# SYSTEM
## BEZPIECZEŃSTWA
## W CYBERPRZESTRZENI RP

WARSZAWA
2018

Recenzenci:
płk dr hab. inż. Piotr Dela, prof. ASzWoj
dr hab. Mirosław Karpiuk, prof. UWM

Redakcja naukowa:
prof. dr hab. inż. Waldemar Kitler
dr hab. Katarzyna Chałubińska-Jentkiewicz, prof. ASzWoj
dr Katarzyna Badźmirowska-Masłowska

Opracowanie redakcyjne:
Lech Mleczko i Zbigniew Moszumański

Opracowanie językowe i korekta:
Krystyna Koziorowska

Opracowanie graficzne i projekt okładki:
Anna Skowrońska IDEAPRESS



Publikacja dofinansowana ze środków Akademii Sztuki Wojennej

Teksty zawarte w publikacji są efektem realizacji zadania badawczego „System cyberbezpieczeństwa RP – model rozwiązań prawnych" w ramach programu GRANT BADAWCZY MON [Nr umowy GB/4/2018/2018/DA]

ISBN 978-83-944423-5-4 (miękka oprawa)
**ISBN 978-83-68170-14-6 (pdf)**
ISBN 978-83-68170-15-3 (epub)
ISBN 978-83-68170-16-0 (mobi)

Wydanie I

Wydawca:
Wydawnictwo Towarzystwa Wiedzy Obronnej
ul. 11 Listopada 17/19, 03-446 Warszawa
www.two.edu.pl
e-mail: kontakt@two.edu.pl

SKŁAD
Agencja Wydawnicza IDEAPRESS
Łukowska 1/149, 04-113 Warszawa
www.ideapress.pl

# SPIS TREŚCI

# Wstęp

Współczesne społeczeństwo często jest nazywane społeczeństwem informacyjnym, społeczeństwem trzeciej fali lub cyberspołeczeństwem. Na określenie nowej cywilizacji używane są również takie terminy, jak: era informacyjna, era kosmiczna, era elektroniczna czy też globalna wioska. Istnieje wiele definicji. Można przyjąć, że społeczeństwo informacyjne to takie, które posiada instrumenty techniczne i prawne, ale przede wszystkim ma wiedzę, która pozwala mu z tych instrumentów korzystać; dlatego często mówimy o społeczeństwie opartym na wiedzy. Jednym z podstawowych obszarów wiedzy TIK (technologie informacyjno-komunikacyjne – *Information and Communication Technologies*), którego znaczenie wciąż rośnie, jest bezpieczeństwo. Według „Computerworld Polska" (luty 2016, nr 2/1057) wartość rynku związanego z cyberbezpieczeństwem wrosła w 2014 r. w Polsce o 8 proc. i przekroczyła 300 mln dolarów. Z tym faktem wiąże się wzrost zatrudnienia w sektorze TIK, a tendencja ta według analityków ma się utrzymać do 2019 r. Tym samym specjalizacja z zakresu cyberbezpieczeństwa pojawia się na liście najbardziej poszukiwanych kompetencji. Szacunki wskazują także, iż wojsko potrzebuje co roku przynajmniej około 50 specjalistów w zakresie cyberbezpieczeństwa, w tym ekspertów w zakresie kryptografii, organizacji oraz bezpieczeństwa systemów teleinformatycznych, z dobrą znajomością regulacji prawnych związanych z tym obszarem.

Od pewnego czasu pojęcie bezpieczeństwa państwa silnie wiąże się z bezpieczeństwem sieci i cyberprzestrzeni. Należy zaznaczyć, że bezpieczeństwo w cyberprzestrzeni zawsze było obecne w polityce

bezpieczeństwa i obronności państwa jako ważny obszar łączący procedury oraz instrumenty prawne ochrony danych, informacji i systemów. Jest ono niezbędnym elementem prawidłowego postępu naukowo-technicznego i jako takie określa potrzeby ochrony tego obszaru nie tylko z punktu widzenia użyteczności, ale również ze względu na przeciwdziałanie zupełnie nieznanym dotąd zagrożeniom. W dziedzinie cyberbezpieczeństwa pojawia się wiele określeń, takich jak: bezpieczeństwo informatyczne, cyberbezpieczeństwo, bezpieczeństwo teleinformatyczne. W dobie globalnej informatyzacji, także sfery publicznej, w warunkach rozwoju portali społecznościowych, wszechobecnego mailingu, czyli wiadomości rozsyłanych na wiele adresów e-mailowych zgromadzonych w bazie danych, często dochodzi do nieuprawnionych działań, które mogą stanowić naruszenie dóbr osobistych, prawa własności czy praw konsumenckich. Jednak coraz częściej pojawiają się także cyberzagrożenia innego typu, które dotykają struktur władzy publicznej i samego państwa. Współcześnie, kiedy strefa prywatności człowieka wolna od ingerencji osób trzecich stopniowo się kurczy, w jednakowym, a może nawet większym stopniu proces ten dotyczy obszaru prawidłowego działania administracji publicznej oraz jej służb, także sił zbrojnych.

Przetwarzanie informacji w przestrzeni wirtualnej powoduje, iż konieczne staje się regulowanie kwestii dostępu do nich; dostęp ów może się bowiem stać źródłem zagrożeń, nawet w przypadku, kiedy nie mają one charakteru niejawnego. Coraz częściej ataki na informacje lub przy wykorzystaniu informacji przyjmują charakter masowy i wielokierunkowy. Ale nie tylko o ochronę informacji tu chodzi. Zagrożenia, jak określa to definicja cyberprzestrzeni, mogą wynikać z relacji między sieciami, między sieciami i komputerami, a także z relacji użytkowników z sieciami i komputerami; dotyczy to również relacji między użytkownikami oraz między komputerami.

Na ten globalny charakter zagrożeń związanych z bezpieczeństwem w cyberprzestrzeni wskazują kolejne debaty dotyczące przyszłych uregulowań prawnych. Jedną z nich była konferencja na temat „System bezpieczeństwa w cyberprzestrzeni RP", która odbyła się 11 grudnia 2018 r. w Sejmie RP, a której organizatorami byli: Komisja Obrony Narodowej Sejmu RP, Komisja Administracji i Spraw Wewnętrznych Sejmu RP we współpracy z Katedrą Prawa Mediów, Własności Intelektualnej i Prawa

Nowych Technologii Instytutu Prawa i Administracji Obronnej Wydziału Bezpieczeństwa Narodowego Akademii Sztuki Wojennej w Warszawie. W trakcie tego dyskursu pojawiła się dyrektywa wskazująca na potrzebę budowy systemu cyberbezpieczeństwa w Polsce obejmującego różne obszary działania jednostki i państwa oraz różne poziomy interwencji regulacyjnej. Efektem tych analiz jest przekazana w Państwa ręce publikacja. Należy zaznaczyć, że praca ta stanowi samodzielną monografię obejmującą szereg zagadnień, albowiem także poruszana w niej problematyka cyberbezpieczeństwa to obszar interdyscyplinarny obejmujący sektor publiczny oraz sektor prywatny.

Wobec wskazanych powyżej uwarunkowań konieczne stało się ukierunkowanie rozważań naukowych na zagadnienia związane z cyberbezpieczeństwem. To także konieczny element prawidłowego rozwoju społeczeństwa w zakresie organizacji i zarządzania obronnością państwa, zarówno w kontekście zewnętrznego bezpieczeństwa państwowego, jak i bezpieczeństwa wewnętrznego, praktycznie na każdym poziomie funkcjonowania społeczeństwa i samej administracji (struktura rządowa oraz samorządowa z organizacją krajowej infrastruktury państwa).

Należy zatem przyjąć, że cyberbezpieczeństwo jest zjawiskiem interdyscyplinarnym, korzystającym z dorobku wielu innych dziedzin (w tym z różnych dziedzin prawa). Aby jednak wyodrębnić je z całego systemu prawa i administracji publicznej (w tym drugim przypadku przede wszystkim organizacyjnie i podmiotowo), konieczne jest określenie zakresu działania, jakiego sfera ta dotyczy (zarówno w sensie przedmiotowym, podmiotowym, organizacyjnym, jak i funkcjonalnym). Dopiero wówczas będzie możliwe usystematyzowanie przedstawionej problematyki. W naszym przekonaniu jest to zabieg niezbędny w obliczu rozwoju TIK i cyberprzestrzeni oraz zagrożeń z nimi związanych dla obronności państwa i bezpieczeństwa jednostki. Wstępna diagnoza postawiona w niniejszej pozycji stanowi pierwszy krok w próbach dookreślenia zakresu merytorycznego systemu cyberbezpieczeństwa RP.

Waldemar Kitler
Katarzyna Chałubińska-Jentkiewicz
Katarzyna Badźmirowska-Masłowska

I

# Odpowiedzialność w cyberprzestrzeni RP

Katarzyna Chałubińska-Jentkiewicz[1]

# Odpowiedzialność w sieci – diagnoza stanu obecnego

Dynamiczne zmiany cywilizacyjne obserwowane w ostatnich latach na całym świecie są skutkiem gwałtownego rozwoju technik informacyjnych oraz wspomagających je technologii informacyjno-komunikacyjnych. Nową sferą oddziaływania tych procesów jest cyberprzestrzeń jako piąty obszar działań obronnych. Według W. Kitlera dziedziny bezpieczeństwa mogą mieć swoją odrębność i być powiązane z określonymi sektorami państwa, lecz są takie – i będzie ich coraz więcej – które nie mają charakteru branżowego, ale transsektorowy, transdyscyplinarny. Do takich należy np. bezpieczeństwo informacyjne, cybernetyczne, antyterrorystyczne, ustrojowe, informacji niejawnych[2]. W powszechnym rozumieniu bezpieczeństwo jest postrzegane przede wszystkim w negatywnym znaczeniu jako stan cechujący się brakiem zagrożeń, ale także brakiem niebezpieczeństw, pewnością, spokojem, ochroną przed zagrożeniami[3].

---

[1] Dr hab. Katarzyna Chałubińska-Jentkiewicz – prof. Akademii Sztuki Wojennej, kierownik Katedry Prawa Mediów, Własności Intelektualnej i Nowych Technologii, IPiAO WBN.

[2] Zob. *Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, BBN, Warszawa 2013, s. 19 (rys. 1).

[3] Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne.

Osiąga się je przez ochronę zasobów informacyjnych państwa, ochronę przed działaniami wrogimi (dezinformacja i propaganda), a także utrzymywanie zdolności do działań ofensywnych wobec sprawców tych działań. Pojęcie „bezpieczeństwo sieci i informacji" zostało zdefiniowane w Rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 460/2004 z 10 marca 2004 r., ustanawiającym Europejską Agencję do spraw Bezpieczeństwa Sieci i Informacji, jako „odporność sieci lub systemu informacyjnego na zdarzenia przypadkowe lub działania nielegalne albo podstępne, naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych oraz związanych z nimi usług oferowanych lub dostępnych przez te sieci i systemy"[4].

Należy podkreślić, że bezpieczeństwo informacyjne jako tylko jeden z elementów cyberbezpieczeństwa zostało poddane regulacjom na gruncie przepisów karnych (patrz – *Przestępstwa przeciwko informacji* – rozdz. 33 k.k.[5]), przepisów ustawy o ochronie danych osobowych oraz przepisów ustawy o ochronie informacji niejawnych. Wpływ na bezpieczeństwo mają wszystkie interakcje społeczne, a sama kultura bezpieczeństwa określa, jaki jest stosunek danej społeczności do ryzyka, zagrożeń i bezpieczeństwa oraz jakie wartości w tym zakresie uważane są za istotne. Podstawowa konstrukcja internetu opiera się na otwartości zarówno architektury jego infrastruktury, jak i kultury jego twórców i użytkowników. Prostota i łatwość łączenia różnych komputerów pozwoliła na ogromne rozszerzenie liczby użytkowników, a otwarta filozofia jego kształtowania stworzyła z niego ogromnie atrakcyjne, interakcyjne na wielu poziomach medium"[6].

Cyberprzestępczość jest zjawiskiem stosunkowo nowym, jednak bardzo szybko się rozwijającym. Obecnie prawie każdy ma możliwość korzystania z sieci teleinformatycznej i dostępu do jej zasobów. Cyberprzestępczość z racji coraz bardziej powszechnego dostępu do sieci może godzić w interesy państwa, które część swoich spraw przenosi na pole sieci teleinformatycznej, co czasem może nawet doprowadzić

[4] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 460/2004 z dnia 10 marca 2004 r. ustanawiające Europejską Agencję do spraw Bezpieczeństwa Sieci i Informacji.

[5] Kodeks karny z dnia 6.06 1997 r, Dz.U. 1997 nr 88 poz. 553; na podstawie: Dz.U. z 2018 poz. 1600, 2077.

[6] T. Goban-Klas, *Cywilizacja medialna*, Warszawa 2005, s. 151.

do podważenia jego suwerenności[7]. Dzieje się tak, ponieważ nie wszyscy użytkownicy dobrze rozumieją mechanizmy działania sieci teleinformatycznej, co prowadzi do swego rodzaju ignorancji własnego bezpieczeństwa w cyberprzestrzeni[8]. Cyberprzestępczość obejmuje zarówno te czyny, które stanowią odzwierciedlenie przestępczości w świecie rzeczywistym, jak i zupełnie nowe zjawiska, charakterystyczne wyłącznie dla cyberprzestrzeni, a stanowiące zagrożenia dla jednostki czy państwa. W Raporcie głównym o zagrożeniach bezpieczeństwa narodowego wyróżniono około 50 typów zagrożeń, przy czym 18 z nich zawarto w Krajowym Planie Zarządzania Kryzysowego, wśród nich zagrożenie cyberterroryzmem[9]. W przypadku ataków cybernetycznych wymieniono jedynie możliwe skutki ataków cybernetycznych dla ludzi i mienia. Jako potencjalne skutki dla ludności wymienia się: zagrożenie dla życia i zdrowia ludzi spowodowane zakłóceniami systemów energetycznych, sterowania ruchem itp., utratę zaufania do instytucji publicznych, brak możliwości realizacji zadań merytorycznych, brak możliwości komunikacji.

Jako potencjalne skutki dla mienia wymienia się tak zasadnicze punkty, jak: znaczące straty finansowe i gospodarcze oraz skutki społeczne, zakłócenia zaopatrzenia w energię, paliwa, żywność, wodę pitną, zakłócenia pracy infrastruktury przesyłowej.

Z kolei zarządzanie kryzysowe obejmuje wprawdzie swoim zakresem sieci teleinformatyczne, ale bardziej jako jeden z typów sieci przesyłowych, i zarazem w ogóle nie uwzględnia warstwy udostępniania, przetwarzania i przechowywania informacji, która przenika wszelkie aspekty funkcjonowania społeczeństwa informacyjnego. W dokumencie Sprawozdanie z szacowania ryzyka cyberprzestrzeni w administracji rządowej w 2013 r. przyjęto następujące główne kategorie i podkategorie zagrożeń: zagrożenia ukierunkowane na informacje (kradzież informacji celem publikacji bądź sprzedaży, fałszowanie informacji), zagrożenia ukierunkowane na infrastrukturę teleinformatyczną (usunięcie danych, zakłócenie

[7] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno-karne*, Warszawa 2011, s. 24.

[8] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii*, Warszawa 2016, s. 353.

[9] Online <http://rcb.gov.pl/raport-o-zagrozeniach-bezpieczenstwa-narodowego-3/>, dostęp 16.09.2018.

funkcjonowania, przejęcie systemu teleinformatycznego), awarie IT, niedostateczne kompetencje[10].

Podejście regulatorów do zagadnienia cyberprzestrzeni, cyberbezpieczeństwa i cyberodpowiedzialności wynika z utożsamiania tego rodzaju ochrony z potrzebą przeciwdziałania atakom nakierowanym na same sieci, co wydaje się nieuzasadnione, zwłaszcza w kontekście analizy pojęcia cyberprzestrzeni[11]. Wskazane powyżej rozumienie cyberprzestrzeni przeniknęło do języka prawnego razem z początkiem obowiązywania ustawy z 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw[12]. Polska definicja pojęcia cyberprzestrzeni znajduje się w ustawie z 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[13]. Kolejną definicję legalną pojęcia cyberprzestrzeni zawiera ustawa z 21 czerwca 2002 r. o stanie wyjątkowym[14]. Według powyższej ustawy przez cyberprzestrzeń rozumie się „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne określone w art. 3 pkt 3 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[15], wraz z powiązaniami między nimi oraz relacjami z użytkownikami"[16]. Taką samą definicję legalną zawiera ustawa z 18 kwietnia 2002 r. o stanie klęski żywiołowej[17]. Ustawy te odnoszą się

[10] *System bezpieczeństwa cyberprzestrzeni RP*, NASK / CERT Polska s. 62, Warszawa, wrzesień 2015 r. <https://mac.gov.pl/files/nask_rekomendacja.pdf>, dostęp 16.09.2016 r.

[11] Zob. więcej na ten temat: K. Chałubińska-Jentkiewicz, *Cyberprzestępczość jako paradygmat pojęcia bezpieczeństwa w cyberprzestrzeni*, „Wojskowy Przegląd Prawniczy" nr 3 (279) 2016, s. 46-64.

[12] Dz.U. 2011 nr 222, poz. 1323.

[13] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. z 2002 r. nr 156 poz. 1301.

[14] Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz.U. z 2002 r. nr 113 poz. 985.

[15] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. z 2005 r. nr 64 poz. 565.

[16] Art.2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym.

[17] Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, Dz.U. z 2002 r. nr 62 poz. 558.

do zachowań w płaszczyźnie wirtualnej, w jakiej poruszają się podmioty prawa w momencie wystąpienia jednego z trzech stanów nadzwyczajnych. Przyjęta w Założeniach Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej koncepcja krajowego systemu cyberbezpieczeństwa obejmuje m.in. przebudowanie definicji cyberprzestrzeni i jej rozciągnięcie na sferę kluczowych operatorów funkcjonujących w sferze gospodarczej.

**Pojęcie cyberprzestrzeni można zatem sformułować jako syntezę wszystkich fizycznych i technicznych środków pozwalających na wymianę informacji drogą elektroniczną oraz relacji użytkowników posiadających dostęp do jej zasobów.**

Cyberbezpieczeństwo czy bezpieczeństwo sieci jest pojęciem odnoszącym się do zapewnienia ochrony i przeciwdziałania zagrożeniom, które dotykają samej cyberprzestrzeni, jak i funkcjonowania w cyberprzestrzeni, a dotyczy to zarówno sektora publicznego, jak i prywatnego oraz ich wzajemnych relacji. Aczkolwiek zgodnie z art. 2 pkt 4 ustawy z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa[18] – cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Zatem definicja ta odnosi się jednak do zagadnień technicznej natury i ochrony sieci jako takiej. Natomiast na rzecz tego stanowiska, zgodnie z którym cyberbezpieczeństwo ma charakter znacznie szerszy, interdyscyplinarny, przemawia charakterystyka pojęcia cyberzagrożenia jako pojęcia obejmującego swoim zakresem incydenty, jakie pojawiają się w cyberprzestrzeni[19]. Przy czym incydentem zgodnie z art. 2 pkt 5 ustawy o krajowym systemie cyberbezpieczeństwa jest incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Natomiast zgodnie z art. 2 pkt 6 incydent krytyczny to incydent skutkujący znaczną szkodą dla bezpieczeństwa

[18] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560.

[19] Zaznaczyć także trzeba, że jednym z wciąż podstawowych problemów dotyczących odpowiedzialności w sieci jest zagadnienie jurysdykcji terytorialnej, która znalazła zastosowanie w przepisach Konwencji o cyberprzestępczości. Problemy z ustaleniem osoby przestępcy, a jak wiadomo większość przestępstw popełnianych jest w innych państwach niż faktyczne miejsce przebywania przestępcy, utrudnia działania związane z efektywnością ścigania cyberprzestępczości.