*Joanna Worona*
*Uniwersytet w Białymstoku*

# PRACE NACZELNYCH ORGANÓW ADMINISTRACJI PAŃSTWOWEJ A CYBERBEZPIECZEŃSTWO POLSKI

## 1. Wprowadzenie

Cyberbezpieczeństwo kraju jest jednym z głównych celów strategicznych w obszarze bezpieczeństwa każdego z państw. Systematycznie wzrastająca liczba zagrożeń i incydentów w cyberprzestrzeni oraz stopień i ich zaawansowania stanowi aktualnie jeden z istotniejszych problemów w świetle zapewnienia niezakłóconego funkcjonowania państwa, gospodarki i społeczeństwa. Zagrożenia w cyberprzestrzeni są tak różnorodne, że niezbędna jest skoordynowana praca różnych organów centralnej administracji państwowej.

Naczelne organy administracji państwowej RP od lat podejmują działania w celu zapewnienia cyberbezpieczeństwa kraju. Choć zagadnienie ma charakter międzyresortowy, to główne prace mają miejsce w m.in. Ministerstwie Obrony Narodowej, Ministerstwie Spraw Wewnętrznych i Administracji oraz Ministerstwie Cyfryzacji[1]. Celem prowadzonych projektów jest zapewnienie bezpieczeństwa cyberprzestrzeni za pomocą tworzenia odpowiednich ram prawnych, procedur i systemów wymiany informacji pomiędzy administracją publiczną a innymi podmiotami i użytkownikami sieci.

## 2. Cyberbezpieczeństwo państwa – pojęcie

Informację, w tym informację przekazywaną za pomocą systemu komputerowego bez wątpienia można uznać za strategiczny zasób państwa podlegający ochronie. Swobodny i niezakłócony przepływ informacji jest niezbędny z punktu widzenia państwa, które jest coraz bardziej uzależnione od prawidłowego funkcjonowania systemów informatycznych. E. Nowak i M. Nowak uznają, że bezpieczeń-

1 Od listopada 2015 r. Ministerstwo Cyfryzacji zastąpiło Ministerstwo Administracji i Cyfryzacji.

stwo informacyjne jest to „taki stan warunków wewnętrznych i zewnętrznych, który pozwala państwu na posiadanie, przetwarzanie i swobodę rozwoju społeczeństwa informacyjnego. Stan ten jest osiągnięty, gdy spełnione są następujące warunki: nie są zagrożone strategiczne zasoby informacyjne państwa, organy władzy podejmują decyzje w oparciu o wiarygodne, istotne, dokładne i aktualne informacje, zaś przepływ informacji między tymi organami nie jest zakłócony, bezpieczeństwo sieci teleinformacyjnych (publicznych, resortowych i prywatnych tworzących krytyczną infrastrukturę teleinformatyczną państwa), prawny system ochrony informacji oraz ochrona danych osobowych obywateli są z mocy prawa gwarantowane przez państwo, zapewnione jest prawo obywateli do prywatności, instytucje publiczne i prywatne zbierając informacje o obywatelach, organizacjach i ich działalności, nie naruszają norm prawnych, obywatele i ich przedstawiciele (media, organizacje pozarządowe, parlamentarzyści, organy kontrolne) posiadają dostęp do informacji o działalności władz państwa”[2].

W Białej Księdze Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej bezpieczeństwo informacyjne (w tym cyberbezpieczeństwo) państwa zostało zdefiniowane jako: „transsektorowy obszar bezpieczeństwa, którego treść (cele, warunki, sposoby, środki) odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa.[3]” W dokumencie strategicznym Polityka Ochrony Cyberprzestrzeni RP stwierdzono z kolei, że bezpieczeństwo cyberprzestrzeni jest to „zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni”.[4]

Definicję cyberbezpieczeństwa Polski odnajdziemy również w Doktrynie Cyberbezpieczeństwa RP (dalej: DC RP) z 2015 r. W dokumencie tym przyjęto, że cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni) jest to „proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni[5].” Z kolei za bezpieczeństwo cyberprzestrzeni RP uznano „część cyberbezpieczeństwa państwa, obejmującą zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych”[6].

2 E. Nowak, M. Nowak, Zarys teorii bezpieczeństwa narodowego. Zarządzenie bezpieczeństwem, Warszawa 2011, s. 103.
3 Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013, s. 248.
4 Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa 2013, s. 5.
5 Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, Warszawa 2015, s. 7-8.
6 *Ibidem*, s. 8.

## 3. Zagrożenia w cyberprzestrzeni

Rozwój Internetu i nowych technologii spowodował, iż państwo musi zmierzyć się z nowymi, nieznanymi wcześniej formami zagrożeń, tj. cyberwojna, cyberataki, walka informacyjna, konflikt hybrydowy czy asymetryczny. Przestrzeniami, które winne podlegać szczególnej ochronie są systemy informatyczne, jako część infrastruktury krytycznej państwa. Systemy teleinformatyczne zarządzają dziś tak istotnymi elementami infrastruktury, jak systemy zaopatrzenia w energię, paliwa, wodę i żywość, systemy finansowe, transportowe, sieci łączności czy też służby ochrony zdrowia. Zakłócenie poprawnego działania takich systemów może doprowadzić do paraliżu komunikacyjnego państwa i ogromnych strat finansowych. Wskazane systemy narażone są na cztery zasadnicze grupy zagrożeń: cyberprzestępczość, cyberinwigilację, cyberterroryzm i cyberwojny.[7] Ponadto, nie mniej istotne są zagrożenia związane z działalnością sił przyrody lub przypadkami losowymi[8].

Kluczowe zagrożenia w cyberprzestrzeni Rzeczypospolitej Polskiej zostały szczegółowo opisane w Doktrynie Cyberbezpieczeństwa RP z 2015 r.:

1. wymiar wewnętrzny:
   a. cyberprzestępczość, cyberprzemoc, cyberprotesty i cyberdemonstracje,
   b. celowe ataki na systemy łączności uniemożliwiające niezakłócone funkcjonowanie podsystemów kierowania bezpieczeństwem narodowym, obronnością i ochroną oraz podsystemów wsparcia gospodarczego i społecznego,
   c. kradzież i naruszenie integralności oraz poufności danych podmiotów prywatnych, zwłaszcza sektorów finansowych, transportowych, energetycznych i zdrowia publicznego,
   d. zakłócenie działalności dostawców usług teleinformatycznych,
   e. cyberprzestępczość dotykająca obywateli RP, tj. kradzieże danych czy kradzieże tożsamości,
2. wymiar zewnętrzny:
   a. cyberkryzysy, cyberkonflikty z udziałem podmiotów państwowych, jak i niepaństwowych, groźba cyberwojny,
   b. cyberszpiegostwo innych państw i podmiotów pozapaństwowych, w tym organizacji terrorystycznych,
   c. działalność organizacji eksternistycznych, terrorystycznych oraz zorganizowanych transnarodowych grup przestępczych w cyberprzestrzeni.[9]

7 Z. Husak, Ochrona bezpieczeństwa państwa przed zagrożeniami cybernetycznymi w Unii Europejskiej, (w:) W. Lis (red.), Bezpieczeństwo państwa. Zagadnienia podstawowe, Lublin 2014, s. 56.

8 M. Marczyk, Bezpieczeństwo teleinformatyczne wobec ataków cyberterrorystycznych, (w:) M. Górka (red.), Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Warszawa 2014, s. 50.

9 Z. Husak, Ochrona..., *op. cit.*, s. 10-13.

O sprawności systemu cyberbezpieczeństwa państwa w dużej mierze decyduje odpowiednie zaplanowanie i funkcjonowanie warstwy operacyjnej, która jest w stanie szybko i efektywnie reagować na wszelkie pojawiające się incydenty i zagrożenia w cyberprzestrzeni. Przede wszystkim, by system ten był efektywny, winien zapewniać szybką i skoordynowaną reakcję różnych organów na sytuacje kryzysowe. Prawidłowe funkcjonowanie systemu nie jest możliwe bez stworzenia odpowiednich ram organizacyjno-prawnych, proceduralnych oraz szczegółowego określenia kompetencji poszczególnych organów państwa.

W niniejszym opracowaniu skupimy się nad pracami polskich naczelnych organów administracji rządowej w zakresie bezpieczeństwa cyberprzestrzeni. Wśród najważniejszych prac w zakresie cyberbezpieczeństwa Rzeczpospolitej Polskiej wymienić należy omówione poniżej dokumenty:

## 4. Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 (RPOC RP 2011-2016)

Program przygotowany przez Radę Ministrów RPOC RP na lata 2011-2016 jest kontynuacją programu o tożsamej nazwie przyjętego na lata 2009-2011. Jego głównym celem jest zapewnienie ciągłego bezpieczeństwa cyberprzestrzeni, co ma nastąpić za pomocą utworzenia ram organizacyjno-prawnych, systemu wymiany informacji i koordynacji działań pomiędzy administracją publiczną a pozostałymi użytkownikami sieci. Ponadto, w programie postawiono sobie za cel zwiększenie zabezpieczeń teleinformatycznej infrastruktury krytycznej państwa, zdefiniowanie kompetencji podmiotów publicznych w zakresie cyberbezpieczeństwa i stworzenie spójnego systemu zarządzania bezpieczeństwem w cyberprzestrzeni dla podmiotów administracji publicznej.[10]

Do najważniejszych założeń programu zaliczyć należy:

- zdefiniowanie pojęć dotyczących cyberprzestrzeni,
- wprowadzenie ścigania z urzędu naruszeń bezpieczeństwa w cyberprzestrzeni przeciwko podmiotom administracji publicznej i infrastruktury krytycznej,
- ustanowienie Pełnomocnika Rządu ds. Ochrony Cyberprzestrzeni RP oraz pełnomocników ds. ochrony cyberprzestrzeni w ramach poszczególnych jednostek organizacyjnych,
- powołanie Międzyresortowego Zespołu Koordynującego ds. Ochrony Cyberprzestrzeni RP, którego głównym zadaniem ma być koordynacja działania instytucji realizujących program,

10 Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, Warszawa 2010, s. 7.

- umocowanie prawne Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL[11] oraz sektorowych punktów kontaktowych,
- kształcenie kadry urzędniczej, przedsiębiorców i społeczeństwa w zakresie cyberbezpieczeństwa,
- rozbudowa zespołów reagowania na incydenty bezpieczeństwa teleinformatycznego w administracji publicznej.[12]

## 5. Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej

W Doktrynie Cyberbezpieczeństwa RP z 2015 r. za cel strategiczny przyjęto „zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni, w tym adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych – zwłaszcza teleinformatycznej infrastruktury krytycznej państwa – a także kluczowych dla funkcjonowania społeczeństwa prywatnych podmiotów gospodarczych, w szczególności wchodzących w skład sektorów: finansowego, energetycznego i ochrony zdrowia”[13]. Realizacja wymienionego celu ma zostać osiągnięta za pomocą celów operacyjnych, tj.: rozpoznawania, zapobiegania i zwalczania cyberzagrożeń, ochrony własnych zasobów i systemów, a w przypadku wystąpienia ataku – sprawnego odtworzenia newralgicznych systemów tworzących cyberprzestrzeń.[14] Ma to nastąpić poprzez zbudowanie i systematyczne doskonalenie zintegrowanego, ponadresortowego systemu cyberbezpieczeństwa, na który będzie składać się podsystem kierowania (koordynujący działania podmiotów rządowych i pozarządowych), podsystemy: operacyjne i wsparcia (samodzielnie prowadzące ofensywne i defensywne cyberoperacje)[15].

Podsystem kierowania miałby powstać poprzez poszerzenie zadań i kompetencji istniejącego ponadresortowego organu pomocniczego Rady Ministrów ds. szeroko rozumianego cyberbezpieczeństwa. Organ ten wyposażony miałby być w kompetencje doradcze, konsultacyjne, koordynacyjne oraz kompetencję koordynacji współpracy międzynarodowej. System kierowania cyberbezpieczeństwem winien być wsparty technicznymi centrami kompetencyjnymi, podległymi odpowiednim ministrom, które będą odpowiedzialne za wzmacnianie cyberbezpieczeństwa poszczególnych sektorów.[16] Podsystem operacyjny oparty został na Siłach Zbrojnych RP, które powinny umiejętnie bronić i chronić własne systemy teleinformatyczne i zgromadzone tam dane oraz prowadzić działania ofensywne i defen-

11 CERT (ang. *Computer Emergency Response Team*) – zespół reagowania na incydenty komputerowe. Jego zadaniem jest całodobowe nadzorowanie ruchu w cyberprzestrzeni i podejmowania natychmiastowych kroków w razie wystąpienia zagrożenia.
12 Rządowy Program..., *op. cit*., s. 15-27.
13 Doktryna..., *op. cit*., s. 10.
14 *Ibidem*.
15 *Ibidem,* s. 9.
16 *Ibidem*, s. 18.

sywne w cyberprzestrzeni. Za konieczne uznano też implementowanie standardów NATO w zakresie cyberobrony i rozwijanie cybernetycznych zdolności wywiadu i kontrwywiadu. Ostatnim podsystemem mają być publiczne i prywatne ogniwa wsparcia zapewniające współpracę sektorów publicznego i prywatnego w dziedzinie cyberbezpieczeństwa.[17]

## 6. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej (POC RP)

Głównym celem wydanego przez Ministerstwo Administracji i Cyfryzacji oraz ABW dokumentu jest „osiągniecie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa[18]". POC RP zakłada wprowadzenie corocznych sprawozdań jednostek administracji rządowej podsumowujących wyniki tzw. szacowania ryzyka w każdym sektorze. Dokument zakłada zwiększenie bezpieczeństwa portali administracji rządowej, wprowadzenie najlepszych praktyk i standardów w celu optymalizacji funkcjonowania cyberprzestrzeni RP. Nie mniej istotnym założeniem programu jest prowadzenie szkoleń z zakresu bezpieczeństwa cyberprzestrzeni, kształcenie kadry urzędniczej, edukowanie społeczeństwa, ale też programy badawcze i rozwój zespołów bezpieczeństwa.[19]

POC RP ustanawia również trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe w Cyberprzestrzeni Rzeczypospolitej Polskiej:

- poziom I – poziom koordynacji realizowany przez ministra właściwego ds. informatyzacji,
- poziom II – reagowanie na incydenty komputerowe za pomocą:
  - Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL
  - Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych (realizacja zadań w sferze militarnej)
- poziom III – poziom realizacji, w którym administratorzy odpowiadają za poszczególne systemy teleinformatyczne.[20]

## 7. System Bezpieczeństwa Cyberprzestrzeni RP

Ekspertyza przygotowana przez instytut badawczy Naukowej i Akademickiej Sieci Komputerowej (NASK) na zlecenie MCiA opisuje obecną sytuację prawnoorganizacyjną w dziedzinie ochrony cyberprzestrzeni Polski. Zaproponowano w niej

17 *Ibidem*, s. 19-22.
18 Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa 2013, s. 6.
19 *Ibidem*, s. 11-17.
20 *Ibidem*, s. 18.

trzy warianty organizacji przyszłego systemu, który miałby zapewnić cyberbezpieczeństwo RP:

- wariant zdecentralizowany (rozproszony) – zakłada wykorzystanie istniejących rozwiązań i instytucji w zakresie bezpieczeństwa cyberprzestrzeni, tj. CERT czy organów ABW i MON,[21]
- wariant pośredni – zakłada pewien stopień centralizacji poprzez powołanie koordynatora w postaci ministerstwa bądź ABW jako organizacji reagującej w warstwie operacyjnej,[22]
- wariant scentralizowany – zakłada stworzenie jednej, głównej instytucji – Narodowego Centrum Cyberbezpieczeństwa.[23]

Po dogłębnej analizie wymienionych wyżej wariantów zarekomendowano wybór wariantu rozproszonego, jako najbardziej optymalnego. Przyjęto, że ewolucja obecnego systemu powinna zostać zbudowana na podwalinach istniejących doświadczonych podmiotów.[24] Przyjęto również kluczowe rekomendacje mające na celu zwiększenie bezpieczeństwa cyberprzestrzeni RP:

- określenie ram systemu ochrony cyberprzestrzeni,
- precyzyjne określenie mechanizmów współpracy pomiędzy organami różnych szczebli,
- zharmonizowanie dokumentów strategicznych z zakresu cyberprzestrzeni – a docelowo utworzenie jednolitej strategii ochrony cyberprzestrzeni RP oraz powołanie instytucji koordynującej działania administracji publicznej w tym zakresie,
- powołanie zespołu szybkiego reagowania na zagrożenia i incydenty cyberbezpieczeństwa na poziomie krajowym,
- powołanie organu opiniodawczego i doradczego ds. cyberbezpieczeństwa dla Rady Ministrów,
- powołanie Krajowego Centrum Analitycznego – organu dokonującego analizy zagrożeń cyberprzestrzeni, reagowania na ataki i rekomendowania działań profilaktycznych,
- opracowanie wieloletniego Narodowego Programu do Walki z Cyberprzestępczością,
- edukowanie kadry kierowniczej przedsiębiorstw i instytucji,
- ustanowienie minimalnych standardów postępowania w poszczególnych sektorach.[25]

21 *Ibidem,* s. 107-109.
22 *Ibidem*, s. 119-120.
23 *Ibidem*, s. 124.
24 *Ibidem*, s. 156.
25 *Ibidem*, s. 175-178.

## 8. Podsumowanie

Państwo powinno podejmować działania w celu wprowadzenia co najmniej minimalnych standardów zapewniających cyberbezpieczeństwo kraju. Zadanie to przypadło naczelnym organom administracji. Na przestrzeni ostatnich lat wydano kilka dokumentów mających na celu ustalenie polityki państwa w obszarze cyberbezpieczeństwa. Polska częściowo wywiązała się już z założeń przedstawionych wyżej projektów. Jako przykład wymienić należy chociażby powołanie w MON -ie Systemu Reagowania na Incydenty Komputerowe czy Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni[26].

Szczególnie ważną inicjatywą jest powołanie Systemu Reagowania na Incydenty Komputerowe, realizującego zadania w zakresie koordynacji procesów wykrywania i reagowania na cyberzagrożenia systemów i sieci teleinformatycznych resortu obrony narodowej[27]. Od 2008 r. w ramach ABW funkcjonuje też CERT.GOV. PL, który ma za zadanie wykrywanie cyberzagrożeń i przeciwdziałanie cyberzagrożeniom oraz reprezentację RP w kontaktach międzynarodowych, w tym zakresie współpracy wojskowej w porozumieniu z Centrum Koordynacyjnym Systemu Reagowania na Incydenty Komputerowe MON.[28]

Najsłabszym elementem w procesie wdrażania polityki cyberbezpieczeństwa jest człowiek. Dobrym kierunkiem jest zatem tworzenie komórek eksperckich ds. cyberbezpieczeństwa w jednostkach administracyjnych, kształcenie pracowników oraz edukacja społeczeństwa. Budowanie cyberbezpieczeństwa państwa musi odbywać się na wielu szczeblach – zapewniających ochronę nie tylko przed cyberprzestępcami, ale również cyberterrorystami oraz służbami obcych państw[29].

Na krytykę zasługuje jednak brak koordynacji działań administracji w zakresie cyberbezpieczeństwa RP. Związek programów takich jak POC RP a Doktryna Cyberbezpieczeństwa RP jest luźny, a ich relacja nie do końca jasna. Programy częściowo powielają te same rekomendacje, chociażby w zakresie konieczności edukacji pracowników administracji i społeczeństwa. Brak jest jednego dokumentu – na wzór kompleksowych uregulowań państw zachodnich – będącego holistyczną strategią ochrony cyberprzestrzeni Polski. Taki stan rzeczy powoduje niepewność i niejasność systemu, brak jasno sprecyzowanych kompetencji poszczególnych organów i chaos organizacyjny. Brak jednolitego systemu cyberbezpieczeństwa RP może w obliczu cyberkryzysu doprowadzić do poważnego zagrożenia obronności kraju, jego gospodarki i rozwoju.

26 System..., *op. cit.*, s. 8-9.
27 http://srnik.wp.mil.pl/pl/index.html (data dostępu: 20.01.2016 r.).
28 J. Grubicka, Bezpieczeństwo państwa polskiego wobec cyberterroryzmu, (w:) P. Sienkiewicz (red.), Metodologia badań bezpieczeństwa narodowego. Tom V. Seria: monografie, Warszawa 2013, s. 284.
29 M. Karnowska-Werner, Zagrożenia bezpieczeństwa w cyberprzestrzeni, (w:) M. Górka (red.), Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Warszawa 2014, s. 300-301.

## BIBLIOGRAFIA

Grubicka Joanna. 2013. Bezpieczeństwo państwa polskiego wobec cyberterroryzmu. W Metodologia badań bezpieczeństwa narodowego. Tom V. Seria: monografie. Warszawa: Akademia Obrony Narodowej.

Husak Zbigniew. 2014. Ochrona bezpieczeństwa państwa przed zagrożeniami cybernetycznymi w Unii Europejskiej. W Bezpieczeństwo państwa. Zagadnienia podstawowe. Lublin: Wydawnictwo KUL.

Nowak Eugeniusz, Nowak Maciej. 2011. Zarys teorii bezpieczeństwa narodowego. Zarządzanie bezpieczeństwem. Warszawa: Wydawnictwo Difin.

Marczyk Maciej. 2014. Bezpieczeństwo teleinformatyczne wobec ataków cyberterrorystycznych. W Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku. Warszawa: Wydawnictwo Difin.

Karnowska-Werner Maria. 2014. Zagrożenia bezpieczeństwa w cyberprzestrzeni. W Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku. Warszawa: Wydawnictwo Difin.

Joanna Worona

# SUPREME STATE ADMINISTRATION AUTHORITIES WORKS ON POLISH CYBERSECURITY

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats, and hazards. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. In the last few years the supreme state administration authorities of Poland have been taking necessary steps to ensure minimum cyberspace security standards. Government bodies are trying to assure appropriate legal framework, procedures and systems of information exchange between public administrations and other states and cyberspace users. In light of the risk and potential consequences of cyber events, such as those experienced in Estonia and Georgia, strengthening the security and resilience of cyberspace has become one of the most important homeland security mission.

Keywords: cybersecurity, cyberspace, cyberspace security strategy, public administration

Słowa kluczowe: administracja publiczna, cyberbezpieczeństwo, cyberprzestrzeń, strategia bezpieczeństwa cyberprzestrzeni