Kamil Goryń
ORCID: 0000-0003-3021-028X
Uniwersytet w Białymstoku

Perspektywy zagrożeń cyfrowych w dokumentach doktrynalnych Rzeczypospolitej Polskiej

ABSTRAKT: Rosnąca rola cyberprzestrzeni w budowaniu bezpieczeństwa narodowego wymusza uwzględnienie wyzwań i zagrożeń płynących z tego obszaru w dokumentach doktrynalnych. W artykule podjęto próbę wskazania głównych zmian, jakie zaszły na przestrzeni lat w strategiach bezpieczeństwa. Dokonano przy tym analizy ich zgodności z elementami środowiska bezpieczeństwa bezpośrednio i pośrednio wpływającymi na cyberbezpieczeństwo.

Słowa kluczowe: cyberprzestrzeń, zagrożenia, wyzwania, strategia bezpieczeństwa, bezpieczeństwo narodowe

ABSTRACT: Increasing role of cyberspace in national security demands new approach that focuses more on cyberthreats. Article explains differences present in national security strategies, that changes over years to meet the requirements of modern world.

Key words: cyberspace, threats, challanges, security strategy, national security

Wstęp

Rozwój technologiczny wpływa na kształtowanie środowiska bezpieczeństwa, radykalnie zmieniając polityki i strategie kreowane przez państwa w XXI wieku. Powyższe stwierdzenie niewątpliwie jest truizmem. Jednak

z racji tego, iż dynamiczne przemiany trwają już od wielu lat, niejednokrotnie umyka nam, jak wielki jest ich wpływ na obarczone wysoką bezwładnością organizmy państwowe i społeczne. Celem moim jest naszkicowanie obrazu zagrożeń cyfrowych dla Polski, opisanych w dokumentach doktrynalnych.

Obszarem niewiedzy, który skłonił mnie do podjęcia pracy badawczej, jest wpływ rozwoju technologicznego na kształt strategii bezpieczeństwa państwa. Wyrażony jest on poprzez pytanie badawcze: *W jaki sposób scharakteryzowano cyberzagrożenia wpływające na środowisko bezpieczeństwa Polski w dokumentach strategicznych?* Punktem wyjścia do znalezienia odpowiedzi na tak sformułowany problem badawczy jest zidentyfikowanie kluczowych zależności pomiędzy rozwojem technologii, w szczególności technologii informacyjnych, a wyzwaniami, szansami oraz zagrożeniami dla bezpieczeństwa narodowego zidentyfikowanymi w dokumentach doktrynalnych.

Wstępne badania przeprowadzone w tym zakresie pozwoliły mi na sformułowanie następującej hipotezy: *Rozwój technologiczny stanowi jedną z najistotniejszych zmiennych wpływających na współczesne środowisko bezpieczeństwa Polski. Powszechny dostęp do Internetu, połączony ze wzmożoną cyfryzacją poszczególnych aspektów funkcjonowania społeczeństwa oraz państwa, stanowi jeden z najbardziej newralgicznych obszarów wpływających na bezpieczeństwo narodowe. Odzwierciedlenie tego stanu rzeczy w dokumentach doktrynalnych pozwala na wskazanie ogólnych kierunków działań, które należy podjąć w celu wyzyskania szans i zminimalizowania zagrożeń dla bezpieczeństwa.*

W celu weryfikacji postawionej hipotezy roboczej podjęta została próba przeanalizowania dokumentów doktrynalnych, opisujących polityki i strategie administracji publicznej w obszarze zapewnienia bezpieczeństwa w cyberprzestrzeni. Uzupełnieniem było omówienie wybranych incydentów bezpieczeństwa oraz wykorzystania technologii informacyjnych w celach ofensywnych itp.

Rozwój Internetu a wpływ na bezpieczeństwo

Rozwój i upowszechnienie technologii informacyjnych jest faktem. Ostatnie dziesięciolecia przyniosły olbrzymi postęp w tym zakresie.

Obniżenie kosztów produkcji sprzętu elektronicznego, wzrost jego mocy obliczeniowej i przede wszystkim powszechny dostęp do urządzeń stale podłączonych do Internetu spowodowały zmiany, których charakter jest bezprecedensowy. O ile postęp technologiczny na przestrzeni wieków mógł być opisywany jako ewolucyjny, tak zmiany w zakresie rozwoju technologii informacyjnych mają niewątpliwie **rewolucyjny** charakter. Są ekstremalnie dynamiczne, próg wejścia umożliwiający skorzystanie z nowinek technicznych uległ drastycznemu obniżeniu, a efekt popularyzacji smartfonów i komputerów osobistych podłączonych do Internetu obejmuje praktycznie wszystkie dziedziny funkcjonowania państwa i społeczeństwa. Nigdy wcześniej żaden wynalazek nie doprowadził do tak drastycznych i holistycznych zmian. Niezależnie, czy mówimy tu o wynalezieniu druku czy też rewolucji przemysłowej, które niewątpliwie przyczyniły się do transformacji relacji społecznych i państwowych. Synergia, jaka wystąpiła w ostatnich dziesięcioleciach pomiędzy poszczególnymi nowinkami technicznymi, upowszechniającymi się w ramach rewolucji informacyjnej, drastycznie zmieniła naszą rzeczywistość i nierozerwalnie spięła ją z cyberprzestrzenią. Oczywiście przy założeniu, że nie wystąpi żaden kataklizm, który bezpowrotnie pozbawi nas możliwości korzystania z elektroniki itd.

Ogólny wpływ technologii na kształt i trendy rozwojowe obecnego świata jest trudny do przecenienia. Poruszałem to zagadnienie w tekście *Jak technologie kontrolują nasze życie*[1], jednak sama rewolucja technologiczna określana jako megatrend wpływający na otaczającą nas rzeczywistość opisywana była m.in. przez prof. T. Aleksandrowicza[2].

Ideą, jaka leżała u podstaw stworzenia globalnej Sieci, było znaczące ułatwienie przepływu i agregowania informacji. Twórcy ARPANET[3] w swoich

---

1 K. Goryń, *Jak technologie kontrolują nasze życie*, „Nowa Konfederacja" 2018, nr 9 (99), https://nowakonfederacja.pl/jak-technologie-kontroluja-nasze-zycie, [dostęp: 01.06.2020].

2 Por. T.R. Aleksandrowicz, *Kluczowe megatrendy w bezpieczeństwie państwa XXI wieku*, Difin, Warszawa 2020, s. 38-70 oraz T.R. Aleksandrowicz, *Świat w sieci. Państwa, społeczeństwa, ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego,* Wyd. 2, Difin, Warszawa 2020, s. 63-153.

3 Advanced Research Projects Agency Network – pierwsza rozległa sieć komputerowa w oparciu o protokół TCP/IP, mająca na celu ułatwienie wymiany informacji pomiędzy oddalonymi od siebie jednostkami badawczymi wyposażonymi w komputery. Uważana za bezpośredniego poprzednika Internetu.

pracach skupiali się na stworzeniu narzędzia umożliwiającego wymianę informacji naukowcom i ten cel stanowił priorytet działań. Wszelkie mechanizmy bezpieczeństwa zaimplementowane do tworzonych rozwiązań skupiały się na zapewnieniu wysokiej jakości komunikacji. Aspekty związane z ochroną przed przechwyceniem bądź podsłuchaniem przesyłanych danych przez osoby postronne były pomijane lub marginalizowane. Wynikało to z faktu, iż pierwotnie skupiano się na udostępnieniu nowych funkcjonalności, natomiast ewentualne zagrożenia mitygowano poprzez wydzielenie i ograniczenie dostępu do kluczowych podsieci jedynie dla zaufanych użytkowników. W latach osiemdziesiątych ubiegłego wieku doprowadziło to do ostatecznego rozdzielenia wojskowej i cywilnej części Sieci, ze względu na rosnące ryzyko związane z atakami *crackerów*. Nie spowodowało to jednak istotnych zmian w samej architekturze, która dalej w pierwszej kolejności miała służyć do stabilnego przesyłania informacji. Trend ten można zaobserwować również obecnie wśród twórców oprogramowania i urządzeń, które nie muszą spełniać wysokich wymogów w ramach bezpieczeństwa cyfrowego. Przykładem w tym zakresie mogą być urządzenia przynależące do kategorii *IoT*[4], a także różnorodne aplikacje mobilne i webowe, w których zignorowano dobre praktyki programistyczne oraz pominięto testy bezpieczeństwa.

Podsumowując, Internet nie został zaprojektowany z myślą o bezpiecznym i dyskretnym przesyłaniu danych, zwłaszcza w obecnym rozumieniu tego pojęcia. Jedyne zaimplementowane mechanizmy bezpieczeństwa obejmowały weryfikację poprawności przesyłanych i otrzymywanych danych, które były i są podatne na różnorodne zakłócenia elektromagnetyczne.

Podobne tendencje można zauważyć także w wypadku budowania sieci telefonii komórkowych, również tworzonych z myślą o ułatwieniu komunikacji. Pierwotne założenia, zapewniające względnie wysoką poufność przesyłanych danych, oparte były na bardzo wysokim progu wejścia, odnoszącym się do konieczności posiadania zaawansowanego technicznie wyposażenia. Koszt dostępu do technologii oraz wymóg operowania specjalistyczną wiedzą przez wiele lat stanowił wystarczający poziom zabezpieczeń, chroniący przed ingerencją osób niepowołanych.

---

[4] Internet of Things, tzw. Internet rzeczy, czyli różnorodne urządzenia podłączone do Internetu, np. kamery, sterowniki przemysłowe, drukarki itp.

Niestety, wspomniany wcześniej wzrost mocy obliczeniowej powszechnie dostępnych komputerów, wzbogacony o rozwój wolnego oprogramowania oraz uwolnienie kodów źródłowych wielu zamkniętych do niedawna technologii, doprowadziły do pojawienia się nowych gatunkowo zagrożeń. Próg wejścia obniżył się nie tylko dla użytkowników końcowych, ale również osób zainteresowanych przełamywaniem zabezpieczeń i atakowaniem systemów teleinformatycznych. Obecnie do przeprowadzenia ataku nie są wymagane żadne zaawansowane urządzenia oraz specjalistyczna wiedza. Wystarczy dowolny komputer osobisty bądź smartfon podłączony do Internetu. Wszelkie niezbędne informacje przedstawiane są np. w postaci przystępnych filmów instruktażowych, opisujących krok po kroku, w jaki sposób należy przeprowadzić atak. Również narzędzia uległy znacznemu uproszczeniu, czego przykładem jest graficzny interfejs *Armitage* do narzędzia *Metasploit.* Umożliwia on zautomatyzowane i skrajnie ułatwione zaatakowanie wybranego celu, dzięki wybraniu opcji „Hail mary"[5].

Wzrost wyzwań w cyberprzestrzeni jest dodatkowo napędzany poprzez coraz większą cyfryzację, obejmującą praktycznie każdy aspekt naszego życia. Połączone jest to z jednoczesnym pozbawieniem użytkowników technologii prywatności, gdyż aktywność każdej osoby posiadającej smartfon jest monitorowana praktycznie przez 24 godziny na dobę.

Należy zauważyć, iż:

> technologia rozszerzyła naszą rzeczywistość o jej wirtualny odpowiednik i na stałe weszła w praktycznie wszystkie dziedziny naszego życia. Szacuje się, że obecnie jest ok. 2,5 miliarda użytkowników smartfonów, a do roku 2020 liczba ta zbliży się do 2,9 miliarda. Wiele ułatwień, jakich doświadczyliśmy dzięki upowszechnieniu nowinek technicznych, możliwych do opisania wspólnym przedrostkiem „smart", ma jednak swoją cenę, której wielu użytkowników nie

[5] „Hail mary" można przetłumaczyć jako „Zdrowaś Maryjo". Jest to opcja uruchamiająca olbrzymią ilość ataków wykorzystujących wszelkie potencjalnie pasujące podatności dobrane w oparciu o informacje i usługi znalezione na urządzeniu będącym ofiarą ataku. Skorzystanie z tej funkcjonalności nie wymaga od osoby atakującej praktycznie żadnej wiedzy i umiejętności, pozwalając jednocześnie na sprawne przełamanie zabezpieczeń różnorodnych systemów poprzez zautomatyzowanie wielu faz ataku. Przykład wykorzystania przedstawiony jest m.in. na nagraniu udostępnionym przez twórcę tego oprogramowania: https://youtu.be/m5Z5nC6B9k, [dostęp: 22.05.2020].

> jest świadomych. O ile dawniej kontrola tego, z kim i o czym rozmawiamy, wymagała specjalnych uprawnień i żmudnej pracy zespołu ludzi, o tyle w chwili obecnej sami udostępniamy osobom postronnym olbrzymie ilości prywatnych danych. Jest to ciekawe zjawisko, szczególnie gdy zwrócimy uwagę, iż poza światem wirtualnym dalej z wielką starannością próbujemy dbać o zachowanie prywatności[6].

Szerzej temat prywatności został poruszony przez autora w cytowanej publikacji, jednak dla uchwycenia pełnego kontekstu niezbędne jest wskazanie na związek pomiędzy rozwojem technologii a dobrowolnym zrzekaniem się prywatności przez coraz większą część społeczeństwa. Jest to sytuacja generująca dodatkowe wyzwania, zwłaszcza z perspektywy administracji publicznej, gdyż z jednej strony tworzy ona szansę na zniwelowanie negatywnych zjawisk budujących się w społeczeństwie z odpowiednim wyprzedzeniem. Z drugiej strony, z punktu widzenia bezpieczeństwa narodowego, generuje zagrożenia, upowszechniając wiedzę o panujących nastrojach społecznych, preferencjach politycznych, światopoglądzie itd. dużej części społeczeństwa, co jest bezwzględnie wykorzystywane w walce informacyjnej. Udokumentowaniem takich działań jest akt oskarżenia[7] przeciwko osobom zaangażowanym w działania dezinformacyjne skierowane w obywateli Stanów Zjednoczonych, mające w założeniu wpłynąć na wyniki wyborów prezydenckich z 2016 roku.

Podsumowując, informacja odgrywa współcześnie coraz większą rolę. Rozwój technologii umożliwia nie tylko coraz większą cyfryzację, podnoszącą sprawność funkcjonowania i przetwarzania informacji, obejmującą poszczególne aspekty funkcjonowania współczesnych państw, ale także przyczynia się do aktywowania nowych jakościowo zjawisk, z jakimi współczesne organizmy państwowe nie miały okazji się zmierzyć.

---

6 K. Goryń, *Rozwój technologiczny a prywatność. Rzecz o (nie)świadomym „ekshibicjonizmie"*, [w:] *Prawa człowieka wobec wyzwań współczesnego świata*, A. Czubik, D. Dziwisz, E. Szczepankiewicz-Rudzka (red.), Księgarnia Akademicka, Kraków 2019, s. 329.

7 R.S. Mueller [Special Counsel U.S. Department of Justice], *Indictment*, https://www.justice.gov/file/1080281/download, [dostęp: 22.05.2020].

Cyberbezpieczeństwo w dokumentach doktrynalnych

Dokumentem uznanym za podstawowy w tym obszarze jest *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*. Jest to dokument opisujący w sposób syntetyczny i całościowy ogólne kierunki działań służących zapewnieniu bezpieczeństwa państwa i obywateli. Treści zawarte w dokumencie z 2020 roku zestawione zostały z jego wcześniejszymi wydaniami, w celu wychwycenia zmian w podejściu do tematu i identyfikacji wyzwań płynących z cyberprzestrzeni. Analiza uzupełniona została o zapisy zawarte w Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015 roku oraz wybrane dokumenty Sojuszu Północnoatlantyckiego.

Na wstępie należy podkreślić, iż istotny jest sam fakt powstania specjalnego dokumentu omawiającego kluczowe problemy związane z zapewnieniem bezpieczeństwa w cyberprzestrzeni. Może to być wskaźnikiem uchwycenia tego, jak istotny jest to obszar w funkcjonowaniu nowoczesnego państwa. Jednak samo tworzenie doktryn oraz strategii nie podnosi poziomu bezpieczeństwa, które wymaga podejmowania realnych działań skoncentrowanych na niwelowaniu zagrożeń i wyzyskiwaniu szans.

Strategie Bezpieczeństwa Narodowego

W dokumencie z 2020 roku cyberbezpieczeństwu poświęcono osobny podrozdział w ramach Filaru I opisującego bezpieczeństwo państwa i obywateli. Wydzielonym obszarem pokrewnym jest również „przestrzeń informacyjna", która w obecnych uwarunkowaniach jest nierozerwalnie powiązana z cyberprzestrzenią.

Ogólnym założeniem strategicznym jest „Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji"[8]. Co do zasady takie sformułowanie należy ocenić pozytywnie.

---

8 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, Warszawa 2020, s. 20.

Bezsprzecznie wszelkie działania mające na celu podniesienie poziomu bezpieczeństwa są słuszne. Twórcy strategii podeszli do zagadnienia holistycznie i nie ograniczyli się w swoich założeniach wyłącznie do sektora publicznego oraz militarnego. Jest to szczególnie ważne w sytuacji, gdy sektor prywatny i ogół społeczeństwa padają ofiarą cyberzagrożeń równie często (jeżeli nie częściej), co podmioty podległe administracji publicznej.

Doprecyzowaniem celu ogólnego jest 6 celów szczegółowych przedstawionych w podpunktach 4.1–4.6. Pierwszy z nich wskazuje, iż należy „zwiększać poziom odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej oraz osiągnąć zdolność do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia”[9]. Jest to, oczywiście, uszczegółowienie celu ogólnego, z wyraźnym zaakcentowaniem dwóch osi podziału: publiczno-prywatnej oraz militarno-cywilnej. Z jednej strony pozwala to na całościowe uchwycenie podmiotów, które powinny zostać objęte ochroną. Z drugiej strony jednak typologia ta nie pokrywa się z podejściem prezentowanym przez praktyków zajmujących się zapewnieniem cyberbezpieczeństwa, którzy oś podziału budują w oparciu o charakterystykę zagrożeń i systemów będących pod ich opieką. Lepszym odzwierciedleniem realnie podejmowanych działań cechuje się druga część punktu 4.1, wskazująca na potrzebę prewencji, bieżącego zwalczania oraz ścigania sprawców przyczyniających się do powstania cyberzagrożeń[10].

Kolejnym celem szczegółowym wskazanym w strategii jest wzmacnianie defensywnego potencjału państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa. Na poziomie strategicznym został on zdefiniowany w sposób ogólny, natomiast bardziej szczegółowe informacje znajdują się w Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz Uchwale nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Dokumenty te zostaną szerzej omówione w dalszej części opracowania. Na tym etapie warto zwrócić uwagę na zapis zawarty w ustawie o krajowym systemie cyberbezpieczeństwa, gdzie

9 Ibidem, s. 20.

10 Por. ibidem, s. 20.

wskazano, iż powodem ich opracowania była 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, co może sugerować, iż uregulowanie omawianego obszaru nastąpiło pod wpływem zobowiązań wewnątrzwspólnotowych, a nie w wyniku samodzielnie zidentyfikowanych potrzeb.

W punkcie 4.3 zaznaczono, iż należy „uzyskać zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni”[11]. W mojej opinii ten cel strategiczny jest zdefiniowany w sposób błędny. W pierwszej kolejności **pełne spektrum działań** jest to zakres stanowczo wykraczający poza możliwości Rzeczypospolitej Polskiej. Po drugie irracjonalne jest ograniczanie się wyłącznie do **działań militarnych**, które nawet w przyjętej w strategii typologii (omawianej powyżej) stanowią wyłącznie jeden z obszarów aktywności. Jeśli przyjmiemy założenie, iż cele strategiczne powinny być realne i mierzalne, w omawianym wypadku możemy mówić wyłącznie o mierzalności.

Kolejny cel szczegółowy wskazuje, iż należy „rozwijać krajowe zdolności w obszarze testowania, badania, oceny i certyfikacji rozwiązań i usług z obszaru cyberbezpieczeństwa”[12]. Jest to założenie jak najbardziej słuszne, gdyż pomimo globalnego charakteru zagrożeń dla cyberbezpieczeństwa lokalnie funkcjonujemy w oparciu o prawo krajowe i wspólnotowe, które wpływa na specyfikę funkcjonowania zarówno podmiotów prywatnych, jak i publicznych. Z tego względu wskazane jest dopasowanie ogólnodostępnych wytycznych oraz norm do urealnionych potrzeb wynikających z analizy wyzwań odnoszących się do cyberbezpieczeństwa Polski.

W punkcie 4.5[13] wskazano na konieczność budowania tzw. *cyber awareness* w stosunku do jednostek funkcjonujących w ramach zorganizowanych struktur administracji publicznej, jak i w społeczeństwie. Posiłkując się moją dotychczasową pracą badawczą, sądzę, że jest to cel na tyle istotny, iż powinien znajdować się znacznie wyżej w hierarchii, gdyż ostatecznie to od ludzi wykorzystujących rozwiązania teleinformatyczne zależy w największym stopniu poziom bezpieczeństwa. Brak świadomości zagrożeń

11 Ibidem, s. 20.

12 Ibidem.

13 Por. ibidem.

u użytkowników stanowi jedno z największych wyzwań związanych z wykorzystaniem nowych technologii i bezpośrednie zagrożenie dla przestrzeni informacyjnej państwa opisanej w rozdziale 5. Z tego choćby względu waga omawianego celu jest szczególnie istotna i powinna być zaznaczona, przynajmniej, poprzez przeniesienie go wyżej w hierarchii celów szczegółowych.

Punkt 4.6 stanowi podsumowanie i spięcie wcześniej wymienionych celów, przy okazji uszczegóławiając obszary kluczowe z perspektywy państwa, takie jak *machine learning, IoT*, szerokopasmowy przesył danych (w tym sieci 5G) oraz współpracę pomiędzy sektorem prywatnym oraz publicznym (reprezentowanym m.in. przez uczelnie oraz ośrodki badawcze)[14].

Rozdział 5. Strategii z 2020 roku skupia się dodatkowo na bezpieczeństwie przestrzeni informacyjnej, która została tu wskazana jako wyodrębniony obszar wymagający podjęcia określonych działań. W podpunkcie 5.1 wprowadzono typologię, w której zaznaczono, iż przestrzeń informacyjna wymaga ochrony w warstwie wirtualnej, fizycznej oraz poznawczej[15]. Należy zauważyć, iż co najmniej dwie ze wskazanych kategorii bodaj częściowo zazębiają się z omawianą wyżej cyberprzestrzenią, co w szerszej perspektywie uzależnia sukces w jednym obszarze od powodzenia działań podejmowanych w innym.

W praktyce, biorąc pod uwagę zależność pomiędzy rozwojem technologicznym a przepływem oraz przetwarzaniem informacji, osiągnięcie celów opisanych w rozdziale 5. jest uwarunkowane choćby częściowym sukcesem działań podejmowanych w celu zapewnienia bezpieczeństwa cyberprzestrzeni. Powyższe wnioski potwierdza dodatkowo analiza innych fragmentów opisywanej strategii, która łączy ze sobą przestrzeń informacyjną oraz cyberprzestrzeń. Ogólnie jednak należy uznać, iż Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2020 roku jest w obszarach zapewnienia cyberbezpieczeństwa oraz bezpieczeństwa informacyjnego w miarę spójna.

Ciekawe wyniki niesie porównanie ze sobą obecnie obowiązującej Strategii ze *Strategią Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*

14 Por. ibidem, s. 20.

15 Por. ibidem, s. 21.

2014. W pierwszej kolejności dokument z roku 2014 posiadał inną formę, w ramach której cyberbezpieczeństwo nie funkcjonowało jako wydzielony obszar, któremu poświęcono szczególną uwagę. Wskazane ono było jako cel strategiczny, sformułowany pod postacią „zapewnienia bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni"[16], wynikający ze zdefiniowanych wcześniej interesów narodowych.

Sama cyberprzestrzeń wymieniana była w kontekście:

- potencjału ochronnego[17],
- ogólnej charakterystyki zagrożeń związanych z rozwojem technologii i ich rosnącego wpływu na bezpieczeństwo narodowe[18],
- konieczności nawiązywania współpracy międzynarodowej w celu skutecznego przeciwdziałania zagrożeniom w cyberprzestrzeni[19],
- bezpieczeństwa systemu teleinformatycznego Rzeczypospolitej Polskiej oraz *cyber awareness*[20],
- nowego obszaru walki zbrojnej[21],
- współpracy sojuszniczej[22],
- stworzenia instytucji oraz ram prawnych odpowiedzialnych za budowanie cyberbezpieczeństwa[23].

W praktyce można zauważyć, iż Strategia z 2014 roku kładła większy nacisk na współpracę sojuszniczą, co należy ocenić pozytywnie, biorąc pod uwagę globalny charakter wyzwań płynących z cyberprzestrzeni. Aspiracje w zakresie prowadzenia działań ofensywnych były bardziej stonowane, co również należy ocenić pozytywnie. Niezmiennie w obu dokumentach wskazywano na konieczność sformowania jednostek w Siłach Zbrojnych RP odpowiedzialnych za prowadzenie działań w cyberprzestrzeni, a także własnych zdolności kryptograficznych. Mniejszą rolę poświęcono

16 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014*, Warszawa 2014, s. 12.

17 Por. ibidem, s. 14.

18 Por. ibidem, s. 19.

19 Por. ibidem, s. 20.

20 Por. ibidem, s. 25, 46.

21 Por. ibidem, s. 29, 43.

22 Por. ibidem, s. 32.

23 Por. ibidem, s. 46.

natomiast uzyskaniu zdolności w zakresie kontrolowania przestrzeni informacyjnej, wskazując na potencjalną kolizję z wolnościami obywatelskimi.

W porównaniu do obu omówionych wyżej dokumentów *Strategia Bezpieczeństwa Narodowego 2007* prezentuje się bardzo ubogo. Pojęcie cyberbezpieczeństwa *sensu stricto* w niej nie występuje. Wzmianki o potencjalnych zagrożeniach w cyberprzestrzeni pojawiają się wyłącznie w kontekście przestępczości zorganizowanej, która ma stanowić zagrożenie dla systemów teleinformatycznych[24]. Szerzej opisane zostało bezpieczeństwo informacyjne oraz teleinformatyczne, jednak ogólne założenia skupiały się na zapewnieniu stabilności systemów powiązanych z infrastrukturą krytyczną oraz ochroną informacji niejawnych[25]. Przypomina to w pewnym zakresie podejście stosowane m.in. w latach osiemdziesiątych w odniesieniu do ARPANET, gdzie bezpieczeństwo zapewniano poprzez doraźne podejmowanie działań w odpowiedzi na pojawiające się zagrożenia, bez próby wdrożenia rozwiązań w samych założeniach tworzonej technologii.

Swoistym uzupełnieniem strategii z 2014 roku jest *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015*[26]. Dokument ten poświęcony jest analizie wyzwań płynących z cyberprzestrzeni. Podzielony został na cztery główne części opisujące:

1. Cele strategiczne RP w dziedzinie cyberbezpieczeństwa.
2. Środowisko cyberbezpieczeństwa RP.
3. Koncepcje zadań operacyjnych w dziedzinie cyberbezpieczeństwa.
4. Koncepcje zadań preparacyjnych w dziedzinie cyberbezpieczeństwa.

Niestety, ogólna wartość merytoryczna omawianego dokumentu jest dalece niezadowalająca. Autorzy popełnili istotny błąd już na etapie formułowania definicji cyberprzestrzeni RP, którą powiązali terytorialnie z obszarem Rzeczypospolitej Polskiej[27]. Wskazać należy, iż niemożliwe

---

24 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2007 roku*, Warszawa 2007, s. 10, 19.

25 Por. ibidem, s. 20-21.

26 *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015*, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf, [dostęp: 01.07.2020].

27 Por. ibidem, s. 7.

jest sztywne powiązanie określonych obszarów cyberprzestrzeni z wybranym terytorium. Oczywiście, korelacja istnieje, jednak kluczową cechą cyberprzestrzeni jest jej globalny charakter i tworzenie powiązań (rozumianych np. jako węzły sieci) ignorujących ograniczenia geograficzne. Bliższa prawdy byłaby definicja opisująca cyberprzestrzeń RP w kategorii siły wpływu na obywateli zamieszkujących terytorium Polski, obejmująca kluczowe serwisy informacyjne czy też wykorzystywane usługi.

Inne problemy, które pojawiają się przy lekturze omawianego dokumentu, to stawianie nierealnych i w dużej części niemierzalnych celów, wyraźne skoncentrowanie się na aspektach militarnych i marginalizowanie (lub wręcz ignorowanie) przemian społecznych, których katalizatorem jest rozwój technologii i powszechny dostęp do Internetu. Dokument opublikowany został w maju 2015 roku i *de facto* ignorował fenomen portali społecznościowych czy też działań dezinformacyjnych. Wskazane działania „hybrydowe" przedstawiane były głównie w kontekście konfliktów zbrojnych, takich jak np. wojna we wschodniej części Ukrainy. Należy przy tym przypomnieć, że w tym samym czasie trwały intensywne działania podejmowane przez Rosję, mające na celu zakłócenie nadchodzących wyborów prezydenckich w USA, które były gatunkowo różne od szpiegostwa przemysłowego czy też konfliktu „hybrydowego". Twórcy omawianej doktryny nie dostrzegli tych zagrożeń, tak samo jak np. kwestii związanych z rozwojem druku 3D czy też, szerzej, rozprzestrzenianiem, popularyzacją i obniżeniem kosztów urządzeń i oprogramowania, które można wykorzystać w celach ofensywnych.

Zwrócono natomiast uwagę na to, iż konieczne jest posiadanie dostępu do kodów źródłowych nabywanego sprzętu wojskowego, co samo w sobie miało „gwarantować informatyczne panowanie (kontrolę) nad nim"[28]. Założenie to (zawarte w punkcie 5.) samo w sobie stanowi **realne zagrożenie** dla cyberbezpieczeństwa państwa, gdyż buduje fałszywe przeświadczenie, że samo posiadanie dostępu do kodów źródłowych wykorzystywanego oprogramowania jest warunkiem wystarczającym do zrozumienia zasad

[28] Por. ibidem, s. 11.

jego działania i prawidłowej obsługi. W rzeczywistości jest to jedynie jeden z elementów, który bez posiadania zaplecza w postaci kadry ekspertów mogących poddać realnej analizie posiadane wyposażenie, nie podnosi w żaden sposób zdolności bojowych. Paradoksalnie, samo posiadanie kodu źródłowego oprogramowania, wykorzystywanego np. przez siły zbrojne, może sprowokować przeciwników do podejmowania działań mających na celu np. ich wykradzenie, co dodatkowo zwiększa poziom zagrożeń.

Jednym z pozytywnych elementów, na który warto zwrócić szczególną uwagę, są jasne wytyczne w zakresie konieczności budowania zdolności do działań ofensywnych w cyberprzestrzeni. Pod tym względem dokument ten należy ocenić pozytywnie, gdyż biorąc pod uwagę specyfikę aktywności związanej z zapewnianiem bezpieczeństwa w cyberprzestrzeni niezbędne jest symultaniczne budowanie zarówno zdolności ofensywnych, jak i defensywnych.

Podsumowując, analiza trzech ostatnich Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej pozwala zauważyć wyraźne zmiany w postrzeganiu cyberbezpieczeństwa, które ewoluowało od zapewnienia bezpiecznej łączności i ochrony informacji niejawnych do szerszego postrzegania go z perspektywy ochrony całej cyberprzestrzeni, ściśle powiązanej z funkcjonowaniem sfer cywilno-militarnej, publiczno-prywatnej oraz bezpieczeństwem informacyjnym, z którym się nierozerwalnie zazębia.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024

Dokumentem doktrynalnym dotyczącym cyberbezpieczeństwa jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 opublikowana w Monitorze Polskim 30 października 2019 r.

Z racji swojego charakteru poświęcony jest on działaniom, które państwo powinno zrealizować do roku 2024 w obszarze cyberbezpieczeństwa. Celem głównym opisanym w strategii jest „Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie

wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji"[29]. Jego rozwinięciem są poniższe cele szczegółowe[30]:

1. Rozwój krajowego systemu cyberbezpieczeństwa.
2. Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.
3. Zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni.
4. Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa.
5. Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

W odniesieniu do celu pierwszego autorzy strategii zauważają, iż umocowanie prawne w zakresie budowy krajowego systemu cyberbezpieczeństwa, wynikające z przepisów państwowych oraz międzynarodowych, pozwala podjąć prace nad budową systemu. Jednak zwracają również uwagę na to, iż najprawdopodobniej konieczne będzie zmodyfikowanie poszczególnych ustaw w celu lepszego dostosowania ich do otaczającej rzeczywistości.

Najlepiej duch wyzwań stojących przed Polską oddaje ostatni akapit części 5.1, wskazujący, iż:

> Z uwagi na dynamikę procesów zachodzących w obszarze cyberbezpieczeństwa niezbędne będzie ciągłe monitorowanie zjawisk tam zachodzących i inicjowanie ewentualnych zmian w przepisach prawa. Propozycje kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa będą opiniowane przez Kolegium do Spraw Cyberbezpieczeństwa działające przy Radzie Ministrów. Jest to organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności zespołów CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa[31].

---

29 Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, Monitor Polski. Dziennik Urzędowy Rzeczypospolitej Polskiej, poz. 1037, s. 8.

30 Ibidem, s. 8-9.

31 Por. ibidem, s. 10-11.

Poza koniecznością stałego monitoringu przepisów autorzy wskazują, iż niezbędne jest włączenie w ten proces przedstawicieli podmiotów liniowych, zajmujących się bezpośrednim zwalczaniem cyberzagrożeń.

Uzupełnieniem pierwszego celu szczegółowego jest opis stanu docelowego, oczekiwanego po uruchomieniu systemu teleinformatycznego, wspierającego współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa. Odpowiadać ma on za generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa, zgłaszanie i obsługę incydentów, szacowanie ryzyka na poziomie krajowym oraz ostrzeganie o cyberzagrożeniach[32]. Uruchomienie takiego rozwiązania niewątpliwie przyczyniłoby się do podniesienia poziomu cyberbezpieczeństwa w kraju, pod warunkiem, iż system ten sam nie padłby ofiarą skutecznego ataku, tak jak miało to miejsce w Grecji na początku 2020 roku[33]. Pozytywnie należy ocenić zaakcentowanie konieczności współpracy pomiędzy obszarami militarnym i cywilnym[34]. Sama strategia stosuje różnorodne typologie podziału podmiotów wymagających ochrony przed cyberzagrożeniami, jednak zauważyć można wyraźny wpływ charakterystyczny dla praktycznego podejścia do cyberbezpieczeństwa, czego przykładem jest m.in. wyodrębnienie obszarów IT oraz OT[35]. Podejście takie w sposób znaczący podnosi wartość całego dokumentu, który, pomimo swojego wysokopoziomowego charakteru, dominującego w dokumentach strategicznych, mocno odnosi się do obszaru, który ma kształtować w ramach całego środowiska bezpieczeństwa.

Drugi z celów szczegółowych omawia wyzwania niższego poziomu, w ramach których wskazuje na konieczność wprowadzenia ujednolicenia wymogów stawianych wykorzystywanemu sprzętowi oraz oprogramowaniu[36]. Przy czym autorzy nie ograniczają się tu wyłącznie do oceny bezpieczeństwa „produktów końcowych", ale wprowadzają pojęcie bezpiecznego

---

32 Por. ibidem, s. 11.

33 mfr/mk/, *Greckie instytucje rządowe padły ofiarą cyberataku*, https://www.pap.pl/pap-technologie/592412%2Cgreckie-instytucje-rzadowe-padly-ofiara-cyberataku.html, [dostęp: 31.05.2020].

34 Por. Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa..., s. 12.

35 Por. ibidem, s. 12.

36 Por. ibidem, s. 15.

łańcucha dostaw[37]. Jest to bardzo istotny fragment strategii, gdyż wskazuje on bezpośrednio na szanse, jakie można wyzyskać, poprzez adekwatne odpowiedzi na wyzwania dotyczące obowiązku zapewnienia cyberbezpieczeństwa.

Bardzo pozytywnie należy również ocenić propozycje zawarte w punkcie 6.3, wskazujące na konieczność regularnego prowadzenia testów penetracyjnych i wdrożenia innych mechanizmów, pozwalających na względnie bezpieczne wykrycie podatności w systemach teleinformatycznych i ich wyeliminowanie przy zminimalizowanym ryzyku dla użytkowników końcowych.

Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa, stanowiące trzeci cel szczegółowy, rozbite jest na cztery cele cząstkowe[38]:

- rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa,
- nastawienie na rozwój współpracy między sektorem publicznym i prywatnym,
- stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa,
- uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni.

Z poszczególnych elementów składowych najuważniej warto przyjrzeć się ostatniemu z nich, skoncentrowanemu na uzyskaniu możliwości realizowania pełnego spektrum działań militarnych. Głębsza analiza celu cząstkowego pozwala zauważyć, iż autorzy skupiają się wyłącznie na aktywności defensywnej, a mianowicie rozpoznawaniu zagrożeń, ochronie i obronie sieci teleinformatycznej oraz zwalczaniu źródeł cyberzagrożeń[39]. Oczywiście zawieranie w strategii deklaracji o podejmowaniu działań w celu uzyskania zdolności ofensywnych nie zawsze stanowi rozsądne działanie np. z perspektywy współpracy międzynarodowej. Jednak należy zaznaczyć, że dokument marginalizuje aktywności choćby w zakresie SigInt[40] i koncentruje aktywność badawczo-rozwojową na obszarach defensywnych.

---

37 Por. ibidem, s. 16.

38 Por. ibidem, s. 17-19.

39 Por. ibidem, s. 19.

40 SigInt – Signal Intelligence, wywiad radioelektroniczny.

Czwarty cel szczegółowy skupia się na budowaniu *cyber awareness*, czyli ogólnej świadomości obrazującej wyzwania stojące przed społeczeństwem i administracją publiczną, związane z coraz mocniejszym splątaniem świata fizycznego z jego wirtualnym odpowiednikiem. Również w tym zakresie należy pozytywnie ocenić podjęte założenia, które koncentrują się na ogólnym podniesieniu poziomu wiedzy na temat technologii wykorzystywanej przez ogół społeczeństwa. Podstawowym problemem w zwalczaniu wszelkich zagrożeń, w tym również tych występujących w cyberprzestrzeni, jest niski poziom świadomości społecznej. Bez zrozumienia zasad działania wykorzystywanej technologii nie da się skutecznie zabezpieczyć użytkowników przed najpowszechniejszymi zagrożeniami.

Ofiarą postępu technologicznego padają m.in. prywatność czy też wolności obywatelskie, które traktowane były do niedawna jako niezbywalne. Z jednej strony rozwój technologii wpływa na ułatwienie dostępu do wiedzy, z drugiej może powodować zamykanie poszczególnych osób w bańkach informacyjnych, które przyczyniają się do pogłębienia błędów poznawczych. Z tego względu każde działania edukacyjne podejmowane w tym obszarze należy traktować jako zjawisko pozytywne.

Ostatnim z celów szczegółowych jest aspiracja do zbudowania silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa. Jest to cel o tyle wyjątkowy, iż w pełni skupia się na wyzyskaniu szans, jakie niosą ze sobą wyzwania płynące z cyberprzestrzeni[41]. W pierwszej kolejności autorzy strategii skupili się na przekuciu wyzwań na szanse zacieśnienia współpracy sojuszniczej w ramach NATO, UE oraz ONZ. Zawarcie powyższych założeń w dokumencie doktrynalnym samo w sobie nie wzmacnia naszej pozycji w omawianych organizacjach, jednak bezwzględnie obrazuje, z jakimi podmiotami się utożsamiamy i chcemy współpracować.

Ostatecznie realizacja założonego celu, powiązana z wcześniej wyartykułowanymi działaniami, powinna w sposób znaczący przyczynić się do wzrostu bezpieczeństwa w cyberprzestrzeni, co stanowiłoby zniwelowanie potencjalnych zagrożeń. Jednocześnie podniesienie zdolności w obszarach defensywnych, wprowadzenie standaryzacji w zakresie wymagań stosowanych do systemów teleinformatycznych, jak i opracowanie, i wdrożenie

41 Por. ibidem, s. 22-23.

autorskich rozwiązań pozwoliłoby wyzyskać szanse związane z rozwojem technologicznym.

Aktualna wizja cyberbezpieczeństwa w dokumentach doktrynalnych

Z przeprowadzonej analizy strategii opracowywanych na przestrzeni ostatnich lat można zauważyć wyraźną ewolucję w zakresie podejścia do omawianego zagrożenia. Pierwotnie cyberprzestrzeń nie była traktowana jako wydzielone środowisko obejmujące coraz większą ilość aspektów funkcjonowania państwa i społeczeństwa. Wszelkie zagrożenia kojarzone były głównie z cyberprzestępczością i zakłóceniami w dostępie do usług kluczowych, kojarzonych z infrastrukturą krytyczną. Uzupełnieniem było skupienie się na ochronie informacji niejawnych, które ze swojej natury związane były głównie z funkcjonowaniem wojska i służb specjalnych.

Na przestrzeni lat nastąpiła jednak ewolucja, której najpełniejszy obraz znajduje się w omówionej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Pomimo iż jest to dokument o charakterze doktrynalnym i wysokopoziomowym, widać w nim wyraźny wpływ osób bezpośrednio związanych z zapewnianiem cyberbezpieczeństwa i reagowaniem na incydenty w cyberprzestrzeni. Jest to zjawisko bardzo pozytywne, gdyż wykorzystanie wiedzy i doświadczenia osób posiadających praktyczne kompetencje w obszarze ochrony IT oraz OT jest kluczowe dla skutecznej mitygacji zagrożeń.

Samo cyberbezpieczeństwo nie jest już wyłącznie ograniczone do wybranych operatorów infrastruktury krytycznej, ale w większym stopniu odpowiada wyzwaniom płynącym z cyberprzestrzeni. Jest wieloaspektowym środowiskiem wpływającym na funkcjonowanie praktycznie każdego obszaru życia państwowego i społecznego. W praktyce jest nierozerwalnie związane m.in. z bezpieczeństwem informacyjnym, które ze względu na coraz większą ilość informacji przetwarzanych cyfrowo jest w coraz większym stopniu uzależnione od rozwoju technologicznego.

Warte podkreślenia jest też zaakcentowanie wysokiej dynamiki przemian zawarte w Strategii Cyberbezpieczeństwa RP, która *de facto* stanowi dokument o charakterze bardziej operacyjnym niż strategicznym. Jednak wytyczone przez nią kierunki działania pozwalają na osiągnięcie celów, cechujących się mierzalności i realnością.

Wizja cyberbezpieczeństwa a studium wybranych przypadków

Analiza dokumentów doktrynalnych jest tylko jednym z obszarów, który może posłużyć do uchwycenia tego, w jaki sposób postrzegane jest cyberbezpieczeństwo w Polsce. Istotnym uzupełnieniem jest analiza problemów i rozwiązań występujących w kluczowych dla państwa obszarach. Pominę więc mniej istotne przykłady zagrożeń płynących z cyberprzestrzeni, skupiając się na obszarach kluczowych, występujących w praktycznie każdym z omawianych powyżej dokumentów.

Pierwszym z nich będzie zamówienie i wdrożenie zaktualizowanego serwisu internetowego Agencji Wywiadu. Serwis uruchomiony na początku 2018 roku posiada liczne braki obrazujące bardzo niski poziom świadomości zagrożeń płynących z cyberprzestrzeni u osób podejmujących decyzję o jego wykorzystaniu. Szerzej problem został opisany na portalu internetowym Zaufana Trzecia Strona[42].

W praktyce serwis ten nie spełnia praktycznie żadnych wymogów, które powinny zostać zrealizowane, aby możliwe było bezpieczne wykorzystanie go w celach rekrutacji potencjalnych kandydatów do służby. Co więcej, sam serwis został napisany bez spełniania tzw. dobrych praktyk programistycznych (pozostawiono fragmenty kodu pozwalające zidentyfikować twórcę) i z pewnością nie spełnia wymogów *security by design* oraz *privacy by design* opisanych m.in. w Strategii Cyberbezpieczeństwa RP.

Pomimo wskazanych niedociągnięć, które w wypadku strony internetowej służącej do rekrutacji funkcjonariuszy i pracowników wywiadu cywilnego można uznać za poważne podatności ułatwiające poznanie ich personaliów, nie podjęto żadnych realnych działań naprawczych. Wskazać należy, iż wiedza o dobrych praktykach, dostępna w domenie publicznej, została ewidentnie zignorowana, mimo że wywiad cywilny jest organizacją szczególnie ważną w systemie bezpieczeństwa państwa.

Innym przykładem wykorzystania luki w systemie teleinformatycznym, w celu przeprowadzenia działań ofensywnych przeciwko Rzeczypospolitej Polskiej, jest włamanie na stronę Akademii Sztuki Wojennej, którego

---

42 *Długa lista problemów z nową stroną internetową Agencji Wywiadu*, https://zaufanatrzeciastrona.pl/post/dluga-lista-problemow-z-nowa-strona-interne-towa-agencji-wywiadu, [dostęp: 01.06.2020].

wynikiem było zamieszczenie spreparowanego listu otwartego, którego autorstwo przypisano gen. bryg. dr. inż. Ryszardowi Parafianowiczowi[43].

W tym wypadku autorzy ataku doprowadzili do podmiany treści na serwisie uczelni wojskowej, a także wybranych portalach informacyjnych, które wykorzystano do rozpowszechnienia spreparowanej odezwy uderzającej we współpracę na linii Polska–USA oraz obecność militarną sojuszników na terenie RP.

Oba opisywane incydenty wskazują, iż świadomość cyberzagożeń w opisywanych instytucjach, przy okazji spełniających wszelkie wymogi, aby zostać uznane za szczególnie ważne dla systemu bezpieczeństwa narodowego, jest stanowczo zbyt niska.

Prowadząc własne badania w przedmiotowym obszarze, byłem w stanie zidentyfikować inne potencjalne wektory ataku na opisywane instytucje, które w dalszym ciągu pozostają dostępne z Internetu.

Pokazuje to, że pomimo prawidłowo określonych celów strategicznych, nawet w ramach instytucji odpowiedzialnych za budowanie cyberbezpieczeństwa, wiedza w tym zakresie nie jest powszechna, a wdrożenie rozwiązań mających na celu zminimalizowanie zagrożeń płynących z cyberprzestrzeni stanowi skomplikowane wyzwanie, które wymaga zaangażowania odpowiednich sił i środków.

Wnioski

Na przestrzeni lat zauważyć można rosnącą dojrzałość dokumentów doktrynalnych w obszarze omawiającym cyberprzestrzeń i płynące z niej wyzwania. Podobnie jak samo pojęcie bezpieczeństwa narodowego ewoluowało na przestrzeni lat, tak samo środowisko bezpieczeństwa wraz z pojęciem cyberbezpieczeństwa ulegało ewolucji.

Obecnie obowiązujące strategie bezpieczeństwa, w szczególności Strategia Bezpieczeństwa Cyberprzestrzeni na lata 2019–2024, ujmują zagadnienie holistycznie, definiując precyzyjnie cele w tym obszarze. Wstępna hipoteza robocza stanowiąca odpowiedź na pytanie badawcze: *W jaki*

---

43 *Fałszywy list polskiego generała na stronie akademii Sztuki Wojennej*, https://zaufanatrzeciastrona.pl/post/falszywy-list-polskiego-generala-na-stronie-www-akademii-sztuki-wojennej, [dostęp: 01.06.2020].

sposób scharakteryzowano cyberzagrożenia wpływające na środowisko bezpieczeństwa Polski w dokumentach strategicznych?, musiała zostać zmodyfikowana.

W obecnym kształcie przyjmuje ona następującą formę: *Rozwój technologiczny stanowi jedną z najistotniejszych zmiennych wpływających na współczesne środowisko bezpieczeństwa Polski. Powszechny dostęp do Internetu, połączony ze wzmożoną cyfryzacją poszczególnych aspektów funkcjonowania społeczeństwa oraz państwa, stanowi jeden z najbardziej newralgicznych obszarów wpływających na bezpieczeństwo narodowe. Odzwierciedlenie tego stanu rzeczy w dokumentach doktrynalnych pozwala na wskazanie ogólnych i szczegółowych kierunków działań, które należy podjąć w celu wyzyskania szans i zminimalizowania zagrożeń dla bezpieczeństwa. Niestety, pomimo obecności wiedzy eksperckiej w domenie publicznej, czego wskaźnikiem są prawidłowo sformułowane dokumenty doktrynalne, nie jest ona powszechna, a jej braki są szczególnie odczuwalne w podmiotach pełniących kluczową rolę w budowaniu bezpieczeństwa narodowego Polski.*

Bibliografia

Aleksandrowicz T.R., *Kluczowe megatrendy w bezpieczeństwie państwa XXI wieku*, Difin, Warszawa 2020.

Aleksandrowicz T.R., *Świat w sieci. Państwa, społeczeństwa, ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego,* Difin, Warszawa 2020.

Długa lista problemów z nową stroną internetową Agencji Wywiadu, https://zaufanatrzeciastrona.pl/post/dluga-lista-problemow-z-nowa-strona-internetowa-agencji-wywiadu.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf.

Fałszywy list polskiego generała na stronie Akademii Sztuki Wojennej, https://zaufanatrzeciastrona.pl/post/falszywy-list-polskiego-generala-na-stronie-www-akademii-sztuki-wojennej.

Goryń K., *Jak technologie kontrolują nasze* życie, „Nowa Konfederacja" 2018, nr 9 (9), https://nowakonfederacja.pl/jak-technol ogie-kontroluja-nasze-zycie.

Goryń K., *Rozwój technologiczny a prywatność. Rzecz o (nie)świadomym „ekshibicjonizmie"*, [w:] *Prawa człowieka wobec wyzwań współczesnego świata*, A. Czubik, D. Dziwisz, E. Szczepankiewicz-Rudzka (red.), Księgarnia Akademicka, Kraków 2019.

mfr/mk/, *Greckie instytucje rządowe padły ofiarą cyberataku,* https://www.pap.pl/pap-technologie/592412%2Cgreckie-instytucje-rzadowe-padly-ofiara-cyberataku.html.

Mueller R.S. [Special Counsel U.S. Department of Justice], *Indictment*, https://www.justice.gov/file/1080281/download.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014, Warszawa 2014.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, Warszawa 2020.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2007 roku, Warszawa 2007.

Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Monitor Polski. Dziennik Urzędowy Rzeczypospolitej Polskiej, poz. 1037.