Helena Giebień

Cyberbezpieczeństwo w Federacji Rosyjskiej. Zarys problemu

Uwagi wstępne

Rozwój globalnej informacyjnej sieci, jaką jest Internet, oprócz pozytywnych aspektów bycia jej użytkownikiem niesie ze sobą także zagrożenia. Od lat 90. XX w. wraz z pojawieniem się systemu World Wide Web, nastąpił gwałtowny rozwój sieci. Według danych „Digital Report" z początku 2018 r. ponad 4 mld osób posiada dostęp do Internetu, czyli ok. 53% światowej populacji[1]. Użytkownicy sieci, oprócz korzystania z poczty elektronicznej i ze światowego zasobu informacji zawartych na stronach internetowych, posiadają możliwości nawiązania relacji poprzez upowszechnienie sieci społecznościowych, korzystają z bazy naukowych publikacji i in. Ponadto czerpią korzyści z możliwości biznesowych, takich jak realizacja przelewów bankowych, zawarcie transakcji handlowych, zakupy, etc. Otwarta sieć internetowa przyciągnęła także osoby, grupy cyberprzestępców, których celem stał się zarówno jej zwykły użytkownik, jak i całe instytucje, państwa, przedsiębiorstwa.

Dynamiczny rozwój Internetu oraz coraz szersze wykorzystanie go w różnych sferach działalności ludzkiej nie tylko zmieniło charakter przestępstw dokonywanych drogą elektroniczną, lecz poskutkowało powstaniem nowych form i możliwości ich dokonania. Warto przy tym podkreślić, że zauważalna jest zależność między rozwojem sieci informacyjnej w danym obszarze działalności ludzkiej a rodzajem aktualnego zagrożenia. Na przykład w latach 60. XX w. sieci komputerowe przeważnie były wykorzystywane w instytucjach wojskowych i naukowych, za główne zagrożenie uważano wówczas utratę informacji tajnej oraz nieupoważniony do niej dostęp. W latach 70. XX w. niepokojono się wzrostem przestępczości gospodarczej w obszarze komputerowych technologii mającej swój wyraz w łamaniu systemów komputerowych banków oraz gospodarczej działalności szpiegowskiej. Z kolei lata 80. XX w. przyniosły inny rodzaj przestępczości –

[1] S. Kemp, *Digital in 2018: World's Internet users pass the 4billion mark* [30 I 2018], https://wearesocial.com/blog/2018/01/global-digital-report-2018 (20 IV 2018).

łamanie zabezpieczeń komputerowych oraz nielegalne rozpowszechnianie programów komputerowych[2].

Pojawienie się globalnej sieci Internet i dynamiczny jej rozwój poczynając od lat 90. XX w., o czym wspomniano wyżej, przyczyniło się do powstania szerokiego spektrum problemów związanych z cyberprzestępstwami. W latach 2005-2008 powstały nowe zagrożenia dla użytkowników sieci, takie jak rozpowszechnianie programów służących do wykonywania określonych czynności przez maszynę na polecenie człowieka, tzw. „botów", które w rękach cyberprzestępców potrafią siać spustoszenie w komputerach. Poza tym integracja sieci telekomunikacyjnych oraz ich konwergencja, stworzenie możliwości dostępu do Internetu za pośrednictwem telefonów komórkowych (smartfonów) i ciągłe udoskonalanie urządzeń łączących z Internetem, w tym także wykorzystanie komunikatorów (np. GG, Whatsapp, Viber) stwarza pole do nadużyć tych technologii. Większość cyberprzestępstw w Internecie charakteryzuje przede wszystkim wysoki poziom ukrycia popełnionego przestępstwa, który zapewnia właśnie specyfika sieci informacyjnej, np. takie jak złożone mechanizmy uzyskania anonimowości. Kolejna kwestia, to transgraniczny charakter cyberprzestępstw, dzięki którym przestępca oraz ofiara mogą znajdować się w różnych państwach oraz kontynentach. Cyberprzestępcy są odpowiednio przygotowani, posiadają wiedzę i doświadczenie, ich działalność wskazuje na intelektualne przygotowanie. Przestępczość w sieci także charakteryzuje się złożonością, brakiem stałych standardów, kreatywnością, częstą zmianą sposobów dokonywania cyberprzestępstw oraz stosowanych do tego specjalnych metod. Mają także możliwość dokonania przestępstw w kilku miejscach jednocześnie. Mogą ponadto łączyć względnie słabe zasoby poszczególnych komputerów w potężną broń do dokonania przestępstwa. Ofiary przestępstw przeważnie nie wiedzą o tym, że padły ofiarą cyberprzestępcy, dowiadują się po czasie, że np. brakuje środków finansowych na koncie. Przestępcy zdalnie, bez kontaktu fizycznego z ofiarą, realizują swoje cele. Warto podkreślić, iż nie da się tradycyjnymi sposobami zwalczyć cyberprzestępczości lub jej zapobiec. Niezbędna jest odpowiednio wykształcona i przygotowana kadra w tym zakresie i oczywiście nic nie zastąpi ostrożności i uważności użytkowników sieci.

Cyberprzestępcy łamią prawo m.in. dokonując kradzieży danych osobowych, naruszają prawa własności intelektualnej, uderzają w sferę finansową kradnąc środki z kont użytkowników. Raport Norton Cyber Security Insights z 2017 r. informuje, że w 20 państwach biorących udział w badaniu hakerzy okradli 978 mln osób, powodując straty na 146,3 mld EUR. W siedmiu krajach Europy Zachod-

[2] Zob. więcej: С.В. Бондаренко, *Виртуальные сетевые сообщества девиантного поведения* [28 VIII 2017], http://cyberpsy.ru/articles/bondarenko-internet-deviantnost/ (13 IV 2018).

niej (Francji, Niemczech, Włoszech, Holandii, Hiszpanii, Szwecji i Wielkiej Brytanii) cyberprzestępcy okradli 98,2 mln ludzi na kwotę 23,3 mld EUR[3].

Mamy także do czynienia z cyberterrorystami[4], którzy wykorzystują sieci komputerowe „jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe, itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań"[5]. Według polskiego MSZ najczęściej celem ataków cyberterrorystów padają rządowe strony internetowe, infrastruktura bankowa oraz infrastruktura krytyczna[6]. Rok 2007 jest przez badaczy tematu postrzegany jako punkt przełomowy – zakrojony na szeroką skalę początek cyberwojen[7]. Do najbardziej niecodziennych ataków cybernetycznych można zaliczyć: atak na Estonię w maju 2007 r., na Litwę na przełomie czerwca-lipca 2008 r., na Gruzję w sierpniu 2008 r.[8]. Wspomniany wyżej cyberatak w Estonii

---

[3] *2017 Norton Cyber Security Insights Report. Global Results*, http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-CA.pdf (15 IV 2018).

[4] Za twórcę tego pojęcia uznaje się Barry'ego Collina, pracownika Institute for Security and Intelligence z Kalifornii, który w latach 80. XX w. użył go dla określenia połączenia cyberprzestrzeni i terroryzmu. D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 79. Według B. Collina, cyberterroryzm to świadome wykorzystanie systemu informacyjnego, sieci komputerowej lub jej części składowych w celu wsparcia lub ułatwienia terrorystycznej akcji. K.C. White, *Cyber-Terrorism: Modem Mayhem,* Carlisle 1998, s. 3, http://www.dtic.mil/dtic/tr/fulltext/u2/a345705.pdf (12 III 2018). Zob. więcej na temat rozważań na temat pojęcia „cyberterroryzm": T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, nr 1, s. 173-187.

[5] J.A. Lewis, *Assessing the risk of cyber terrorism, cyber war and other cyber threats* [2002], https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (27 III 2018).

[6] Infrakstruktura krytyczna (IK) to rzeczywiste i cybernetyczne systemy (obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa. Należą do niej następujące systemy: zaopatrzenia w energię, surowce energetyczne i paliwa; łączności; sieci teleinformatycznych; finansowe; zaopatrzenia w żywność; zaopatrzenia w wodę; ochrony zdrowia; transportowe; ratownicze; zapewniające ciągłość działania administracji publicznej; produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. Zob. więcej: *Narodowy Program Ochrony Infrastruktury Krytycznej* [2015], https://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-20151.pdf (25 III 2018).

[7] А. Масалков, *Особенности киберпреступлений в России: инструменты нападения и защита информации*, Москва 2018, s. 11.

[8] Eksperci twierdzą, że za cyberatakiami stoją rosyjscy hakerzy, których wspiera moskiewski rząd lub też którzy pracują dla rządu. Zob.: *Rosyjscy hakerzy – największa broń Kremla* [7 V 2015], http://www.newsweek.pl/swiat/cyberwojna-rosja-hakerzy-usa,artykuly,362722,1.html (20 III 2018); Д. Мельников, *Русские хакеры: что ломают, за сколько и почему они лучшие в мире* [16 IV 2016], https://life.ru/t/технологии/401683/russkiie_khakiery_chto_lomaiut_za_skolko_i_pochiemu_oni_luchshiie_v_mirie (13 V 2018). Por.: *Cyberterroryzm*,

na instytucje rządowe, sieci energetyczne, banki przez rosyjskich hakerów, został określony jako pierwsza cyberwojna[9]. Dany incydent jest pierwszym w historii, kiedy za pomocą ataku cybernetycznego obcemu państwu udało się sparaliżować na pewien czas funkcjonowanie ważnych instytucji państwowych i prywatnych[10].

Cyberprzestrzeń[11] jest intensywnie wykorzystywana przez siatkę organizacji terrorystycznych takich jak ISIS, Al-Kaidę. Wykorzystują np. sieci społecznościowe takie jak „VKontakte", „Instagram", „Twitter", „Telegram", „Facebook" i in., mass media, w tym także YouTube w celu zaszczepienia własnej ideologii i wartości oraz zwerbowania potencjalnych wykonawców zamachu terrorystycznego[12].

Cyberprzestępstwo w Rosji

Federacja Rosyjska jak i wiele innych krajów świata spotyka się z problemem zagrożenia w cyberprzestrzeni. Celem niniejszego artykułu jest analiza problemów cyberbezpieczeństwa w Rosji, ukazanie skali cyberprzestępstw oraz ich wpływu

http://www.antyterroryzm.gov.pl/CAT/antyterroryzm/wspolpraca-zagraniczna/cyberterroryzm/566,Cyberterroryzm.html (28 III 2018). Zob.: *Dni, które wstrząsnęły Estonią* [12 V 2018], https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html (28 III 2018); Ł. Michalik, *Pole walki: cyberprzestrzeń. Kiedy haker staje się żołnierzem?,* https://gadzetomania.pl/1471,pole-walki-cyberprzestrzen-kiedy-haker-staje-sie-zolnierzem (28 III 2018). Więcej na temat cyberterroryzmu zob. np.: B. Olszewski, *Militarne zwalczanie cyberterroryzmu,* https://www.researchgate.net/publication/308608021_Militarne_zwalczanie_cyberterroryzmu_The_Use_of_The_Military_Forces_Against_Cyber_Terrorism (15 III 2018); T. Szubrycht, *op.cit.*; H. Tokarski, *Cyberprzestępczość a profilaktyka*, [w:] *Współczesne zagrożenia zdrowa i bezpieczeństwa publicznego,* Z.W. Grajek, M. Knaś, A. Sęk (red.), Suwałki 2016, s. 311-329; K. Bielski, *Cyberrteroryzm – nowe zagrożenie bezpieczeństwa państwa w XXI wieku*, „Acta Politica" 2015, nr 34, s. 93-109.

9 *Dni, które wstrząsnęły Estonią.…*

10 Zob. więcej: *Raport: Cyberwojna jako rzeczywistość XXI wieku*, www.geopolityka.org/analizy/1813-cyberwojna-jako-rzeczywistosc-xxi-wieku (12 II 2015).

11 Cyberprzestrzeń w ujęciu ogólnym rozumiemy jako cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami, mającą charakter wirtualny (nieprzestrzenny w sensie fizycznym, aterytorialny, ageograficzny) całość istniejących w świecie powiązań powstałych i realizowanych bądź przez technologie informatyczne i ich fizyczne manifestacje, bądź też na ich podstawie. A. Bógdał-Brzezińska, M. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 37–39.

12 Doskonale dany temat poruszył w pracy licencjackiej Paweł Wójcik, *Propaganda Państwa Islamskiego: cele, metody, konsekwencje*, Wrocław 2017 (promotor Helena Giebień, recenzent Jarosław Jarząbek). Zob. więcej: E.A. Кошечкина, К вопросу *о* проблемах противодействия кибертерроризму, „Омский Научный Вестник. Серия 'Общество. История. Современность'" 2017, № 4, s. 97-101. M. Kopczewski, *Elementy infrastruktury krytycznej państwa (organizacji) – jako obiekty narażone na ataki cyberterrorystyczne*, http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2011/054.pdf (24 III 2018).

na funkcjonowanie państwa oraz przedstawienie prób rozwiązania danego problemu.

Prezydent Rosyjskiej Federacji Włodzimierz Putin podczas Międzynarodowego Kongresu o Cyberbezpieczństwie w Moskwie 6 VII 2018 r. konstatował, że Rosja zajmuje pierwsze miejsce w Europie pod względem liczby użytkowników globalnej sieci, mówiąc o ich liczbie ponad 90 mln[13]. W związku z rosnącą liczbą internautów wzrasta także liczba cyberataków. Ofiarami ataków w przestrzeni informacyjnej, jak już wspomniano w tekście, padają m.in. firmy, banki, osoby prywatne, organizacje, państwa. Celem przestępców są zarówno dobra materialne, jak i informacje. Np. straty w sektorze gospodarki Federacji Rosyjskiej w 2018 r. mogą osiągnąć ok. 1 tryliona RUB (czyli ponad 1% PKB kraju). W 2017 r. z kolei Sberbank oszacował straty na 600-650 mld RUB[14]. Zauważana jest tendencja wzrostowa strat ekonomicznych.

Według danych przewodniczącego Stowarzyszenia Regionalnych Banków „Rosja" Anatolija Aksakowa w 2012 r. praktycznie 20% przestępstw dokonanych w cyberprzestrzeni na świecie przypadło na Rosję. Według danych rosyjskiego MSW w 2014 r. zarejestrowano ok. 11 tys. cyberprzestępstw. Natomiast w pierwszej połowie 2015 r. liczba cyberprzestępstw wzrosła o 67% w porównaniu z rokiem 2014[15]. Z kolei w 2016 r. odnotowano 66 tys. przestępstw z wykorzystaniem współczesnych technologii informacyjnych, a w pierwszej połowie 2017 r. dane przestępstwa wzrosły o 30%[16]. Dane z 2018 r. wskazują na dalszy wzrost cyberprzestępstw, który wyniósł na początku roku 40 tys.[17].

W Federacji Rosyjskiej odsetek cyberprzestępstw w 2017 roku stanowił 4,4% ogólnej liczby wszystkich zarejestrowanych przestępstw. Najbardziej rozpowszechnionym cyberprzestępstwem jest nielegalny dostęp do informacji komputerowych (art. 272 Kodeksu Karnego FR) oraz tworzenie, wykorzystanie oraz rozpowszechnienie szkodliwych programów komputerowych (art. 273 KK FR). O ile w 2017 r. zarejestrowano 1883 wymienionych wyżej rodzajów cyberprzestępstw, to już w pierwszej połowie 2018 r. było ich 1233. Najwięcej zarejestrowano (w 2017 r.) w Republice Udmurckiej (194), Republice Komi (132), w obwodach omskim (75), władymirskim (66), kirowskim (64), wołgogradzkim (60), w Moskwie (60), Kraju Krasnodarskim (51). Przy czym o 19,6% zmniejszyła się

---

[13] А. Гамов, *Путин: Россия – первая в Европе по числу пользователей глобальной сети* [6 VII 2018], https://www.kp.ru/daily/26852.7/3894001/ (12 VII 2018).

[14] *Сбербанк: Потери РФ от киберпреступности в 2018 г могут достигнуть 1 трлн руб.* [24 V 2018], https://1prime.ru/state_regulation/20180524/828856897.html (15 VI 2018).

[15] А. Михайлова, *Проблемы кибербезопасности в России и пути их решения* [20 I 2014], http://www.garant.ru/article/520694/ (20 II 2018).

[16] К. Минак, *Киберпреступность в России выросла в шесть раз* [29 XI 2017], https://360tv.ru/news/obschestvo/kiberprestupnost-v-rossii-vyrosla-v-shest-raz/ (20 II 2018).

[17] *В МВД сообщили о количестве зарегистрированных киберпреступлений в России* [6 VII 2018], https://ria.ru/society/20180706/1524114695.html (12 VII 2018).

liczba przeprowadzonych dochodzeń (z 903 do 726) w sprawie łamania artykułów 272 oraz 273 KK FR oraz zwiększyła się liczba niewykrytych przestępstw o 30,5% (z 790 do 1031). W sumie wykrywalność cyberprzestępstw stanowiła 41,3%. Cyberprzestępcy łamią także art. 159.3 KK FR wykorzystując nielegalnie elektroniczny sposób dokonania płatności. Liczba danego rodzaju przestępstw w pierwszym półroczu 2018 r. zwiększyła się siedmiokrotnie w porównaniu z 2017 r. Najwięcej przestępstw danego rodzaju zarejestrowano w Kraju Stawropolskim (66), obwodzie murmańskim (52), Republice Tatarstan (37), Moskwie (34), obwodzie saratowskim (31)[18].

Według materiałów analitycznych Sberbanku ok. 40% cyberprzestępstw na terenie Rosji popełniają nastolatkowie w wieku 14-15 lat. Najczęściej wykorzystują oni dla swoich celów różne socjotechniki, dzięki którym w 80% łamią prawo. Specjaliści potwierdzają, iż co drugi atak hakerów jest skierowany na sektor finansowy[19].

Badacze tematu twierdzą, iż oficjalne dane statystyczne na temat cyberprzestępstw w Rosji są co najmniej pięciokrotnie zaniżone. Niektóre firmy nie nagłaśniają sprawy z różnych przyczyn (np. obawa przed utratą klientów, prestiżu). Szacuje się, że do wiadomości publicznej trafia tylko 20% informacji o dokonanych cyberatakach[20].

Rosyjscy eksperci, analizując rodzaje cyberataków wyróżnili wśród nich najbardziej niebezpieczne: atak DDoS – rozproszona odmowa dostępu, jedna z wielu metod wykorzystywanych do blokowania internetowych serwisów lub blokowania łączy internetowych; oszukiwanie w bankowych systemach informatycznych – bezprawne wysyłanie elektronicznych poleceń zapłaty z celem kradzieży środków finansowych; spam – masowe wysyłanie niechcianych wiadomości na skrzynki poczty elektronicznej; sprzedaż szybszego przesyłu internetowego – polega na usłudze instalowania programów na dużą liczbę komputerów oraz usługi polegającej na przekierowaniu internautów na określone strony internetowe[21]; programy partnerskie – nielegalna sprzedaż leków, sprzedaż podróbek towarów, nielegalnego oprogramowania, itd.

Oprócz „rodzimych" cyberprzestępców, którzy działają wewnątrz kraju, Rosja stoi przed wyzwaniem skutecznej ochrony państwa i obywateli przed cyberatakami z zewnątrz. Należy podkreślić, że o ile technologia rozwija się dość szybko, to niestety systemy zabezpieczeń nie nadążają ze skutecznym pełnieniem swojej funkcji. Cyberprzestępczość rośnie w siłę nie z roku na rok, lecz z miesiąca

---

[18] *В России в 2017 году было совершено почти 90,6 тыс. киберпреступлений* [14 VIII 2018], http://www.banki.ru/news/lenta/?id=10614845 (14 VIII 2018).

[19] А. Кузнецов, *„Сбербанк": треть кибепреступников – школьники* [4 VII 2018], https://www.iguides.ru/main/security/sberbank_tret_kiberprestupnikov_shkolniki/ (20 VII 2018).

[20] *Ibidem*.

[21] Szczególnie dotyczy to wewnątrzrosyjskiego rynku cyberprzestępczości.

na miesiąc. Zagrożenie na poziomie międzynarodowym coraz bardziej stanowią propaństwowi hakerzy (wspierani przez rządy swoich państw)[22], którzy nie tylko zajmują się szpiegostwem na rzecz swojego kraju, lecz również kradną pieniądze oraz urządzają cyberdywersje.

W 2017 r. do największych cyberataków ze strony propaństwowych hakerów, pod względem zasięgu oraz wyrządzonych szkód, należą ataki z wykorzystaniem wirusów szyfrujących[23]. Zobrazować dany problem można na przykładzie wirusa szyfrującego WannaCry, który zaatakował 200 tys. komputerów w 150 państwach. Wirus znalazł się w sieci uniwersytetów w Chinach, w fabryce Renault we Francji oraz Nissana w Japonii, zaatakował firmę telekomunikacyjną Telefonica w Hiszpanii oraz operatora kolei Deutsche Bahn w Niemczech. Szkody oszacowano na 1 mld USD. Prawdopodobnie ataku dokonała północnokoreańska grupa Lazarus, choć także nie wykluczają udziału w nim rosyjskich hakerów[24].

Kolejny incydent z wirusem szyfrującym miał miejsce 27 VI 2017 r. Wówczas na Ukrainie zarejestrowano przeprowadzony na dużą skalę cyberatak za pomocą CTB Lockera „Not Petya"[25]. Poszkodowane zostały także firmy w Rosji (Rostneft, Baszneft, Home Credit Bank, Evraz i in.), USA (np. biofarmaceutyczny koncern Merck), Indiach, Australii oraz innych państwach, powodując spustoszenie w ponad 80 firmach na świecie (np. wirus spowodował duże straty w dużej logistycznej firmie w Danii Moller-Maersk – od 200 do 300 mln USD). Prawdopodobnie cyberatak został przeprowadzony przez grupę Black Energy[26].

Dnia 24 X 2017 r. na Ukrainie i Rosji ponownie doszło do cyberataku za pomocą wirusa szyfrującego pod nazwą „BadRabbit" przez wspomnianą wyżej grupę Black Energy. Wskutek ataku zostały zablokowane komputery i serwery kijowskiego metra, Ministerstwa Infrastruktury, międzynarodowego lotniska „Odessa". W Rosji zaatakowano redakcje federalnych mass mediów, próbowano złamać zabezpieczenia infrastruktury banków[27].

Cyberprzestępcy chętnie atakują infrastruktury bankowe, o czym możemy się przekonać analizując raporty banków oraz firm zajmujących się bezpieczeństwem

---

[22] W tekście zostało wspomniane o rosyjskich prorządowych hakerach, którzy zaatakowali krytyczną infastrukturę informacyjną Estonii, Litwy, Ukrainy, Gruzji.

[23] Zob.: *Szyfruje dyski i żąda okupu. Jak działa wirus Petya?* [27 VI 2017], https://www.tvp.info/32991912/szyfruje-dyski-i-zada-okupu-jak-dziala-wirus-petya (21 III 2018).

[24] *И.* Сачков, *Эхо кибервойны* [15 V 2017], https://www.group-ib.ru/blog/wannacryptor (21 III 2018).

[25] Zob. więcej: *Petya покоряет Украину* [27 VI 2017], https://www.group-ib.ru/blog/petya (21 III 2018). Na Ukrainie doszło do ataków m.in. na Dneprowski System Elektroenergetyczny, Mondelez International, Oszczadbank, Mars, „Nowa Poczta", Nivea, TESA, Metro Kijowskie, na komputery Gabinetu Ministrów oraz rządu Ukrainy, sklepy „Auchan", lotnisko Borispil.

[26] *Ibidem*.

[27] Zob. więcej: *BadRabbit прыгнул* [24 X 2017], https://www.group-ib.ru/blog/badrabbit (21 III 2018).

informatycznym (np. firma Symantec Corp.). Rosyjskie banki szczególnie intensywnie zaatakowano jesienią 2017 r. Niemniej jednak specjaliści z Group-IB[28] w corocznym raporcie pod koniec października odnotowali pozytywną zmianę – celowe ataki na rosyjskie banki zmniejszyły się o 33%. Tłumaczyli ten fakt tym, iż cyberprzestępcy swoją uwagę zaczęli także kierować na banki w innych państwach i regionach, takich jak USA, Europa, Ameryka Łacińska, Azja oraz Bliski Wschód. Dane pod koniec 2017 r. jednak nie były już tak optymistyczne – zarejestrowano cały szereg cyberataków na rosyjskie banki z kodami SWIFT (międzynarodowy system przekazywania informacji finansowej) przez przestępczą grupę Cobalt[29].

W połowie grudnia 2017 r. zarejestrowano udane ataki na banki w Rosji, które korzystają z kodów SWIFT, prawdopodobnie dokonane przez wspomnianą wyżej grupę Cobalt. Dana cyberprzestępcza grupa próbowała ukraść 1 mln USD, jednak nie udało jej się zrealizować w pełni zamierzeń – ukradli tylko 10% zamierzonej kwoty. Oddział Rosyjskiego Banku Centralnego zajmujący się bezpieczeństwem informacyjnym FinCert postrzega grupę Cobalt jako największe zagrożenie dla instytucji kredytujących. Według firmy Group-IB, Cobalt przeprowadziła ok. 50 skutecznych ataków na banki na całym świecie: w Rosji, Hiszpanii, Rumunii, Wielkiej Brytanii, Holandii, Białorusi, Polsce, Estonii, Bułgarii, Gruzji, Mołdawii, Kirgizji, Armenii, Tajlandii oraz Malezji. Nadal są rejestrowane ich próby zainfekowania komputerów przy pomocy zawartych w mailingu wirusów[30].

Pod koniec 2017 r. firma Group-IB w swoim raporcie opisała także grupę „niewidzialnych" hakerów MoneyTaker, która w ciągu półtora roku zaatakowała 20 banków i firm w USA, Rosji i Wielkiej Brytanii. Przez dłuższy czas pozostawali oni niewidzialni. Wykorzystywali w swoich działaniach ogólnodostępne środki, celowo ukrywali elementy rozpoznawcze oraz zawsze zacierali ślady po dokonanych cyberatakach. Najważniejszym celem grupy MoneyTaker są usługi przetwarzania płatności oraz systemy międzybankowych przelewów. W Rosji udało im się zawładnąć kwotą 72 mln RUB, dla porównania w USA podczas jednego ataku udało im się ukraść 500 tys. USD. Interesującym jest fakt, iż ich ofiarą w Rosji padają nieduże regionalne banki. Do jednego z rosyjskich banków udało im się włamać z domowego komputera administratora IT. Wykradali nie tylko pieniądze

[28] Group-IB jest jedną z wiodących międzynarodowych firm zajmujących się zapobieganiem oraz śledztwem cyberprzestępstw i oszustw z wykorzystaniem high-tech. Jest także pierwszym rosyjskim dostawcą rozwiązań *threat intelligence*, który znalazł się w sprawozdaniach niezależnego amerykańskiego przedsiębiorstwa analityczno-badawczego, specjalizującego się w zagadnieniach strategicznego wykorzystania technologii oraz zarządzania technologiami Gartner, analitycznej firmy International Data Corporation oraz firmy Forrester (jedna z najbardziej wpływowych firm badawczych i doradczych na świecie).

[29] Group-IB, *Итоги 2017* [27 XII 2017], https://www.group-ib.ru/blog/report2017 (21 III 2018).

[30] *Ibidem*.

z banków, ale także dokumenty wewnętrzne, instrukcje, rozporządzenia, dane związane z transakcjami[31].

Przytoczone wyżej przykłady zarówno wewnątrzkrajowych, jak i międzynarodowych cyberataków w Rosji tylko w niewielkim stopniu obrazują skalę poruszanego zagadnienia. Niemniej jednak dają możliwość wglądu w rodzaj, strategie oraz motywacje cyberprzestępców. Wskazują na potrzebę globalnej walki z danym problemem, która nie będzie w pełni efektywna bez międzynarodowej współpracy ekspertów oraz odpowiednich służb. Najbardziej groźnym rodzajem cyberataków jest cyberterroryzm, który może doprowadzić do tragicznej w skutkach destabilizacji w poszczególnych państwach (np. w sferze gospodarczej, militarnej). Opracowując strategie bezpieczeństwa nie da się pominąć zagadnień związanych z zapewnieniem cyberbezpieczeńtwa. Rozwój technologii, który bazuje na programach zdalnie sterowanych za pomocą komputerów, coraz szerzej i głębiej obejmuje wszystkie gałęzie ludzkiej egzystencji. Powstaje zatem potrzeba zapewnienia skutecznej ochrony systemów wojskowych, przedsiębiorstw, krytycznej infrastruktury, nad którą intensywnie pracują i którą wdrażają państwa na całym świecie.

Kwestie cyberbezpieczeństwa w Rosji

W celu zabezpieczenia jednostek, organizacji oraz państwa przed zagrożeniami płynącymi z cyberprzestrzeni zarówno wewnątrz kraju jak i zewnątrz, władze FR opracowały doktrynę cyberbezpieczeństwa państwa. Poza tym jednym z kroków na drodze rozwiązania problemów bezpieczeństwa w sieci podjętych przez FR są reformy ustawodawstwa w tym zakresie oraz nawiązanie współpracy z innymi państwami.

Współcześnie cyberbezpieczeństwo wiąże się z problemem terroryzmu, o czym w tekście zostało już wspomniane. Środkami ochrony oraz ataków w cyberprzestrzeni są zainteresowane różne nielegalne struktury oraz grupy. W związku z tym kwestia cyberbezpieczeństwa jest rozpatrywana na najwyższym szczeblu władzy, stanowi jeden z głównych tematów w trakcie spotkań głów państw oraz ministrów odpowiednich resortów poszczególnych państw. Rosja w 2015 r. podpisała umowę o cyberbezpieczeństwie z Chinami, planuje także podpisać podobną umowę z USA[32]. W tym samym roku umowy zawarły Chiny i USA, Chiny i Wielka Brytania. Państwa w ramach zawartych umów zobowiązują się nie tylko współpracować, lecz także nie dopuszczać do wzajemnych cyberataków. Rada Bezpieczeństwa

[31] Zob. więcej: *MoneyTaker: охота на невидимку* [11 XII 2017], https://www.group-ib.ru/blog/moneytaker (22 III 2018).

[32] *Россия готова подписать договор о кибербезопасности с США, заявил Путин* [10 III 2018], https://ria.ru/world/20180310/1516074759.html (20 IV 2018).

Rosji zleciła podległym organom do 1 VII 2018 r. opracować scenariusze przeprowadzenia dwustronnych konsultacji z Niemcami, Francją, Izraelem, Koreą Południową oraz Japonią. Kremlowskie władze planują podpisać z powyższymi państwami umowy o współpracy w dziedzinie cyberbezpieczeństwa[33].

Oprócz wyżej wymienionej umowy podpisanej z Chinami, Rosja zawarła także porozumienia w danej dziedzinie z Indiami, Republiką Południowej Afryki, Białorusią i Kubą. Państwa-strony umowy zobowiązały się wspólnie reagować na zagrożenia cybernetyczne, wymieniać się informacją oraz współpracować z organami ścigania i innymi kompetentnymi instytucjami, pracować nad ujednoliceniem prawodawstwa. Rosja ponadto zobowiązała się wraz z innymi państwami do przygotowania specjalistów, do wspierania badań naukowych oraz inicjatyw partnerskich w organizacjach międzynarodowych.

W owocnym zacieśnieniu współpracy Rosji z państwami Europy Zachodniej i USA przeszkadzają skandale związane z aktywnością rosyjskich hakerów, którzy byli m.in. oskarżani o ingerencję w wybory prezydenckie w USA. Niemcy i Francja także oskarżają Rosję o ingerencję w ich wewnętrzne procesy polityczne[34].

Rosja liczy na to, że umowy bilateralne oraz umowy zawarte w ramach BRICS i Szanghajskiej Organizacji Współpracy będą sprzyjać, w perspektywie kilku lat, przyjęciu ogólnych zasad odpowiedzialnego zachowywania się państw w cyberprzestrzeni w ramach ONZ[35].

Dyrektor Departamentu ds. nowych wyzwań i zagrożeń rosyjskiego MSZ Ilja Rogaczew podał do publicznej wiadomości, że Rosja planuje jesienią 2018 r. zaproponować Zgromadzeniu Ogólnemu ONZ przyjęcie własnego opracowanego projektu karnoprawnej konwencji o cyberbezpieczeństwie. Według I. Rogaczewa celem danej rezolucji jest wywołanie dyskusji o istocie problemów, które są opisane w projekcie konwencji i dotyczą efektywnego zwalczania cyberprzestępstw w dziedzinie informacyjno-komputerowych technologii. Nadmienił także, że inne państwa Rosję krytykują za wspieranie hakerów, cyberprzestępców, lecz nie zgłaszają żadnych realnych propozycji oprócz Rosji, która zgłosiła własny projekt – owoc półtorarocznej pracy ekspertów[36]. Zaproponowana przez Rosję rezolucja ma być alternatywą dla Konwencji Budapesztańskiej Rady Europy o Cyberprzestępczości z 2001 r. Rosyjska strona nie akceptuje art. 32, ust. B o ponadgranicznym dostępie do przechowywanych danych, zarzucając, iż jest to łamanie praw

---

[33] *Россия пригласит пять государств к партнерству по кибербезопасности* [30 XI 2017], https://pravo.ru/news/view/146263/ (14 IV 2018).

[34] Zob. np.: С. Гурьянов, *Русских хакеров обвинили во взломе минобороны Германии* [28 II 2018], https://vz.ru/news/2018/2/28/910461.html (14 IV 2018).

[35] Zob. więcej: А.В. Бедрицкий, *Международные договоренности по киберпространству: возможен ли консенсус?*, s. 119-136, https://riss.ru/images/pdf/journal/2012/4/10.pdf (14 IV 2018).

[36] *РФ предложит на Генассамблее ООН уголовно-правовую конвенцию по кибербезопасности* [3 VII 2018], http://tass.ru/politika/5342231 (14 IV 2018).

autorskich, własności prywatnej, ingerencja w sprawy wewnętrzne obcego państwa. Nie wyraża zgody na to, by zagraniczne służby specjalne mogły ingerować w sieć komputerową FR bez oficjalnego zawiadomienia, albowiem może to zagrażać bezpieczeństwu i suwerenności państwa. W rosyjskim projekcie konwencji jest także zawarty zapis o wymianie danych, lecz ma się on odbywać „na innej, ściśle prawnej podstawie", co ma być uzgodnione w toku dyskusji nad konwencją. Według I. Rogaczewa projekt uwzględnia równoprawną interakcję działających mechanizmów lub tworzenia nowych, na bazie współpracy w dziedzinie karnoprawnej między różnymi państwami. Nie odpowiada też Moskwie proponowany wybór – albo Konwencja Budapesztańska albo nic[37].

Federacja Rosyjska na arenie międzynarodowej w kwestiach cyberbezpieczeństwa jest dość aktywna: dąży do wzmocnienia współpracy w ramach umów bilateralnych, w ramach działania wyspecjalizowanych jednostek organizacji międzynarodowych w zakresie cyberbezpieczeństwa, zgłasza propozycje ustawodawcze i in. Natomiast na przeszkodzie intensyfikacji współdziałania w danym obszarze z innymi państwami stoją zarzuty innych państw o wspieranie przez Kreml rodzimych cyberterrorystów i hakerów, czemu strona rosyjska zaprzecza. Warto zwrócić także uwagę na brak ujednoliconego ustawodawstwa w badanej kwestii i uniwersalnej definicji cyberbezpieczństwa, co także utrudnia, z perspektywy Rosji, owocną współpracę w zwalczaniu cyberataków. Mimo wyżej wymienionych trudności Moskwa jest nastawiona na dalszą owocną współpracę z państwami i międzynarodowymi organizacjami, takimi jak np. BRICS, ONZ, G20, WTO.

Kwestie bezpieczeństwa Rosja reguluje uzupełnianiem i nowelizacją krajowej bazy ustawodawczej, powołaniem odpowiednich organów i instytucji[38].

---

[37] *Ibidem*.

[38] Istotne z punktu widzenia cyberbezpieczństwa Rosji są następujące wybrane akty prawne: *Федеральный закон от 26 VII 2017 г. № 187-ФЗ „О безопасности критической информационной инфраструктуры Российской Федерации"*; *Приказ ФСТЭК России от 6 XII 2017 г. № 227 „Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации"*; *Постановление Правительства РФ от 8 II 2018 г. № 127 „Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений"*; *Постановление Правительства РФ от 17 II 2018 г. № 162 „Об утверждении Правил осуществления государственного контроля* в *области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"*; *Приказ ФСТЭК России от 21 XII 2017 г. № 235 „Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"*; *Федеральный закон „О безопасности" 2010 г.*; *„Стратегия обеспечения национальной безопасности Российской Федерации до 2020 года" – Указ Президента РФ № 537 от 12 IX 2009 (в ред. от 1 VII 2014)*; *„Уголовный кодекс Российской Федерации" от 13 VI 1996 N 63-ФЗ (ред. от 29 VII 2018)*.

Nie stanowią wyjątku problemy cyberbezpieczeństwa – w tym aspekcie stara się sprostać wymogom zmieniającej się rzeczywistości i wykorzystując narzędzia prawne skutecznie odpowiedzieć na nowo powstające formy cyberprzestępczości.

W 1997 r. wszedł w życie nowy Kodeks Karny FR, który w art. 28 uwzględnił „przestępstwa w sferze informacji komputerowej". Rok później przy MSW FR powstało Biuro ds. zwalczania przestępstw w dziedzinie wysokich technologii. Z kolej w 2001 r. Biuro zostało przekształcone w Biuro „K", które działa do dziś i wchodzi w skład Biura specjalnych przedsięwzięć technicznych MSW Rosji[39]. Głównym zadaniem Biura „K" jest prowadzenie czynności operacyjno-rozpoznawczych w celu zwalczania przestępstw związanych z wysokimi technologiami. Specjaliści Biura „K" jako pierwsi w Rosji zajęli się cyberprzestępstwami. W pierwszej kolejności udało im się postawić zarzuty osobom, które nie tylko rozpowszechniały w Internecie materiał pornograficzny z udziałem dzieci, lecz nakłaniali małoletnich do świadczenia usług seksualnych. Zostały ówcześnie udokumentowane pierwsze przestępstwa związane z tworzeniem i wykorzystaniem złośliwych programów oraz z nielegalnym wejściem w posiadanie informacji komputerowych. Współcześnie Biuro „K" dokłada wszelkich starań w celu znalezienia sprawców i wykrycia następujących przestępstw: łamanie zasad eksploatacji środków przechowywania, opracowania lub przekazywania informacji komputerowej oraz sieci informacyjno-telekomunikacyjnych (art. 274 KK FR); nielegalny dostęp do informacji komputerowej (art. 272 KK FR); tworzenie, wykorzystanie, rozpowszechnianie złośliwych programów komputerowych (art. 273 KK FR); oszustwa komputerowe (art. 159.6 KK FR); wykorzystanie małoletnich w celu produkcji nagrań pornograficznych lub przedmiotów (art. 242.2 KK FR); czyny lubieżne (art. 135 KK FR); nielegalny handel specjalnymi technicznymi środkami przeznaczonymi dla tajnego uzyskania informacji (art. 138.1 KK FR); łamanie praw autorskich i pokrewnych (art. 146 KK FR)[40].

Warto podkreślić, iż Biuro „K" ma swoje oddziały we wszystkich regionach Rosji. Taki rodzaj „decentralizacji" sprzyja bardziej efektywnej pracy w wykryciu cyberataków i przeciwdziałaniu cyberprzestępstwom zarówno na poziomie regionalnym, jak i międzynarodowym.

Do sukcesów jednego z oddziałów Biura „K" (konkretnie oddziału 41) można zaliczyć rozpracowanie w ciągu półtora roku zorganizowanej grupy hakerów, którzy dokonali kilku tysięcy włamań na konta elektroniczne. Grupa działała od 2013 r., a jej ofiarą padły elektroniczne systemy płatności, banki oraz podmioty prawne. Grupa atakowała za pomocą dobrze przemyślanego, celowego *fishingu* (z wykorzystaniem socjotechnik) z różnych państw (grupa przestępcza w tym

---

[39] Zob.: *Управление „К" МВД России*, https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (13 V 2018).

[40] А. Масалков, *op.cit.*, s. 169-171.

celu wyjeżdżała za granicę) oraz korzystała ze specjalnego oprogramowania oraz technologii ukrycia swojego miejsca pobytu. Na początku 2017 r. pracownikom Biura „K" udało się zidentyfikować wszystkich członków przestępczej grupy. Łączna wartość szkód w wyniku przestępczej działalności wyniosła ponad 500 mln RUB[41].

W rosyjskim Kodeksie Karnym odpowiedzialność za przestępstwa w sferze informacji komputerowej jest przewidziana w rozdziale 28 KK FR, ze szczególnym uwzględnieniem następujących artykułów: 272 – nielegalny dostęp do informacji komputerowej; 273 – tworzenie, wykorzystanie, rozpowszechnianie złośliwych programów komputerowych; 274 – łamanie zasad eksploatacji środków przechowywania, opracowania lub przekazywania informacji komputerowej oraz sieci informacyjno-telekomunikacyjnych. Niektórzy eksperci uważają, iż istniejące ustawodawstwo o odpowiedzialności za przestępstwa w sferze informacji komputerowych uwzględnia tylko przestępstwa komputerowe, czyli przestępstwa, które są popełniane przy zastosowaniu komputerów i informacji komputerowej (cyberbezpieczeństwa) a nie uwzględnia innych przestępstw dokonywanych z ich wykorzystaniem. Podkreślają przy tym, że na poziomie porozumień państw obszaru WNP, dokumenty dotyczące cyberprzestępstw są bardziej dopracowane, niż KK FR[42].

Istotnym z punktu widzenia cyberbezpieczeństwa w Rosji jest ustawa o bezpieczeństwie krytycznej infrastruktury informatycznej (KII)[43], która weszła w życie 1 I 2018 r. W celu wyjaśnienia ogólnych zasad zawartych w danej ustawie, poszczególne organy uchwalają odpowiednie akty prawne. Uwzględniono także prowadzenie rejestru ważnych obiektów KII oraz dla podmiotów IKK wyznaczono obowiązki, m.in. kierownik podmiotu IKK ma obowiązek powołać komisję, która przygotuje spis obiektów KII oraz nada tym obiektom odpowiednią kategorię. Z dniem 5 III 2018 r. obowiązują przypisy dotyczące wymogów powołania systemu bezpieczeństwa ważnych obiektów KII.

Podsumowując powyższe rozważania należy stwierdzić, że Federacja Rosyjska dąży do wzmocnienia systemów ochrony przestrzeni wirtualnej zarówno na poziomie ustawodawczym, jak i wykonawczym.

---

41 *Ibidem*, s. 173.

42 Zob. więcej: В.А. Номоконов, Т.Л. Тропина, *Кибепреступность как новая криминальная угроза*, „Криминология вчера, сегодня, завтра" 2012, № 1, https://cyberleninka.ru/article/v/kiberprestupnost-kak-novaya-kriminalnaya-ugroza (18 IV 2018).

43 Федеральный закон от 26 VII 2017 г. N 187-ФЗ „О безопасности критической информационной инфраструктуры Российской Федерации", https://rg.ru/2017/07/31/bezopasnost-dok.html (18 IV 2018).

Uwagi końcowe

Kwestie zapewnienia bezpieczeństwa w sieci, infrastruktury krytycznej, przeciwdziałania cyberterroryzmowi stanowią jeden z najbardziej istotnych i nadrzędnych celów państw świata. Federacja Rosyjska także postawiła sobie za cel zbudowanie efektywnego systemu bezpieczeństwa w tym zakresie. Według danych Ministerstwa Łączności i Komunikacji Masowej FR z końca 2017 r. Rosja zajęła dziesiąte miejsce w rankingu cyberbezpieczeństwa Międzynarodowego Związku Telekomunikacyjnego. Tym samym wyprzedziła wysokorozwinięte pod względem technologicznym państwa jak Japonię i Norwegię, a także Wielką Brytanię (12 miejsce), Południową Koreę (13 miejsce), Finlandię (16 miejsce), Niemcy (24 miejsce) oraz Włochy (31 miejsce)[44].

Pomimo sukcesów w wykrywaniu cyberprzestępców oraz odpieraniu cyberataków poziom zabezpieczenia użytkowników nie jest nadal zadowalający. Nie jest do końca także zadowalająca współpraca międzynarodowa w tym zakresie. Należy wziąć pod uwagę szereg zarzutów kierowanych w stronę Rosji o sprzyjanie działalności propaństwowych grup hakerskich, które efektywnie blokują krytyczną infrastrukturę innych państw. Mimo zawiłości problemu i wzajemnych zarzutów, rosyjskie władze, zdając sobie sprawę z powagi zagrożeń płynących z sieci, są nastawione na ścisłą międzynarodową współpracę w dziedzinie cyberbezpieczeństwa. W tym celu Rosja podpisuje szereg umów bilateralnych oraz stara się aktywnie uczestniczyć w pracach organizacji międzynarodowych.

Władze rosyjskie są świadome stojących przed nimi szeregu wyzwań przed zapewnieniem skutecznej ochrony cyberprzestrzeni. Przede wszytkim kluczowym zadaniem jest podniesienie poziomu przygotowania rosyjskich specjalistów w walce z cyberprzestępczością, tworzenie skutecznej infrastruktury i zabezpieczeń przed cyberatakami oraz rozwój i doskonalenie międzynarodowego systemu wymiany informacji o zagrożeniach w sieci.

[44] Zob. *The Global Cybersecurity Index, GIC* 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (20 IV 2018). W badaniu wzięły udział 193 państwa.

Abstract

Helena Giebień

**Cybersecurity in the Russian Federation.
Outline of the problem**

The article undertakes the issues of cybersecurity in Russia. It shows the scale of cybercrime, their impact on the functioning of the states and attempts to solve the problem. The main thesis of the article states that the Russia Federation seeks to enhance its cyberspace security systems both on the legislative and executive level, trying to protect state's institutions and critical infrastructure as well as cooperating with other states and international organizations.

The articles analyses primary and secondary sources such as legal acts, reports, scientific literature, and Russian press, to present the research problem and draw conclusions.

The research shows that the Russian authorities are aware of the multiple challenges they have to face to ensure the efficient security of the cyberspace. Among the key elements are the raise of the level of competence of Russian specialists fighting cybercrimes, creation of the efficient infrastructure and protection against cyber attacks as well as improving the international system of information exchange on threats in the network. Russia faces also the challenge to strengthen multilateral cooperation with other states, based on mutual trust, especially in the face of a negative image of Russia resulting from the activities of hackers, connected to the state, who can paralyze the critical infrastructure of the other states.

Keywords: cybersecurity, cyber terrorism, cyber attack, cyberwar, Russian Federation

References

2017 Norton Cyber Security Insights Report. Global Results, http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-CA.pdf.

BadRabbit prygnuł, 24 X 2017, https://www.group-ib.ru/blog/badrabbit.

Bielski K., *Cyberrteroryzm – nowe zagrożenie bezpieczeństwa państwa w XXI wieku*, „Acta Politica" 2015, nr 34.

Bierickij A.W., *Mezdunarodnyje dogoworennosti po kiberprostranstwu: wozmozen li konsensus?,* https://riss.ru/images/pdf/journal/2012/4/10_.pdf.

Bondarenko S.W., *Wirtualnyje setewyje soobszczestwa dewiatnogo powedenija,* 28 VIII 2017, http://cyberpsy.ru/articles/bondarenko-internet-deviantnost/.

Bógdał-Brzezińska A., Gawrycki M., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym* świecie, Warszawa 2003.

Cyberterroryzm, http://www.antyterroryzm.gov.pl/CAT/antyterroryzm/wspolpraca-zagraniczna/cyberterroryzm/566,Cyberterroryzm.html.

Cyberwojna jako rzeczywistość XXI wieku, www.geopolityka.org/analizy/1813-cyberwojna-jako-rzeczywistosc-xxi-wieku.

Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.

Dni, które wstrząsnęły Estonią, 12 V 2018, https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html.

Federalnyj zakon ot 26 ijula 2017 g. N 187-FZ „O bezopasnosti kriticzeskoj informacionnoj infrastruktury Rossijskoj Federacii", https://rg.ru/2017/07/31/bezopasnost-dok.html.

Gamow A., *Putin: Rossia – perwaja w Ewrope po czislu polzowatelej globalnoj sieti*, 6 VII 2018, https://www.kp.ru/daily/26852.7/3894001/.

Group-IB, *Itogi 2017*, 27 XII 2017, https://www.group-ib.ru/blog/report2017.

Gurjanow S., *Russkich hakerow obwinili wo wzlomie minoborony Germanii*, 28 II 2018, https://vz.ru/news/2018/2/28/910461.html.

Kemp S., *Digital in 2018: World's Internet users pass the 4billion mark*, 30 I 2018, https://wearesocial.com/blog/2018/01/global-digital-report-2018.

Kopczewski M., *Elementy infrastruktury krytycznej państwa (organizacji) – jako obiekty narażone na ataki cyberterrorystyczne*, http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2011/054.pdf.

Koszeczkina E.A., *K woprosu o problemach protiwodejstwija kiberterrorizmu,* „Omskij Naucznyj Westnik. Seria 'Obszczestwo. Istoria. Sowremennost'" 2017, nr 4.

Kuznecow A., *„Sberbank": tret kiberprestupnikow – szkolniki,* 4 VII 2018, https://www.iguides.ru/main/security/sberbank_tret_kiberprestupnikov_shkolniki/.

Lewis J.A., *Assessing the risk of cyber terrorism, cyber war and other cyber threats*, 2002, Center for Strategic and International Studies, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

Masalkow A., *Osobennosti kiberprestuplenij w Rossii: instrumenty napadenija i zaszczita informacii,* Moskva 2018.

Melnikow D., *Russkije hakery: czto* łomajut*, za skolko i poczemu oni luczszije w mire*, 16 IV 2016, https://life.ru/t/технологии/401683/russkiie_khakiery_chto_lomaiut_za_skolko_i_pochiemu_oni_luchshiie_v_mirie.

Michajlowa A., *Problemy kiberbezopasnosti w Rossii i puti ich reszenija*, 20 I 2014, http://www.garant.ru/article/520694/.

Michalik Ł., *Pole walki: cyberprzestrzeń. Kiedy haker staje się żołnierzem?*, https://gadzetomania.pl/1471,pole-walki-cyberprzestrzen-kiedy-haker-staje-siezolnierzem.

Minak K., *Kiberprestupnost w Rossii wyrosla w szest raz,* 29 XI 2017, https://360tv.ru/news/obschestvo/kiberprestupnost-v-rossii-vyrosla-v-shest-raz/.

MoneyTaker: ochota na newidimku, 11 XII 2017, https://www.group-ib.ru/blog/moneytaker.

Narodowy Program Ochrony Infrastruktury Krytycznej, 2015, https://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-20151.pdf.

Nomokonow W.A., Tropina T.L., *Kibeprestupnost kak nowaja kriminalnaja ugroza*, „Kriminologia wczera, siegodnia, zawtra" 2012, nr 1, https://cyberleninka.ru/article/v/kiberprestupnost-kak-novaya-kriminalnaya-ugroza.

Olszewski B., *Militarne zwalczanie cyberterroryzmu*, https://www.researchgate.net/publication/308608021_Militarne_zwalczanie_cyberterroryzmu_The_Use_of_The_Military_Forces_Against_Cyber_Terrorism.

Petya pokoriajet Ukrainu, 27 VI 2017, https://www.group-ib.ru/blog/petya.

RF predlozit na Genassamblee OON ugolowno-prawowuju konwenciju po kiberbezopasnosti, 3 VII 2018, http://tass.ru/politika/5342231.

Rossia gotowa podpisat' dogowor o kiberbezopasnosti s SSzA, zajawił Putin, 10 III 2018, https://ria.ru/world/20180310/1516074759.html.

Rossia priglasit piat gosudarstw k partnerstwi po kiberbezopasnosti, 30 IX 2017, https://pravo.ru/news/view/146263/.

Rosyjscy hakerzy – największa broń Kremla, 7 V 2015, http://www.newsweek.pl/swiat/cyberwojna-rosja-hakerzy-usa,artykuly,362722,1.html.

Saczkow I., *Echo kiberwojny*, 15 V 2017, https://www.group-ib.ru/blog/wannacryptor.

Sberbank: Poteri RF ot kiberprestupnosti w 2018 g. mogut dostignut 1 trln rub., 24 V 2018, https://1prime.ru/state_regulation/20180524/828856897.html.

Szubrycht T.*, Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, nr 1.

Szyfruje dyski i żąda okupu. Jak działa wirus Petya?, 27 VI 2017, https://www.tvp.info/32991912/szyfruje-dyski-i-zada-okupu-jak-dziala-wirus-petya.

The Global Cybersecurity Index, GIC 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

Tokarski H., *Cyberprzestępczośc a profilaktyka*, [in:] *Współczesne zagrożenia zdrowa i bezpieczeństwa publicznego,* Z.W. Grajek, M. Knaś, A. Sęk (eds.), Suwałki 2016.

Uprawlenije „K" MWD Rossii, https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii.

W MWD soobszczili o koliczestwe zaregestrorowannych kiberprestuplenij w Rossii, 6 VII 2018, https://ria.ru/society/20180706/1524114695.html.
W Rossii w 2017 godu było sowerszeno poczti 90,6 tys. kibeprestuplenij, 14 VIII 2018, http://www.banki.ru/news/lenta/?id=10614845.
White K.C., *Cyber-Terrorism: Modem Mayhem*, Carlisle 1998, http://www.dtic.mil/dtic/tr/fulltext/u2/a345705.pdf.

Helena Giebień – dr politologii, adiunkt w Zakładzie Badań Wschodnich w Instytucie Studiów Międzynarodowych Uniwersytetu Wrocławskiego. ORCID: 0000-0003-3764-2114