

PRZESTĘPCZOŚĆ TELEINFORMATYCZNA 2017

POD REDAKCJĄ
JERZEGO KOSIŃSKIEGO



SZCZYTNO 2018



PRZESTĘPCZOŚĆ TELEINFORMATYCZNA 2017

pod redakcją
Jerzego Kosińskiego

Szczytno 2018

Recenzenci

dr hab. Grzegorz Krasnodębski

dr hab. Arkadiusz Lach



© Wszelkie prawa zastrzeżone — WSPol. Szczytno

ISBN 978-83-7462-638-5

e-ISBN 978-83-7462-639-2

Druk i oprawa:

Dział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie

ul. Marszałka Józefa Piłsudskiego 111, 12-100 Szczytno

tel. 089 621 51 02, faks 089 621 54 48

e-mail: wwip@wspol.edu.pl

Objętość: 25,36 ark. wyd. (1 ark. wyd. = 40 tys. znaków typograficznych)

SPIS TREŚCI

WSTĘP	7
Rozdział 1 — Krzysztof Jan JAKUBSKI	
Analiza działań rządowych w zakresie cyberbezpieczeństwa za okres trwania TAPT.....	13
ANALYSIS OF GOVERNMENT CYBERSECURITY ACTIVITIES FOR THE EXISTENCE OF TAPT	
Rozdział 2 — Maciej SZMIT	
Kiss Smarter — uwagi o celach Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.....	43
KISS SMARTER - COMMENTS ON THE OBJECTIVES OF THE CYBERSECURITY STRATEGY OF THE REPUBLIC OF POLAND FOR 2017-2022	
Rozdział 3 — Krzysztof LIDERMAN	
Dziesięć definicji	57
TEN DEFINITIONS	
Rozdział 4 — Jarosław SORDYL	
Bezpieczeństwo IT pod kontrolą — wyzwania dla zespołu CERT (Computer Emergency RespOnSe Team).....	71
IT SECURITY UNDER CONTROL - CHALLENGES FOR THE COMPUTER EMERGENCY RESPONSE TEAM (CERT)	
Rozdział 5 — Marcin SZYMCZAK	
Ujęcie infrastruktury krytycznej w opisie sabotażu komputerowego określonego w art. 269 Kodeksu karnego	79
AN APPROACH TO THE CRITICAL INFRASTRUCTURE IN DESCRIPTION OF THE COMPUTER SABOTAGE REFERRED IN ART. 269 POLISH PENAL CODE	
Rozdział 6 — Andrzej ADAMSKI	
Kryminalizacja narzędzi hakerskich w europejskim i polskim prawie karnym	87
CRIMINALIZATION OF HACING TOOLS IN EUROPEAN AND POLISH CRIMINAL LAW	
Rozdział 7 — Paweł OPITEK	
Legalny haking w Polsce — krytyczna ocena uregulowań Kodeksu karnego	115
LEGAL HACKING IN POLAND — CRITICAL ASSESSMENT OF THE PENAL CODE REGULATIONS	
Rozdział 8 — Marcin SZYMCZAK, Tomasz GONTARZ, Aleksander LUDYNIA	
Prawna dopuszczalność testów penetracyjnych i wykonywania czynności w ramach programów bug bounty po nowelizacji przepisów kodeksu karnego.....	133
LEGAL RESTRICTIONS OF PENETRATION TESTING AND TAKING ACTION UNDER THE BUG BOUNTY PROGRAMMES AFTER THE AMENDMENT TO THE CRIMINAL CODE	

Rozdział 9 — Adam E. PATKOWSKI	
Big Data w służbie służb — sięganie po owoc zakazany(?)	143
BIG DATA IN SERVICE FOR LEA — REACHING FOR THE FORBIDDEN FRUIT (?)	
Rozdział 10 — Damir DELIJA, Goran OPARNICA	
Digital forensic approach to open source intelligence (OSINT)	161
KRYMINALISTYCZNE PODEJŚCIE DO INTERNETOWEGO BIAŁEGO WYWIADU (OSINT)	
Rozdział 11 — Jacek CHARATYNOWICZ	
Wirtualne waluty. Zagrożenia i wyzwania. Aspekt regulacyjny	169
VIRTUAL CURRENCIES. THREATS AND CHALLENGES. CONTROL ASPECT	
Rozdział 12 — Paweł OPITEK	
Przestępczość z wykorzystaniem kryptowalut oraz ich status w postępowaniu karnym	183
CRYPTOCURRENCIES IN CRIMINAL OFFENSES AND THEIR STATUS IN CRIMINAL PROCEEDINGS	
Rozdział 13 — Jerzy CICHOWICZ	
Rekomendacje VI Forum Bezpieczeństwa Banków	205
VI SECURITY BANKING FORUM RECOMMENDATIONS	
Rozdział 14 — Paweł OLBER	
Problematyka zabezpieczania i analizy zawartości cyfrowych źródeł dowodowych	209
PROBLEMS FOR GATHERING AND ANALYSIS OF DIGITAL EVIDENCE	
Rozdział 15 — Kinga SZĘDZIELARZ	
Perspektywy wykorzystania narzędzi analizy kryminalnej w postępowaniu karnym na etapie postępowania sądowego	231
PERSPECTIVES TO USE CRIMINAL ANALYSIS TOOLS IN CRIMINAL PROCEEDINGS AT THE STAGE OF COURT PROCEEDINGS	
Rozdział 16 — Tadeusz WIECZOREK, Krystian MĄCZKA, Marcin SZYMCZAK	
Zabezpieczenie integralności danych wynikowych pracy skanera 3D jako dokumentacji miejsca zdarzenia	247
PROTECTING THE INTEGRITY OF THE 3D SCANNER WORK RESULT DATA AS A DOCUMENTATION OF THE CRIME SCENE	
Rozdział 17 — Liu DE PENG	
3G wireless network based image transmission system design and implementation	255
PROJEKT I WDROŻENIE SYSTEMU TRANSMISJI OBRAZU W BEZPRZEWODOWEJ SIECI 3G	
Rozdział 18 — Paweł BARANIECKI	
Usługi VoWiFi i VoLTE w aspekcie obowiązków prawem nakazanych: retencji i kontroli treści przekazu	267
VOWIFI AND VOLTE SERVICES IN THE ASPECTS OF RIGHTS OBLIGATIONS: RETENTION AND CONTENT OF THE TRANSFER OF CONTENT	

Rozdział 19 — *Mikołaj WOJTAŁ*

Tryb uzyskania danych osobowych sprawcy czynu niedozwolonego popełnionego w Internecie — środki dostępne poza procedurą karną. Doświadczenia praktyczne.....	275
--	-----

MODE OF OBTAINING PERSONAL DATA OF PERPETRATOR IN THE CASE COMMITTED IN THE INTERNET — THE MEASURES AVAILABLE BEHIND THE PENAL PROCEDURE. PRACTICAL EXPERIENCES

Rozdział 20 — *Grzegorz MATYNIAK*

Kradzież tożsamości.....	283
--------------------------	-----

IDENTITY THEFT

Rozdział 21 — *Wojciech WARCZAK*

Naruszenia praw własności intelektualnej w Internecie	299
---	-----

INFRINGING INTELLECTUAL PROPERTY RIGHTS IN THE INTERNET

Rozdział 22 — *Piotr NIEMCZYK*

Model „biznesu” kradzieży i dystrybucji własności intelektualnej w Internecie	313
---	-----

BUSINESS MODEL OF THE INTELLECTUAL PROPERTY THEFT AND DISTRIBUTION IN THE INTERNET

Rozdział 23 — *Monika GÓRA*

Pomoc w bezprawnym rozpowszechnianiu utworów audiowizualnych — odpowiedzialność prawno-karna	325
--	-----

HELP IN THE UNLAWFUL DISTRIBUTION OF AUDIOVISUAL WORKS — LEGAL RESPONSIBILITY

Rozdział 24 — *Kamil BOJARSKI*

Prawne aspekty modyfikacji kodu oprogramowania w celu unieszkodliwienia systemów DRM.....	341
---	-----

LEGAL ASPECTS OF SOFTWARE MODIFICATION FOR THE DISABLING OF DRM SYSTEMS

Rozdział 25 — *Paulina MUSIAŁOWSKA*

Partnerstwo publiczno-prywatne w zakresie zwalczania przestępstw nielegalnego obrotu sfalszowanymi produktami leczniczymi w Internecie	353
--	-----

PUBLIC-PRIVATE PARTNERSHIP IN COMBATING ILLICIT TRADE IN COUNTERFEIT MEDICINES IN THE INTERNET

Rozdział 26 — *Paulina SAMUEL*

Problematyka przestępczości farmaceutycznej w ujęciu prawno-kryminologicznym	365
--	-----

THE PHENOMENON OF PHARMACEUTICAL CRIME IN LEGAL AND CRIMINOLOGICAL CONTEXT

Rozdział 27 — *Maciej JANKOWSKI*

Skutki powszechnego udostępniania globalnych technologii teleinformatycznych, ze szczególnym uwzględnieniem międzynarodowego i wewnętrznego bezpieczeństwa	379
--	-----

THE IMPACTS OF WIDESPREAD ACCESS TO GLOBAL ICT TECHNOLOGIES WITH SPECIAL CONSIDERATIONS IN INTERNATIONAL AND INTERNAL SECURITY

Rozdział 28 — *Tomasz SIEMIANOWSKI*

Cyberprzemoc wśród małoletnich użytkowników internetu.

Prezentacja wyników badań własnych 393

CYBERBULLYING AMONG THE MINORS INTERNET USERS. PRESENTATION
OF RESULTS OF OWN RESEARCH

WSTĘP

Dwadzieścia lat w technologiach teleinformatycznych brzmi jak wieczność, a w czerwcu 2017 roku, w Wyższej Szkole Policji w Szczytnie miała miejsce dwudziesta edycja międzynarodowej konferencji naukowo-praktycznej pt. „Techniczne Aspekty Przestępczości Teleinformatycznej” (TAPT). Ilość chętnych do uczestniczenia w tym przedsięwzięciu, która przekroczyła 400 osób, świadczy dobitnie, że jego idea nie zestarzała się. Ciągłe istnieje bardzo duże zapotrzebowanie na tego typu forum — na forum wymiany informacji i doświadczeń pomiędzy policjantami, prokuratorami, przedstawicielami innych służb państwowych, biegłymi, prywatnym sektorem teleinformatycznym oraz nauką.

Specyfiką TAPT, ukształtowaną przez lata, jest łączenie wiedzy i doświadczeń sektora prywatnego — począwszy od platformy Allegro, wieloletniego partnera WSPol w organizacji konferencji, poprzez banki do firm z obszaru infrastruktury krytycznej, ale także naukowców z różnych uczelni oraz funkcjonariuszy organów ścigania. Dzielenie się wiedzą i potrzebami, wspólne rozwiązywanie problemów, sprawiają, że dzięki wytworzonej na TAPT synergii, wszyscy widzą światło w tunelu, które prowadzi do bezpiecznej cyberprzestrzeni.

W 2017 roku organizatorami XX Międzynarodowej Konferencji Naukowej byli: Instytut Badań nad Przestępczością Kryminalną i Terroryzmem, działające w nim Centrum Analityczno-Wywiadowcze i Doskonalenia Zwalczania Cyberprzestępczości oraz Grupa Allegro sp. z o.o.. W konferencji uczestniczyło 403 uczestników z Polski, Brazylii, Chorwacji, Niemiec, Rosji, Wielkiej Brytanii i Stanów Zjednoczonych. Pierwszy raz w historii konferencji zdarzyło się, że jej inauguracji dokonywał Komendant-Rektor WSPol — insp. dr Marek Fałdowski w towarzystwie osób z instytucji istotnych w kontekście zwalczania cyberprzestępczości: Podsekretarza Stanu w MSWiA — Pana Tomasza Zdzikota, przedstawiciela Interpolu — Pana Silvino Schlickmann Juniora (Interpol Director Cybercrime), przedstawiciela EC3 Europolu — Pana Marcina Skowronka. Na konferencji obecni także byli przedstawiciele nauki — członkowie Komitetu Programowego TAPT:

prof. Ewa Gruza — z Uniwersytetu Warszawskiego,
prof. Andrzej Adamski — z Uniwersytetu Mikołaja Kopernika,
prof. Paweł Czechowski — z Uniwersytetu Warszawskiego,
płk prof. Piotr Dela — z Akademii Sztuki Wojennej,
kmdr. prof. Grzegorz Krasnodębski — z Akademii Marynarki Wojennej,
prof. Arkadiusz Lach — z Uniwersytetu Mikołaja Kopernika,
dr inż. Krzysztof Liderman — z Wojskowej Akademii Technicznej,
dr inż. Adam E. Patkowski — z Wojskowej Akademii Technicznej,

ale także prof. Jerzy Surma z SGH oraz prof. Tadeusz Wieczorek z Politechniki Śląskiej.

W czasie konferencji ogłoszono 46 referatów, odbyła się debata ekspercka i przeprowadzono 4 warsztaty. W wystąpieniach zostały poruszone tematy związane z i pokrewne do technicznych aspektów przestępczości teleinformatycznej, m.in.: zwalczanie cyberprzestępczości w aspekcie organizacyjnym, obserwowane trendy cyberprzestępczości, współpraca prywatno-publiczna w zwalczaniu cyberprzestępczości, bezpieczeństwo teleinformatyczne, elektronicznych instrumentów płatniczych, kryptowalut i urządzeń mobilnych, bezpieczeństwo danych osobowych, monitorowanie zagrożeń w internecie, w szerokim zakresie ujawnianie, pozyskiwanie, zabezpieczanie, analiza i prezentacja dowodów cyfrowych. Przedstawiona została praktyka zwalczania cyberprzestępczości oraz narzędzia wspomagające zwalczanie cyberprzestępczości (zarówno komercyjne, jak i opracowywane samodzielnie przez funkcjonariuszy). Wszystkie rozważania zwracały uwagę na niezbędność współpracy publiczno-prywatnej w zwalczaniu cyberprzestępczości i konieczność działań wykraczających poza granice państwa.

Wprowadzające w tematykę konferencji wystąpienie wygłosił minister Tomasz Zdzikot, który przypomniał pierwsze cyberprzestępstwa oraz wskazał obserwowane tendencje rozwojowe tej przestępczości. Podkreślił także zaangażowanie MSWiA oraz WSPol w działania mające na celu podniesienie cyberbezpieczeństwa. W pierwszym dniu konferencji ogłoszono następujące referaty:

- Interpol support in cybercrime combating — Silvino Schlickmann Junior, Interpol Director Cybercrime,
- The role of European Cyber Crime Centre (EC3) in combating cybercrime — Marcin Skowronek, Europol,
- Odpowiedź Policji na migrację przestępczości do sieci Internet — Dominik Rozdziałowski, Dyrektor Biura dw. z Cyberprzestępczością KGP,
- FBI — cyberprzestępczość — zagrożenia i analiza przykładów — Justin Kolenbrander, Szef Biura FBI w Polsce,
- Kto i po co atakował polskie banki na przełomie 2016-2017 — Ireneusz Parafjańczuk, Team Cymru,
- Współpraca publiczno-prywatna w zwalczaniu cyberprzestępczości w serwisach ogłoszeniowych — Wojciech Kiszka, Tomasz Wawrzukowicz, OLX Group; Dorota Piernicka, KWP Gdańsk,
- Przegląd bezpieczeństwa — Krzysztof Liderman, WAT,
- Kryminalizacja narzędzi hakerskich w polskim i europejskim prawie karnym na tle nowelizacji Kodeksu karnego z dnia 23 marca 2017 r — Andrzej Adamski, UMK Toruń,
- Uzyskiwanie dowodów w drodze kontroli przekazów informacji po zmianach z lat 2016-2017 — Arkadiusz Lach, UMK Toruń,
- Big Data w służbie służb — sięganie po owoc zakazany — Adam E. Patkowski, WAT.

W pierwszym dniu konferencji miała miejsce debata ekspercka. W debacie aktywny udział wzięli: min. Tomasz Zdzikot, MSWiA; mł. insp. dr. Marek Fałdowski, WSPol; Prof. Andrzej Adamski, UMK; Prof. Paweł Czechowski, UW; Prof. Piotr Dela, ASzWoj; Prof. Grzegorz Krasnodębski, AMW; Prof. Arkadiusz Lach, UMK; Prof. Tadeusz Wieczorek, Pol. Śląska; Prok. Dr inż. Agnieszka Gryszczyńska, PO Warszawa; Karolina Makowska, członek zarządu Stowarzyszenia Sygnał; Robert Kośla, Microsoft; Piotr Balcerzak, ZBP; Dominik Rozdziałowski, Dyrektor Biura dw. z Cyberprzestępczością KGP; Łukasz Jędrzejczak oraz Jarosław Cholewiński, Naczelnicy Wydziałów w Biurze dw. z Cyberprzestępczością KGP. Tematyka debaty obejmowała:

- system zwalczania cyberprzestępczości (czy istnieje w Polsce taki system, jak powinien na poziomie krajowym być utworzony, aby najlepiej współpracował np. z EC3),
- rolę i miejsce służb w zwalczaniu cyberprzestępczości (kto powinien pełnić rolę wiodącą w całym systemie i w obszarze służb),
- współpracę prywatno-publiczną w zwalczaniu cyberprzestępczości (jak powinny układać się relacje organów ścigania i sektora prywatnego we wspólnym obszarze zainteresowań, jaki model przyjęty w innych krajach takiej współpracy jest najlepszy),
- współpracę z sektorem akademickim (jakiego rodzaju wsparcie, oprócz analiz post factum mogą zaproponować policji uczelnie, jak w ten proces może włączyć się WSPol),
- współpracę międzynarodową w zwalczaniu cyberprzestępczości (z kim należy obowiązkowo współpracować w pionie policyjnym i w sektorze prywatnym),
- pracę operacyjną w Internecie, możliwości ofensywnej pracy w Internecie (jakich możliwości brakuje polskiej Policji, „dozwolony haking” w działaniach służb ochrony prawa — czy i w jakim zakresie można wykorzystać),
- problem ustalenia właściwej jednostki lub komórki organizacyjnej Policji, która będzie prowadziła czynności o charakterze procesowym,
- oględziny czy przeszukanie (jak przeprowadzać te czynności w środowisku bardzo wrażliwym na modyfikacje, zdalne przeszukanie, przeszukanie rozszerzone, a także brak wykorzystania przez Policję net flow (dane o połączeniach, obowiązek przekazywania, retencji)),
- standardy zabezpieczenia i analizy dowodów cyfrowych (masowe błędy, studia podyplomowe z zakresu informatyki śledczej).

Wnioski wypływające z debaty będą sukcesywnie wykorzystywane z procesie edukacyjnym i badawczym WSPol.

Również w pierwszym dniu, równoległe do sesji plenarnej przeprowadzone zostały warsztaty przygotowane przez firmę Passus SA z zakresu bezagentowego zabezpieczenia użytkownika aplikacji webowej.

Drugiego dnia, w dwóch ścieżkach równoległych, wygłoszono szereg zróżnicowanych wystąpień. W pierwszej ścieżce, związanej ściśle z technicznymi

aspektami przestępstw i dowodami cyfrowymi, prezentowane były następujące referaty:

- Historia włamania do systemu bankowości internetowej — Mariusz Burdach, Prevenity, Od zera do botmastera — Adam Heartle, zaufanatrzeciastrona.pl, „I DON'T WANNACRY” wszystko co chcielibyście wiedzieć o ransomware, a boicie się zapytać — Marek Krauze, Trend Micro, Wpływ nowoczesnych technologii na ewolucję przestępstw popełnianych z wykorzystaniem instrumentów płatniczych — Jarosław Biegański, ekspert ZBP, Digital forensic approach to open source intelligence (OSINT) — Damir Delija, Goran Oparnica, INSIG2,
- Obietnice/Promises — Zbigniew Jakubowski, Compendium,
- SMS recovery from NAND memory of erased eMMC chip. Data remnants in NAND after erasure — Patryk Płudowski, Rusolut,
- Uszkodzone dyski twarde — techniki laboratoryjne odzyskiwania danych — Witold Sobolewski, VSDATA,
- RA — wstępna analiza Triage — Tomasz Boroń, KWP Bydgoszcz,
- Automatyczne pobieranie i przetwarzanie danych retencyjnych — Grzegorz Piaskowski, KWP Katowice
- Projekt OKO — Daniel Konwiński, KWP Bydgoszcz
- Zmierzch ery blokerów — Wojciech Pilszak, e-detektywi
- Co wie o Nas sieć? — Marcin Matysek, KWP Bydgoszcz

Natomiast w ścieżce dedykowanej zarządzaniu bezpieczeństwem, socjotechnice i prawnym oraz organizacyjnym aspektom cyberbezpieczeństwa wygłoszono następujące wystąpienia:

- Ścigać przestępców czy edukować ofiary w temacie cyberprzestępczości? Analiza najczęściej występujących zagrożeń i źródeł problemów w cyberświecie — Maciej Kołodziej, e-detektywi,
- Phishing — wykorzystanie publicznych zasobów informacyjnych — Agnieszka Gryszczyńska, UKSW,
- Fokus na użytkownika. Phishing, ransomware, inżynieria społeczna, kradzież tożsamości — skuteczne narzędzia w rękach cyberprzestępców — Beata Legowicz, Instytut Informatyki i Gospodarki Cyfrowej SGH,
- Socjotechnika w działaniach cyberprzestępców — Ryszard Piotrowski, KWP Wrocław,
- KISS SMARTER — uwagi o celach Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 — Maciej Szmit, Orange,
- NC Cyber a strategia cyberbezpieczeństwa RP — Krzysztof Silicki, NASK,
- Krajowy System Cyberbezpieczeństwa — Piotr Balcerzak, ZBP,
- RODO a cyberbezpieczeństwo — jak będzie przebiegać obsługa naruszeń ochrony danych osobowych — Joanna Karczewska, ISACA Katowice,
- WiFi Calling i usługi VoLTE w kontekście retencji oraz LIHI — Paweł Baraniecki, Polkomtel,

- Interfejs LIHI 2.0 — Bartłomiej Burczyński, Intrasoft,
 - Bezpieczeństwo IT pod kontrolą — wyzwania dla zespołu CERT PSE — Jarosław Sordyl, PSE,
 - CERT ENERGA — aspekty organizacyjne i techniczne wdrożenia — Bogusław Kowalski, ENERGA,
 - Transgraniczność jako sposób uniknięcia odpowiedzialności karnej przy oszustwach zaliczkowych — studium przypadku — Maciej Bojczuk, KWP Wrocław.
- Równolegle, do wymienionych dwóch ścieżek obrad, odbywały się warsztaty:
- Zabezpieczanie i analiza pamięci RAM z wykorzystaniem darmowych narzędzi — Daniel Suchocki, Forsec,
 - Pismak6 — Interfejs dla Podmiotów Uprawnionych — Jakub Różecki, Intrasoft,
 - Ransomware cd. — Marek Krauze, Trend Micro.
- W ostatnim, trzecim dniu konferencji ogłoszono następujące referaty:
- Analiza powłamaniowa — Adam Ziaja, Red Team,
 - Blockchain jako nowe pole działań cyberprzestępców — Judyta Kasperkiewicz, WPiA UŚ,
 - Co w RAM-ie piszczy? — Daniel Suchocki, ForSec,
 - Zajęcie i zabezpieczenie majątkowe na kryptowalutach — Paweł Opitek, Prokuratura Kraków,
 - Analiza zawartości pamięci RAM systemu Windows 10 z punktu widzenia informatyki śledczej — Krzysztof Bińkowski, NET COMPUTER,
 - Specyfika i zasady efektywnej współpracy z giełdą kryptowalut na przykładzie BitBay.net — Artur Kubiak, Sylwester Suszek, BitBay,
 - Brudne białe kołnierzyki — Andrzej Niemiec, PRIM,
 - Zwalczanie rozpowszechniania treści pedofilskich w sieci — studium przypadku — Beata Bartosiewicz-Dziekciowska, Chomikuj.pl; Jarosław Cholewiński, BC KGP,
 - Analiza urządzeń mobilnych — wersja ekstremalna — Dariusz Walczak, Cybercop.pl,
 - Oszustwa SMS Premium — Jan Klima, KWP Kraków.

Warto podkreślić, aktywny udział uczestników konferencji, uzupełniających, dyskutujących, komentujących przekazywane treści. Prezentacje do większości wygłoszonych wystąpień, udostępnione przez prelegentów znajdują się pod adresem: https://1drv.ms/f/s!Ak_k-SJ89Sw3hXbi6TUu4FSnlair.

W monografii zebrano 29 rozdziałów. Część z nich jest rozwinięciem i uszczegółowieniem wystąpień z konferencji TAPT-20. Integralną częścią monografii są także rozdziały, które powstały z myślą o czytelnikach zainteresowanych cyberprzestępczością, ale związane były z innymi jej objawami, niż poruszane na konferencji TAPT-20 — naruszeniami praw własności intelektualnej, przestępczością przeciwko systemom bankowym oraz cyberprzemocą.

Duże zróżnicowanie tematyczne monografii świadczy o szerokim zakresie pojęcia cyberprzestępczość, używanego często jako ekwiwalent pojęcia przestępczość teleinformatyczna. Zróżnicowanie zakresu merytorycznego powinno sprawić, że każdy znajdzie w monografii teksty, które będą go satysfakcjonować. Podsumowując monografia powinna być przydatna dla wszystkich osób, które zajmują się zapewnieniem bezpieczeństwa wykorzystania nowoczesnych technologii teleinformatycznych oraz ściganiem sprawców cyberprzestępstw, w szczególności studentów kierunków związanych z bezpieczeństwem wewnętrznym, kryminologią, prawem oraz informatyką.

Jerzy KOSIŃSKI

Rozdział 1

ANALIZA DZIAŁAŃ RZĄDOWYCH W ZAKRESIE CYBERBEZPIECZEŃSTWA ZA OKRES TRWANIA TAPT

dr Krzysztof Jan JAKUBSKI¹

STRESZCZENIE: Przedstawiając swoje działania w budowaniu cyberpolicji w Polsce, autor analizuje działania administracji rządowej, powstawanie kolejnych dokumentów i struktur. Przedstawia także analizę najnowszego dokumentu rządowego — Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 przyjętych Uchwałą Nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r.

SŁOWA KLUCZOWE: cyberpolicja, cyberbezpieczeństwo, cyberprzestępczość, cyberprzestrzeń, ABW, Policja, KGP, NASK, rząd, MSWiA, MSW, NIK, Ministerstwo Cyfryzacji, Polityka bezpieczeństwa cyberprzestrzeni RP, Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Zamiast wstępu

Czytając w informacji o terminie kolejnego spotkania, iż *dwudziesty TAPT nie ma racji bytu, gdyż o wszystkim już dyskutowaliśmy i wszystko jest znane*, długo zastanawiałem się nad tymi słowami. Przypomniała mi się moja historia tego, w jaki sposób zainteresowałem się problemem przestępczości komputerowej. Nigdy nie byłem i nie czułem się informatykiem, no może jestem w miarę sprawnym użytkownikiem systemów informatycznych. Dla mnie — jak zresztą i dla wielu z mojego pokolenia — pojawienie się na rynku „maszyny ZX Spectrum” spowodowało rozbudzenie emocji. Z rozrzewnieniem wspominam pierwszy mój komputer — Timex Sinclair 2048, a potem długie zbieranie funduszy na coś lepszego. Tym lepszym był już klon PC — polski składak XT/286 z procesorem Intel 80286 o częstotliwości 6 MHz, dyskiem twardym 20 MB Seagate ST-225 i kartą graficzną Herkules. W przeciwieństwie do wielu nie wciągnąłem się w programowanie, choć pewne aplikacje w języku Basic tworzyłem. Za to szukałem możliwości wykorzystania komputera, nie tylko do gier lub jako zamiennika inteligentnej maszyny do pisania, ale także do analiz. Mogę się pochwalić, że mój prywatny komputer posłużył do dokonania analizy kilku tysięcy recept na narkotyki zrealizowanych w aptekach na terenie kilku województw wschodnich, w prowadzonym przeze mnie postępowaniu przygotowawczym przeciwko kilku lekarzom handlującym

¹ Ekspert ds. zwalczania cyberprzestępczości, kojot@jakubski.eu.

Dolarganem i Fentanylem, a analizy opracowane przy pomocy „Polonusa” — spolszczonej wersji dBASE III, stały się jednym z podstawowych materiałów dowodowych. Jednocześnie starałem się pozyskać jak najwięcej informacji na temat możliwości wykorzystania najpierw komputerów, a potem sieci komputerowych dla celów przestępczych. Nadużycia popełniane przez użytkowników systemów informatycznych były bowiem aż do końca lat 80 XX w. bagatelizowane, a jeszcze dekadę wcześniej niektórzy autorzy negowali w ogóle szkodliwość i znaczenie tych czynów. Zmiana stanowiska władz państw wysoko rozwiniętych nastąpiła w latach 90 XX w., kiedy dostrzeżono transgraniczność działalności komputerowej poprzez możliwość komunikacji za pomocą sieci Internet. Dodatkowo ogromne tempo rozwoju technologicznego, który wspomaga użytkowników komputerów oferując coraz to nowsze, szybsze urządzenia, łatwiejsze w użyciu, możliwe do obsługi przez nie-informatyków, rozpoczęło lawinowy wzrost strat powodowanych komputerowymi nadużyciami. W połowie lat 80. XX w. koszty związane z oszustwami elektronicznymi w świecie amerykańskiego biznesu szacowano na ok. 100 mln dolarów USA rocznie, by pod koniec lat 90. tego samego stulecia wycenić straty kradzieży przez komputer na ok. 3-7,5 miliardów dolarów USA². Wskazuje się również na różnicę między konsekwencjami finansowymi tradycyjnych napadów na banki, które jednorazowo tracą wtedy ok. 8 tys. USD a „ceną” kradzieży informacji z systemów komputerowych szacowaną na 100 tys. USD czy oszustwa komputerowego, za które bank „płaci” ok. pół miliona USD³.

Zmiana miejsca służby na Zakład Prawa Wyższej Szkoły Policji w Szczytnie spotęgowała zainteresowania naukowe. Efektem było kilka artykułów naukowych⁴, opublikowanych już po moim przejściu do Biura Dochodzeniowo-Śledczego KGP, gdzie dzięki przychylności ówczesnego kierownictwa kontynuowałem badania i rozpoznanie tematu. W tym czasie nawiązałem szereg kontaktów, które znacznie poszerzyły moją wiedzę, a udział — za zgodą Dyrektora BD-Ś KGP — w kilkunastu konferencjach poświęconych bezpieczeństwu sieci komputerowych pozwolił na poznanie światka najlepszych polskich hackerów końca lat 90. XX wieku. Dodatkowo kilka postępowań przygotowawczych, które

² K. J. Jakubski, *Przestępczość komputerowa: podział, definicja, możliwość jej ścigania i zapobiegania* [w:] Brunon Hołyst (red.), „Postępy Kryminalistyki”, z. 1, rok 1, Warszawa-Legionowo 1997.

³ K. J. Jakubski, *Wyludzanie towarów i usług na podstawie numerów kart kredytowych przez Internet* [w:] Internet 2000 prawo — ekonomia — kultura, praca zbiorowa pod red. R. Skubisza, „Vebra” Lublin 2000, s. 249 i n.

⁴ Przestępczość komputerowa — zarys problematyki, *Prokuratura i Prawo* 1996, nr 12, s. 34–50; Przestępczość komputerowa — podział i definicja, *Problemy Kryminalistyki* 1997, nr 217, s. 31–38; Przestępczość komputerowa: podział, definicja, możliwości jej ścigania i zapobiegania, *Postępy kryminalistyki* 1997, zeszyt 1, s. 6–43; Komputerowy nośnik informacji jako dokument w polskim procesie karnym, *Przegląd Policyjny* 1997, nr 3 (47), s. 5–18; Rozpowszechnianie pornografii w sieci komputerowej Internet, *Prokuratura i Prawo* 1997, nr 7–8.

nadzorowałem i w których wykonywałem osobiście szereg czynności procesowych, pozwolił mi poznać problemy dowodowe związane z przestępczością komputerową. Obok bowiem takich spraw, jak zmiana stron NASK-u przez „Gumisia”, gdzie procesowo nie udało się doprowadzić do przedstawienia zarzutów rozpoznanemu sprawcy, były także takie jak doprowadzenie do skazania dwóch mieszkańców Tarnowskich Gór za rozpowszechnianie pornografii dziecięcej w Internecie⁵. Pierwsza sprawa pozwoliła poznać środowisko, druga była priorytetowa — bowiem Szwedzi zagrozili wówczas NASK-owi odcięciem jedyne go wówczas łącza do sieci Internet.

Pod koniec 1995 r. szereg dyskusji z podinsp. Andrzejem Knapem i podinsp. Janem Hajdukiewiczem z Biura dw. z PG zaowocowało pomysłem na przekonanie kierownictwa KGP o potrzebie powołania struktury, która zajęłaby się problematyką rozwijającego się nowego kierunku przestępczości. W efekcie powołano Samodzielną Sekcję ds. Przestępczości Komputerowej, Analiz i Logistyki w strukturze Biura dw. z Przestępczością Gospodarczą KGP. Jednostka ta w okresie swojej działalności zajmowała się głównie ściganiem piractwa komputerowego oraz naruszaniem praw intelektualnych, a w jej składzie osobowym trzon stanowiły osoby zajmujące się logistyką Biura (sekretarki, maszynistki, kierowcy) bowiem sprawami przestępczości komputerowej zajmowało się najpierw dwóch, a po 1996 r. trzech oficerów, którzy prowadzili rozpoznanie zjawisk patologicznych związanych z funkcjonowaniem systemów komputerowych. W maju 1998 r., po kolejnej reorganizacji KGP, gdy rozwiązano Biuro Dochodzeniowo-Śledcze i Biuro dw. z PG, a powołano Biuro Koordynacji Służby Kryminalnej KGP, w Wydziale ds. Przestępczości Gospodarczej powołano Zespół ds. Przestępczości Komputerowej, do którego dołączono decyzją Dyrektora Biura również moją osobę. Zespół zajmował się koordynacją działań jednostek terenowych policji w następującym zakresie zagadnień⁶:

- zagrożenia ze strony sieci komputerowych, w tym kradzież informacji, włamania do systemów komputerowych (hacking), rozpowszechnianie informacji prawnie zabronionych, komunikacja grup przestępczych, oszustwa komputerowe;
- zagrożenia będące wynikiem wykorzystania komputerów jednostanowiskowych (komputer jako wyspecjalizowane narzędzie przestępcze);
- zagrożenia bankowych systemów kart do obrotu bezgotówkowego (fałszerstwo kart płatniczych — *skimming*, wyłudzenie towarów zamawianych na odległość na podstawie komputerowo generowanych numerów kart — *carding* itp.);
- zagrożenia będące wynikiem rozwoju sieci telekomunikacyjnych (kradzież impulsów telefonicznych, klonowanie telefonów komórkowych w systemach

⁵ Sprawa V Ds 67/96/S Prokuratury Wojewódzkiej w Katowicach.

⁶ Por. K.J. Jakubski: *Ściganie oszustw w Sieci* (wybrane zagadnienia) [w:] *Internet i nowe technologie — ku społeczeństwu przyszłości* (praca zbiorowa pod redakcją ks. prof. dr hab. T. Zasępy i dr R. Chmury), Wyd. Święty Paweł 2003, s. 555- 556.

telefonii analogowej, klonowanie kart SIM w systemach komórkowej telefonii cyfrowej, przechwytywanie kont abonentów telefonii cyfrowej poprzez wykorzystanie sprzętu komputerowego itp.);

- zagrożenia będące wynikiem naruszania dóbr intelektualnych (nielegalna produkcja i dystrybucja kaset wideo i audio, programów komputerowych, wydawnictw książkowych i podrobionych wyrobów markowych firm itp.).

Zespół, bardzo zresztą nieliczny, ciągle nawiązywał nowe kontakty, wspomagając jednostki terenowe w konkretnych sprawach i starał się szkolić policjantów w zwalczaniu przestępstw dokonywanych za pomocą nowych technologii. Dzięki naszym działaniom udało się zorganizować dużą ilość szkoleń, w tym zagranicznych, a dzięki naszym inspiracjom oraz ogromnemu zaangażowaniu ówczesnego asystenta w Wyższej Szkole Policji — komisarza mgr inż. Jerzego Kosińskiego, rozpoczęto w Szczytnie, m.in. TAPT oraz konferencje naukowe „Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych”⁷. Ponadto zespół, poza czynnościami koordynacyjnymi, wykonywał szereg działań, które były wynikiem specyfiki tej kategorii przestępczości. Należały do nich głównie: współpraca operacyjna z centralnymi dostawcami usług w sieciach komputerowych, centrami rozliczającymi płatności kartami płatniczymi i wydawcami takich kart zarówno ze środowiska bankowego, jak i poza-bankowego oraz organizacjami chroniącymi prawa autorskie.

Niestety decyzja o kolejnej reorganizacji w Policji przyspieszyła moją decyzję o rozstaniu się z mundurem noszonym blisko 26 lat, zwłaszcza, iż propozycja zostania Naczelnikiem Wydziału Bezpieczeństwa jednego z banków wydawała się kusząca. Likwidacja w 2004 r. pierwszego zespołu ds. przestępczości komputerowej, skutkowałą, m.in. zerwaniem szeregu nawiązanych wówczas kontaktów oraz odejściem ze służby lub przejściem do innych, nie mających nic wspólnego z dotychczasowymi zadaniami, funkcjonariuszy już przygotowanych do specyficznych zadań⁸.

⁷ Tu muszę zaznaczyć, że o możliwość realizacji tych konferencji mocno walczyło wówczas, faworyzowane przez kierownictwo KGP Centrum Szkolenia Policji w Legionowie, bowiem założenia wstępne przewidywały międzynarodowy charakter tych konferencji, a w Legionowie tworzono wówczas Międzynarodowe Centrum Szkolenia Policji. Nie ukrywam, że ostateczne umiejscowienie tych konferencji w WSPol., to (cóż sentyment do miasta w którym co prawda krótko, bo tylko przez trzy lata byłem wykładowcą, pozostał) moje oraz Jerzego Kosińskiego zwycięstwo.

⁸ Przykładowo - młodemu oficerowi, którego sam wyłapałem w czasie nauki w WSPol. (zainteresowanie tematyką, biegła znajomość 3 języków obcych) i po jej zakończeniu ściągnąłem do KGP (gdzie bardzo szybko nawiązał doskonale kontakty, w tym międzynarodowe oraz osiągał bardzo dobre wyniki w wyjątkowo specyficznej dziedzinie, która się zajmował), zaproponowano pracę w komisariacie, bo jak stwierdzono nie miał doświadczenia policyjnego (fakt — do WSPol. przyszedł z cywila). W efekcie kolega od lat kontynuuje to co zaczął w KGP, ale w wyspecjalizowanej komórce Europolu, gdzie go bardzo cenią i z tego co wiem do kraju wracać nie zamierza.

Analiza działań rządowych przed powstaniem Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022

Od czerwca 2007 r. w strukturze Biura Kryminalnego KGP, w Wydziale Zaawansowanych Technologii⁹, powołano Sekcję Wsparcia Zwalczania Cyberprzestępczości (WZC). Do zadań tej sekcji należało przede wszystkim

⁹ W świetle Załącznika Nr 2 do Zarządzenia Nr 460 KGP z dnia 24.05.2007 r. (Dz.Urz. KGP 07.09.78) do zadań Wydziału należało:

- 1) ocenianie funkcjonujących i wdrażanie nowych ogólnokrajowych systemów usprawniających kontrolę operacyjną, lokalizację terminali i pozyskiwanie informacji w sieciach telekomunikacyjnych oraz teleinformatycznych;
- 2) organizowanie serwisu oraz doposażenia ogólnokrajowych systemów kontroli w sieciach telekomunikacyjnych oraz innych specjalizowanych systemów teleinformatycznych techniki operacyjnej;
- 3) udział w pracach związanych z modernizacją eksploatowanych systemów oraz projektowaniem i wdrożeniem nowych systemów wsparcia pracy operacyjnej Policji i rozpoznania zagrożeń związanych z wykorzystaniem nowych usług i technologii;
- 4) udział w pracach związanych z zapewnieniem bezpieczeństwa informacji przetwarzanych w sieciach teleinformatycznych techniki operacyjnej;
- 5) administrowanie i wykonywanie bieżących i okresowych zadań związanych z funkcjonowaniem nadzorowanych systemów kontroli operacyjnej;
- 6) dokumentowanie czynności związanych z zarządzanymi kontrolami operacyjnymi i przeprowadzaniem przy użyciu nadzorowanych systemów kontroli operacyjnej;
- 7) wykonywanie zadań na rzecz uprawnionych organów;
- 8) współpraca z przedstawicielami służb techniczno-administracyjnych przedsiębiorców telekomunikacyjnych w sprawach prowadzonych przez Policję;
- 9) współpraca z przedsiębiorcami serwisującymi eksploatowane systemy;
- 10) wstępna weryfikacja i analiza informacji operacyjnych zbieranych przez jednostki Policji;
- 11) rozpoznanie nowych rodzajów zagrożeń pojawiających się w sieciach teleinformatycznych;
- 12) uzyskiwanie informacji o czynach zabronionych oraz sprawcach przestępstw popełnianych przy wykorzystaniu nowych usług i technologii;
- 13) pomoc w zabezpieczaniu, do celów operacyjnych, cyfrowych nośników informacji, a w szczególnych przypadkach odzyskiwanie danych i ich analiza;
- 14) inicjowanie i prowadzenie szkoleń w zakresie techniki operacyjnej dla policjantów i współpracujących z nimi prokuratorów;
- 15) współpraca z administratorami i właścicielami sieci komputerowych i przedsiębiorcami telekomunikacyjnymi w sprawach prowadzonych przez Policję;
- 16) dokonywanie ustaleń sprawców przestępstw, popełnionych z wykorzystaniem nowych technologii informatycznych, na potrzeby zagranicznych i krajowych organów ścigania;
- 17) zapewnianie wsparcia technicznego i merytorycznego przy realizacji międzynarodowej pomocy prawnej.

monitorowanie zagrożeń związanych z cyberprzestępczością, a także identyfikowanie, testowanie oraz wdrażanie zaawansowanych narzędzi technicznego wsparcia zwalczania cyberprzestępczości oraz pomoc w rozwiązywaniu skomplikowanych spraw i realizacja ustaleń internetowych we współpracy z ISP i ICP, czyli dostawcami usług internetowych. Pracownicy Sekcji Zaawansowanych Technologii uczestniczyli także w europejskich i międzynarodowych inicjatywach związanych ze zwalczaniem cyberprzestępczości. Równolegle w Wydziałach Techniki Operacyjnej KWP utworzone zostały komórki zaawansowanych technologii, których podstawowym zadaniem było wsparcie wydziałów kryminalnych w zastosowaniu specjalistycznej wiedzy i narzędzi informatycznych¹⁰. Kolejna reorganizacja powoduje, że od 2010 r. w Biurze Służby Kryminalnej KGP funkcjonuje Wydział Wsparcia Zwalczania Cyberprzestępczości, którego głównymi zadaniami stało się:

- stałe monitorowanie oraz analizowanie zagrożeń występujących w Internecie w ramach prowadzonych prostych form pracy operacyjnej,
- współpraca poza procesowa z podmiotami zewnętrznymi w zakresie prowadzenia ustaleń telekomunikacyjnych i teleinformatycznych,
- udzielanie wsparcia technicznego podczas wykonywania zadań przez komórki zwalczające przestępczość komputerową.

Od 2008 r., w ówczesnym Ministerstwie Spraw Wewnętrznych i Administracji oraz m.in. w ABW prowadzone były czynności mające na celu przygotowanie kompleksowej, narodowej strategii przeciwdziałania zagrożeniom występującym w cyberprzestrzeni. W toku prac powstało siedem kolejnych projektów strategii:

- „Rządowy program ochrony cyberprzestrzeni RP na lata 2008–2011” (listopad 2008 r.);
- „Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011” (styczeń 2009 r.);
- „Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011” — założenia (marzec 2009 r.);
- „Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2015” (maj 2010 r.);
- „Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2016” (czerwiec 2010 r.);
- „Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2020” (kwiecień 2011 r.);
- „Polityka bezpieczeństwa cyberprzestrzeni RP” (maj 2011 r.).

¹⁰ Por. Cyberkryminalni — rozmowa z mł. insp. Radosławem Chinalskim, Zastępcą Dyrektora Biura Kryminalnego KGP, *Nauka w służbie Policji*, kwartalnik policyjny, CSP 2009 nr 1, <http://kwartalnik.csp.edu.pl/kp/archiwum-1/2009/nr-12009/1097,CYBER-KRYMINALNI.html> (dostęp 14.05.2017 r.)

Żaden z wymienionych dokumentów nie został zatwierdzony przez Radę Ministrów i przyjęty do realizacji, co wynikało przede wszystkim z ich niskiej jakości oraz nierzetelnego przygotowania. W styczniu 2012 r., w reakcji na wydarzenia związane z protestami ACTA, w nowoutworzonym MAiC, wznowiono prace prowadzone wcześniej w byłym MSWiA, mające na celu przygotowanie narodowej strategii ochrony cyberprzestrzeni. W wyniku prac, przygotowano projekt dokumentu pt. „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej”, który we wrześniu 2012 r. został przekazany przez Ministra Administracji i Cyfryzacji do konsultacji międzyresortowych i społecznych, a następnie w marcu 2013 r., do rozpatrzenia przez Stały Komitet Rady Ministrów. „**Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej**”¹¹ została przyjęta uchwałą Rady Ministrów Nr 111/2013 z dnia 25 czerwca 2013 r., a koordynację realizacji jej postanowień powierzono ministrowi właściwemu ds. informatyzacji. Pominę analizę Polityki¹² i muszę przyznać, iż założenia jej były prawidłowe. Część działań w niej zawartych została wykonana, zwłaszcza w zakresie analitycznym. Jednakże należy stwierdzić, że tempo prac i efekty końcowe nie były zadowalające. Potwierdza to cytowana poniżej informacja z 30 czerwca 2015 r. Najwyższej Izby Kontroli w tym zakresie¹³, z którą częściowo się zgadzam:

„Kluczowym czynnikiem paraliżującym aktywność państwa w tym zakresie był brak jednego ośrodka decyzyjnego, koordynującego działania innych instytucji publicznych. Nie zidentyfikowano podstawowych zagrożeń dla krajowej infrastruktury teleinformatycznej oraz nie wypracowano narodowej strategii ochrony cyberprzestrzeni, stanowiącej podstawę dla działań podnoszących bezpieczeństwo teleinformatyczne. Nie określono też struktury i ram prawnych krajowego systemu ochrony cyberprzestrzeni, nie zdefiniowano obowiązków i uprawnień jego uczestników oraz nie przydzielono zasobów niezbędnych do skutecznej realizacji zadań. A co najważniejsze nie przygotowano procedur reagowania w sytuacjach kryzysowych, związanych z cyberprzestrzenią.

W ocenie NIK, istotnym czynnikiem wpływającym negatywnie na realizację zadań w obszarze bezpieczeństwa w cyberprzestrzeni było niewystarczające zaangażowanie kierownictwa administracji rządowej, w tym Prezesa Rady Ministrów, w celu rozstrzygania kwestii spornych między poszczególnymi urzędami oraz zapewnienia współdziałania organów i instytucji związanych z bezpieczeństwem teleinformatycznym państwa.

Jako działania pozytywne w obszarze ochrony cyberprzestrzeni można wskazać w szczególności:

¹¹ [http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersja pl.pdf](http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersja%20pl.pdf) (dostęp 14.05.2017 r.)

¹² Dokonał tego J. Skrzypczak, *Polityka Ochrony Cyberprzestrzeni RP*, „Przegląd Strategiczny” 2014, nr 7, s. 133-144

¹³ NIK o bezpieczeństwie w cyberprzestrzeni, <https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.htm>, (dostęp 14.05.2017 r.)

- powołanie i utrzymywanie na wysokim poziomie zespołów CERT¹⁴ (zespołów ds. bezpieczeństwa informatycznego) przez takie instytucje jak NASK, ABW oraz MON;
- utworzenie przez Ministra Obrony Narodowej systemu reagowania na incydenty komputerowe w resorcie obrony narodowej oraz wyspecjalizowanej jednostki - Narodowego Centrum Kryptologii;
- upowszechnianie przez Rządowe Centrum Bezpieczeństwa wytycznych i dobrych praktyk z zakresu ochrony teleinformatycznej infrastruktury krytycznej;
- prowadzenie przez NASK i Policję aktywnych działań edukacyjnych dotyczących m.in. przestępczości komputerowej i bezpieczeństwa w cyberprzestrzeni.

NIK zauważa, że poszczególne kontrolowane podmioty posiadały własne, odrębne procedury zapobiegania zagrożeniom w cyberprzestrzeni. Ale suma tych systemów nie tworzyła spójnej całości - jednego spójnego systemu.

Kontrola wykazała, że Minister Administracji i Cyfryzacji, któremu bezpośrednio przypisano obowiązki związane z ochroną cyberprzestrzeni, nie realizował należących do niego zadań w zakresie inicjowania i koordynowania działań innych podmiotów w dziedzinie bezpieczeństwa teleinformatycznego państwa. Minister Administracji i Cyfryzacji nie dysponował zasobami pozwalającymi na realną realizację zadań dotyczących zarządzania krajowym systemem ochrony cyberprzestrzeni oraz nie miał uprawnień do oddziaływania na inne instytucje, które odmawiały współpracy lub nierzetelnie i nieterminowo wywiązywały się z przypisanych im obowiązków.

Minister Spraw Wewnętrznych nie realizował żadnych zadań związanych z budową krajowego systemu ochrony cyberprzestrzeni. Działania Ministra w obszarze bezpieczeństwa IT ograniczały się do własnych sieci oraz systemów resortowych - jednak nawet w tym zakresie były prowadzone w sposób nierzetelny.

NIK zauważyła, że obowiązujące obecnie przepisy Prawa telekomunikacyjnego są wadliwie sformułowane i nie mogą być w praktyce wykorzystywane do realizacji zadań związanych z bezpieczeństwem IT. Było to przyczyną zaniechania wykonywania obowiązków przez Prezesa Urzędu Komunikacji Elektronicznej, dotyczących w szczególności pozyskiwania informacji o incydentach występujących w cyberprzestrzeni oraz informowania obywateli o zagrożeniach związanych z korzystaniem z Internetu.

¹⁴ CERT (Computer Emergency Response Team) jest nazwą zastrzeżoną przez Carnegie Mellon University i jej używanie wymaga zgody tego uniwersytetu. Zgodę taką posiada CERT Polska. Dyrektywa NIS posługuje się nazwą CSIRT. „Sieć CSIRT” to struktura organizacyjna o której mowa w art. 12 Dyrektywy NIS. „CSIRT” lub „CERT” lub „Zespół reagowania na incydenty komputerowe” oznacza grupę osób składającą się z analityków bezpieczeństwa, zorganizowaną w celu opracowywania, rekomendowania i koordynowania działań mających na celu wykrywanie, powstrzymywanie i zwalczanie skutków wynikających z incydentów, a także pozyskanie informacji na temat istoty tych incydentów

Koordynowany przez Rządowe Centrum Bezpieczeństwa system zarządzania kryzysowego nie jest komplementarny i spójny z działaniami w zakresie bezpieczeństwa teleinformatycznego oraz w niewystarczającym stopniu uwzględnia nowe zagrożenia dla infrastruktury krytycznej państwa, jakimi są zagrożenia występujące w cyberprzestrzeni.

Jednostki organizacyjne Policji podejmowały działania związane ze zwalczaniem przestępczości komputerowej oraz aktywnie uczestniczyły w kampaniach edukacyjno-informacyjnych, dotyczących bezpiecznego korzystania z Internetu. Komendant Główny Policji nie podjął natomiast rzetelnych działań w celu wdrożenia w Policji realnego i kompleksowego systemu reagowania na zagrożenia i incydenty w cyberprzestrzeni.

Minister Obrony Narodowej aktywnie realizował zadania w zakresie budowy resortowego systemu reagowania na incydenty komputerowe oraz uczestniczył w budowie krajowego systemu ochrony cyberprzestrzeni.

Kierownictwo Agencji Bezpieczeństwa Wewnętrznego realizowało zadania związane z zapobieganiem i reagowaniem na incydenty komputerowe w systemach podmiotów administracji państwowej, polegające m.in. na stworzeniu i utrzymywaniu systemu wczesnego ostrzegania ARAKIS.GOV oraz Zespołu CERT.GOV.PL. Aktywność ABW podlegała jednak istotnym ograniczeniom, wynikającym w szczególności z niewystarczających zasobów i braku formalnego umocowania Zespołu CERT.GOV.PL.

Kierownictwo Naukowej i Akademickiej Sieci Komputerowej podejmowało liczne działania, które NIK oceniła jako dobre praktyki w zakresie ochrony cyberprzestrzeni. Dotyczyły one w szczególności powołania i utrzymywania zespołu CERT Polska.

NIK odnotowała, że od 2008 roku prowadzone były prace nad narodową strategią ochrony cyberprzestrzeni. Kolejne wersje tego dokumentu nie były jednak zatwierdzane ze względu na ich nierzetelne przygotowanie i sprzeczne interesy różnych instytucji, zaangażowanych w przygotowywanie strategii. W czerwcu 2013 r. Rada Ministrów przyjęła „Politykę ochrony cyberprzestrzeni Rzeczypospolitej Polskiej” - dokument będący wynikiem źle rozumianego kompromisu, nieprecyzyjny i obciążony licznymi błędami merytorycznymi. Nieliczne zadania wynikające bezpośrednio z „Polityki” nie były realizowane przez większość skontrolowanych przez NIK podmiotów, co pozwala stwierdzić, że praktyczne zastosowanie strategii w celu poprawy bezpieczeństwa teleinformatycznego państwa było raczej symboliczne.

Wciąż nie zostały opracowane także założenia systemu finansowania działań związanych z ochroną cyberprzestrzeni RP. Nie przydzielono żadnych dodatkowych środków na ich realizację, co w ocenie NIK, praktycznie sparaliżowało działania podmiotów państwowych w zakresie bezpieczeństwa teleinformatycznego. Zasoby poszczególnych jednostek objętych kontrolą były bowiem nieadekwatne w stosunku do przypisanych im obowiązków.

Nie prowadzono żadnych prac legislacyjnych, które miałyby na celu unormowanie zagadnień związanych z bezpieczeństwem teleinformatycznym państwa. Nie przeprowadzono inwentaryzacji rozproszonych w różnych aktach prawnych przepisów związanych z cyberbezpieczeństwem, ani nie zdefiniowano pożądanych kierunków zmian legislacyjnych. Nie przygotowano nawet założeń aktu normatywnego, określającego strukturę krajowego systemu ochrony cyberprzestrzeni i jego uczestników.

W Polsce wciąż nie funkcjonuje spójny krajowy system reagowania na incydenty komputerowe. Czynności z zakresu reagowania na incydenty są realizowane przez funkcjonujące niezależnie od siebie państwowe i prywatne zespoły CERT, zajmujące się swoimi własnymi obszarami oddziaływania. Kierownictwo administracji państwowej nie podejmowało działań w celu wypracowania założeń pożądanej struktury zespołów reagowania, ustanowienia kanałów wymiany informacji oraz powołania CERTu narodowego, koordynującego działania wielu podmiotów i odpowiadającego za współpracę międzynarodową.

Minister Administracji i Cyfryzacji, który zgodnie z zapisami strategii odpowiada za koordynację krajowego systemu reagowania na incydenty komputerowe, nie realizował żadnych zadań w tym zakresie.

Administracja państwowa nie dysponuje wiedzą na temat skali i rodzaju incydentów występujących w cyberprzestrzeni, a ustanowiony w Prawie telekomunikacyjnym system zbierania i rejestrowania takich informacji okazał się być całkowicie nieskuteczny.

Tworzone w Polsce plany kryzysowe, w tym w szczególności Krajowy Plan Zarządzania Kryzysowego, odnosiły się wyłącznie do zdarzeń konwencjonalnych, takich jak np. katastrofy naturalne i nie uwzględniały zmiany charakteru zagrożeń, wynikającej m.in. z postępu technologicznego. Obowiązujące przepisy dotyczące zarządzania kryzysowego oraz Prawa telekomunikacyjnego nie były wykorzystywane w celu opracowania procedur obowiązujących w sytuacjach kryzysowych związanych z cyberprzestrzenią, a kierownictwo odpowiedzialnych podmiotów państwowych nie dostrzegało potrzeby podjęcia działań w tym zakresie.

NIK dostrzega wysiłki podejmowane przez ABW (we współpracy z NASK) w celu realizacji projektu dotyczącego wytworzenia, utrzymywania i rozbudowy systemu wczesnego ostrzegania - ARAKIS.GOV. W ramach tego przedsięwzięcia w kilkudziesięciu instytucjach publicznych zainstalowano sondy systemu, dzięki którym uzyskiwano informacje o zagrożeniach w sieci Internet. Jednak ze względu na braki finansowe, dobrowolność udziału w projekcie oraz instalowanie sond wyłącznie w podmiotach publicznych, zasięg oddziaływania systemu ARAKIS.GOV oraz pozyskiwanych za jego pomocą danych miały ograniczony zakres.

Administracja publiczna nie wypracowała dotąd zintegrowanego i systemowego wspierania przez państwo badań w obszarze ochrony cyberprzestrzeni oraz możliwości praktycznego zastosowania ich wyników w celu poprawy bezpieczeństwa teleinformatycznego.”

Jak widać ocena NIK w zakresie podejścia podmiotów rządowych do cyberbezpieczeństwa jest miażdżąca¹⁵, choć nie bardzo rozumiem dlaczego winą obarcza się głównie Ministra Administracji i Cyfryzacji, na którego barki nałożono — moim zdaniem — zbyt wiele obowiązków. Zresztą informacja o wynikach kontroli, w którym wychwala się rolę ABW i służb wojskowych, a neguje w czambuł cywilów, z samej istoty jest podejrzana, zwłaszcza, iż znane były już wcześniej rozbieżne stanowiska oraz współzawodnictwo kierownictwa MSWiA i ABW w zakresie pożądanej struktury koordynacji systemu ochrony cyberprzestrzeni, w tym spory personalne dotyczące powołania i obsadzenia stanowiska Pełnomocnika Rządu ds. Ochrony Cyberprzestrzeni RP, a niektóre pomysły ABW (choćby umiejscowienie, na podstawie stanowiska kierownictwa MSWiA i ABW ze stycznia 2008 r., Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL w strukturach tej służby) można uznać za co najmniej dyskusyjne. Ponadto MCiA przygotowywało w tym czasie założenia do założeń przyszłej ustawy o cyberbezpieczeństwie, a w międzyczasie trwały prace i ustalenia nad dyrektywą NIS.

Nieciekawie brzmiały słowa z protokołu kontroli NIK w odniesieniu do MSW „Minister Spraw Wewnętrznych odpowiadający za sprawy bezpieczeństwa i zarządzania kryzysowego nie realizował żadnych zadań związanych z bezpieczeństwem państwa i jego infrastruktury w kontekście ochrony teleinformatycznej. W szczególności, Minister nie podejmował działań w celu zawarcia w Krajowym Planie Zarządzania Kryzysowego procedur reagowania na zdarzenia związane z cyberprzestrzenią, co wyjaśniano niezidentyfikowaniem przez właściwe komórki Ministerstwa ryzyk w tym obszarze. MSW nie współpracowało również efektywnie z przedsiębiorcami telekomunikacyjnymi w realizacji nałożonych na nich obowiązków, dotyczących przygotowania planów działań w sytuacjach szczególnych zagrożeń. Minister Spraw Wewnętrznych, przekazując przedsiębiorcom informacje służące identyfikacji ryzyk dla ich działalności, nie wskazywał żadnych zagrożeń związanych z cyberprzestrzenią i rutynowo przedstawiał coroczną „Ocenę zagrożenia bezpieczeństwa powszechnego w Polsce”, odnoszącą się wyłącznie do zagrożeń konwencjonalnych, takich jak powodzie, trzęsienia ziemi, pożary itd. Minister wyjaśnił, że nie informowano o ryzykach związanych z bezpieczeństwem teleinformatycznym, ponieważ obowiązujące

¹⁵ Por. także „Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej”, Informacja o wynikach kontroli, Departament Porządku i Bezpieczeństwa Wewnętrznego NIK, KPB-4101-002-00/2014, Nr ewid. 42/2015/P/14/043/K, https://www.nik.gov.pl/kontrola/wyniki-kontroli-nik/pobierz,kpb~p_14_043_201406171048381403002118~01,typ,kk.pdf; (dostęp 14.05.2017 r.); „Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu”, Informacja o wynikach kontroli, Departament Administracji Publicznej NIK, KAP-4101-002-00/2014, Nr ewid. 205/2014/P/14/004/K, https://www.nik.gov.pl/kontrola/wyniki-kontroli-nik/pobierz,kap~p_14_004_201405280743421401263022~01,typ,kk.pdf (dostęp 14.05.2017 r.)

przepisy nie nakładają wprost obowiązku przekazywania przedsiębiorcom informacji na temat tej konkretnej kategorii zagrożeń. Działania Ministra Spraw Wewnętrznych w obszarze bezpieczeństwa IT ograniczały się do własnych sieci oraz systemów resortowych, natomiast były one prowadzone bez należytego przygotowania oraz bez wdrożenia w MSW zapisów „Polityki”¹⁶

Nie wiem, czy wyniki kontroli, czy też prace nad Ustawą z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r., były przyczyną zmian organizacyjnych w Policji. W załączniku do konwencji zlecono bowiem Wydziałowi Wsparcia Zwalczania Cyberprzestępczości BSK KGP realizowanie zadań punktu kontaktowego, o którym mowa w art. 35 Konwencji Rady Europy o cyberprzestępczości¹⁷. W dniu 15 lipca 2014 r. rozkazem organizacyjnym nr 31/14 z dnia 26 czerwca 2014 r. w sprawie zmian organizacyjno-etatowych w Komendzie Głównej Policji, wprowadzona została zmieniona struktura organizacyjna Biura Służby Kryminalnej Komendy Głównej Policji. Dotychczasowy Wydział Wsparcia Zwalczania Cyberprzestępczości zmienił nazwę na Wydział do walki z Cyberprzestępczością. Zmiana była konsekwencją ukierunkowania zadań Wydziału na bardziej aktywne i bezpośrednie działania w zakresie identyfikowania zagrożeń przestępstwami w sieci Internet oraz ujawniania i ścigania ich sprawców¹⁸. Do zadań komórki w KGP należało w szczególności¹⁹:

- inicjowanie i koordynowanie działań Policji w zakresie identyfikowania głównych zagrożeń przestępstwami w sieci Internet, metod i form ich zwalczania oraz współdziałania jednostek Policji z organami i podmiotami pozapolicyjnymi w celu ich skutecznego zwalczania;
- współpraca na szczeblu krajowym i międzynarodowym z instytucjami państwowymi oraz sektorem prywatno — publicznym w zakresie pozyskiwania informacji o metodach i formach przestępstw popełnianych w cyberprzestrzeni, w tym pozyskiwanie i współpraca z Osobowymi Źródłami Informacji;
- opracowywanie rodzaju współpracy z podmiotami sektorów publicznych, prywatnych i akademickich oraz ustalanie kanałów i sposobu gromadzenia i wymiany informacji o przestępstwach oraz zabezpieczenia dowodów cyberprzestępstw;
- opracowanie koncepcji wykorzystania kwalifikowanych środków pracy operacyjnej do ofensywnego rozpoznawania i zwalczania przestępstw związanych z siecią Internet oraz prowadzenie form pracy operacyjnej;

¹⁶ Realizacja przez podmioty państwowe zadań..., op. cit., s. 40

¹⁷ Dz.U. 2015 poz. 728 <http://dziennikustaw.gov.pl/du/2015/728>

¹⁸ <http://www.policja.pl/pol/kgp/bwik/aktualnosci-1/biezace-informacje/101696,Zmiany-w-Biurze-Sluzby-Kryminalnej-Komendy-Glownej-Policji.html> (dostęp 14.05.2017 r.)

¹⁹ Informacja ze strony - <http://www.policja.pl/pol/kgp/bsk/struktura/wydzialy/wydzial-do-walki-z-cybe/87086,Wydzial-doWalki-z-Cyberprzestepczoscia.html> - aktualnie niedostępna

- prowadzenie wieloźródłowych konsultacji technicznych i współpracy z podmiotami krajowymi i zagranicznymi zmierzających do rozpoznawania i implementowania nowoczesnych rozwiązań w walce z przestępczością popełnianą w świecie wirtualnym;
- wdrażanie i utrzymywanie dedykowanych systemów teleinformatycznych realizujących zadania takie jak: monitorowanie sieci Internet pod kątem wykrywania przestępstw, nielegalnych treści, wykrywanie użytkowników korzystających z sieci anonimowych, zapewnienie zdalnego dostępu do dedykowanych systemów komórkom powołanych w ramach komend wojewódzkich (stołecznej) Policji;
- opiniowanie i opracowywanie propozycji zmian legislacyjnych w zakresie bezpieczeństwa teleinformatycznego;
- organizowanie oraz udział w doskonaleniu zawodowym policjantów w zakresie właściwości wydziału;
- prowadzenie czynności operacyjno-rozpoznawczych, w tym form pracy operacyjnej w zakresie właściwości wydziału.

MSWiA dostrzegło także problem świata wirtualnego²⁰ zwłaszcza, że nie potrzeba już bowiem ogromnych nakładów finansowych, ani lat studiów technicznych, aby ściągnąć pliki z innego komputera, czy „podrzucić” złośliwy program nie lubianemu sąsiadowi, zwłaszcza jeżeli zgłębi się zasoby sieciowe i z łatwością znajdzie tam wszystkie potrzebne do dokonania czynu narzędzia i informacje²¹. W swoim Raporcie o stanie bezpieczeństwa państwa za rok 2015 już napisało:

„Cyberprzestrzeń pozostaje obszarem działania zarówno indywidualnych przestępców, jak i zorganizowanych grup przestępczych oraz środowisk ekstremistycznych i organizacji terrorystycznych. Upowszechnienie dostępu do Internetu, w kontekście globalnego charakteru cyberprzestrzeni, przy jednocześnie stosunkowo dużej możliwości zachowania anonimowości i popełniania przestępstw na terenie jednego państwa z obszaru innego, sprzyja występowaniu różnego rodzaju zagrożeń zarówno dotyczących bezpieczeństwa systemów informatycznych, jak i o charakterze stricte przestępczym (przestępczość o charakterze ekonomicznym, kryminalnym i narkotykowym). Istotne jest również, że cyberzagrożenia mają charakter elastyczny i bezpośrednio zależny od kierunków rozwoju nowoczesnych technologii.”²²

²⁰ Tu chcę zwrócić uwagę na to, że większość wniosków i informacji jakie Autor przedstawiał w swoich publikacjach, w okresie jego służby było przekazywane kierownictwu KGP w postaci stosownych dokumentów służbowych.

²¹ Por. K.M. Mazur, *Polskojęzyczna społeczność przestępczość zorganizowana w sieci DARKNET*, ICTLAW.pl, Poznań 2016

²² Raport o stanie bezpieczeństwa w Polsce w 2015 r., MSWiA, s. 260-261, <https://bip.mswia.gov.pl/download/4/29642/file.file> (dostęp 14.05.2017 r.)

Analiza zapisów Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 (KRPC RP) są kontynuacją działań, podejmowanych w przeszłości przez administrację rządową oraz dokumentem koncepcyjnym i wykonawczym w stosunku do Strategii Bezpieczeństwa Narodowego RP - **Doktryną cyberbezpieczeństwa RP** opublikowaną przez Biuro Bezpieczeństwa Narodowego w 2015 r.²³ Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 (KRPC RP) zostały przyjęte Uchwałą Nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r.²⁴

Celem głównym KRPC RP ma być zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych w taki sposób, by w roku 2022 Polska była krajem bardziej odpornym na ataki i zagrożenia płynące z cyberprzestrzeni, a dzięki synergii działań wewnętrznych i międzynarodowych cyberprzestrzeni RP stanowić będzie bezpieczne środowisko umożliwiające realizowanie wszystkich funkcji państwa i pozwalając na pełne wykorzystywanie potencjału gospodarki cyfrowej, przy równoczesnym poszanowaniu praw i wolności obywateli. Cel główny realizowany ma być poprzez cztery cele szczegółowe.

Cele jak najbardziej wskazane, ale czy realne do osiągnięcia?

Pierwszy cel szczegółowy — Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa, ma być zrealizowany poprzez:

- dostosowanie otoczenia prawnego do potrzeb i wyzwań w obszarze cyberbezpieczeństwa,
- udoskonalenie struktury krajowego systemu cyberbezpieczeństwa,
- zwiększenie efektywności współdziałania podmiotów zapewniających bezpieczeństwo cyberprzestrzeni RP,
- zwiększenie bezpieczeństwa teleinformatycznego usług kluczowych i cyfrowych oraz infrastruktury krytycznej,
- opracowanie i wdrożenie standardów oraz dobrych praktyk bezpieczeństwa sieci i systemów informatycznych,
- wypracowanie i wdrożenie systemu zarządzania ryzykiem na poziomie krajowym,

²³ Doktryna cyberbezpieczeństwa RP, BBN, 2015, <https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf> (dostęp 14.05.2017 r.)

²⁴ <https://mc.gov.pl/aktualnosci/strategia-cyberbezpieczenstwa-przyjeta-przez-rzad> (dostęp 01.06.2017 r.)

- zapewnienie bezpiecznego łańcucha dostaw,
- zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń.

Hasłowo brzmi to prosto, ale jak z realizacją? Przykładowo w celu implementowania do prawa polskiego przepisów Konwencji o cyberprzestępczości znowelizowane zostały odnośne przepisy kodeksu karnego, w tym w szczególności zawarte w rozdziale XXXIII k.k. zatytułowanym *Przestępstwa przeciwko ochronie informacji*. Ale dla mnie nadal nie zrozumiałym jest dlaczego ustawodawca łagodniej traktuje sprawcę oszustwa komputerowego (art. 287 kk) od oszustwa klasycznego (286 k.k.). Problemem jest postępowanie dowodowe. Polskie przepisy proceduralne w tym zakresie są nie zmienione i w dalszym ciągu dylematem jest co zabezpieczać - kopie danych czy cały sprzęt, jak traktować logi systemowe, co może być śladem przestępstwa popełnianego w sieci.

Absurdem jest także pozostawienie w polskim prawie ponad 62 ustaw definiujących pojęcia ochrony i tajemnicy informacji, nie zawsze ze sobą skorelowanych, przez co przykładowo pojęcie „informacja poufna” nie zawsze oznacza to samo. Drobne różnice widać także w podstawowych pojęciach między tak kluczowymi dla ochrony informacji ustawami jak: Ustawa o ochronie danych osobowych i Ustawa o ochronie informacji niejawnych, gdzie jedna definiuje system informatyczny jako *zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych*, a druga system teleinformatyczny definiuje *jako system, który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji*. Niby różnica niewielka, ale czy potrzebna? Zresztą praktyka pokazuje dużo więcej bolączek, gdy przykładowo następuje zbieg wielu ustaw chroniących przecież to samo dobro jakim jest informacja, a są różnice w postępowaniu z nimi. Urząd skarbowy może być tu szkolnym przykładem — ta sama informacja może być tam chroniona jako informacja niejawna, informacja stanowiąca tajemnicę skarbową albo informacja stanowiąca daną osobową — każda ustawa obowiązująca naczelnika US, a właściwie przepisy wykonawczego do nich, inaczej określają sposób przetwarzania w zakresie zbierania, przechowywania, archiwizowania informacji oraz dokumentowania tych czynności dla potrzeb tego urzędu. Co mają zrobić pracownicy spółek Skarbu Państwa, w których wytyczne w zakresie ochrony informacji przygotowuje pełnomocnik ochrony podległy prezesowi spółki oraz administrator bezpieczeństwa informacji umiejscowiony w pionie administracji podległej innemu członkowi zarządu w tej spółce, i wytyczne te są ze sobą niespójne. Czyje wytyczne są ważniejsze? Wbrew pozorom, takie zdarzenia to praktyka dnia dzisiejszego. A chronione jest to samo dobro — informacja, czasami w postaci danych informatycznych. Brak organu koordynującego i wprowadzającego regulacje w zakresie ochrony informacji jest dzisiaj szczególnie widoczny.

Niepokojąco brzmią słowa Grzegorza Małeckiego²⁵, który napisał „*należy zbudować samodzielną służbę odpowiedzialną za cyberbezpieczeństwo, cyberwywiad oraz wywiad radioelektroniczny, tzw. SIGINT (na wzór amerykańskiej NSA czy brytyjskiej GCHQ). Obowiązujący model, w którym zadania realizują — według własnego uznania — istniejące agencje, jest absolutnie nieefektywny i pozbawiony racji bytu. W ten sposób mamy do czynienia z marnowaniem ograniczonych zasobów ludzkich i finansowych.*” Nie wiem, czy przypadkiem ten punkt widzenia Autora nie wiąże się z aktualnie podawanymi przez media niesnaskami pomiędzy ministrem cyfryzacji Anną Streżyńską a MON i jest wyraźnym określeniem, po której stronie Autor się opowiada, zwłaszcza, że swojej opinii nie argumentuje. Zamiast natomiast wnioskowanej przez G. Małeckiego „*samodzielnej instytucji, mającej status centralnego organu administracji państwowej, odpowiedzialnej za wykonywanie polityki państwa w zakresie zarządzania informacjami niejawnymi oraz wydawanie poświadczeń bezpieczeństwa uprawniających do dostępu do tajemnic państwowych*”, bardziej marzyłoby mi się powołanie samodzielnej lub będącej w strukturach Ministerstwa Cyfryzacji instytucji będącej odpowiednikiem niemieckiego Bundesamt für Sicherheit in der Informationstechnik (BSI - Federalne Biuro Bezpieczeństwa informacji).²⁶ Można byłoby tam też przekazać zadanie w zakresie zarządzania informacjami niejawnymi postulowane przez G. Małeckiego. Problematyka bezpieczeństwa systemów informatycznych dotyczy nie tylko instytucji rządowych i samorządowych, ale w znacznie większej części sfery prywatnej. A ta część użytkowników, nie zawsze chce mieć jakiegokolwiek kontakty z państwowymi służbami specjalnymi, zwłaszcza po utracie zaufania do tych instytucji w zakresie utrzymania tajemnicy takich kontaktów. A adres do korespondencji Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL - Warszawa, ul. Rakowiecka 2A kojarzy się jednoznacznie. I pamiętajmy, że w Polsce istnieje ogromna ilość organizacji i stowarzyszeń pozarządowych, które już w tej chwili mogą poszczycić się dużymi osiągnięciami w zakresie bezpieczeństwa systemów informatycznych. Dodam tylko, że stworzenie takiej instytucji wcale nie byłoby wbrew pozorom trudne, ostatecznie z własnego doświadczenia i znajomości z ludźmi wiem, że w niemieckiej BSI duża grupa pracowników, to oddelegowani tam funkcjonariusze BKA i innych służb państwowych.

Mam wątpliwości co do tego, czy kolejna reorganizacja w Policji i utworzenie w dniu 1 grudnia 2016 r. wyspecjalizowanego Biura do walki z Cyberprzestępczością KGP ułatwi walkę z przestępczością związaną z użyciem najnowocześniejszych technologii. Od dwóch lat przed powstaniem Biura każda komenda wojewódzka Policji łącznie z komendą stołeczną miały wydziały do walki z cyberprzestępczością.

²⁵ Grzegorz Małecki: Bezglowe służby, publikacja: 07.05.2017 aktualizacja: 09.05.2017, <http://www.rp.pl/Publicystyka/305079942-Bezglowe-sluzby.html#ap-1>, (dostęp 14.05.2017 r.)

²⁶ https://www.bsi.bund.de/DE/Home/home_node.html

Porównanie tabeli 14.1, 14.2, 14.3 i 14.4²⁷ Raportu o stanie bezpieczeństwa w Polsce w 2015 r. z informacjami zawartymi w Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku, przygotowanym przez CERT.GOV.PL²⁸, wyraźnie potwierdza jednak tezę, że polskie organa ścigania analizują procesowo minimalną ilość incydentów w sieci. Zespół CERT.GOV.PL łącznie zarejestrował 16123 zgłoszeń, z których aż 8914 zostało zakwalifikowanych jako faktyczne incydenty. Liczba alarmów o priorytecie wysokim (1429) w systemie gromadzącym i analizującym informacje pozwalające na określenie lokalizacji geograficznej źródeł, z których podejmowano ataki na polskie sieci administracji publicznej ARAKIS-GOV, również nie ma odzwierciedlenia w tabeli 4.

Tabela 1. Liczba postępowań wszczętych przez Policję z wybranych artykułów k.k. dotyczących cyberprzestępczości w latach 2009-2015

	2010	2011	2012	2013	2014	2015
art. 200a §1-2 k.k. (przestępstwa związane z pedofilią)	34	64	84	129	154	281
art. 269 §1-2 k.k.(atak na zasoby lub urządzenia informatyczne instytucji państwowych lub samorządowych)	7	3	9	14	9	4
art. 269a k.k.(atak na system komputerowy lub sieć teleinformatyczną)	22	38	35	37	27	52
art. 269b k.k.(udostępnianie urządzeń, programów lub danych służący popełnianiu przestępstw)	35	38	21	42	47	58

Źródło: KGP

²⁷ Raport o stanie bezpieczeństwa w Polsce w 2015 r., op. cit., s. 264-266

²⁸ Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r., Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, kwiecień 2016, <http://www.cert.gov.pl/download/3/183/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2015roku.pdf> (dostęp 14.05.2017 r.)

Tabela 2. Liczba przestępstw stwierdzonych przez Policję z wybranych artykułów k.k. dotyczą-cych cyberprzestępczości w latach 2009-2015

	2010	2011	2012	2013	2014	2015
art. 200a §1-2 k.k (przestępstwa związane z pedofilią).	6	62	74	132	151	286
art. 269 §1-2 k.k.(atak na zasoby lub urządzenia informatyczne instytucji państwowych lub samorządowych)	0	5	5	9	7	4
art. 269a k.k.(atak na system komputerowy lub sieć teleinformatyczną)	18	30	30	34	52	111
art. 269b k.k.(udostępnianie urządzeń, programów lub danych służący popełnianiu przestępstw)	71	29	27	28	43	44

Źródło: KGP

Tabela 3. Liczba przestępstw stwierdzonych przez Policję, w odniesieniu do których w polu „modus operandi” wskazano cechy związane z Internetem lub systemami komputerowymi w latach 2013-2015*

	2013	2014	2015
1	2	3	4
art. 190a §1-3 k.k. (uporczywe nękanie, tworzenie fałszywych tożsamości, fałszywych profili, podszywanie się pod osobę)	442	687	951
art. 196 k.k. (obraza uczuć religijnych innych osób)	9	7	4
art. 200b k.k. (publiczne pochwalanie i propagowanie zachowań pedofilskich)	1	3	2
art. 202 §1 k.k. (rozpowszechnianie pornografii w sposób narzucający tego rodzaju treści osobom, które sobie tego nie życzą)	10	23	22

1	2	3	4
art. 202 §3, 4, 4a, 4b k.k. (produkowanie, utrwalanie, sprowadzanie, przechowywanie, posiadanie, rozpowszechnianie, prezentowanie i uzyskiwanie dostępu do treści pedofilskich, związanych z prezentowaniem przemocy i zoofilskich)	2096	2307	396
art. 256 §1 i 2 k.k. (propagowanie ustrojów totalitarnych oraz treści rasistowskich i ksenofobicznych oraz wytwarzanie i utrwalanie takich treści w celu rozpowszechniania)	84	213	234
art. 257 k.k. (publiczne znieważanie grupy ludności albo poszczególnych osób z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości)	33	99	171
art. 266 §1 k.k. (nielegalne ujawnienie informacji uzyskanej w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową)	8	9	9
art. 266 §2 k.k. (ujawnienie informacji niejawniej o klauzuli „zastrzeżone” lub „poufne” przez funkcjonariusza publicznego)	1	0	0
art. 268 §1 i 2 k.k. (nielegalne niszczenie, uszkodzanie usuwanie, zmienianie zapisu istotnej informacji albo znaczne utrudnianie lub udaremnianie możliwości zapoznania się z nią)	155	123	93
art. 268a §1-2 k.k. (niszczenie, uszkodzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych informatycznych albo w istotnym stopniu zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywanie takich danych)	332	374	395
art. 271 §1-3 k.k. (wystawienie przez funkcjonariusza publicznego lub inną uprawnioną osobę dokumentu, w którym poświadcza nieprawdę co do okoliczności mającej znaczenie prawne)	144	9	456
art. 286 §1-3 k.k. oraz art. 286 §1 w zw. z art. 294 §1 (oszustwo)	30 977	36 394	40 499

Źródło: KGP

Tabela 4. Liczba śledztw ABW związanych z przestępczością w cyberprzestrzeni w latach 2010-2015

	2010	2011	2012	2013	2014	2015
art. 267 k.k. (włamania do systemów komputerowych)	2	3	1	3	2	0
art. 268a k.k. (atak na zasoby informatyczne)	0	0	1	0	0	0
art. 269 k.k. (atak na zasoby lub systemy informatyczne instytucji państwowych lub samorządowych)	0	3	2	1	0	0
art. 269a k.k. (zakłócanie pracy systemu komputerowego lub sieci teleinformatycznej)	1	0	1	1	0	1
art. 269b k.k. (udostępnianie urządzeń, programów lub danych służący popełnianiu przestępstw)	0	1	0	0	0	0
art. 287 k.k. (oszustwo komputerowe)	1	1	1	1	1	1
RAZEM	4	8	6	6	3	2

Źródło: ABW

A trzeba pamiętać, że przeprowadzenie postępowania przygotowawczego, nawet w sytuacji niewiary w możliwość ustalenia lub ukarania sprawcy, pozwala na procesowe zabezpieczenie dowodów na rzecz ich późniejszego wykorzystania. Już słyszę głosy, że takie działania popsują statystyki wykrywalności (i tak nadrabiane danymi dotyczącymi zwalczania piractwa komputerowego), ale część Raportu o stanie bezpieczeństwa przygotowana przez Ministerstwo Sprawiedliwości wyraźnie wskazuje, że w tym zakresie jest sporo do nadrobienia: *W 2015 roku w sądach rejonowych z art. 268a k.k. (niszczenie lub uszkodzanie danych informatycznych) osądzono łącznie 32 osoby, z czego 24 skazano. Kary pozbawienia wolności w zawieszeniu orzeczono w przypadku 10 osób. Uniewinniono 4 osoby. Z art. 269a k.k. (zakłócanie pracy systemu komputerowego lub sieci*

teleinformatycznej) w sądach rejonowych osądzono 4 osoby, z czego 3 skazano. Z art. 269b k.k. (wytwarzanie, pozyskiwanie, zbywanie, udostępnianie, urządzenia lub programu komputerowego do popełniania przestępstw) w 2015 roku w sądach rejonowych osądzono łącznie 243 osoby, z czego 238 skazano. Kary pozbawienia wolności orzeczono w przypadku 191 osób, w tym w zawieszeniu wobec 152. Uniewinniono 3 osoby. Ponadto na podstawie art. 287 k.k. (oszustwo komputerowe gospodarcze) w 2015 roku w sądach rejonowych osądzono łącznie 109 osób, z czego 97 skazano. Kary pozbawienia wolności orzeczono w przypadku 73 osób (w tym w zawieszeniu 56).²⁹

Należy tu wyraźnie zaznaczyć, że bez odpowiedniej statystyki nie ma wiedzy i nie można robić badań. Nie można prowadzić racjonalnej analizy ryzyka.

W kwestii tempa reagowania na incydenty instytucje państwowe mogą jeszcze sporo poprawić. Do ataku WannaCry doszło w piątek 12 maja 2017 r. i choć infekował komputery na całym świecie od samego rana, to eksperci poza Hiszpanią i Wielką Brytanią zdali sobie sprawę ze skali ataku dopiero około godziny 15. Do wieczora o ataku wiedział już cały świat bezpieczeństwa IT i informacja zaczęła pojawiać się w mediach. Zanim ktokolwiek obudził się w instytucjach do tego powołanych, problem zasygnalizował Sekurak (12.05.2017 17:40 w piątek)³⁰, tego samego dnia o godzinie 21:09 udało się temat opisać dość szeroko przez Zaufaną Trzecią Stronę³¹, a dwa dni później dołączył także Niebezpiecznik³². Natomiast w sobotę, 13 maja 2017 r., komunikat wydał rzecznik prasowy Ministra Koordynatora Służb: „Znajdujący się w gestii ABW Cert.gov.pl nie odnotował żadnych poważnych incydentów związanych z atakami hakerskimi w ostatnim czasie. Również NASK zajmujący się cyberbezpieczeństwem prywatnych podmiotów nie zgłasza sygnałów o incydentach. Duży atak hakerski, który miał miejsce na skalę światową, nie dotyczy Polski”³³. Jednakże 15 maja po południu zespół CERT Polska opublikował bardzo sensowny i merytoryczny artykuł³⁴ na temat zagrożenia WannaCry wskazując na ponad tysiąc potencjalnych infekcji polskich adresów IP (w momencie pisania tego artykułu liczba ta wzrosła podobno do ok. 4000)³⁵.

²⁹ Raport o stanie bezpieczeństwa w Polsce w 2015 r., op. cit., s. 26

³⁰ <https://sekurak.pl/masowy-atak-na-publiczna-sluzbe-zdrowia-w-uk-chaos-ransomware-i-grozba-globalnego-ataku> (dostęp 01.06.2017r.)

³¹ <https://zaufanatrzeciastrona.pl/post/masowa-niezwykle-skuteczna-kampania-ransomware-wylacza-cale-firmy> (dostęp 01.06.2017r.)

³² <https://niebezpiecznik.pl/post/zamkniete-szpitala-i-zaklady-pracy-uderzenie-robaka-wannacry-i-olbrzymie-straty-na-calym-swiecie> (dostęp 01.06.2017r.)

³³ <https://www.premier.gov.pl/wydarzenia/aktualnosci/komunikat-rzeczniaka-prasowego-ministra-koordynatora-sluzb.html> (dostęp 01.06.2017r.)

³⁴ <https://www.cert.pl/news/single/wannacry-ransomware> (dostęp 01.06.2017r.)

³⁵ Por. Komunikacja polskich instytucji państwowych na temat WannaCry — analiza, <https://zaufanatrzeciastrona.pl/post/komunikacja-polskich-instytucji-panstwowych-na-temat-wannacry-analiza> (dostęp 01.06.2017r.)

Cieszę się, iż wreszcie dostrzeżono potrzebę wypracowania rekomendacji w zakresie zabezpieczeń technicznych, konfiguracji systemów, procedur bezpiecznej eksploatacji i bezpiecznego użytkowania. Opracowane rekomendacje mają dotyczyć podmiotów, które nie są lub nie będą z mocy prawa zobowiązane do stosowania określonych rozwiązań, jak również obywateli. Pierwsze ruchy już widać — na zlecenie Ministerstwa Cyfryzacji, Instytut Łączności — Państwowy Instytut Badawczy opracował materiał analityczny pod tytułem „Normy jako podstawa do opracowywania i wdrażania standardów bezpieczeństwa teleinformatycznego w projektach realizowanych przez MC w ramach Programu Operacyjnego Polska Cyfrowa”³⁶. KRPC RP obiecuje również przygotowanie polityk informacyjnych dopasowanych do potrzeb poszczególnych grup odbiorców. Obecnie rekomendacje takie dla systemów przetwarzających informacje niejawne przygotowuje ABW, kilka rekomendacji i zaleceń w zakresie przetwarzania danych osobowych przygotowało GODO. Dla administracji rekomendacjami takimi były po części zapisy Rozporządzenia 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 teleinformatycznych³⁷. Rzeczywistość jest jednak bardziej brutalna, bo jak czytamy w materiałach NIK *„W 15 urzędach, tj. 62,5% objętych kontrolą nie opracowano i nie wdrożono Polityki Bezpieczeństwa Informacji (dalej PBI), która jest elementem systemu zarządzania bezpieczeństwem informacji./.../ Nie opracowano pisemnych procedur zarządzania uprawnieniami użytkowników do pracy w systemach informatycznych w jednym a w 13 innych urzędach (54,2%) stwierdzono nieprawidłowości /.../ konta w systemach informatycznych 20 byłych pracowników (z 310 objętych badaniem) nie zostały zablokowane i pozostawały wciąż aktywne /.../ Zasady bezpiecznej pracy użytkowników przy wykorzystaniu komputerów przenośnych zgodne z wymogami określonymi w § 20 ust. 2 pkt 8 rozporządzenia KRI ustanowiono tylko w 11 urzędach (45,8%) /.../ W dziewięciu urzędach (tj. 37,5%) w okresie objętym kontrolą nie przeprowadzono audytu w zakresie bezpieczeństwa informacji w systemach informatycznych”*³⁸. Jako wzorzec dla realizowania tego zadania można wskazać na, od lat podejmujący działania w tym zakresie, wspomniany już niemiecki Bundesamt für Sicherheit in der Informationstechnik (BSI), którego strona internetowa, poza wytycznymi technicznymi zawiera szereg szczegółowych podpowiedzi praktycznych i opracowań naukowych. Stworzenie organizmu, który będzie pełnił nie tylko role koordynacyjną, ale też analityczną i badawczą na temat

³⁶ https://mc.gov.pl/files/ekspertyza_il_pib_normy_bezpieczenstwa_2016.pdf (dostęp 01.06.2017r.)

³⁷ Dz. U. z 2012 r., poz. 526 ze zm.

³⁸ „Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych...”, op. cit., s. 14 i n.

cyberbezpieczeństwa jest potrzebą chwili. On powinien tworzyć też materiały edukacyjne i służyć wsparciem dla służb i sektorów.

Drugi cel szczegółowy — **wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom**, realizowany ma być poprzez:

- zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym, występującej w cyberprzestrzeni,
- uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni,
- zbudowanie zdolności w zakresie analizy zagrożeń na poziomie krajowym,
- zbudowanie systemu bezpiecznej komunikacji na potrzeby bezpieczeństwa narodowego.

Postulaty te nie są jednak nowe i pojawiły się już wcześniej w Doktrynie cyberbezpieczeństwa BBN, która wręcz stwierdzała: *Siły Zbrojne RP powinny dysponować zdolnościami obrony i ochrony własnych systemów teleinformatycznych i zgromadzonych w nich zasobów, a także zdolnościami do aktywnej obrony i działań ofensywnych w cyberprzestrzeni. Powinny być zintegrowane z pozostałymi zdolnościami SZ RP, aby zwiększyć narodowy potencjał odstraszania (zniechęcania, powstrzymywania) potencjalnego agresora. Powinny być też gotowe, samodzielnie i we współpracy z sojusznikami, do prowadzenia operacji ochronnych i obronnych na dużą skalę w razie cyberkonfliktu, w tym cyberwojny.*³⁹

Ponadto w ramach realizacji drugiego celu zamierza się stworzyć centrum analityczne, którego rolę ma pełnić Narodowe Centrum Cyberbezpieczeństwa, którego zadaniem ma być, m.in. wymiana informacji między przedstawicielami biznesu reprezentującymi różne sektory gospodarki, każdy o innej specyfice, takiej jak infrastruktura krytyczna (transport, energia, telekomunikacja, IT, banki), a instytucjami takimi jak ZUS czy inne organy administracji publicznej, pozwalająca na szybkie reagowanie na zagrożenia i incydenty. Jeżeli jednak NCC będzie działać w strukturach NASK-u i będzie składać się z czterech pionów: badawczo-rozwojowego, operacyjnego, szkoleniowego i analitycznego⁴⁰, to niestety nie spełni roli odpowiednika niemieckiego BSI.

Kolejny element to zbudowanie bezpiecznej komunikacji. Niepokoić może to, że w KRPC RP ani słowem nie wspomina się o Narodowym Centrum Kryptologii, które realizuje zadania związane z prowadzeniem badań, projektowaniem, budową, wdrażaniem, użytkowaniem oraz ochroną narodowych technologii kryptologicznych na potrzeby polskiej administracji publicznej i wojska, a które jakieś osiągnięcia ma, skoro MON na swoich stronach internetowych informuje: *Polski zespół, koordynowany przez Narodowe Centrum Kryptologii zajął szóste miejsce wśród 20 zespołów biorących udział w przeprowadzonych w dniach 25-28 kwietnia,*

³⁹ Doktryna cyberbezpieczeństwa RP, op.cit., s. 19

⁴⁰ NCC - na straży cyberbezpieczeństwa, 04.07.2016, <https://mc.gov.pl/aktualnosci/ncc-na-strazy-cyberbezpieczenstwa> (dostęp 15.05.2017 r.)

*największych na świecie i najbardziej zaawansowanych pod kątem technicznym ćwiczeniach międzynarodowych z zakresu obrony cybernetycznej — Locked Shields.*⁴¹ Wreszcie, planowane są testy i audyty. Przewiduje się tutaj prawne uregulowanie programów bug-bounty (czyli sprawdzeń systemów bezpieczeństwa, przeprowadzanych przez hakerów zgłaszających akces do programu), które są coraz popularniejsze na świecie.

Trzeci cel szczegółowy — zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni, realizowany poprzez:

- rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa,
- zbudowanie mechanizmów współpracy między sektorem publicznym i prywatnym,
- zwiększanie kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni,
- stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli.

Znowu hasła szczytne i nośne. KRPC RP odwołuje się tutaj do Programu Cyberparku Enigma z Planu Morawieckiego⁴², co ma pozwolić na konkutowanie na rynku europejskim technologii IT. Ciekawym rozwiązaniem jest również zapowiedź hubów innowacyjnych, które mają wesprzeć polskie przedsiębiorstwa na globalnym rynku oraz zwrócenie dużej uwagi na wsparcie start-upów. W zrealizowaniu celu trzeciego ma również pomóc współpraca między sektorem państwowym i prywatnym, choć nie podano konkretnych rozwiązań w tym obszarze. Rozumiany całościowo potencjał narodowy nie może zostać zbudowany bez badań i rozwoju w obszarze bezpieczeństwa teleinformatycznego. Dlatego planuje się w ramach Narodowego Centrum Badań i Rozwoju uruchomienie programu badawczego, który będzie miał na celu przygotowanie i wdrożenie metod ochrony przed zagrożeniami pochodzącymi z cyberprzestrzeni.

Niestety obawiam się o ich realizację, czy nie będą to hasła papierowe. Przykłady projektu EPAR czy polskich technologii grafenu są bardzo wymowne.

Ostatni punkt to edukacja zarówno na poziomie eksperckim, administracji państwowej, jak i zwykłych obywateli, aby zwiększyć świadomość zagrożeń pochodzących ze świata wirtualnego. Polskim problemem jest to, że o kwestii „cyber...” w administracji decydowały przez długie lata osoby, dla których komputer był inteligentną maszyną do pisania, narzędziem do gier lub ewentualnym medium do czytania wiadomości, a zatrudnieni przez nich informatycy mieli za zadanie pilnować sprawności sprzętu, w tym głównie tego, czy w drukarce jest

⁴¹ <http://www.mon.gov.pl/aktualnosci/arttykul/najnowsze/locked-shields-2017-12017-04-28> (dostęp 15.05.2017 r.).

⁴² Plan na rzecz Odpowiedzialnego Rozwoju, Ministerstwo Rozwoju, s.24 https://www.mr.gov.pl/media/14840/Plan_na_rzecz_Odpowiedzialnego_Rozwoju_prezentacja.pdf (dostęp 15.05.2017 r.).

papier lub czy jest prąd w gniazdku. Widać to nie tylko w kwestii cyberbezpieczeństwa, ale także, a może głównie, w sferze samego zastosowania informatyki i jej możliwości. Nie wiem więc, czy bardziej potrzebny jest wzmocniony system szkoleń dla wszystkich pracowników podmiotów istotnych dla funkcjonowania bezpieczeństwa w cyberprzestrzeni, czy też system szkoleń dla decydentów, którzy zarządzają administracją.

Ciekawie też brzmi zapis *W celu zapewnienia merytorycznego wsparcia dla kierowników jednostek administracji rządowej w zakresie zarządzania cyberbezpieczeństwem utrzymana zostanie zasada powoływania w tych jednostkach Pełnomocników do spraw bezpieczeństwa cyberprzestrzeni*. To już trzecie stanowisko w administracji rządowej — po pełnomocniku ochrony (informacji niejawnych) lub podległym mu inspektorze bezpieczeństwa teleinformatycznego oraz administratorze bezpieczeństwa informacji (w ramach ochrony danych osobowych) — którego zadaniem będzie zabezpieczanie i nadzór nad bezpieczeństwem systemów informatycznych. Czy koordynatorem ich zadań będzie, mający z reguły niewielkie pojęcie o tych systemach i cyberbezpieczeństwie, kierownik jednostki administracji rządowej?

Czwarty cel szczegółowy — **zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa** realizowany ma być poprzez:

- aktywną współpracę międzynarodową na poziomie strategiczno-politycznym,
- aktywną współpracę międzynarodową na poziomie operacyjnym i technicznym.

Współpraca międzynarodowa na poziomie strategiczno-politycznym ma się oprzeć na takich organizacjach jak NATO, ONZ i UE. W przypadku Unii Europejskiej wspomniano o Wspólnej Polityce Bezpieczeństwa i Obronności, jednak na razie współpraca w zakresie cyberbezpieczeństwa w jej ramach jest ograniczona — choć może być dalej rozwijana. Dodatkowo zwrócono uwagę na ugrupowania regionalne jak Grupa Wyszehradzka czy państwa regionu Morza Bałtyckiego. Wskazuje się również na konieczność udziału polskich ekspertów w forach oraz konferencjach międzynarodowych.

W ramach współpracy operacyjno-technicznej KRPC RP wspominają o konieczności dołączenia do różnych międzynarodowych sieci CSIRT oraz aktywności na innych forach wymiany informacji i dokonywania analiz sytuacji bezpieczeństwa IT danego sektora, poprzez inne międzynarodowe sieci współpracy typu FIRST, czy TF-CSIRT, platformy wymiany informacji typu MISP, czy n6 oraz w ramach współpracy dwu- i wielostronnej. Podkreślono też konieczność opracowania wspólnych procedur działania w ramach UE i NATO oraz Grupy V4. Podkreślono także, iż współpraca na tym poziomie będzie służyła nie tylko skutecznemu przeciwdziałaniu zagrożeniom w cyberprzestrzeni, ale przyczyni się do wymiany doświadczeń pomiędzy personelem technicznym w ramach wspólnych przedsięwzięć. Będzie również okazją do promowania polskich rozwiązań technologicznych i polskiej kadry eksperckiej.

KRPC RP uchwalono na okres 5 lat. Koordynatorem wdrażania i monitorowania KRPC RP ustanowiono ministra właściwego do spraw informatyzacji. Jest

to rozwiązanie ze wszech miar słuszne. Trzeba się bowiem zgodzić ze słowami minister cyfryzacji Anny Streżyńskiej *„Wszystkie resorty, zarówno wiodące w tej dziedzinie, jak i te, które jedynie muszą zachować bezpieczeństwo, są zmuszone, żeby ze sobą współpracować. Każdy ma swoje zadania i jakąś ważną rolę do odegrania. Poza Ministerstwem Cyfryzacji, które pełni rolę koordynującą i realizuje zadania wynikające z ustawy działowej, mamy jeszcze trzy inne organy, w których obszarze działalności znajdują się zadania z zakresu cyberbezpieczeństwa. Są to MON, MSWiA z Policją i ABW. Do MON należą wszystkie kwestie związane z obroną i zagrożeniami zewnętrznymi, do MSWiA — zagrożenia przestępcze i naruszenia prawa (te wątki zwykle „kończą się” u ministra sprawiedliwości), a do ABW — ochrona infrastruktury krytycznej i państwowej. Trwają nieustanne rozmowy z tymi trzema kluczowymi resortami. Poza tym są jeszcze: BBN (doktryna obronna), KNF, NBP i wiele wspomagających instytucji. Z rozmów i uzgodnień wynika, że konieczne jest wskazanie, kto za co odpowiada. Następnie należy ująć całość problematyki w ramy wspólnego planu czy strategii i wreszcie zapewnić infrastrukturę, która będzie gwarantować bezpieczeństwo.”*⁴³ Istotnym zapisem KRPC RP jest także obowiązek poddawania ich, po dwóch latach od przyjęcia oraz w czwartym roku obowiązywania, przeglądowi i ocenie efektów oddziaływania, którego wyniki przedstawiane będą Radzie Ministrów.

Celowo pomijam punkt KRPC RP mówiący o jej finansowaniu — bo zdaję sobie sprawę, że wielokrotnie koszty dobrego zabezpieczenia przewyższają koszty zakupu infrastruktury systemu informatycznego, nie mówiąc już o kosztach osobowych. Administracja państwowa jest raczej kiepsko płatnym pracodawcą dla informatyka, a w zabezpieczeniach powinni pracować najlepsi.

Reasumując ten wątek, należy jednoznacznie stwierdzić, że powstanie dokumentu miało ogromny sens, choć w mojej ocenie jest to dokument bardzo ogólny i jego pełna ocena będzie możliwa po powstaniu *Planu działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa*, do którego opracowania minister cyfryzacji we współpracy z członkami Rady Ministrów, kierownikami urzędów centralnych, Dyrektorem Rządowego Centrum Bezpieczeństwa, jest zobowiązany w terminie do sześciu miesięcy od przyjęcia KRPC RP. Biorąc pod uwagę osobowość aktualnej minister ds. cyfryzacji, mogę mieć nadzieję, że KRPC RP nie staną się jedynie dokumentem o charakterze propagandowym — manifestującym zaangażowanie rządu polskiego w ochronę cyberprzestrzeni.

Zamiast zakończenia

Zdaję sobie sprawę, że niniejszy rozdział nie w pełni oddaje całość problemu i jest mocno przesiąknięty subiektywizmem autora. Z założenia nie miało to być

⁴³ Streżyńska dla Cyberdefence24.pl: Cyberbezpieczeństwo ma charakter cywilny, publikacja: 22 lipca 2016, <http://www.cyberdefence24.pl/415458,strezynska-dla-cyberdefence24pl-cyberbezpieczenstwo-ma-charakter-cywilny>, (dostęp 14.05.2017 r.).

opracowanie stricte naukowe, a osobiste spojrzenie osoby, która w pewnym okresie życia tej tematyce poświęciła sporo wysiłku. Żałuję, że nie wszystko się udało — szczególnie uważam, że błędem jest przerzucanie na policyjne jednostki szczebla wojewódzkiego większości zadań związanych ze ściganiem cyberprzestępczości. Do dnia dzisiejszego uważam, że jest to marnotrawienie sił i środków. W kraju o takiej wielkości jak Polska, potrzeba jest stworzenia jednego silnego ośrodka, którego zadaniem byłoby:

- ✓ monitorowanie cyberprzestrzeni;
- ✓ weryfikacja i analiza informacji operacyjnych zbieranych przez jednostki Policji;
- ✓ dokonywanie ustaleń sprawców przestępstw, popełnionych z wykorzystaniem nowych technologii informatycznych, na potrzeby zagranicznych i krajowych organów ścigania;
- ✓ zapewnianie wsparcia technicznego i merytorycznego przy realizacji działań policyjnych.

W jednostkach szczebla wojewódzkiego powinny natomiast znajdować się małe zespoły realizacyjne i pracujące operacyjnie na własnym terenie. Nawet w USA komórki do zwalczania cyberprzestępczości nie znajdują się w każdym stanie.

Kolejny element to ciągła reorganizacja i zmiany struktur, czasami argumentowana tzw. wzmocnieniem kadrowym. Wzmocnienie kadrowe jest zależne nie tylko od liczby przyznanych etatów i przypisanych doń uposażeń, bo to załatwia się jedną zdecydowaną decyzją polityczną (przydział odpowiednich środków finansowych), ale przede wszystkim doświadczeniem i wiedzą działających policjantów, których szkolenie jest naprawdę kosztowne i czasochłonne. Ponadto częste reorganizacje sprzyjają niepewności i tymczasowości wśród funkcjonariuszy, a to także nie służy efektom. Cieszy mnie natomiast to, że wreszcie dostrzeżono problem i mam nadzieję, że obecnie działający cyberpolicjanci nie mają takich problemów jak ja, kiedy nie udało mi się przekonać przełożonych — w tym dyrektora Biura Informatyki KGP, iż dla potrzeb zespołu potrzebny jest co najmniej jeden komputer z łączem do Internetu spoza puli adresów IP przypisanych do Policji lub jakichkolwiek instytucji rządowych. Pozostaje mi też satysfakcja z tego, że konferencja Techniczne Aspekty Przestępczości Komputerowej, do powstania której przyłożyłem swój niewielki kamyczek, świętuje swoje dwudziestolecie.

Bibliografia

1. Doktryna cyberbezpieczeństwa RP, BBN, 2015, <https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf>.
2. Jakubski K.J., Komputerowy nośnik informacji jako dokument w polskim procesie karnym, *Przegląd Policyjny* 1997, nr 3 (47).
3. Jakubski K.J., Przestępczość komputerowa — podział i definicja, *Problemy Kryminalistyki* 1997, nr 217.

4. Jakubski K.J., Przestępczość komputerowa — zarys problematyki, Prokuratura i Prawo 1996, nr 12.
5. Jakubski K.J., Przestępczość komputerowa: podział, definicja, możliwość jej ścigania i zapobiegania [w:] B. Hołyst (red.), Postępy Kryminalistyki, z. 1, rok 1, Warszawa-Legionowo 1997.
6. Jakubski K.J., Przestępczość komputerowa: podział, definicja, możliwości jej ścigania i zapobiegania, Postępy kryminalistyki 1997, zeszyt 1.
7. Jakubski K.J., Ściganie oszustw w Sieci (wybrane zagadnienia) [w:] T. Zasępa, R. Chmura (red.), Internet i nowe technologie- ku społeczeństwu przyszłości, Wyd. Święty Paweł, 2003.
8. Jakubski K.J., Wyłudzenie towarów i usług na podstawie numerów kart kredytowych przez Internet [w:] R. Skubisz (red.), Internet 2000 prawo — ekonomia — kultura, Vebra, Lublin 2000.
9. Mazur K.M., Polskojęzyczna społeczność przestępczość zorganizowana w sieci DARKNET, ICTLAW.pl, Poznań 2016.
10. Prokuratura i Prawo, 1997, nr 7–8.
11. Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r., Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, 2016.
12. Raport o stanie bezpieczeństwa w Polsce w 2015 r., MSWiA, <https://bip.mswia.gov.pl/download/4/29642/file.file>.
13. 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 (Dz.U. z 2016 r. poz. 113).
14. Skrzypczak J., Polityka Ochrony Cyberprzestrzeni RP, Przegląd Strategiczny, 2014, nr 7.
15. Sprawa V Ds 67/96/S Prokuratury Wojewódzkiej w Katowicach.
16. <http://dziennikustaw.gov.pl/du/2015/728>.
17. <http://kwartalnik.csp.edu.pl/kp/archiwum-1/2009/nr-12009/1097,CYBER-KRYMINALNI.html>.
18. <http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersja.pl.pdf>.
19. <http://www.cert.gov.pl/download/3/183/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2015roku.pdf>.
20. <http://www.cyberdefence24.pl/415458,strezynska-dla-cyberdefence24pl-cyberbezpieczenstwo-ma-charakter-cywilny>.
21. <http://www.mon.gov.pl/aktualnosci/arttykul/najnowsze/locked-shields-2017-12017-04-28>.
22. <http://www.policja.pl/pol/kgp/bsk/struktura/wydzialy/wydzial-do-walki-z-cybe/87086,Wydzial-doWalki-z-Cyberprzestepczoscia.html>.