UNIWERSYTET Andrzeja Frycza Modrzewskiego w Krakowie

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE

e-ISSN 2451-0718
ISSN 1899-6264

2024
Nr 3 (LVI)

DOI: 10.48269/2451-0718-btip-2024-3-008
Data wpłynięcia: 9.04.2024
Data akceptacji: 25.06.2024

Marceli Herman

dr, Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
https://orcid.org/0009-0004-8709-4632

Analiza zagrożeń polskiej infrastruktury cybernetycznej w latach 2010–2024. Część I: Lata 2010–2016

Wprowadzenie

Zagrożenia cybernetyczne polegają na zakłócaniu poprawnego działania infrastruktury państwowej oraz elementów składowych całego systemu bezpieczeństwa państwa. Instytucje i służby dysponujące odpowiednimi narzędziami do przeciwdziałania temu zjawisku nieustannie ewoluują, dostosowując swoje możliwości (prawne, techniczne, kooperacyjne itp.) do minimalizacji skutków tychże ataków bądź ich wczesnego wykrywania i neutralizacji.

Rzeczpospolita Polska jako kraj członkowski Unii Europejskiej, członek struktur bezpieczeństwa zbiorowego NATO, Organizacji Narodów Zjednoczonych, Organizacji Bezpieczeństwa i Współpracy w Europie, Światowej Organizacji Handlu oraz innych, w tym polsko-ukraińskiej współpracy wojskowej, jest narażona na liczne i wszechstronne zagrożenia cybernetyczne, jak również znajduje się w kręgu zainteresowania zewnętrznych podmiotów (ugrupowania hakerskie, służby specjalne itp.). Dlatego w celu optymalizacji bezpieczeństwa cybernetycznego w Polsce konieczne jest wypracowanie zmian o charakterze prawnym, organizacyjnym i technologicznym, zapewniających odpowiednią kooperację poszczególnych elementów systemu bezpieczeństwa państwa i pożądany poziom bezpieczeństwa cyberprzestrzeni oraz jej użytkowników.

W niniejszym artykule przeprowadzono analizę incydentów cybernetycznych oraz poziomu bezpieczeństwa witryn internetowych administracji publicznej, a także wskazano zasadnicze zagrożenia polskiej infrastruktury cybernetycznej w lata 2010–2016 r. Zastosowano porównawcze i statystyczne metody badawcze. Celem publikacji jest zwrócenie uwagi na proces ewolucji i intensyfikacji zagrożeń cybernetycznych, stanowiących problem dla zapewnienia optymalnego i pożądanego poziomu funkcjonowania państwa.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) definiuje pojęcie cyberbezpieczeństwa jako „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami”[1]. Znacznie szerszy zakres ma definicja opracowana przez National Initiative for Cybersecurity Careers and Studies (NICCS), organizację podległą Cybersecurity and Infrastructure Security Agency (CISA), określająca cyberbezpieczeństwo jako: „strategię, politykę i normy dotyczące zarówno bezpieczeństwa cyberprzestrzeni, jak i działania w niej, obejmujące z jednej strony pełen zakres czynności ukierunkowanych na redukcję zagrożeń, zmniejszenie podatności na nie i odstraszanie, międzynarodowe zaangażowanie, reagowanie na zdarzenia, zaś z drugiej – elastyczną politykę prewencyjną, uwzględniającą odpowiednie operacje w sieci komputerowej, zapewnienie informacji, działania organów ścigania, dyplomacji, wojska, służb wywiadowczych, odnoszące się do bezpieczeństwa i stabilności globalnej infrastruktury informacyjnej i komunikacyjnej”[2].

Trudności definicyjne sprawiają, że niektóre dokumenty odnoszące się do cyberbezpieczeństwa unikają definiowania tego pojęcia, wskazując mniej lub bardziej jego cel i przedmiot ochrony.

Statystyki zgłoszeń faktycznych oraz potwierdzonych incydentów cybernetycznych w latach 2010–2016

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL jako podmiot odpowiedzialny za monitorowanie zagrożeń cyberbezpieczeństwa i incydentów komputerowych w roku 2010 odnotował 621 zgłoszeń faktycznych[3], natomiast

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.U. L 151 z 7.06.2019, art. 2.

[2] Z. Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej” 2016, t. 3, nr 2(10), s. 108.

[3] Wszystkie zgłoszenia, bez weryfikacji, oficjalnie przyjęte przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL.

zakwalifikowanych i potwierdzonych incydentów[4] było 155[5]. W 2011 r. zaobserwowano nieznaczny wzrost liczby zgłoszeń – 854, z których 249 zakwalifikowano jako incydenty faktyczne[6]. Dużą liczbę zgłoszeń wzanotowano w 2012 r. (1168, z czego zakwalifikowanych zostało 457). Ten wzrost był wynikiem protestów internetowych w sprawie ratyfikacji umowy ACTA (Anti-Counterfeiting Trade Agreement)[7]. W roku 2013 widać było tendencję wzrostową liczby otrzymanych zgłoszeń i incydentów. Zarejestrowanych zostało 8817 zgłoszeń, z których 5670 zakwalifikowano jako incydenty[8]. Wzrost liczby zgłoszeń uwarunkowany był zastosowaniem nowych źródeł danych dostarczających informacji o wykrytych zdarzeniach cybernetycznych w sektorze administracji rządowej, co znacznie wzmocniło ich identyfikację, oraz obsługą dużej liczby zgłoszeń przy zastosowaniu platformy N6 (Network Security Incident eXchange)[9]. W 2014 r. zarejestrowano 12 017 zgłoszeń, z czego 7498 zakwalifikowano jako incydenty. Tak duże wartości spowodowane były upublicznieniem informacji o poważnym zagrożeniu cybernetycznym wynikającym z zaistnienia błędów bezpieczeństwa w popularnej bibliotece kryptograficznej OpenSSL, tzw. Heartbleed[10]. Wartości rejestrowanych zgłoszeń sukcesywnie wzrastały i tak w 2015 r. Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL zarejestrował łącznie 16 123 zgłoszeń, z których 8914 zakwalifikowano jako faktyczne incydenty[11]. W 2016 r. odnotowano 19 954 zgłoszenia o potencjalnym wystąpieniu incydentu komputerowego w obszarze kompetencyjnym Zespołu, jednak faktyczne naruszenie bezpieczeństwa teleinformatycznego wystąpiło w 9288 przypadkach[12].

---

4 Zweryfikowane i potwierdzone incydenty.

5 Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL [dalej: CERT.GOV.PL], *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 r.*, Warszawa 2011, s. 7, https://csirt.gov.pl/download/3/121/Analizaroczna2010.pdf [dostęp: 11.03.2024].

6 CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 r.*, Warszawa 2012, s. 7, https://csirt.gov.pl/download/3/137/Raportroczny2011.pdf [dostęp: 11.03.2024].

7 CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 r.*, Warszawa 2013, s. 5, https://csirt.gov.pl/download/3/158/RaportostaniebezpieczenstwacyberprzestrzeniRPw2012roku.pdf [dostęp: 11.03.2024].

8 CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 r.*, Warszawa 2014, s. 5, https://csirt.gov.pl/download/3/165/RaportostaniebezpieczenstwacyberprzestrzeniRPw2013roku.pdf [dostęp: 11.03.2024].

9 Dzięki tej usłudze przedsiębiorstwa i instytucje są informowane o problemach bezpieczeństwa w ich infrastrukturze cybernetycznej, w postaci: infekcji szkodliwym oprogramowaniem, hostowania szkodliwej treści (np. phishing) czy podatności w aplikacjach internetowych, zob. *n6*, CERT Polska, https://cert.pl/n6 [dostęp: 09.02.2024].

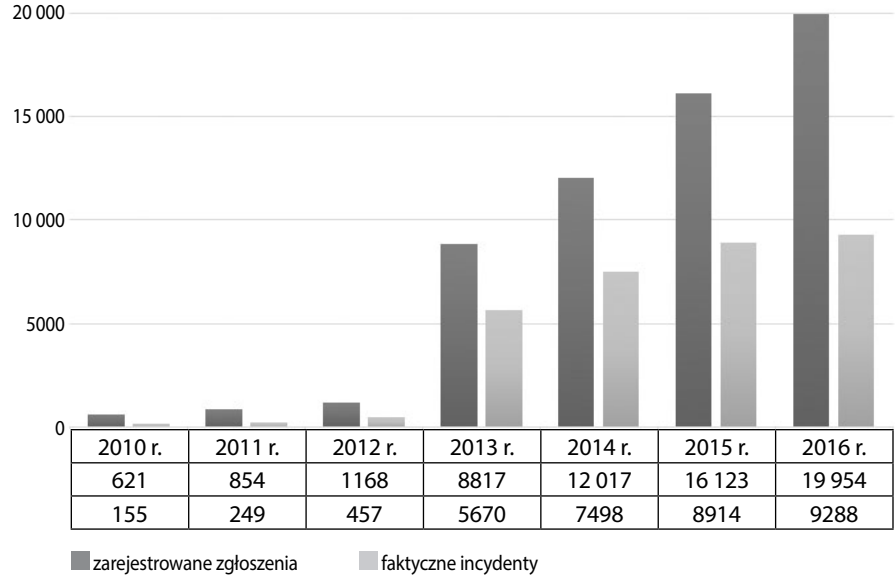
10 CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, Warszawa 2015, s. 6, https://csirt.gov.pl/download/3/172/RaportostaniebezpieczenstwacyberprzestrzeniRPw2014roku.pdf [dostęp: 11.03.2024].

11 CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r.*, Warszawa 2016, s. 7, https://csirt.gov.pl/download/3/183/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2015roku.pdf [dostęp: 11.03.2024].

12 CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 r.*, Warszawa 2017,

Analizowaną statystykę zgłoszeń i incydentów w przestrzeni internetowej przedstawia wykres 1.

Wykres 1. Statystyki zgłoszeń i incydentów w latach 2010–2016



2010 r.	2011 r.	2012 r.	2013 r.	2014 r.	2015 r.	2016 r.
621	854	1168	8817	12 017	16 123	19 954
155	249	457	5670	7498	8914	9288

Źródło: opracowanie własne na podstawie Raportów o stanie bezpieczeństwa cyberprzestrzeni RP w latach 2010–2016.

Badanie poziomu bezpieczeństwa witryn internetowych administracji publicznej z zastosowaniem systemu wczesnego ostrzegania ARAKIS-GOV

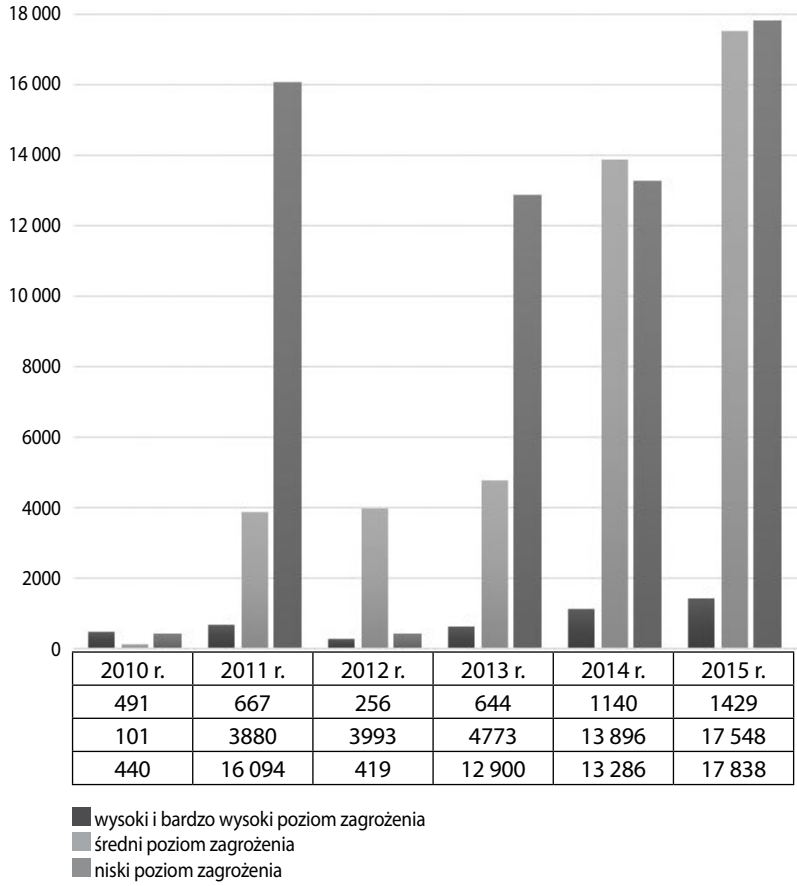
W związku z dużym zagrożeniem cybernetycznym w 2010 r. i zarejestrowaniem 28 109 alarmów infrastruktury cybernetycznej, przebadano przy użyciu system wczesnego ostrzegania ARAKIS-GOV 93 witryny należące do 63 instytucji państwowych. Stwierdzono 1277 błędów w tym: 451 błędów o bardzo wysokim poziomie zagrożenia, 40 błędów o wysokim poziomie zagrożenia, 440 błędów o niskim poziomie zagrożenia i 346 błędów oznaczonych jako informacyjne. Wśród podatności o wysokim lub bardzo wysokim poziomie zagrożenia przeważały błędy typu Cross Site Scripting, Blind SQL Injection oraz SQL/XPath Injection. Istotnym problemem było stosowanie nieaktualnych wersji oprogramowania[13]. W 2011 r. zarejestrowano spadek liczby rejestrowanych alarmów względem roku wcześniejszego – 20 634 alarmy.

s. 7–8, https://www.csirt.gov.pl/download/3/185/RaportostaniebezpieczenstwacyberprzestrzeniRPw2016roku.pdf [dostęp: 11.03.2024].

13 CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 r.*, *op. cit.*, s. 19.

Wykryto 667 błędów o bardzo wysokim poziomie zagrożenia (wzrost względem roku poprzedzającego uwarunkowany był zastosowaniem sond monitorujących przestrzeń cybernetyczną). Priorytet niski miało 77,96% ogółu incydentów (CERT.GOV.PL nie podał dokładnej ich liczby); odnotowano też 3880 błędów o średnim poziomie zagrożenia (niższe wartości wynikały z zastosowania udoskonalonej konfiguracji mechanizmów systemowych – korelacyjnych)[14]. W kolejnym roku (2012) przy wykorzystaniu systemu ARAKIS.GOV przebadano 67 witryn należących do 33 instytucji państwowych. Zarejestrowano 20 327 alarmów, stwierdzając 1133 błędy, w tym: 188 o bardzo wysokim poziomie zagrożenia, 68 o wysokim poziomie zagrożenia, 419 o niskim poziomie zagrożenia oraz 458 błędów informacyjnych (wykres 2).

Wykres 2. Liczba alarmów wygenerowanych przez system ARAKIS.GOV w latach 2010–2015



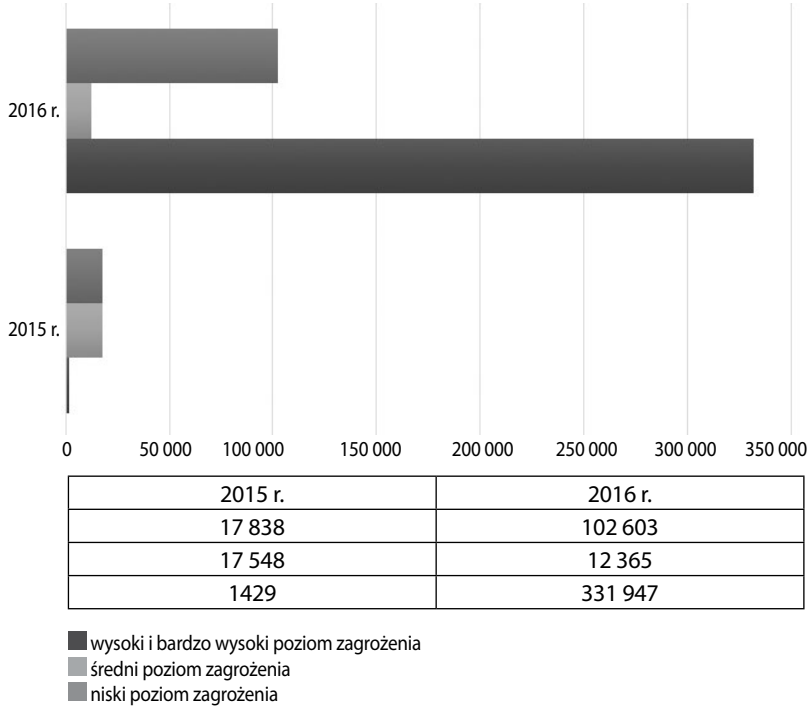
2010 r.	2011 r.	2012 r.	2013 r.	2014 r.	2015 r.
491	667	256	644	1140	1429
101	3880	3993	4773	13 896	17 548
440	16 094	419	12 900	13 286	17 838

Źródło: opracowanie własne na podstawie Raportów o stanie bezpieczeństwa cyberprzestrzeni RP w latach 2010–2015.

[14] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 r.*, *op. cit.*, s. 11.

Jako podatności o wysokim lub bardzo wysokim poziomie zagrożenia niezmiennie przeważały błędy typu SQL Injection/Blind SQL oraz Cross Site Scripting. Ponadto istotnym problemem było również wykorzystywanie nieaktualnych wersji oprogramowania[15].

Wykres 3. Liczba alarmów wygenerowanych przez system ARAKIS.GOV w latach 2015–2016



2015 r.	2016 r.
17 838	102 603
17 548	12 365
1429	331 947

Źródło: opracowanie własne na podstawie Raportów o stanie bezpieczeństwa cyberprzestrzeni RP w latach 2015–2016.

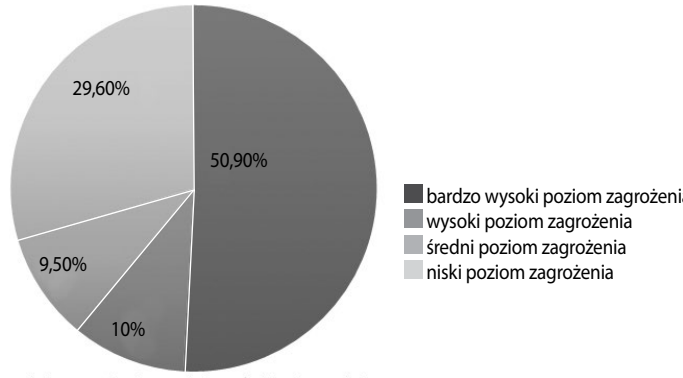
W 2013 r. zarejestrowano 18 317 alarmów. Wykryto 644 alarmy o wysokim poziomie zagrożenia, 4773 alarmy o średnim poziomie zagrożenia, a także 12 900 o niskim poziomie zagrożenia[16]. System ARAKIS-GOV w 2014 r. zarejestrował 28 322 alarmy, w tym: 1140 o wysokim poziomie zagrożenia, 13 896 o średnim poziomie zagrożenia, 13 286 o niskim poziomie zagrożenia[17]. W 2015 r. nastąpiła zdecydowana intensyfikacja zagrożeń cybernetycznych – zarejestrowano 36 815 alarmów. Wykryto 1429 alarmów o wysokim poziomie zagrożenia, 17 548

[15] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 r.*, *op. cit.*, s. 10–11.
[16] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 r.*, *op. cit.*, s. 5.
[17] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, *op. cit.*, s. 9.

o średnim poziomie zagrożenia oraz 17 838 o niskim poziomie zagrożenia[18]. Ponad dwunastokrotnie więcej alarmów zostało wygenerowanych w roku 2016, 446 915 zaistniałych przypadków. Liczbę alarmów wygenerowanych przez system ARAKIS. GOV w latach 2015–2016 przestawia wykres 3.

Wśród zanotowanych alarmów wskazano: 279 181 alarmów o bardzo wysokim poziomie zagrożenia (wymagających natychmiastowej reakcji – duże ryzyko przełamania zabezpieczeń), 52 766 alarmów o wysokim poziomie zagrożenia (wymagających wzmożonej uwagi – średnie ryzyko przełamania zabezpieczeń), 12 365 alarmów o średnim poziomie zagrożenia (informujących o dobrze znanym zagrożeniu – małe ryzyko przełamania zabezpieczeń), 102 603 alarmy o niskim poziomie zagrożenia (alarmy informacyjne dotyczące aktualnej sytuacji sieci internetowej)[19]. Graficzne przestawienie poziomu zagrożenia alarmów przedstawia wykres 4.

Wykres 4. Poziom zagrożeń cybernetycznych w latach 2010–2016.



Źródło: opracowanie własne na podstawie Raportów o stanie bezpieczeństwa cyberprzestrzeni RP w latach 2010–2016.

Zagrożenia polskiej infrastruktury cybernetycznej w latach 2010–2016

W roku 2010 zasadnicze rodzaje zagrożeń dla sieci instytucji państwowych ukierunkowane były na użytkowników sieci administracji publicznej, w postaci eksfiltracji dokumentów (szpiegostwo komputerowe opierające się na rozpowszechnianiu niewiarygodnych/zainfekowanych załączników poczty elektronicznej, a także stosowanie socjotechniki). Ponadto dotyczyły wykorzystywania błędów w aplikacjach WWW (podmiany treści oficjalnych witryn internetowych instytucji administracji publicznej). Innym rodzajem ataków w 2010 r. było skanowanie przestrzeni adresowej

[18] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r.*, *op. cit.*, s. 23–24.
[19] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 r.*, *op. cit.*, s. 7.

polegające na prowadzeniu rekonesansu topologii określonej sieci przed wykonaniem planowanego ataku cybernetycznego[20].

Charakterystyczne dla zagrożeń sfery cybernetycznej w 2011 r. było wykorzystywanie złośliwego oprogramowania (ZeuS, Spyeye) szpiegującego urządzenia mobilne. Wektorem infekcji były przeglądarki internetowe, a także załączniki w przesyłanych wiadomościach email. Ponadto rok 2011 charakteryzował się występowaniem ataków na centrale telefonii internetowej VoIP jednostek administracji publicznej, które przeprowadzano z zagranicznych przestrzeni adresowych, m.in. z: Palestyny, Azerbejdżanu, Korei Północnej i Afganistanu. W tym samym roku odnotowano intensyfikację ataków na urządzenia mobilne: automatyczne wysyłanie wiadomości tekstowych o podwyższonej płatności oraz kradzież danych wrażliwych[21].

W 2012 r. zasadnicze zagrożenia środowiska „cyber" stanowiły botnety, klasyfikowane jako typ złośliwego oprogramowania wytworzonego w celu przejęcia zdalnej kontroli nad komputerem. Celem ataku były: kradzież informacji, atak na inne systemy, propagacja infekcji na inne komputery, rozsyłanie niepożądanej i zainfekowanej korespondencji, inwigilacja itp. W 2012 r. liczba wykrytych komputerów zainfekowanych złośliwym oprogramowaniem w sieciach instytucji administracji państwowej wynosiła 3837 przy zastosowaniu specjalistycznego oprogramowania, m.in.: ZeuS, Citadel, Rustock, Slenfbot, DNSChanger (największy procent infekcji: ZeuS-P2P – 73%, Citadel – 17%). Ponadto rok 2012 charakteryzował się częstym występowaniem zjawiska haktywizmu, ukierunkowanego na podmiany stron internetowych, przekierowania na fałszywe witryny internetowe, wysyłanie niechcianej poczty, ataki typu DDoS (Distributed Denial of Service), powodujące przeciążenie serwerów poprzez nieustanne wysyłanie pakietów, co uniemożliwia dostęp do zasobów własnych[22].

Rok 2013 odznaczał się zwiększonym występowaniem zagrożeń cybernetycznych polegających na podatności serwerów DNS znajdujących się w przestrzeni adresowej instytucji administracji państwowej. Podmiot atakujący wysyłał zapytanie do serwerów DNS, dokonując zamiany adresu źródłowego na adres IP ofiary. Następnie serwery DNS wysyłały odpowiedzi na adresy IP ofiar, w wyniku czego bardzo duża liczba przesyłanych pakietów obciążała łącza serwerowe, powodując zakłócenie prawidłowego funkcjonowania (np. *amplification attack*, atak ze zwielokrotnieniem, będący jedną z odmian ataku DDoS)[23]. Kolejnym rodzajem zagrożeń odznaczającym się największą częstotliwością infekowania infrastruktury cybernetycznej były opisywane już botnety. Polska cyberprzestrzeń w 2013 r. mierzyła się także z typologią ataków ukierunkowaną na usługi Microsoft Windows Internet Information Services (IIS) Server Translate Header attempt oraz Outbound Teredo traffic. Pierwszy rodzaj ataku

[20] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 r.*, *op. cit.*, s. 50.
[21] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 r.*, *op. cit.*, s. 45–46.
[22] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 r.*, *op. cit.*, s. 45–47.
[23] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 r.*, *op. cit.*, s. 37–41.

polegał na wykorzystaniu żądania HTTP posiadającego spreparowane nagłówki, których celem była odmowa świadczenia usługi dla niektórych serwerów IIS. Skuteczność ataku miała swoje odzwierciedlenie w częstotliwości jego stosowania (18-proc. udział w statystykach w 2013 r.). Atak Outbound Teredo traffic omijał procedury zapory blokującej, w efekcie czego pozyskiwał informacje za pośrednictwem spreparowanego ruchu IPv6. To zagrożenie w 2013 r. i stanowiło 17% całości sklasyfikowanych ataków na infrastrukturę cybernetyczną[24].

W 2014 r. ataki na polską infrastrukturę cybernetyczną przybierały rozmaite formy. Jednym z nich była kampania phishingowa Energetic Bear, wymierzona w firmy sektora energetycznego[25]. Zasadniczym jej celem było uzyskanie dostępu do określonej jednostki komputerowej/systemu teleinformatycznego poprzez zastosowanie trzech, kompatybilnych ze sobą wektorów ataków. Wykorzystywano wiadomości typu *spear phishing*, w których implementowane było złośliwe oprogramowanie jako załącznik. Dodatkowo jednym z wektorów ataku było zastosowanie techniki *watering hole* w celu infekcji potencjalnej ofiary złośliwym oprogramowaniem (*LightsOut exploit kit*), ściągniętym ze skompromitowanej wcześniej witryny internetowej. Trzecim wektorem ataku było umieszczenie złośliwego oprogramowania pod postacią aktualizacji do oprogramowania stosowanego w sterownikach przemysłowych, wykorzystując skompromitowane strony producentów. Obiektem ataku były amerykańskie i europejskie firmy energetyczne, sektor zbrojeniowy, sektor IT oraz agencje rządowe z 23 krajów świata, w tym z Polski[26]. Kolejną kampanią cyberszpiegowską ukierunkowaną na struktury Sojuszu Północnoatlantyckiego, instytucje administracji publicznej, firmy energetyczne oraz telekomunikacyjne w krajach Unii Europejskiej i w Ukrainie, a także amerykańskie uczelnie wyższe była kampania SandWorm. Atakujący infekowali urządzenia poprzez wykorzystywanie szeregu podatności (m.in. CVE-2014-4114) w błędach mechanizmu Windows OLE. Do kompromitacji urządzenia wykorzystywano oprogramowanie BlackEnergy[27]. W omawianych kampaniach korzystano z technik inżynierii społecznej (np. podszywania się pod znane wizerunki firm lub innych podmiotów) w celu wyłudzenia danych wrażliwych. Ataki kierowane były do instytucji administracji publicznej, używano wiadomości e-mail, zainfekowanych załączników i spreparowanych stron internetowych. Stosowano najczęściej języki skryptowe w postaci kodów zawierających zestaw poleceń dla określonej aplikacji (makro), tak aby zautomatyzować powtarzające się czynności i dokonać zmian systemowych, omijając interakcje z użytkownikiem. Wykorzystywano również pliki z rozszerzeniem .scr (Windows Screen Saver) oraz .pif (Program Information

[24] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 r.*, *op. cit.*, s. 47.

[25] Nazwy alternatywne: Dragon Fly (nazwa nadana przez firmę *Symantec*) oraz Crouching Yeti (nazwa nadana przez firmę Kaspersky Lab).

[26] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, *op. cit.*, s. 16–17.

[27] *Ibidem*, s. 19–20.

File), imitujące dokumenty tekstowe[28]. W 2015 r. zarejestrowano wzrost liczby incydentów phishingowych (257 wykrytych incydentów – wzrost o 116% względem 2014 r.). Wymienione ataki wykorzystywały wizerunki następujących podmiotów: Helpdesk, DHL, Poczta Polska, PKO, ING, Alior, Mbank, PKO BP S.A. Tematyka ataków dotyczyła kwestii nieuregulowanych wierzytelności, odbioru przesyłki, spraw urzędowych. Proces ataku polegał na przesyłaniu złośliwego oprogramowania w formacie wykonywalnym ukrytym w archiwach, wraz z hasłem przekazywanym w dalszej części wiadomości. Formatem dokumentu był .doc pakietu Microsoft Office lub odnośniki HTTP do zasobów hostujących złośliwe oprogramowanie[29]. Helpdesk – atak polegał na wyłudzeniu danych uwierzytelniających w postaci loginu i hasła. Atakujący informowali o konieczności aktualizacji lub weryfikacji konta, przekroczeniu określonego limitu pojemności konta lub zawieszeniu konta, uzasadniając to kwestiami bezpieczeństwa; DHL – wektorem ataku była kompromitacja określonych witryn internetowych, następnie wykorzystanie ich jako serwery hostujące oprogramowanie złośliwe; Poczta Polska – wektor ataku obejmował oprogramowanie złośliwe (załącznik) oraz skompromitowane witryny Poczty Polskiej hostujące oprogramowanie złośliwe; PKO BP S.A. – wektor ataku ukierunkowany był na wykorzystanie skompromitowanych domen internetowych, podszywających się pod domeny atakowanego banku, w celu wyłudzenia danych wrażliwych (imię, nazwisko, PESEL, nr karty kredytowej, kod CVV itp.). Ujawniono następujące, skompromitowane domeny: hxxp://autoryzacja-ipko.com, hxxp://weryfikacja-ipko.com, hxxp://www.iipko.com, hxxp://ipko-weryfikacja.com, hxxp://pkobp-weryfikuj.com, hxxp://informacja-ipko.com[30]. W kolejnym roku (2016) odnotowano 6-proc. wzrost incydentów względem 2015 r. co przekładało się na 4158 incydentów w skali rocznej. Najliczniej występującym rodzajem zagrożeń w 2016 r. był klient botnet (spadek liczby wykrytych zagrożeń z 4284 w 2015 r., do 2836 w 2016 r.). Poza tym wśród najczęściej występujących zagrożeń cybernetycznych były ataki z kategorii inżynieria społeczna (382 incydentów, co stanowiło wzrost względem roku poprzedniego o około 33%)[31].

Podsumowanie

Wartym podkreślenia jest wskazanie przyczyn politycznych, militarnych oraz społecznych determinujących intensyfikację ataków lub zewnętrzne zainteresowanie polską infrastrukturą cybernetyczną. W analizowanym przedziale czasowym występowało wiele czynników zwracających uwagę świata lub regionu na Rzeczpospolitą Polską, których wykorzystanie mogło doprowadzić do osłabienia prawidłowego

[28] *Ibidem*, s. 21–25.
[29] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r.*, *op. cit.*, s. 41–42.
[30] *Ibidem*, s. 43–49.
[31] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 r.*, *op. cit.*, s. 12–13.

funkcjonowania państwa, jego sił zbrojnych lub infrastruktury cybernetycznej. Zasadniczym czynnikiem w 2010 r. była Tragedia Smoleńska: spreparowane treści związane z tą tematyką służyły prowadzeniu walki informacyjnej i do ataków cybernetycznych na organy administracji publicznej lub instytucje państwa. Zainteresowanie polską przestrzenią cybernetyczną było potęgowane także przez aspekt militarny w postaci organizacji ćwiczeń Wojska Polskiego pod kryptonimem Anakonda 2010, Baltops 2010, Borsuk 2010 (organizowanych również systematycznie w kolejnych latach). Ponadto polskie kontyngenty wojskowe uczestniczyły w działaniach poza granicami państwa. Rok 2011 sprzyjał zainteresowaniu polską przestrzenią cybernetyczną ze względu na polskie przewodnictwo w Radzie Unii Europejskiej od 1 lipca do 31 grudnia 2011 r., co wiązało się z koniecznością zapewnienia bezpieczeństwa infrastruktury informatyczno-telekomunikacyjnej. Innym wydarzeniem była organizacja Mistrzostw Europy w Piłce Nożnej EURO 2012. W obszarze cyberprzestrzeni prowadzono liczne działania zmierzające do zapewnienia bezpieczeństwa teleinformatycznego imprezy, tj. koordynację reagowania na incydenty komputerowe lub obsługę zdarzeń w sieciach instytucji odpowiedzialnych za prawidłowy przebieg Mistrzostw. Podpisanie przez stronę polską porozumienia ACTA doprowadziło do zorganizowania w dniach 21–25 stycznia 2012 r. akcji protestacyjnych w całym kraju, w ramach których przeprowadzono liczne ataki cybernetyczne DDoS oraz *website defacement* (podmiany witryn internetowych) ukierunkowane na instytucje administracji państwowej, w tym: Kancelarię Sejmu RP, Kancelarię Prezydenta RP, Kancelarię Prezesa Rady Ministrów, Ministerstwo Spraw Zagranicznych, Ministerstwo Sprawiedliwości, Ministerstwo Edukacji Narodowej, Kancelarię Senatu RP, Ministerstwo Kultury i Dziedzictwa Narodowego, Ministerstwo Obrony Narodowej, Komendę Główną Policji oraz Centralne Biuro Antykorupcyjne. Ponadto w 2012 r. została powołana inicjatywa społeczna zrzeszająca aktywistów internetowych sprzeciwiających się znacznemu ograniczaniu swobód obywatelskich na potrzeby zapewnienia bezpieczeństwa państwa. Przedmiotowa organizacja odnosiła się do walki z: projektem INDECT (Inteligentny system informacyjny wspierający obserwację, wyszukiwanie i detekcję dla celów bezpieczeństwa obywateli w środowisku miejskim), projektem Czysty Internet, Europejską Strategią na rzecz Lepszego Internetu dla Dzieci (ESNRLIDD), chipami RFID, nowelizacją ustawy o zgromadzeniach, zmianą ustawy o zapobieganiu epidemiom oraz ustawy o inspekcji sanitarnej. Innymi czynnikami polityczno-społecznymi wzbudzającymi chęć dokonania ataków cybernetycznych w Polsce była aneksja Półwyspu Krymskiego przez Rosję i konflikt militarny w Ukrainie (od 2014 r.), wybory prezydenckie i parlamentarne w Polsce (2015 r.). W lipcu 2016 r. zorganizowano dwa wydarzenia o znaczeniu międzynarodowym, które jednocześnie potencjalnie mogły generować możliwość wystąpienia większej niż zazwyczaj aktywności cyberprzestępców lub służb wywiadowczych w polskiej infrastrukturze

cybernetycznej: w Warszawie odbywał się Szczyt Sojuszu Północnoatlantyckiego NATO, a w Krakowie – Światowe Dni Młodzieży.

Cele ataków cybernetycznych są zróżnicowane – mogą być ukierunkowane na gromadzenie informacji niejawnych (lub jawnych), zakłócenie poprawności funkcjonowania określonego podmiotu (systemu bezpieczeństwa państwa, instytucji, obiektów użyteczności publicznej itp.), szerzenie dezinformacji w określonym kierunku (np. skłócenia społeczeństwa wokół kwestii mniejszości narodowych w danym państwie, wzmocnienia wizerunku danego państwa jako posiadacza znacznego i nowoczesnego potencjału militarnego i gospodarczego, zachęcenia bądź zniechęcenia społeczeństwa do rozpoczęcia działań wojennych itp.). Ponadto ataki cybernetyczne mogą przybierać charakter przestępczy (wyłudzenia środków finansowych, gromadzenie danych wrażliwych o osobach itp.). Dlatego istotą optymalnego funkcjonowania systemu przeciwdziałania zagrożeniom cybernetycznym jest sprawne funkcjonowanie wszystkich podsystemów bezpieczeństwa państwa. Ważnym aspektem jest zwiększenie świadomości społecznej dotyczącej zagrożeń i form ataków. W opisywanym przedziale czasowym 2010–2016 nie było jeszcze jednego aktu prawnego o randze ustawy normującego problematykę cyberbezpieczeństwa w Polsce. Ustawa o krajowym systemie cyberbezpieczeństwa została wdrożona w 2018 r., wcześniej bazowano na aktach prawnych rangi wykonawczej. W celu optymalizacji poziomu bezpieczeństwa cybernetycznego, zasadne jest dostosowywanie zakresu prawnego, kompetencji i możliwości technicznych służb (specjalnych, bezpieczeństwa publicznego), strategii bezpieczeństwa cybernetycznego państwa i świadomości społecznej oraz analizy informacji przekazywanych przez krajowe i zagraniczne agendy wywiadowcze o realnych lub potencjalnych zagrożeniach.

Bibliografia

Akty prawne i dokumenty

Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych, Dz.U. z 2005 r., nr 212, poz. 1766.

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, tekst. jedn. Dz.U. z 2017 r., poz. 2247.

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, Warszawa 2015.

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, tekst jedn. Dz.U. z 2016 r., poz. 904.

Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP, tekst. jedn. Dz.U. z 2022 r., poz. 2065.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tekst jedn. Dz.U. z 2023 r., poz. 913 .

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.U. L 151 z 7.06.2019.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Ministerstwo Cyfryzacji, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [dostęp: 16.02.2024].

Opracowania

CERT Polska, https://cert.pl [dostęp: 9.02.2024].

Chmielewski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016, t. 3, nr 2(10), s. 103–128.

Cyberbezpieczeństwo, red. C. Banasiński, M. Rojszczak, Wolters Kluwer, Warszawa 2020.

Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y?, Portal GOV.pl, https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y [dostęp: 16.02.2024].

Kuc B., Ścibiorek Z., Zarys metodologii nauk o bezpieczeństwie, Wydawnictwo Adam Marszałek, Toruń 2018.

Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydawnictwo Naukowe PWN, Warszawa 2017.

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 r.*, Warszawa 2011, https://csirt.gov.pl/download/3/121/Analizaroczna2010.pdf [dostęp: 11.03.2024].

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 r.*, Warszawa 2012, https://csirt.gov.pl/download/3/137/Raportroczny2011.pdf [dostęp: 11.03.2024].

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 r.*, Warszawa 2013, https://csirt.gov.pl/download/3/158/RaportostaniebezpieczenstwacyberprzestrzeniRPw2012roku.pdf [dostęp: 11.03.2024].

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 r.*, Warszawa 2014, https://csirt.gov.pl/download/3/165/RaportostaniebezpieczenstwacyberprzestrzeniRPw2013roku.pdf [dostęp: 11.03.2024].

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, Warszawa 2015, https://csirt.gov.pl/download/3/172/RaportostaniebezpieczenstwacyberprzestrzeniRPw2014roku.pdf [dostęp: 11.03.2024].

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r.*, Warszawa 2016, https://csirt.gov.pl/download/3/183/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2015roku.pdf [dostęp: 11.03.2024].

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 r.*, Warszawa 2017, https://www.csirt.gov.pl/download/3/185/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2016roku.pdf [dostęp: 11.03.2024].

Stallings W., Brown L., *Bezpieczeństwo systemów informatycznych. Zasady i praktyka*, t. 1–2, tłum. Z. Płoski, R. Meryk, Helion, Gliwice 2019.

Tanner N.H., *Blue Team i cyberbezpieczeństwo*, tłum. A. Łapuć, Helion, Warszawa 2021.
Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Wolters Kluwer, red. G. Szpor, A. Gryszczyńska, K. Czaplicki, Warszawa 2019.

Analiza zagrożeń polskiej infrastruktury cybernetycznej w latach 2010–2024. Część I: Lata 2010–2016

Streszczenie

Zagrożenia wynikające z ciągłej zmienności w przestrzeni geopolitycznej, militarnej czy społecznej warunkują konieczność dostosowywania się infrastruktury cybernetycznej do współczesnych realiów. Zagrożenia cybernetyczne ewoluowały w ostatnich latach, rosła ich intensywność i były ukierunkowane na wiele płaszczyzn funkcjonowania państwa. Artykuł opisuje eskalację zasadniczych zagrożeń infrastruktury cybernetycznej w Polsce na przestrzeni 2010–2016 r., ponadto dokonuje analizy incydentów cybernetycznych oraz poziomu bezpieczeństwa witryn internetowych administracji publicznej. Warta podkreślenia jest tendencja wzrostowa liczby oficjalnych zgłoszeń i incydentów cybernetycznych potwierdzonych przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, a także alarmów cybernetycznych wygenerowanych przez system wczesnego ostrzegania o zagrożeniach w sieci internetowej ARAKIS.GOV. Powagę sytuacji wzmacnia fakt, iż ponad połowa wszystkich występujących zagrożeń cybernetycznych w polskiej przestrzeni internetowej w latach 2010–2016 miała status „wysokiego poziomu zagrożenia", co stanowiło zasadnicze wyzwanie dla funkcjonowania państwa.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, incydent cybernetyczny, infrastruktura cybernetyczna, system bezpieczeństwa państwa, zagrożenie cybernetyczne

Analysis of threats to Polish cyber infrastructure in 2010–2024: part I (2010–2016)

Abstract

Threats resulting from constant variability in the geopolitical, military or social space determine the need to adapt the cyber infrastructure to contemporary realities. Cyber threats have evolved over the years, intensifying and directing their activities at many levels of the state's functioning. This article describes the escalation of the main threats to cyber infrastructure in Poland over the period from 2010 to 2016, and also analyzes cyber incidents and the level of security of public administration websites. It is worth emphasizing the increasing tendency in the number of official reports and confirmed cybernetic incidents by the CERT.GOV.PL incident response team, as well as cybernetic alarms generated by the early threat warning system on the internet network ARAKIS.GOV. The seriousness of cyber threats is reinforced by the fact that more than half of all cyber threats occurring in the Polish Internet space over the period from 2010 to 2016 were classified as "high threat", which constituted a fundamental challenge to the functioning of the state.

Keywords: cybersecurity, cyberspace, cyber incident, cyber infrastructure, state security system, cyber threat