Diana Mazepa

Narodowa Strategia Bezpieczeństwa Cybernetycznego Republiki Macedonii Północnej i Plan Działania 2018-2022

Wprowadzenie

Cyberbezpieczeństwo jest współcześnie jednym z ważniejszych zagadnień związanych z bezpieczeństwem i strategiami rozwoju państw. Problematyka ta zyskuje na znaczeniu w związku z wielowymiarowością i różnorodnością zagrożeń, globalizacją, dynamicznym postępem technologicznym czy zagrożeniami o charakterze hybrydowym. Republika Macedonii Północnej, a wcześniej Republika Macedonii, ze względu na swoje położenie geopolityczne oraz perspektywę dołączenia do struktur euroatlantyckich odwołuje się do rozwoju tego aspektu bezpieczeństwa.

Badania nad cyberbezpieczeństwem to nadal dziedzina rozwijająca się i poddająca się dynamicznym zmianom. Istnieje wiele definicji zróżnicowanych pojęć związanych z cyberprzestrzenią i cyberbezpieczeństwem. Amerykański politolog, Joseph Nye definiuje cyberprzestrzeń w sposób następujący:

> Cyber jest prefiksem oznaczającym czynności związane z komputerem i spektrum elektromagnetycznym. Domena internetowa obejmuje komputery korzystające z Internetu, ale także intranety[1], technologie komórkowe, kable światłowodowe i komunikację kosmiczną. Cyberprzestrzeń ma warstwę infrastruktury fizycznej, która jest zgodna z ekonomicznymi prawami rywalizujących aktorów i prawami politycznymi suwerennej jurysdykcji i kontroli. Ten aspekt Internetu nie jest tradycyjnym „dobrem wspólnym". Ma on jednak także warstwę wirtualną lub informacyjną z rosnącymi zyskami ekonomicznymi i praktykami politycznymi, które utrudniają kontrolę legislacji[2].

---

1 Jedna z odmian sieci wewnętrznej w organizacjach lub przedsiębiorstwach, opierająca się o technologię internetową i upraszczająca komunikację pracowników, łącząc systemy informatyczne i infrastrukturę komputerową.

2 J. Nye, *Nuclear Lessons for Cyber Security?*, s. 19-20, https://citizenlab.ca/cybernorms2012/nuclearlessons.pdf (30 VIII 2019).

Jedną z najczęstszych definicji jest sformułowana przez Departament Obrony Stanów Zjednoczonych, która została utworzona na potrzeby słownika terminologii wojskowej oraz powiązanej, według której cyberprzestrzeń to: „Globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery"[3]. W definicji tej znajduje się jedynie odwołanie do technologicznych aspektów cyberprzestrzeni, nie koncentrując się na elementach społecznych. Definicja ta jednak, jak już zostało wspomniane wyżej, została stworzona na potrzeby słownika nazewnictwa wojskowego, dlatego też koncentruje się na kwestiach technicznych.

Na gruncie europejskim także można znaleźć liczne definicje. Jedną z nich może być opublikowana w 2011 r. w Wielkiej Brytanii: „Cyberprzestrzeń to interaktywna domena stworzona z cyfrowych sieci, która jest wykorzystywana do przechowywania, modyfikowania oraz przekazywania informacji. Jej częścią jest Internet, ale zawierają się w niej także inne systemy informacyjne, które obsługują nasz biznes, infrastrukturę oraz wspomagają świadczenie usług[4]", albo na gruncie niemieckim, definicja opublikowana Strategii Cyberbezpieczeństwa Niemiec z 2011 r.:

> Cyberprzestrzeń jest wirtualną przestrzenią wszystkich systemów technologii informacyjnej powiązanych na poziomie danych w skali globalnej. Fundament cyberprzestrzeni stanowi Internet jako uniwersalna oraz powszechnie dostępna sieć oferująca połączenia oraz transport, która może być uzupełniana oraz rozszerzana dalej przez dowolną ilość dodatkowych sieci danych. Systemy IT działające w wyizolowanej przestrzeni nie stanowią przestrzeni cybernetycznej[5].

Definicji przestrzeni cybernetycznej jest wiele, skupiają się one na różnorodnych aspektach w mniejszym lub większym stopniu, nierzadko pomijając wiele czynników zawartych w innej terminologii. Reasumując, można zauważyć, że cyberprzestrzeń jest złożonym środowiskiem, skupiającym nie tylko fizyczne składniki, tj. sieci, systemy, oprogramowania czy zawarte w nich informacje, ale jest interaktywna, kierowana przez jej użytkowników, zarówno indywidualnych jak i przedsiębiorstw, a także państwa i organizacje.

Obecnie znaczenie cyberprzestrzeni, ochrony jej i jej użytkowników są kluczowymi obszarami dla nowoczesnych aktorów państwowych i niepaństwowych. Kwestie definicyjne cyberprzestrzeni poszczególnych podmiotów mają duży

---

[3] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, s. 227, https://www.abw.gov.pl/download/1/1284/Segregator13.pdf (30 VIII 2019).

[4] *Ibidem*, s. 229.

[5] *Ibidem*, s. 230.

wpływ na ich podejście do bezpieczeństwa cybernetycznego. Jeżeli terminologia wyłącza z zakresu aspekty społeczne jak np. użytkowników sieci, to bezpieczeństwo tak ujętej przestrzeni cybernetycznej będzie zdecydowanie mocniej skupiać się na ochronie technologicznej i analogicznie, im więcej składowych ma definicja, tym ochrona będzie odnosić się do większej ilości elementów.

Często cyberbezpieczeństwo określane jest jako zapobieganie uszkodzeniom, ochronie, oraz w perspektywie przywracania zdolności do poprawnego funkcjonowania komputerów, systemów łączności elektronicznej czy też usług komunikacji odbywających się w cyberprzestrzeni. Mówi się tutaj także o ochronie informacji zawartych w przestrzeni komunikacji elektronicznej, mającej na celu zachowanie poufności i uwierzytelnieniu osób upoważnionych do tych informacji[6].

W dużej mierze bezpieczeństwo cybernetyczne odnosi się do trzech, skorelowanych ze sobą poziomów: ochrony komputerów, nośników pamięci oraz informacji w nich zwartych jako pierwszym obszarze, kolejno budowaniu umiejętności ochrony przed atakami i cyberprzestępczością, zarówno po stronie wewnętrznych regulacji i praw, jak i zabezpieczeń technologicznych, a także podnoszenia świadomości wśród użytkowników sieci na temat zagrożeń wynikających z korzystania z cyberprzestrzeni[7].

Ochrona tego obszaru stała się współcześnie jednym z najczęściej podejmowanych tematów. Państwa i inne podmioty zdają sobie sprawę, że stabilność i rozwój są w dużej mierze zależne od bezpieczeństwa cybernetycznego. Wraz z podnoszeniem świadomości na temat zagrożeń w przestrzeni cybernetycznej rośnie także liczba incydentów komputerowych i cyberataków. Republika Macedonii Północnej również jest narażona na tego typu zdarzenia, dlatego też stoi przed licznymi wyzwaniami, które pozwolą wypracować właściwy poziom zabezpieczeń cyberprzestrzeni i użytkowników sieci.

W listopadzie 2017 r. podczas rozmów o bezpieczeństwie cybernetycznym ogłoszono rozwój strategii cyberbezpieczeństwa państwa macedońskiego[8]. W grudniu 2017 r. powołano Grupy Robocze, które rozpocząć miały opracowywanie tego aspektu polityki w zakresie cywilnym i wojskowym, przygotowanie ustawy dotyczącej cyberbezpieczeństwa kraju, ustanowienie instytucji odpowiedzialnej za koordynowanie działań i współpracę transgraniczną oraz dostosowanie

---

6 M. Cavelty Dunn, *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, London 2008, s. 19-23.

7 H. W. Fisher, *The role of the new information technologies in emergency mitigation, planning, response and recovery*, „Distaster Prevention and Management. An International Journal" 1998, vol. 7, no. 1, s. 28-37.

8 *Annual National Programme of the Republic of Macedonia for NATO membership 2017/2018*, s. 27, http://www.mfa.gov.mk/images/stories/GNP/GNP-2017-2018-MNR-web.pdf (7 I 2019).

przepisów do dyrektywy 2016/1148 Komisji Europejskiej[9]. Do czasu wprowadzenia nadrzędnego programu bezpieczeństwa cybernetycznego istniał szereg pomniejszych ustaw regulujących niektóre kwestie dotyczące sieci, jak np. ustawa o danych osobowych[10], ustawa o handlu elektronicznym[11], ustawa o komunikacji elektronicznej[12] czy ustawa o danych elektronicznych i elektronicznym podpisie[13]. W 2018 r. po raz pierwszy Ministerstwo Społeczeństwa Informacyjnego i Administracji wprowadziło pierwszą narodową strategię cyberbezpieczeństwa na lata 2018-2022.

Mocny rozwój bezpieczeństwa cybernetycznego kraju nie jest dyktowany jedynie chęcią dopasowania się do europejskich standardów, lecz także tym, że w Macedonii dynamicznie notuje się postęp we wprowadzaniu i rozwoju telekomunikacji i społeczeństwa informacyjnego. Odwołując się do danych Biura Statystycznego Republiki Macedonii Północnej, w 2011 r. 55% gospodarstw domowych miało dostęp do Internetu, podczas gdy w 2018 r. ten wskaźnik wzrósł do 79,3%[14], natomiast użytkowników między 15 a 74 rokiem życia było 56,7% (w 2011 r.), następnie w 2018 odsetek wzrósł do 79,2%[15]. Z kolei 94,4% przedsiębiorstw w Macedonii korzysta aktywnie z komputera oraz dostępu do sieci[16], a 53,9% z nich posiada strony internetowe[17]. Z firm korzystających z Internetu 89,6% udostępnia tam podstawowe dane dotyczące produktów i usług oraz ich cen, 51,7% ma odniesienia do mediów społecznościowych, a 21% przyjmuje zamówienia lub rezerwacje online[18]. Z każdym rokiem wzrasta też odsetek handlu

---

9 Zob. więcej: *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=CS (7 I 2019).

10 Zob. więcej: *Law on personal data protection*, http://www.ceecprivacy.org/pdf/Law on Personal Data Protection.pdf (7 I 2019).

11 Zob. więcej: *Закон За Електронска Трговија*, https://www.pravdiko.mk/wp-content/uploads/2013/11/Zakon-za-elektronska-trgovija-02-11-2007.pdf (7 I 2019).

12 Zob. więcej: *Закон За Електронските Комуникации*, http://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/zakon_za_elektronski_komunikacii_konsolidiran_032018.pdf (7 I 2019).

13 Zob. więcej: *Закон За Електронски Документи, Електронска Идентификација И Доверливи Услуги*, http://www.mio.gov.mk/sites/default/files/pbl_files/documents/legislation/zededu.pdf (7 I 2019).

14 *Republic of North Macedonia State Statistical Office, Information Society*, http://www.stat.gov.mk/OblastOpsto_en.aspx?id=27 (7 I 2019).

15 *Ibidem.*

16 *Usage of information and communication technologies in enterprises, 2018, Republic of North Macedonia State Statistical Office*, http://www.stat.gov.mk/PrikaziSoopstenie_en.aspx?rbrtxt=76 (7 I 2019).

17 *Ibidem.*

18 *Ibidem.*

elektronicznego w przedsiębiorstwach, co pokazuje, że rozwój tej gałęzi bezpieczeństwa kraju jest niezbędny.

Celem niniejszego artykułu jest analiza najważniejszych założeń macedońskiej strategii bezpieczeństwa cybernetycznego, wyzwań i zagrożeń oraz instytucji odpowiedzialnych za koordynowanie działań wynikających z wypracowanej polityki.

Definicje

Narodowa Strategia Bezpieczeństwa Cybernetycznego Republiki Macedonii Północnej wprowadza kilka definicji istotnych w bezpieczeństwie cybernetycznym:

1) bezpieczeństwo narodowe – system nowoczesnej organizacji państwa i funkcjonowania społeczeństwa w celu prowadzenia określonych działań oraz środków zapobiegawczych i represyjnych w celu obrony podstawowych wartości społecznych i zabezpieczania ich przed zagrożeniami, ryzykiem i wyzwaniami na wszystkich poziomach;
2) cyberprzestrzeń – przestrzeń, w której następuje komunikacja między systemami informatycznymi. W kontekście strategii definicja obejmuje również Internet i wszystkie powiązane z nim systemy teleinformatyczne;
3) cyberbezpieczeństwo – działania i środki ochrony systemów informatycznych, które chronią cyberprzestrzeń przed atakami, zapewniając poufność, integralność i dostępność systemów i informacji w nich zawartych, wykrywanie ataków i incydentów komputerowych, a w przypadku ich wystąpienia uruchamianie mechanizmów reagowania i przywracania systemów do stanu w jakim znajdowały się przed wystąpieniem zagrożenia;
4) zagrożenie cybernetyczne – potencjalna przyczyna incydentu w cyberprzestrzeni, która może spowodować uszkodzenia systemów komputerowych, sieci i innych;
5) incydent cybernetyczny – jedno lub więcej zdarzeń, które mogą naruszać poufność, integralność lub dostępność systemów komputerowych, naruszające bezpieczeństwo;
6) cyberkryzys – zdarzenie lub zdarzenia w cyberprzestrzeni, które mogłyby spowodować lub mogą spowodować znaczące zakłócenia w życiu społecznym, politycznym i gospodarczym Macedonii. Taka sytuacja może wpłynąć na bezpieczeństwo obywateli, system demokratyczny, polityczny, stabilność państwa, jego gospodarkę, środowisko czy inne aspekty bezpieczeństwa narodowego;
7) cyberprzestępczość – obejmuje incydenty w przestrzeni kosmicznej lub przestępstwa, które można popełnić jedynie za pomocą technologii informacyjno-komunikacyjnych poprzez urządzenia i systemy jako środek

popełniania przestępstwa lub jako główny cel tych przestępstw. Przez cyberprzestępczość rozumie się także tradycyjną działalność przestępczą i materiały związane z wykorzystywaniem dzieci;
8) cyberatak – operacje, które mogą być skierowane na jednostki i/lub systemy informatyczne, występować w dowolnym miejscu w cyberprzestrzeni i mające na celu naruszyć poufność, integralność lub dostępność krajowych systemów teleinformatycznych;
9) cyberobrona – proaktywny sposób wykrywania lub odzyskiwania informacji na temat incydentów komputerowych, a także mający na celu działania prewencyjne przed zagrożeniami w cyberprzestrzeni[19].

Główni odbiorcy

Macedońska strategia dzieli interesariuszy na kilka grup odbiorców:
1) sektor publiczny, który definiuje takich odbiorców jak władza, która reprezentuje użytkowników sieci oraz jest zobligowana do podejmowania przedsięwzięć wynikających ze Strategii[20];
2) sektor prywatny – w grupie tej według programu znajdują się podmioty ściśle współpracujące z władzami, szczególnie w aspekcie infrastruktury krytycznej oraz systemu bezpieczeństwa i obrony kraju, inne podmioty, które na różne sposoby wspomagają użytkowników sieci, a także strony, które zobowiązane są przestrzegać założenia wynikające ze strategii bezpieczeństwa cybernetycznego[21];
3) społeczność akademicka – obejmuje wszelkie instytucje oświatowe, zarówno publiczne jak i prywatne, które odgrywają znaczącą rolę w kształtowaniu i rozwijaniu tego sektora bezpieczeństwa Macedonii[22];
4) społeczeństwo oraz organizacje – w grupie tej znaleźli się użytkownicy technologii informacyjno-komunikacyjnych, których cyberbezpieczeństwo obejmuje[23].

---

[19] *Национална Стратегија За Сајбер Безбедност На Република Македонија 2018-2022*, s. 37-40, http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf (1 IX 2019).

[20] *Republic of Macedonia national cyber security strategy 2018-2022*, s. 15, http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/cyber_security_strategy_macedonia_2018-2022_-_eng.pdf (07 I 2019).

[21] *Ibidem.*

[22] *Ibidem.*

[23] *Ibidem.*

Cele macedońskiej polityki cyberbezpieczeństwa

Plany zawarte w powyższym dokumencie, nazwane *The 5C Goals*, zawierają w sobie pięć kluczowych obszarów, w których bezpieczeństwo cybernetyczne ma być wprowadzone lub wzmacniane, by zapewnić je we wszystkich dziedzinach na każdym poziomie: odporność cybernetyczna, cyber-możliwości i cyber-kultura, zwalczanie cyberprzestępczości, ochrona cybernetyczna, współpraca i wymiana informacji:

1) odporność cybernetyczna – na tym polu strategia cyberbezpieczeństwa Macedonii zakłada wzmacnianie technologii informacyjno-komunikacyjnych (ang. *ICT*) poprzez m.in. współpracę sektora publicznego i prywatnego w przypadku pojawiających się incydentów w przestrzeni cybernetycznej, rozpoznawaniu i eliminowaniu wszelkich zagrożeń czy zdefiniowaniu określonej jurysdykcji i działań w celu poprawienia bezpieczeństwa tychże technologii. Celem końcowym jest zapewnienie ochrony, a także udoskonalenie i wykorzystanie rozwiązań, które mają zapewnić bezpieczeństwo kraju i jego obywateli, wykazując w ten sposób odporność na ataki[24] w sieci. Działania mają opierać się m.in. na wzmocnieniu możliwości Narodowego Centrum Reagowania na Incydenty Komputerowe, identyfikacji i ochronie CII (ang. *Critical Information Infrastructure*) oraz IIS (ang. *Internet Information Service*)[25], opracowaniu procedur zarządzania incydentami w przypadku kryzysu, stanu wojennego i stanu wyjątkowego, które umożliwią sprawną współpracę międzyinstytucjonalną, a także komunikację i wymianę informacji między nimi czy stworzenia jednolitych i kompleksowych ram prawnych na rzecz bezpieczeństwa cybernetycznego w Macedonii, analizowaniu i monitorowaniu pojawiających się zagrożeń, definiowaniu procedur przechowywania i ochrony danych przetwarzanych

[24] Przykładami incydentów komputerowych na Bałkanach może być atak w 2012 r. na stronę internetową macedońskiego Ministerstwa Spraw Wewnętrznych zniszczoną przez grupę Kosovo Network Security, zob. więcej: *Ministry of Interior – Macedonia*, http://mvr.gov.mk (1 IX 2019). Seria ataków hakerskich w lutym 2017 r. na strony rządowe w Czarnogórze, zob. więcej: D. Tomovic, *Montonegro on Alert Over New Cyber Attacks* [22 II 2017], https://balkaninsight.com/2017/02/22/montenegro-govt-on-alert-over-new-cyber-attacks-02-21-2017 (1 IX 2019). W lipcu 2019 r. Chorwacja została objęta atakami złośliwym oprogramowaniem SilentTrigger (phishing) mającym na celu infekowanie i przejmowanie systemów komputerowych agencji rządowych, zob. więcej: F. Bussoletti, *Croatia hit by waves of cyber attacks with a new malware: SilentTrigger* [8 VII 2019], https://www.difesaesicurezza.com/en/cyber-en/croatia-hit-by-waves-of-cyber-attacks-with-a-new-malware-silenttrigger (1 IX 2019).

[25] CII to wzajemnie połączone infrastruktury komunikacyjne i informacyjne, niezbędne do utrzymania ważnych funkcji życia społeczeństwa, których zakłócenie lub zniszczenie miałoby poważny skutek (np. dobrobyt ekonomiczny, zdrowie), natomiast IIS to usługa mająca na celu obsługę i utrzymanie własnych stron WWW oraz serwerów FTP.

przez systemy CII i IIS, czy przeprowadzaniu regularnych audytów mających na celu wykrycie i eliminowanie słabych punktów systemów i sieci[26];

2) potencjał cybernetyczny i kultura bezpieczeństwa cybernetycznego – działania wobec tej gałęzi planu mają za zadanie zrozumienie zagrożeń płynących z ICT oraz podnoszenie świadomości zobowiązania do budowania i wzmacniania bezpieczeństwa cybernetycznego każdego podmiotu. Promowanie zaangażowania ma na celu podnoszenie odpowiedzialności i zrozumienie szans i zagrożeń płynących z systemów telekomunikacyjnych. Odniesienie sukcesu na tym polu umożliwi podniesienie bezpieczeństwa na wszystkich poziomach społeczeństwa, zapewniając większą ochronę w odniesieniu do cyberprzestępczości[27]. Działania podejmowane w tym sektorze mają opierać się m.in. na: rozwoju potencjału bezpieczeństwa w sektorze MŚP (małych i średnich przedsiębiorstw), cyklach szkoleń i programów w dziedzinie bezpieczeństwa cybernetycznego, wspieraniu zdolności badawczych i innowacji biznesowych, udziale w krajowych i międzynarodowych projektach, pozyskiwaniu najnowocześniejszych technologii i rozwiązań sprzętowych oraz programowych czy podniesieniu podstawowej wiedzy o bezpieczeństwie cybernetycznym[28];
3) zwalczanie cyberprzestępczości – strategia podkreśla, że cyberprzestępczość może mieć różne wymiary, pojawić się może zarówno w formie nadużyć internetowych jak również bardziej skomplikowanych ataków na systemy. Może być ona motywowana różnymi przyczynami, być wymierzona w różne podmioty i być przeprowadzana przez rozmaite obiekty i jednostki. Dlatego też tak ważne jest rozwijanie rozmaitych sposobów zwalczania przestępstw w tym aspekcie, a przede wszystkim ustanowienie kompleksowego krajowego planu, który będzie określał szanse, wyzwania i zagrożenia, a także odnosił się do niezbędnych działań w zakresie zwalczania ryzyka płynącego z ICT. Działania w tej kwestii to przede wszystkim opracowanie ram prawnych dotyczących cyberprzestępczości, harmonizacja przepisów krajowych z politykami międzynarodowymi, ustanowienie procedur zgłaszania cyberprzestępczości, pogłębianie współpracy regionalnej i międzynarodowej, rozwój istniejących i tworzenie nowych mechanizmów współpracy krajowej, regionalnej i międzynarodowej, wymiana informacji między sektorem publicznym i prywatnym, zapewnianie specjalistycznego kształcenia osób zajmujących się bezpieczeństwem cybernetycznym[29];

---

[26] *Republic of Macedonia National…*, s. 18-19.
[27] *Ibidem*, s. 20.
[28] *Ibidem*, s. 20-21.
[29] *Ibidem*, s. 22-23.

4) ochrona – zabezpieczenie przestrzeni cybernetycznej jest jednym z priorytetów Republiki Macedonii Północnej, która w istotnym stopniu oddziałuje na bezpieczeństwo wewnętrzne i zewnętrzne oraz interesy narodowe. Ponadto w strategii podkreślono, że rozwój obrony cybernetycznej w armii macedońskiej jest ważnym elementem podejścia do obrony narodowej. Jednym z warunków ustanowienia skutecznej obrony jest dopasowanie planów organizacji oferujących usługi cybernetyczne do scenariuszy krajowych (w celu ochrony CII i IIS). Kolejnym istotnym aspektem jest działanie Macedonii jako członka lub partnera licznych organizacji ponadnarodowych (szczególnie NATO i Unii Europejskiej) do harmonizacji krajowych planów z międzynarodowymi oraz aktywna współpraca z podmiotami międzynarodowymi;
5) współpraca i wymiana informacji – na tym polu strategia zakłada wymianę informacji oraz szeroko zakrojoną współpracę nie tylko krajową, ale także ponadnarodową. Aby korzystać z bezpiecznej przestrzeni cybernetycznej oraz przejrzystego korzystania z technologii informacyjno-komunikacyjnych niezbędne jest określenie skutecznych i efektywnych procedur współpracy i wymiany informacji między wszystkimi zainteresowanymi stronami. Współdziałanie międzynarodowe stanowi jeden z kluczowych segmentów w wysiłkach na rzecz zwiększania zdolności do radzenia sobie z zagrożeniami cybernetycznymi. Działanie wymieniane przez ten obszar to m.in. opracowanie wspólnie z instytucjami państwowymi i organizacjami ponadnarodowymi skutecznych kanałów kooperacji i wymiany informacji, aktywny udział w budowaniu międzynarodowych umiejętności radzenia sobie z atakami cybernetycznymi, organizowanie i uczestnictwo w różnych międzynarodowych działaniach i inicjatywach, promowanie i rozwijanie norm, zasad i odpowiedzialnego zachowania państwa zgodnie z międzynarodowymi zasadami, budowanie zaufania pomiędzy instytucjami publicznymi i prywatnymi, międzynarodowymi zespołami CERT i CSIRT[30] czy przyczynianie się do procesu definiowania prawodawstwa międzynarodowego[31].

Instytucje odpowiedzialne

W ciągu trzech miesięcy od wprowadzenia analizowanej strategii opracowany zostać miał Plan Działania. Założono, że wdrażanie wszelkich działań określonych w strategii koordynować będzie Krajowa Rada Bezpieczeństwa Cybernetycznego.

---

[30] CERT – Computer Emergency Response Team, CSIRT – Computer Security Incident Response Team.

[31] *Republic of Macedonia National…*, s. 26-28.

W oparciu o dokument władze, ministerstwa i inne instytucje, określeni jako interesariusze, zobowiązani byli do zaktualizowania lub wdrożenia odpowiednich przepisów i procedur. W tym celu Republika Macedonii utworzyć miała Krajową Radę ds. Bezpieczeństwa Cybernetycznego, która miała na celu monitorowanie działań określonych w Strategii, a także określenia nowych kierunków działań dotyczących tego segmentu bezpieczeństwa[32]. Krajowa Rada ds. Bezpieczeństwa Cybernetycznego według Strategii oraz Planu Działań jest odpowiedzialna za szereg przedsięwzięć podejmowanych w celu ochrony przestrzeni cybernetycznej Macedonii, m.in. systematyczne monitorowanie i koordynację wdrażania dokumentów programowych, uwzględniając wszystkie zaistniałe w międzyczasie zagrożenia, skupianie się na ulepszaniu i uzupełnianiu powyższych dokumentów, określanie wyzwań związanych z zarządzaniem kryzysowym, analizę obecnego poziomu bezpieczeństwa w oparciu o raporty oraz ciągły rozwój i udoskonalanie programów i strategii odpowiedzialnych za cyberbezpieczeństwo. Zgodnie z zamysłem powyższych dokumentów w planach było utworzenie instytucji, która miałaby zajmować się *stricte* cyberbezpieczeństwem i wprowadzać w życie wszystkie działania do zapewnienia takiego bezpieczeństwa, w tym realizować plany i idee Krajowej Rady ds. Cyberbezpieczeństwa.

Za bezpieczeństwo cybernetyczne Macedonii odpowiedzialne jest ponadto Ministerstwo Społeczeństwa Informacyjnego i Administracji. Do zadań tego organu należą m.in. tworzenie rejestrów systemów informacji i komunikacji oraz sprzętu i technologii informacyjnych wykorzystywanych w administracji publicznej, monitorowanie aktualnego stanu systemów i wprowadzanie międzynarodowych standardów sieci i jej bezpieczeństwa[33]. Obecnym ministrem jest Damjan Manchevski. Od 2012 r. w kraju toczono dyskusje na temat utworzenia zespołu reagowania na incydenty komputerowe (tzw. CIRT – *Computer Incident Response Team*) oraz zespołu CERT (*Computer Emergency Response Team*) przy wsparciu technicznym Międzynarodowego Związku Telekomunikacyjnego (ITU)[34]. Macedoński zespół ds. reagowania na incydenty komputerowe (MKD-CIRT) został utworzony na mocy art. 26 ustawy o sieciach łączności elektronicznej[35] w ramach Agencji Łączności Elektronicznej jako oficjalny punkt zajmujący się incydentami występującymi w przestrzeni cybernetycznej[36]. Głównymi zadaniami instytucji

[32] *Ibidem*, s. 29.

[33] *Министерството за информатичко општество и администрација*, http://www.mioa.gov.mk/?q=mk/node/64 (27 VII 2019).

[34] P. Tasevski, *Macedonian Path Toward Cybersecurity*, „Information & Security. An International Journal" 2015, vol. 32, s. 4-5, https://it4sec.org/system/files/3204_macedonia.pdf (27 VII 2019).

[35] Zob. więcej: „Official Gazette of the Republic of Macedonia" 2014, no. 39; „Official Gazette of the Republic of Macedonia" 2014, no. 188; „Official Gazette of the Republic of Macedonia" 2015, no. 44; „Official Gazette of the Republic of Macedonia" 2015, no. 193.

[36] *Агенцијата за електронски комуникации*, https://mkd-cirt.mk/za-nas/ (27 VII 2019).

to przede wszystkim jej kluczowa rola w wykrywaniu zagrożeń w sieciach i systemach informatycznych, ich eliminowanie i łagodzenie skutków, ciągła analiza metod radzenia sobie z incydentami, dostarczanie wskazówek innym użytkownikom sieci na temat zwalczania zagrożeń wynikających z sieci czy współpraca z innymi organami zajmującymi się tym sektorem bezpieczeństwa, zarówno w kraju jak i za granicą[37]. Na MKD-CIRT składają się przede wszystkim wszystkie ministerstwa w Macedonii Północnej, cała administracja publiczna i służby rządu, operatorzy infrastruktury krytycznej, a także duże instytucje różnorodnych gałęzi przemysłu i usług: finansów, transportu, zdrowia czy energetyki. Warto nadmienić, iż zespół ten jest otwarty na współpracę ze wszystkimi stronami, które chciałyby mieć wpływ na poprawę bezpieczeństwa cybernetycznego państwa[38].

W 2017 r. zespół MKD-CIRT utworzył platformę wymiany informacji o złośliwym oprogramowaniu (MISP – *Malware Sharing Information Platform*), służącą do udostępniania, przechowywania i analizowania zagrożeń, luk w cyberprzestrzeni, która dostępna jest dla wszystkich instytucji, operatorów infrastruktury krytycznej oraz dużych firm m.in. finansowych czy transportowych[39]. W tym samym roku zespół reagowania założył stronę internetową, na której oferuje różne opcje zgłaszania incydentów za pomocą internetowego formularza, faksu, korespondencji pisemnej lub e-maila[40]. Macedonia aktywnie współpracuje na gruncie cyberbezpieczeństwa z licznymi zagranicznymi organizacjami i placówkami, w tym m.in. z Komisją Europejską, Bankiem Światowym, NATO, ITU, Global Cyber Security Capacity Center (GCSCC) czy placówkami naukowymi takimi jak np. Uniwersytet Oksfordzki[41]. Współdziałanie Macedonii w polepszaniu cyberbezpieczństwa ma także kluczowe znaczenie w dążeniu kraju do struktur euroatlantyckich.

Podsumowanie

Cyberbezpieczeństwo w Republice Macedonii Północnej nadal jest w fazie początkowego rozwoju, gdyż do tej pory ramy prawne opierały się o wiele odrębnych ustaw, dopiero w 2018 r. ujednolicając ten sektor bezpieczeństwa kraju

---

37 *Ibidem*.

38 *Конституенти*, https://mkd-cirt.mk/za-nas/rfc2350/konstituenti/ (27 VII 2019).

39 *Cybersecurity Capacity Review Former Yugoslav Republic of Macedonia (FYR Macedonia)*, July 2018, s. 26, http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/reports/cmm_fyrom_report_final_13_august2018_2.pdf (27 VII 2019).

40 *Ibidem*.

41 J. Gjorgjioska, *National Cyber Security Strategy and Action Plan 2018-2022*, June 2019, https://mkd-cirt.mk/wp-content/uploads/2019/04/2019Ohrid_1.4.-Jovana-Gjorgjioska-MISA-presentation-05.06.2019.pdf (30 VII 2019).

w Narodowej Strategii. Technologie informatyczne rozwijają się w bardzo szybkim tempie i charakteryzują się zmiennymi trendami. Dlatego też kluczowym celem państw jest zapewnienie bezpieczeństwa sieci, co dotyczy także Republiki Macedonii Północnej, która zmierza do ujednolicania swoich polityk ze standardami zachodnimi. Właściwym podsumowaniem ustanowienia Narodowej Strategii i kierunku Macedonii w obrębie bezpieczeństwa cybernetycznego jest wystąpienie Ministra Społeczeństwa Informacyjnego i Administracji, Damjana Manchevskiego na otwarciu trzydniowych warsztatów na temat bezpieczeństwa cybernetycznego, zorganizowanych pod koniec czerwca 2019 r. w Skopje:

> Cyberprzestrzeń jest wspólna dla globalnych obywateli, administracji publicznych, przedsiębiorstw, społeczeństw obywatelskich, organizacji międzynarodowych, ale także złośliwych użytkowników i organizacji przestępczych. Codziennie stajemy przed wyzwaniami bezpieczeństwa. (…) Musimy zapobiegać cyberprzestępczości. Dlatego tak ważna jest współpraca i dostosowanie regionalne i międzynarodowe. (…) U progu NATO i wkrótce Unii Europejskiej, Macedonia Północna staje się coraz bardziej atrakcyjnym celem dla cyberprzestępczości. Oczywiście bezpieczeństwo cybernetyczne stało się jednym z kluczowych priorytetów rządu. (…) Posiadanie solidnej kultury bezpieczeństwa cybernetycznego jest jednym z fundamentów otwartej, bezpiecznej przestrzeni cybernetycznej. W związku z tym podnoszenie świadomości na temat zagrożeń bezpieczeństwa cybernetycznego i promowanie tego bezpieczeństwa wśród obywateli i organizacji poprzez edukację i dzielenie się dobrymi praktykami stanowi istotny element budowania potencjału krajowego bezpieczeństwa cybernetycznego (…)[42].

Abstract

Diana Mazepa

National Strategy for Cyber Security of the Republic of North Macedonia and Action Plan 2018-2022

Cybersecurity of states and international organizations is one of the most priority issues in the world at the time. The dynamically developing IT systems and the global reach of the Internet, reaching both individual users as well as public administrations and transnational corporations has not only significantly facilitated the storage, sharing or exchange of information, but also the place of criminal attacks and threats to sensitive data in network. Accordingly, national and non-national actors try to constantly monitor threats stem from cyber space, prevent

[42] *North Macedonia Hosts the Regional Workshop for Europe on National Cybersecurity Strategies*, Skopje, 26 VI 2019, http://www.mio.gov.mk/?q=en/print/2610 (31 VII 2019).

them or mitigate their effects, so as not to jeopardize the security of them and their citizens or members. This situation also takes place in the Republic of North Macedonia, which in 2018, in cooperation with international partners and extensive public consultations in the country, announced the first National Cyber Security Strategy for 2018-2022. This article aims to analyze the content contained in the above document and the Action Plan attached to it and to approximate the objectives contained therein.

Keywords: cybersecurity, The Republic of North Macedonia, cyberspace, national cybersecurity strategy

References

Agencijata za elektronski komunikacii, https://mkd-cirt.mk/za-nas/.

Annual National Programme of the Republic of Macedonia for NATO membership 2017/2018, http://www.mfa.gov.mk/images/stories/GNP/GNP-2017-2018-MNR-web.pdf.

Cavelty Dunn, M., *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, London 2008.

Cybersecurity Capacity Review Former Yugoslav Republic of Macedonia (FYR Macedonia), July 2018, http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/reports/cmm_fyrom_report_final_13_august2018_2.pdf.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=CS.

Fisher, H. W., *The role of the new information technologies in emergency mitigation, planning, response and recovery. Distaster Prevention and Management*, „An International Journal" 1998, vol. 7, no. 1.

Gjorgjioska, J., *National Cyber Security Strategy and Action Plan 2018-2022*, June 2019, https://mkd-cirt.mk/wp-content/uploads/2019/04/2019Ohrid_1.4.-Jovana-Gjorgjioska-MISA-presentation-05.06.2019.pdf.

Law on personal data protection, http://www.ceecprivacy.org/pdf/Law on Personal Data Protection.pdf.

Ministerstvoto za informatičko opštestvo i administracija, http://www.mioa.gov.mk/?q=mk/node/64.

Nacionalna Strategija Za Sajber Bezbednost Na Republika Makedonija 2018-2022, http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf.

North Macedonia Hosts the Regional Workshop for Europe on National Cybersecurity Strategies, Skopje, 26 VI 2019, http://www.mio.gov.mk/?q=en/print/2610.
Nye, J., *Nuclear Lessons for Cyber Security?*, https://citizenlab.ca/cybernorms2012/nuclearlessons.pdf.
„Official Gazette of the Republic of Macedonia" 2014, no. 39.
„Official Gazette of the Republic of Macedonia" 2014, no. 188.
„Official Gazette of the Republic of Macedonia" 2015, no. 44.
„Official Gazette of the Republic of Macedonia" 2015, no. 193.
Republic of North Macedonia State Statistical Office, Information Society, http://www.stat.gov.mk/OblastOpsto_en.aspx?id=27.
Republic of Macedonia national cyber security strategy 2018-2022, http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/cyber_security_strategy_macedonia_2018-2022_-_eng.pdf.
Tasevski, P., *Macedonian Path Toward Cybersecurity*, „Information & Security: An International Journal" 2015, vol. 32, https://it4sec.org/system/files/3204_macedonia.pdf.
Wasilewski, J., *Zarys definicyjny cyberprzestrzeni*, https://www.abw.gov.pl/download/1/1284/Segregator13.pdf.
Zakon Za Elektronski Dokumenti, Elektronska Identifikacija I Doverlivi Uslugi, http://www.mio.gov.mk/sites/default/files/pbl_files/documents/legislation/zededu.pdf.
Zakon Za Elektronska Trgovija, https://www.pravdiko.mk/wp-content/uploads/2013/11/Zakon-za-elektronska-trgovija-02-11-2007.pdf.
Zakon Za Elektronskite Komunikacii, http://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/zakon_za_elektronski_komunikacii_konsolidiran_032018.pdf.

Diana Mazepa – mgr stosunków międzynarodowych, doktorantka w Zakładzie Badań Wschodnich w Instytucie Studiów Międzynarodowych Uniwersytetu Wrocławskiego. ORCID: 0000-0003-2286-454X