizacje i aktorów międzynarodowych, pozwalając na ich większą partycypację i wypływy. W wymiarze militarnym, cyber siła, nie tylko oddziałuje na strukturę sił zbrojnych, ale również na **strategie**, jak i to, w jakich warunkach powinny być one używane. [5] Wszystkie te aspekty dotyczą działań w domenie, która przekracza geograficzne ramy państw.

[1] Rand Waltzman, Creating Influence through Information, [w:] Richard Harrison and Trey Herr, Cyber Insecurity: Navigating the Perils of the Next Information Age, Rowman & Littlefield, New York – London, 2016, str. 330.

[2] Krzysztof Liderman [w:] Miron Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015, str. 17

[3] Szeroko wiadomym jest, że Al. Qaeda aktywnie rekrutuje zwolenników wykorzystując Internet, umożliwia transnarodową identyfikację i dostęp do ideologii dżihadyzmu online.

[4] Heather,Harrison, Dinniss, Cyber Warfare and Laws of War, Cambridge University Press, UK, 2012, str. 12 - 13.

[5] John B. Sheldon, The Rise of Cyberpower, [w:] John Baylis, James J. Writz, CollinS. Gray, Strategy in the Contemporary World,
(5th Edition) Oxford University Press, UK, 2016, str. 287-288.

Globalny przepływ informacji a polityka państw w cyberprzestrzeni:

Polityka państw i działania podejmowane w zakresie kontroli przepływu informacji w domenie cyfrowej wpisują się w obszar definiowany jako sprawowanie suwerenności w cyberprzestrzeni. Realistyczna koncepcja suwerenności zakłada, że suwerenność istnieje w postaci kontroli określonego terytorium, zdefiniowanego przez nominalnie granice państwa. [6] W myśl tej koncepcji, państwo posiada wyłączną jurysdykcję i zapewnia własną jurysdykcję poprzez dwie podstawowe zasady: terytorialność i efektywność władzy. Ponieważ domena cyfrowa opiera się na infrastrukturze teleinformatycznej wytworzonej i zbudowanej przez człowieka, o przywiązaniach geograficznych, każdy fizyczny komponent tej konstrukcji podlega prawu i jurysdykcji suwerennej władzy, w tym (dopuszczalnym prawem narodowym) mechanizmom kontroli.

W przypadku domeny cyfrowej, polityka i praktyki państw istotnie różnią się w tym zakresie. Podczas gdy jedni uważają cyberprzestrzeń za *dobro wspólne* (np. państwa wspólnoty europejskiej, Kanada i USA), inni traktują cyberprzestrzeń, jako *wymiar wymagający kontroli* (np. Rosja i Chiny), aby ograniczać jej wpływ na politykę rządu i własnych obywateli. [7] W tym zakresie cyberprzestrzeń traktowana jest z jednej strony jako liberalna platforma zawierzania, kumulacji, przechowywania i czerpania informacji, a z drugiej, plastyczna materia, którą można i należy kształtować i wyposażać w informacje konieczne do uzyskania pożądanych (politycznych) celów. Podejście takie nabiera szczególnego znaczenia gdy w drodze podejmowanych działań w cyberprzestrzeni dochodzi do naruszania zasady suwerenności państw, lub ograniczany jest dostęp własnych obywateli do gwarantowanych, uniwersalnych praw. Zasadniczy problem sięga do fundamentalnej własności cyberprzestrzeni, a właściwie Internetu, który w założeniu miał i powinien być otwarty. Wiele państw uważa, że wymuszanie suwerenności w domenie cyberprzestrzeni nie leży w ich interesie. Dotyczy to szczególnie państw o ustroju liberalno-demokratycznym, których populacje oczekują, że cyberprzestrzeń będzie domeną wolną i otwartą.

Z drugiej strony, wiele państw postrzega kwestię globalnego przepływu informacji, który odbywa się w dużej mierze poza ich kontrolą, jako wyzwanie dla autorytetu i legitymizacji władzy. Dla przykładu, Chiny i inne państwa nie demokratyczne, w szczególności Rosja Władimira Putina, od dawna obawiają się implikacji bezpieczeństwa wynikających z oparcia (uzależnienia) od sieci informacyjnych, prawie w całości pozostających pod kontrolą USA i ich sojuszników.

Na obecną chwilę Internet rzekomo jest - i na wiele sposobów był – bez granic, niemniej błyskawicznie stało się jasne, że państwa mogą sprawować znaczny stopień suwerennej kontroli poprzez medium, czy to monitorując, czy też samodzielnie filtrując zawartość lub też żądając tego od dostawców usług internetowych i innych firm technologicznych, jako warunku uzyskania przez nich licencji.

Globalna dyskusja na temat zarządzania Internetem i cyberbezpieczeństwa dzieli dziś świat na dwa obozy. Z jednej strony mamy do czynienia z gronem państw podobnie myślących (*like-minded states*), do którego należą **Stany Zjednoczone** i inne, głównie **zachodnie liberalne demokracje**.[8] Państwa te opowiadają się za wieloudziałowym/wielostronnym modelem zarządzania Internetem, w ramach którego kompleksowa i stale ewoluująca sieć grupy osób i grup interesu zbiera się, aby wychodzić naprzeciw różnym kwestiom.[9] Członkowie tej grupy opowiadają się za Internetem otwartym, który z zasady wolny jest od restrykcji rządów co do zawartości, i argumentują za skupianiem uwagi na bezpieczeństwie (rozwiązań teleinformatycznych i infrastrukturalnych) sieci, aby zapewnić, że Internet może funkcjonować w sposób „higieniczny" i niezawodny.

Drugi obóz obejmuje państwa spoza grupy państw demokratycznych, pod przewodnictwem **Chin i**

[6] Stephen K. Gourley, "Cyber Sovereignty" [w:] Conflict and Cooperation in Cyberspace: The Challenge to National Security, Tylor & Francis Group, London, New York, 2014, str. 279

[7] Ibid.

[8] Nigel Inkster, China's Cyber Power, IISS, Routledge, 2016. Str. 120.

[9] W wyniku takiego podejścia doprowadzono do utworzenia the **Internet Engineering Task Force** (IETF Grupy Zadaniowej ds. Inżynierii Internetu) - grupy non-profit, w której udział jest otwarty dla każdego, kto posiada wymagane techniczne kwalifikacje i czyim celem jest 'sprawić aby Internet działał lepiej poprzez dostarczanie wysokiej jakości, powiązanych dokumentów technicznych, które wpływają na to jak ludzie konstruują, kierują i używają Internetu. Por. Internet Engineering Task Force, 'Mission Statement', https://www.ietf.org/about/mission.html.

Rosji. Podczas gdy państwa te nie odrzucają koncepcji wieloudziałowej, Chiny i Rosja opowiadają się za o wiele silniejszą rolą rządów narodowych w zarządzaniu Internetem, szczególnie w odniesieniu do kwestii **polityki publicznej i „informacyjnego" cyberbezpieczeństwa**.

Sposób ich skupienia się na **bezpieczeństwie informacji opiera sią na koncepcji walki informacyjnej ery sowieckiej**, w ramach której **państwo chroni swoją przestrzeń informacyjną aby zapewnić, że jej (narodowa) narracja nie jest poddawana wyzwaniom**.[10]

Podejście rosyjskie do kwestii międzynarodowego cyberbezpieczeństwa zakorzenione jest w tradycyjnej koncepcji wojny informacyjnej - działania, które Rosja traktuje jako trwale, a nie w okresach walki kinetycznej. W ramach tej koncepcji, **informacja jest traktowana jako uzbrojenie**, które wymaga kontroli, a kluczem do osiągnięcia tego jest zdolność do zabezpieczenia własnej narodowej strefy informacyjnej zapobiegając wpływowi wrogiej narracji na własną populację. Również w Chinach (które uległy silnemu wpływowi doktryny sowieckiej) taka percepcja została wzmocniona przez rolę jaką odegrały zewnętrznie generowane informacje, doprowadzając do końca Zimnej Wojny a następnie ZSRR. [11] Tak więc, dla państw takich jak Chiny czy Rosja, kształtowanie międzynarodowej agendy na temat cyberbezpieczeństwa, czy też (jak wolą to nazywać) bezpieczeństwa informacyjnego - jest kluczowe w kształtowaniu pola bitwy.

Grupa państw o reżimach niedemokratycznych chciałaby sformalizować globalne struktury zarządzania Internetem w ramach ONZ, w modelu zstępującym, który oddaje rolę decyzyjną rządom narodowym. Takie podejście jest dobrze przyjmowane w krajach rozwijającego się świata, które są na niekorzystnej pozycji jeśli chodzi o digitalizację i są podatne na potężne, destabilizujące siły globalizacji, dla której Internet stał się głównym wektorem. Jednocześnie w toku dyskusji międzynarodowej nad zarzadzaniem Internetem, państwa pozostające w tyle za technologicznie rozwiniętym zachodem podkreślają, że przeważająca pozycja Waszyngtonu umożliwia USA nakładanie technologicznych standardów, które ułatwiają użycie ICT jako środka agresji.[12] Takie obawy znalazły odzwierciedlenie w rewelacjach ujawnionych przez Edwarda Snowdena jesienią 2013 r.

Zagrożenia „informacyjne" w cyberprzestrzeni:

Dziś różnice w interpretacji pojęcia „cyberbezpieczeństwo" nabyły wymowy politycznej. Zasadniczym zagadnieniem, kontestowanych przez państwa dwóch wskazanych powyżej obozów, jest kwestia dostępu do danych w wykonaniu założeń prawa oraz różnice ws. szyfrowania czy filtrowania ich zawartości. (SSL/TSL).

Od okresu poprzedzającego wybuch „Arabskiej Wiosny" (2010-2013) wielu użytkowników w krajach **Bliskiego Wschodu i Afryki Północnej** wykorzystuje Internet na rzecz kampanii politycznych i społecznego aktywizmu. W 2011 roku, w miarę jak zaczęło nasilać się powszechne powstanie w Syrii, decyzją rządu w Damaszku, wszystkie usługi internetowe zostały wstrzymane.[13] Od tego czasu, w środowisku międzynarodowym obserwowane jest nasilenie represji w Internecie. Blokowanie zawartości stron społecznych portali internetowych odnotowywana jest na **Białorusi**. Władze w Ankarze zażądały wprowadzenia procesu filtrowania informacji od dostawców usług internetowych w **Turcji**. Przypadki zewnętrznego reedytowania stron internetowych odnotowano w Kazachstanie.[14] **Iran** stworzył własną wersję **„*Internetu Halal*"** (*National Information Network - NIN*), jako metodę publicznej kontroli dostępu do informacji tylko o charakterze „*halal*" - zgodnej z prawem islamskim.[15]

Rządy państw **Bliskiego Wschodu i Północnej Afryki** inwestują w projekty w obszarze mediów i IT, a jednocześnie przeznaczają nakłady na technologie cenzuralne aby uniemożliwić własnym obywatelom dostęp do spektrum „niewłaściwej" informacji. Paradoksalnie, podczas gdy jedne *zachodnie firmy* budują infrastrukturę ICT niezbędną do ekonomicznego rozwoju tego

[10] Inkster (2016), str. 121.
[11] Timothy L. Thomas, Russian Information Warfare Theory: The Consequences of 2008" [w:] Stephen J. Blank and Richard Weitz (ed.) The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald (Carlisle, PA: Strategic Studies Institute, 2010.

[12] Inkster (2016). Str. 127
[13] Elizabeth Flosk, Syria Internet Services Shut Down as Protestors Fill Street", The Washington Post, Blog Post, 3 June 2011.
[14] Joseph marke, Internet Repression on the Rise Since Arab Spring, Nextgov.com; July 15, 2011.
[15] Iran creates "Halal Internet" to control online information, Reporters Without Borders for Freedom of Information, September 6, 2016; https://rsf.org/en/news/iran-creates-halal-internet-control-online-information, Pobrano: 14.10.2917

regionu, inne *zachodnie firmy* dostarczają technologii cenzuralnych i danych do filtrowania Internetu.[16] Cenzorzy w tym regionie próbują kontrolować zawartość polityczną wykorzystując filtrowanie techniczne, restrykcje fizyczne i dodatkowo – nękanie i aresztowania. Filtrowanie zawartości informacyjnej ze względu na jej obraźliwy charakter pod względem religijnym, moralnym i kulturowym, występuje powszechnie, a jego skala rośnie.

Według raportu Open Net Initiative, liczba państw, które ograniczają dostęp do zawartości Internetu w ostatnich latach dramatycznie wzrosła. Odbywa się to w oparciu o często silne argumenty nie do odparcia, takie jak: „ochrona/zapewnienie intelektualnych praw własności"; „ochrona narodowego bezpieczeństwa", „zachowanie norm kulturowych i wartości religijnych", ochrona dzieci przed pornografią i wykorzystaniem".[17] Jeszcze w 2010 roku ponad 40 państw na świecie używało wysoce restrykcyjnego filtrowania i *firewali* aby zapobiegać dyskusji nt. materiałów o podejrzanym charakterze. Kilkanaście państw angażuje się w **cenzurę polityczną**, którą określa się jako **"perswazyjną"** w Wietnamie, Iranie i Chinach, i jako **„zasadniczą"** w Libii, Etiopii i Arabii Saudyjskiej. Ponad 30 państw filtruje informacje dla celów społecznych, blokując zawartość powiązaną z takimi zagadnieniami, jak sex, hazard i narkotyki. Nawet Stany Zjednoczone i wiele państw europejskich robi to w sposób selektywny.[18] Według raportu *LE VPN* za 2016 rok, pierwszą dziesiątkę państw stosujących najcięższą cenzurę informacji w Internecie stanowią: **Korea Północna, Chiny, Erytrea, Etiopia, Arabia Saudyjska, Iran, Syria, Tunezja, Wietnam i Myanmar (Birma).** Cenzurę Internetu dla utrzymania narodowego bezpieczeństwa stosują: Kuba, Indie, Maroko, **Rosja i Turcja**. [19] Cenzura **mediów społecznościowych** powszechnie stosowana jest w takich państwach (regionach) jak: Zjednoczone Emiraty Arabskie, Bahrajn, Chiny, Indonezja, Iran, Kuwejt, Myanmar, Oman, Zachodnie Wybrzeże i Strefa Gazy, Katar, Arabia Saudyjska, Sudan i Jemen. Selektywne filtrowanie mediów prowadzą m.in. Turcja, Syria, Rosja, Korea Południowa, Indie i Włochy.[20]

Rosja, w swojej polityce informacyjnej wobec cyberprzestrzeni (bezpieczeństwa informacj**i**), stara się przeciwdziałać nie tylko zagrożeniom online, ale także utrzymywać kontrolę nad informacją i interakcjami, które przebiegają w internetowej sieci. Rosyjska interpretacja frazy „cyberbezpieczeństwo' zawiera również zdolność do egzekwowania prawa w celu uzyskiwania informacji o osobach (jednostkach) i ich sprawach. [21] Taka wykładnia negatywnie wpływa na wolność firm oferujących bądź stosujących jako standard informatyczne formuły szyfrowania. Wpływa to również na politykę przechowywania danych – wymaganie aby firma dostawca usług internetowych oferująca swoje usługi w określonym państwie musiała również składować wszystkie dane generowane przez obywateli tego państwa w tym kraju.

Polityka rządu **Chin** w obszarze Internetu zawiera kilka nieco innych, zasadniczych priorytetów. Chińczycy na pierwszym miejscu stawiają: utrzymanie wzrostu gospodarczego, zachowanie społecznej stabilności, wspieranie trwających i przyszłych działań militarnych oraz przeciwdziałanie rozwijaniu norm międzynarodowych mogących podważyć którykolwiek z tych założeń. Chińscy cenzorzy skonstruowali niezwykle elastyczną aranżację technologii filtrowania, blokowania i inwigilacji, kolektywnie zwaną **„Great Firewall of China"**. Nadrzędnym celem tego działania jest monitorowanie i *kształtowanie dyskusji w czasie rzeczywistym*, aby kontrolować przepływ informacji ze źródeł zlokalizowanych na zewnątrz kraju i dotyczących wrażliwych wydarzeń lub zjawisk zachodzących wewnątrz chińskiego państwa. Szyfrowanie, szczególnie dla danych w ruchu jak SSL/TLS może sprawiać problemy, więc w różnych punktach chińscy politycy używają „Great Firewall" aby blokować zaszyfrowane połączenia do sieci wewnątrz Chin.[22] Podczas gdy istnieje wiele grup o zróżnicowanych interesach, co do tego jak kierowany jest Internet w Chinach, zachowanie wpływu Chińskiej Partii

[16] Źródło: https://opennet.net/research/regions/mena - pobrano: 14.10.2017
[17] Open Net Initiative - https://opennet.net/about-filtering
[18] As documented by the Open Net Initiative. Richard Waters and Joseph Menn, "Closing the frontier," Financial Times, March 29, 2010.
[19] Źródło: https://www.le-vpn.com/top-10-censors-internet-avoid-internet-censorship/ Pobrano: 15.10.2017.
[20] Źródło: https://opennet.net/research/data Pobrano: 15.10.2017.
[21] Trey Herr and Heather West, Understanding Internet Security Governance, [w:] Richard Harrison and Trey Herr, Cyber Insecurity: Navigating the Perils of the Next Information Age, Rowman & Littlefield, New York – London, 2016, str. 181 - 187
[22] Ibid.

Komunistycznej i politycznej stabilności wydaje się mieć wagę nadrzędną.

Obok oczywistych korzyści rozwojowych, otwarty charakter Internetu wkracza jednak w politykę państw reżimowych, które mówiąc o bezpieczeństwie domeny cyfrowej, za punkt skupienia przyjmują informację wkraczającą w ich suwerenne terytorium polityczne. Obca informacja, a właściwie jej narracja, traktowana jest jako zagrożenie dla podstaw funkcjonowania struktury cywilizacyjnej, kulturowej, ideologicznej lub religijnej, stanowiących często zasadniczą podstawę legitymizacji władzy takiego państwa. Niestety rok 2016 i działania Rosji w sprawie wyborów prezydenckich w Stanach Zjednoczonych pokazał, że taka interakcja może przyjąć odwrócony charakter, oddziałując również na państwa z grupy liberalnych demokracji.

W kontekście kreowania, kształtowania i manipulacji, informacja w domenie cyfrowej narażona jest na bardzo wyszukane zagrożenia. Aktorzy pozapaństwowi (*Hezbollach, Al. Qaeda, Syrian Electronic Army, propaństwowi haktywiści rosyjscy*) wykorzystują otwartość i liberalizm Internetu do oddziaływania na społeczeństwa obcych państw, starając się wpływać na spójność ich systemu politycznego lub inkorporację własnych ideologii. Jednocześnie, jak to ujawniły przypadki E. Snowdena czy B. Manninga, państwa liberalne, mając za podstawę ochronę narodowego bezpieczeństwa, podejmują działania mające na celu ochronę własnych obywateli, niemniej dostępne instrumenty i mechanizmy oddziaływania w tym zakresie w cyberprzestrzeni, stoją w sprzeczności z powszechnie akceptowalną etyką działania, w poważny sposób podważając zaufanie do narodowych instytucji.

Polska strategia bezpieczeństwa w domenie cyfrowej:

Zachodni twórcy Internetu zakładali wykorzystanie sieci do transferu informacji mających na celu rozwój nauki. Internet ma sens, gdy zachowany jest jego liberalny, otwarty charakter, jako instrumentu generowania informacji, jak i medium jej transferu, zarówno do celów badawczych czy naukowych, jak i finansowych i społecznych. Transfer internetowy, w swoim ponadnarodowym charakterze, zawiera jednak zasadnicze elementy odnoszące się do suwerenności państw. Z jednej strony mówimy o bezpieczeństwie domeny cyfrowej, które definiujemy w kategorii wycinkowej (terytorium państwa lub wspólnoty/organizacji państw, np. UE lub NATO), z drugiej, Internet na poziomie globalnym (i niżej na poziomach regionalnych) zarządzany jest przez gremium międzynarodowych podmiotów i korporacji, dbających o prawidłowe funkcjonowanie „sieci" (ICANN, IANA).

Polskie agendy rządowe, odpowiedzialne za kreowanie polityki w odniesieniu do domeny cyfrowej, w 2014 roku wniosły narodowe stanowisko do koncepcji Komisji Unii Europejskiej w sprawie Internetu i modelu zarządzania Internetem.[23] Ministerstwo Cyfryzacji, w 2014 roku zadeklarowało, że jest za „utrzymaniem i doskonaleniem wielostronnego modelu zarządzania Internetem" i będzie sprzeciwiać się „próbom zastąpienia modelu wielostronnego modelem międzyrządowym". Opowiadamy się za tym aby wypracować wspólne, europejskie stanowisko w sprawie zarządzania Internetem, wskazujące, że zasadniczym „działaniem UE i państw członkowskich powinno być przeciwdziałanie fragmentyzacji Internetu oraz zachowanie jego otwartego i innowacyjnego charakteru".[24] Pod tym względem zaleca się opracować globalne zasady zarządzania Internetem, które winny „zmierzać do:

- zachowania otwartego i wolnego charakteru standardów technicznych i protokołów komunikacji w Internecie,

- zagwarantowania przestrzegania praw człowieka i podstawowych wolności w Internecie, w szczególności wolności wypowiedzi, zakazu cenzury prewencyjnej oraz prawa do prywatności,

- zachowania neutralności technologicznej infrastruktury internetowej oraz zainicjowania szerokiej dyskusji o neutralności sieci w prawdziwie wielostronnym środowisku,

[23] „Rząd RP co do zasady popiera działania zapowiedziane w Komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno – Społecznego i Komitetu Regionów: Polityka wobec Internetu i zarządzanie Internetem: Rola Europy w kształtowaniu przyszłości zarządzania Internetem [COM(2014) 072] oraz docenia wysiłek Komisji włożony w przygotowanie tego cennego dokumentu."

[24] Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Polityka wobec Internetu i zarządzanie Internetem: Rola Europy w kształtowaniu przyszłości zarządzania Internetem. *Data przyjęcia Stanowiska przez Komitet ds. Europejskich – 10 kwietnia 2014r.*

- wzmocnienia potencjału Internetu jako instrumentu promocji demokracji i zróżnicowania kulturowego."[25]

W myśl działań na tym polu, w 2016 r. Ministerstwo Cyfryzacji zaproponowało Strategię Cyberbezpieczeństwa RP na lata 2016 – 2020, [26] a roku bieżącym: Krajowe Ramy Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.[27] Oba dokumenty opatrzono tym samym podtytułem: Poszanowanie praw i wolności w cyberprzestrzeni - Kompleksowe podejście do cyberbezpieczeństwa - Cyberbezpieczeństwo istotnym elementem polityki państwa.

Pierwszy z dokumentów (z 2016) zawiera draft koncepcji zbudowania mechanizmu monitorowania i kontroli cyfrowej mapy transferu danych wewnątrz terytorium RP. Nie można go też traktować jako pełnej strategii operacyjnej wyznaczającej kierunki działania w domenie cyfrowej. „strategia" z 2016 to raczej „manual operacyjny" – wstęp, opisujący pożądany obraz współdziałania poszczególnych elementów administracji i infrastruktury, zasadniczych dla monitorowania zagrożeń i ochrony obiektów administracyjnych oraz państwowych, w tym infrastruktury krytycznej. „Strategia cyberbezpieczeństwa" nie zawiera niestety tego, co nieodłącznie wiąże się z pojęciem „bezpieczeństwa" – oceny czynnika zagrożenia, z którym strategia miałaby mierzy się na poziomie narodowym i obywatelskim.[28]

Ostatni dokument z 2017 roku wnosi nową jakość do tego tematu. Niemniej w tym przypadku nie użyto jednak słowa „strategia", co pozwala przypuszczać, że na jego bazie formułowane mogą być określone strategie sektorowe.[29] Jak podkreślono we wstępie, został opracowany przez grupę składającą się z przedstawicieli resortów: cyfryzacji, obrony narodowej, spraw wewnętrznych i administracji oraz przedstawicieli Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa i Biura Bezpieczeństwa Narodowego. W „Krajowych Ramach Polityki Cyberbezpieczeństwa" określono czemu mają służyć działania organów powołanych w ramach struktury krajowej (zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni). Dokument wskazuje również na **możliwość powiązania działań operatorów infrastruktury krytycznej wykorzystujących systemy teleinformatyczne oraz potrzeb zaangażowania Sił Zbrojnych RP**. Podkreślono, że w kontekście ochrony cyberprzestrzeni polski „rząd będzie w pełni respektować prawo do prywatności oraz stać na stanowisku, że wolny i otwarty Internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa".

Zasada suwerenności pozwala rządom państw na realizację własnej polityki zagranicznej, co obejmuje również działania podejmowane w reakcji na wydarzenia mające źródło za granicą. Pod tym względem Internet może stanowić istotne medium transpozycji zjawisk niepożądanych, które mogą stać w opozycji do interesów państwa. Celem głównym wskazanym w treści *ram politycznych* jest *zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych.* W kontekście analizowanej problematyki bezpieczeństwa i polityki informacyjnej państw w domenie cyfrowej, duże znaczenie dla bezpieczeństwa Polski miałaby realizacja pierwszego celu szczegółowego: **osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa**.[30] Co jednak istotne, przypadki ingerencji w przestrzeń informacyjną Polski (np. działania organizacji ideologicznych lub pro-państwowych lub

[25] Ibid.
[26] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016 – 2020, Ministerstwo Cyfryzacji, Warszawa, 2016 https://www.gov.pl/documents/31305/0/strategia_v_29_09_2016.pdf/b621e7df-dca7-ad54-210c-5d58eec650f0
[27] Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022, Ministerstwo Cyfryzacji, Warszawa, 2017 https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/ f249b627-4050-a6f4-5cd3-351aa025be09
[28] Zapisy o zagrożeniach dla RP zawarto w Doktrynie Cyberbezpieczeństwa RP z 205 roku. W doktrynie bezpośrednio wskazano, że „Cyberprzestrzeń jest polem konfliktu, na którym przychodzi nam zmierzyć się nie tylko z innymi państwami, ale także z wrogimi organizacjami, jak choćby z grupami ekstremistycznymi, terrorystycznymi, czy zorganizowanymi grupami przestępczymi." Tym bardziej dziwi pominięcie tego zagadnienia w Strategii z 2016.
[29] W adresie internetowym kierującym do dokumentu pojawia się jednak słowo "strategia".
[30] Ibid.

narodowościowych obcych/wrogich państw) nie będą podlegać temu założeniu. Cyberbezpieczeństwo w tym przypadku polegać będzie jedynie na ochronie infrastruktury.

Jako użytkownicy Internetu, powinniśmy zdać sobie sprawę, że rozwój domeny cyfrowej postępuje w sposób błyskawiczny nie tylko ze względu na jego integrujący, społeczny charakter. Ogromną rolę w tym procesie odgrywa globalny czynnik komercyjny, w tym multiplikacji terytorium odbiorców - potencjalnych konsumentów usług telekomunikacyjnych i internetowych. Pod tym względem, dla skutecznej implementacji zaproponowanej *strategii* decydujące znaczenie będzie miało przyjęcie narodowej Ustawy o krajowym systemie cyberbezpieczeństwa 9z 31.10.2017 r.).[31] W odwołaniu do decyzji wykonawczej Komisji Europejskiej, w projekcie zawarto wymagania z zakresu cyberbezpieczeństwa, którymi objęci zostaną również **dostawcy usług cyfrowych**, czyli internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe. [32] Sygnalizuje się, że z racji międzynarodowej specyfiki tych podmiotów, obowiązki dla dostawców usług cyfrowych będą objęte łagodniejszym reżimem regulacyjnym.

Władze państwowe we własnym zakresie odpowiadają za realizację polityki bezpieczeństwa na swoim terytorium i zobowiązane są do ochrony obywateli, nie tylko przed atakiem zbrojnym. W przypadku Polski, i innych państw wspólnotowych (UE) i sojuszniczych (NATO), część tego ciężaru może być przeniesiona na szersze agendy, również w kontekście cyberbezpieczeństwa. Niemniej w interesie państwa jest monitorowanie, neutralizacja, przeciwdziałanie i ewentualna (proporcjonalna) odpowiedź wobec zagrożeń wymierzonych przeciwko strategicznym elementom „sieci", od których zależy funkcjonowanie zasadniczych obszarów państwa (sieci energetyczne, systemy bankowe, systemy dostaw wody pitnej, elektrownie, sieci agend bezpieczeństwa). W tym kontekście, niezwykle wrażliwą kwestią jest monitorowanie i zapobieganie inkorporacji do narodowej sfery informacyjnej treści spreparowanych przez aktorów (państwowych lub poza-państwowych) mogłyby wyrządzić szkodę demokratycznie ustanowionym strukturom państwowym lub wpływać na proces wyborczy, czy oddziaływać na podstawę legitymizacji władz. W tym kontekście jest jednak niezwykle ważne odpowiednie rozróżnienie prawdy od informacyjnego fałszu i niepodważalnej atrybucji źródła *fake news*. Należy przyznać, ze pod względem narzędzia, z których mogłyby skorzystać państwa liberalnej demokracji muszą mieć bardzo zaawansowany, a działania w tym zakresie - uzgodniony społecznie charakter.

Warszawa, listopad 2017

[31] https://www.gov.pl/cyfryzacja/projekt-ustawy-o-krajowym-systemie-cyberbezpieczenstwa

[32] Na forum regionalnego ciała European Internet Exchange Association (regionalnego forum zajmującego się koordynacją wymiany internetowych) Polska reprezentowana jest przez francuską firmę Orange TPIX. – źródło: https://www.euro-ix.net/about-euro-ix/members/ - Pobrano: 6.11.2017r.

| PUBLIKACJE

www.stratpoints.eu