PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 111 (2309), 8 CZERWCA 2021 © PISM

BIULETYN

Wojna w sieci. Polityka Rosji w zakresie międzynarodowego bezpieczeństwa informacyjnego

Agnieszka Legucka

Federacja Rosyjska (FR) w kwietniu br. zaktualizowała założenia swojej polityki w zakresie międzynarodowego bezpieczeństwa informacyjnego (MBI). W porównaniu z poprzednią wersją (z 2013 r.) dokument zawiera wskazanie możliwości wybuchu konfliktu międzypaństwowego w efekcie działań w cyberprzestrzeni. FR promuje też koncepcję suwerennego internetu i dąży do zwiększenia swoich wpływów w zakresie globalnych regulacji dotyczących rozwoju sieci. Publikacja dokumentu potwierdza priorytetowe traktowanie bezpieczeństwa informacyjnego w strategii bezpieczeństwa narodowego, a także w polityce zagranicznej FR.

Cele i interesy Rosji. FR podkreśla polityczny i społeczny charakter globalnej konfrontacji w sferze informacyjnej i uważa zmagania w cyberprzestrzeni za część wojny informacyjnej prowadzonej przeciwko niej przez państwa zachodnie. Odróżnia to rosyjskie postrzeganie bezpieczeństwa informacyjnego od dyskursu zachodniego, w którym dominuje troska o bezpieczeństwo danych osobowych i ochronę przed cyberatakami (np. na infrastrukturę krytyczną).

Zgodnie z zatwierdzonym 12 kwietnia br. przez prezydenta Władimira Putina dokumentem Założenia polityki FR w zakresie międzynarodowego bezpieczeństwa informacyjnego Rosja dąży do wzmocnienia roli podmiotów rządowych w przestrzeni informacyjnej. W polityce wewnętrznej jest to podyktowane potrzebą ograniczenia dostępu rosyjskich obywateli do niezależnych treści, aby zapobiegać niepokojom społecznym i destabilizacji wewnętrznej. W wymiarze międzynarodowym Rosja zapowiada dążenie do zapewnienia globalnego pokoju, bezpieczeństwa i stabilności, jednak w rzeczywistości zależy jej na uzyskaniu wpływu na regulowanie sfery informacyjnej. Oznacza to też zmianę rosyjskiej definicji MBI w porównaniu z 2013 r., kiedy podkreślano wagę ochrony praw jednostek, społeczeństw i państw.

Deklarowanym nowym celem polityki FR w zakresie MBI jest przeciwdziałanie konfliktom międzypaństwowym w sferze informacyjnej i regulowanie już istniejących. Według poprzedniej wersji dokumentu celem było tylko zwiększenie wpływu na regulowanie systemu bezpieczeństwa informacyjnego. Władze rosyjskie nadal chcą wzmocnienia kontroli nad ruchem w sieci (tzw. koncepcja suwerennego internetu) oraz nad treściami medialnymi, a także wprowadzenia kodeksu postępowania państw w cyberprzestrzeni. Rosja jest aktywna na wielostronnych forach (w ONZ) poświęconych zagadnieniom bezpieczeństwa informacyjnego i aspiruje do tego, aby stać się twórcą norm w tej dziedzinie.

Założenia polityki Rosji w zakresie bezpieczeństwa informacyjnego są dokumentem planowania strategicznego. Wpisują się w dotychczasowe pomysły FR dotyczące sfery informacyjnej, wskazane m.in. w Doktrynie wojennej z 2014 r., Strategii bezpieczeństwa narodowego z 2015 r. oraz Doktrynie bezpieczeństwa informacyjnego z 2016 r., w których Rosja włączyła broń informacyjną do defensywnego i ofensywnego katalogu zdolności militarnych FR.

Wyzwania i zagrożenia dla Rosji. Zidentyfikowane w dokumencie zagrożenia w ramach MBI dotyczą głównie

wykorzystania technologii w przestrzeni informacyjnej, czyli zakłócenia procesów przetwarzania, przechowywania i dostarczania informacji, a także ataków na oprogramowanie i sprzęt. Wymienione zagrożenia i wyzwania w dziedzinie MBI wyraźnie kontrastują jednak z aktywnością Rosji w sieci. Jako niebezpieczne wskazano m.in. ataki hakerskie. Chociaż rząd FR przyznał, że w ub.r. doszło do wzmożonych włamań do rosyjskich agencji federalnych, to właśnie władze Rosji są najczęściej odpowiedzialne za organizowanie cyberataków w świecie. Do największego z nich doszło w grudniu ub.r. wobec wielu agencji rządowych USA, w tym m.in. Departamentu Skarbu oraz Obrony, gdy tysiące użytkowników, aktualizując oprogramowanie SolarWinds, wprowadziło wirusa do swoich komputerów. Rosja podkreśla ponadto, że wyzwaniem dla niej pozostaje nadal dominacja technologiczna innych państw (tj. USA), jednak rosyjskie wydatki na badania i rozwój są na niskim poziomie (ok. 1% PKB, w porównaniu z UE, która przeznacza ok. 3%).

Kolejnym zagrożeniem wskazanym w dokumencie jest wykorzystanie technologii do celów terrorystycznych, przestępczych i ekstremistycznych. Przepisy dotyczące tych zagrożeń stają się jednak często pretekstem dla władz rosyjskich do sądzenia własnych obywateli. W związku z internetową popularnością opozycjonisty Aleksieja Nawalnego (opublikowany przez niego film o prezydencie Władimirze Putinie miał 116 mln wyświetleń na Youtube) jego Fundacja Walki z Korupcją została w kwietniu br. oskarżona o ekstremizm i w efekcie prawdopodobnie zostanie zdelegalizowana.

Międzynarodowy wymiar polityki Rosji. Jedną z rosyjskich propozycji regulacji MBI jest przyjęcie konwencji tematycznej w ramach ONZ w sprawie bezpieczeństwa w cyberprzestrzeni. Pomysły Rosji dotychczas nie zyskały szerszego poparcia międzynarodowego. FR udało się wprawdzie zdobyć większość głosów w grudniu 2018 r. dla dwóch rezolucji w Zgromadzeniu Ogólnym, ale mają one charakter niewiążący. Pierwsza z nich zwiększała uprawnienia państw w zarządzaniu cyberprzestrzenią, a także stanowiła, że oskarżenia innych państw o bezprawne działania w sieci muszą być uzasadnione i powinny brać pod uwagę wszystkie istotne informacje, łącznie z możliwościami technologicznymi i konsekwencjami, jakie mogą wynikać z takich oskarżeń. Jej efektem jest rozmycie odpowiedzialności strony podejmującej atak. W rezolucji FR zaproponowała też włączenie wszystkich zainteresowanych państw ONZ do Grupy Ekspertów Rządowych ds. Rozwoju Informacji i Telekomunikacji (Group of Govermental Experts, GGE), która przygotowuje zasady postępowania państw w cyberprzestrzeni. Miałoby to umożliwić Rosji przeforsowanie koncepcji suwerennego internetu i w przyszłości przyjęcie wiążącej konwencji.

Druga rosyjska rezolucja dotyczyła zwalczania cyberprzestępstw. Rosji zależy na przekazaniu koordynacji współpracy między państwami z poziomu Rady Europy (RE) do ONZ, ponieważ nie ratyfikowała konwencji RE o walce z cyberprzestępczością z 2001 r. FR nie zgodziła się m.in. na możliwość prowadzenia przez służby innych państw operacji na swoim terytorium, gdyż zdaniem władz mogło naruszać to jej suwerenność.

W zakresie międzynarodowych regulacji sfery informacyjnej FR znajduje zwolenników wśród państw trzecich, m.in. członków Szanghajskiej Organizacji Współpracy (SzOW), Organizacji Układu o Bezpieczeństwie Zbiorowym (OUBZ), a także w ramach ASEAN i BRICS. Wspierają one Rosję zarówno na forum ONZ, jak również w zwalczaniu zagrożeń na poziomie regionalnym. W ramach OUBZ 1 kwietnia 2019 r. weszła w życie Umowa o współpracy państw członkowskich w dziedzinie bezpieczeństwa informacji.

Wnioski. Zaktualizowane założenia polityki FR w zakresie MBI potwierdzają, że w przeciwieństwie do państw zachodnich władze Rosji nie dostrzegają potrzeby ochrony praw człowieka w cyberprzestrzeni. Rosja w zamian kładzie nacisk na suwerenizację przestrzeni informacyjnej, czyli państwową kontrolę ruchu w sieci i przekazów medialnych. Ma to pomóc w umocnieniu reżimu politycznego w Rosji przez ograniczenie jej obywatelom dostępu do niezależnych treści.

Wraz z umacnianiem się reżimów autorytarnych w świecie coraz bardziej prawdopodobna staje się realizacja promowanej przez Rosję koncepcji suwerennego internetu, zarówno na poziomie globalnym (ONZ), jak i regionalnym (OUBZ, SzOW). Chociaż Rosja zyskuje poparcie części członków ONZ, państw afrykańskich i azjatyckich (w tym Chin) dla idei zwiększenia regulacji na poziomie międzyrządowym, dotychczas nie udało jej się przeforsować wiążącej konwencji dotyczącej MBI.

Rosja postrzega sferę informacyjną jako obszar konfrontacji międzynarodowej, w którym może dojść do wybuchu konfliktu między państwami. Mimo deklaracji dotyczących pokoju i zapobiegania cyberatakom Rosja będzie doskonalić możliwości technologiczne w sferze komunikacyjno-informacyjnej i używać ich do celów wojskowo-politycznych. Od aneksji Krymu w 2014 r. Rosja prowadzi skoordynowane działania hybrydowe wobec Ukrainy. Występuje także przeciwko państwom Unii Europejskiej, które stają się obiektem ataków mających podważyć zaufanie społeczeństw do ich rządów, co jest szczególnie istotne w kontekście zbliżających się wyborów w Niemczech (2021 r.) i Francji (2022 r.).

Perspektywa fragmentacji sieci, czyli tworzenia barier w ruchu internetowym, może przynieść negatywne konsekwencje dla państw zachodnich, w tym Polski, ponieważ utrudni komunikację ze społeczeństwami Europy Wschodniej (w Rosji czy na Białorusi). Dlatego polska dyplomacja może wspierać inicjatywy mające na celu zwiększenie bezpieczeństwa w cyberprzestrzeni i umocnienie regulacji międzynarodowych dotyczących ochrony danych osobowych i walki z cyberprzestępczością, bez uszczerbku dla ochrony praw jednostki w sieci.