# Cyberbezpieczeństwo wyzwaniem XXI wieku

Redakcja naukowa
Tomasz Dębowski

ArchaeGraph
*Wydawnictwo Naukowe*

# Cyberbezpieczeństwo wyzwaniem XXI wieku

# Cyberbezpieczeństwo wyzwaniem XXI wieku

Redakcja naukowa
Tomasz Dębowski

ARCHAEGRAPH
*Wydawnictwo Naukowe*

**Redakcja naukowa**
Tomasz Dębowski

**Recenzent**
Prof. UZ dr hab. Piotr Kwiatkiewicz
Uniwersytet Zielonogórski

**Skład i korekta redakcyjna**
Karol Łukomiak

**Projekt okładki**
Karol Łukomiak



ISBN: 978-83-66035-02-7 (Książka)
ISBN: 978-83-66035-03-4 (Ebook)

ArchaeGraph
*Wydawnictwo Naukowe*

Łódź – Wrocław 2018

# Spis treści

# WSTĘP

Tom *Cyberbezpieczeństwo wyzwaniem XXI wieku* jest opracowaniem, które wpisuje się w kontekst rozważań poświęconych wielorakim aspektom bezpieczeństwa w cyberprzestrzeni. Autorzy, którzy zostali zaproszeni do realizacji tego projektu, prezentują różne spojrzenia na tę problematykę.

Pomysłodawcą pierwszego rozdziału – *Główni aktorzy cyberprzestrzeni i ich działalność* jest Tomasz Hoffman. Autor, piszący z perspektywy prawno-politologicznej, posiłkujący się dorobkiem nauk o bezpieczeństwie, koncentruje się na ukazaniu potencjalnych aktorów cyberprzestrzeni, ich działalności, a w tym również zachowań niezgodnych z prawem. Cyberbezpieczeństwo, zdaniem Hoffmana, jest nową dziedziną bezpieczeństwa narodowego, z którą nieodłącznie wiążą się takie wyzwania, jak cyberprzestępczość oraz cyberterroryzm.

Drugi rozdział – *Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa* – wyszedł spod pióra Marka Górki. Badacz dokonał przeglądu aktualnego stanu bezpieczeństwa cybernetycznego w kontekście rozprzestrzeniania się zagrożeń pochodzących z cyberprzestrzeni, tworzonych przez organizacje państwowe oraz niepaństwowe. Górka stoi na stanowisku, że cyberprzestrzeń stała się podstawową cechą świata i stworzyła nową rzeczywistość dla prawie wszystkich krajów, co sprawia, że problemy z cyberprzestępczością oraz cyberbezpieczeństwem mają istotne, globalne znaczenie zarówno w wymiarze politycznym, jak i gospodarczym.

Z przemyśleniami Górki koresponduje tekst Bogusława Węglińskiego – *Cyberterroryści w cyfrowych czasach – profesjonalizacja i digitalizacja współczesnych organizacji terrorystycznych*. Autor poddał analizie ewoluujące wraz z rozwojem technologii instrumentarium wykorzystywane przez grupy terrorystyczne, zwracając uwagę na Internet, który otworzył przed nimi nowe możliwości oddziaływania, a w tym także w sferze kreowania przekazu medialnego. W tekście zawarte są również dociekania dotyczące możliwości użycia przez terrorystów dronów.

Nadmieńmy, że także czwarty rozdział *Ataki cyber-fizyczne a system bezpieczeństwa narodowego*, którego autorem jest Bogusław Olszewski, wpisuje się w nurt wcześniejszych dociekań. W tej części tomu poruszone zostały sprawy związane z niepożądanym oddziaływaniem systemów cyber-fizycznych na bezpieczeń-

stwo otoczenia międzynarodowego. Zdaniem Olszewskiego, ich hybrydowy (cyfrowo-materialny) charakter sprawia, że wpływają nie tylko na logiczną warstwę cyberprzestrzeni, ale także na dziedzinę fizyczną. Umożliwiają m.in. destabilizację porządku wewnętrznego państwa, co w konsekwencji może prowadzić do destrukcyjnych zmian w szerszym, międzynarodowym kontekście. Stanowią zatem wielowymiarowe zagrożenie dla szeroko pojętego systemu bezpieczeństwa globalnego

W rozdziale piątym, Marcin Adamczyk przedłożył tekst *Cyberszpiegostwo w relacjach chińsko-amerykańskich w kontekście potencjalnej zmiany światowego hegemona*. Opracowanie poświęcone jest działaniom Chińskiej Republiki Ludowej w cyberprzestrzeni, ukierunkowanych na nielegalne pozyskanie amerykańskich technologii wojskowych i cywilnych. Zdaniem autora, Państwo Środka jest aktualnie jedynym krajem, który obecnie mógłby rzucić wyzwanie dominacji Stanów Zjednoczonych. Dążenie do uzyskania statusu państwa hegemonicznego wymaga zatem od Pekinu zbudowania odpowiedniej koalicji wspierającej Chiny na arenie międzynarodowej, ale również zmniejszenia dystansu ekonomicznego, jaki dzieli to państwo od Waszyngtonu.

Autorem kolejnego rozdziału jest Kamil Baraniuk, którzy przygotował tekst *Zarys przemian instytucjonalnych rosyjskiego wywiadu radioelektronicznego*. Baraniuk podkreśla, że współczesny wysoki stopień zinformatyzowania społeczeństw i powszechności korzystania z technologii informatycznych sprawia, iż dane o charakterze sygnałowym i elektromagnetycznym stanowią bardzo istotne źródło informacji dla wyspecjalizowanych instytucji, zajmujących się ich gromadzeniem oraz przetwarzaniem. W tym kontekście zarysowuje genezę i przekształcenia instytucjonalne wywiadu radioelektronicznego Federacji Rosyjskiej, a co za tym idzie wojskowe i cywilne instytucje zajmujące się tego rodzaju działalnością na przestrzeni ostatnich kilkudziesięciu lat, przy uwzględnieniu ich zadań, a także zmian personalnych w ich kierownictwie.

Rozdział siódmy napisany został przez dwie autorki z Ukrainy. Tetiana W. Nagachevskaya i Lyudmila Frliksowa przygotowały rozważania zatytułowane *Napriamky formuwannia miżnarodnoji konkurentospromożnosti IT-sektoru Ukrajiny*. Zawierają one analizę stanu i osobliwości kształtowania się międzynarodowej konkurencyjności sektora IT na Ukrainie. Nagachevskaya i Frliksowa zaprezentowały pozycję ukraińskiego sektora IT rozpatrywaną w kontekście *Networked Readiness Index*, który mierzy skłonność do wykorzystywania przez kraje możliwości oferowanych przez technologie informacyjno-komunikacyjne. Ponadto, ukazały

przewagę konkurencyjną i wady ukraińskich firm IT na rynkach międzynarodowych oraz kierunki wzrostu międzynarodowej konkurencyjności sektora informatycznego Ukrainy.

Kolejne dwa rozdziały dotykają problematyki religijnej w cyberprzestrzeni. Autorem dociekań – *Religijne i parareligijne grupy destrukcyjne: wyzwania cyberprzestrzeni* – jest Wojciech Gajewski, który zwraca uwagę na sprawę penetrowania wirtualnej przestrzeni przez destrukcyjne grupy religijne. Jego zdaniem, stanowią one wzrastające zagrożenie nie tylko dla jej indywidualnych użytkowników, ale także zbiorowości społecznych. Religioznawca jest zwolennikiem podejmowania szeroko zakrojonych działań badawczych, edukacyjnych, a także prawnych, które wpłyną na ograniczenie negatywnych następstw ich aktywności w cyberprzestrzeni. Z kolei, Lucjan Klimsza przedłożył tekst *Filozoficzne aspekty działania Internetu w kontekście zadań misyjnych Kościoła*. Autor, który jest duchownym ewangelickim, zwraca uwagę na możliwości, jakie otwiera przed współczesnym chrześcijaństwem dostęp do przestrzeni cyfrowej. Klimsza wyraźnie zaznacza, że obecny Kościół musi być wspólnotą multimedialną, jednakże nie wirtualną, która jest oddalona od człowieka i jego realnej egzystencji. Autor, Internet postrzega zatem jako metamedium umożliwiające przekazywanie treści religijnych, które może być pomocne m.in. w spotkaniu i relacjach człowieka z człowiekiem oraz Boga z człowiekiem.

Dziesiąty rozdziały *Cyberbezpieczeństwo jako konstrukt w polskiej przestrzeni publicznej*, będący rozważaniami o nachyleniu politologicznym, napisał Przemysław Mikiewicz. Tekst jest refleksją nad obecnością kategorii cyberbezpieczeństwa w polskiej przestrzeni publicznej, którą autor zawęził do opiniotwórczego oddziaływania centralnych instytucji państwowych oraz partii politycznych. Autor wskazuje, że pojęcie cyberbezpieczeństwa jest obecne w polskiej przestrzeni publicznej w różnym stopniu w dokumentach rządowych i w programach partii politycznych. Zdaniem Mikiewicza, występuje zasadnicza asymetria pomiędzy oboma typami dokumentów: dokumenty urzędowe poświęcają uwagę cyberbezpieczeństwu w znacznym stopniu, podczas gdy w dokumentach partyjnych kwestia ta jest jedynie wzmiankowana. Tak więc, cyberbezpieczeństwo jawi się jako rodzaj konstruktu, za pomocą którego kreowany jest obraz świata pełnego nienamacalnych niebezpieczeństw, do zwalczania których nieodzowne wydaje się publikowanie dokumentów pod postacią kolejnych doktryn i strategii walki z zagrożeniami w cyberprzrestrzeni.

W nurt rozważań politologicznych wpisują się także dwa kolejne teksty. Autorem pierwszego jest Grzegorz Tokarz, którego dociekania zostały zatytułowane

*Internet jako instrument nawoływania do przemocy – przykład organizacji „Krew i Honor" Polska*. Tekst przybliża działalność polskiej sekcji neonazistowskiej organizacji „Krew i Honor", a w tym zawartość jej strony internetowej, która jest istotnym narzędziem w propagowaniu idei tego środowiska, jak również źródłem informacji o osobach oraz instytucji uznawanych za zdrajców „białej rasy".

Drugi tekst, który zarazem kończy niniejszy tom przygotował Mariusz Kozerski. W rozdziale *Dawne afery polityczne ze współczesnej perspektywy: przykład sprawy Barschela/Pffeifera* analizowana jest rola, jaką media odgrywają w nagłaśnianiu afer politycznych. Autor poddał oglądowi wydarzenia, które rozegrały się w latach 80 XX wieku, w północnoniemieckim landzie Szlezwik-Holsztyn, a w których ważną rolę odegrał opiniotwórczy tygodnik „Der Spiegel". Dodajmy, że Kozerski podejmuje się również próby odpowiedzi na pytanie, w jaki sposób afera kilońska mogłaby przebiegać współcześnie, w kontekście potencjału informacyjnego/opiniotwórczego, którym charakteryzuje się globalna sieć komputerowa.

*Tomasz R. Dębowski*

**Tomasz Hoffmann**

Politechnika Koszalińska

# Głowni aktorzy cyberprzestrzeni i ich działalność

Słowa kluczowe: cyberprzestrzeń, cyberatak, cyberterroryzm, cyberprzestępstwo.

## Wprowadzenie

Problematyka ochrony cyberprzestrzeni stała się ostatnio bardzo licznie eksplorowana przez różnych badaczy zarówno przedstawicieli politologii, prawników, ekonomistów czy informatyków. W zainteresowaniu znalazły się główne przesłanki powstawania różnych zjawisk w tym czynów o charakterze przestępczym, które zostały popełnione w związku z naruszeniem podstawowych zasad funkcjonowania w cyberprzestrzeni. Zjawiska te generują liczne patologie a także sprzyjają powstaniu nowych typów czynów zabronionych. Niniejszy tekst koncentruje się wokół prezentacji głównych aktorów cyberprzestrzeni i ich działalności na różnych forach w obszarze szeroko rozumianej sieci informatycznej.

Problemem badawczym są główni aktorzy penetrujący cyberprzestrzeń i podejmowane przez nich określone działania. Hipoteza badawcza koncentruje się wokół założenia iż aktorów cyberprzestrzeni można podzielić na indywidualnych i instytucjonalnych, z których liczni wykorzystują globalną sieć działań kryminogennych, dlatego należy wdrożyć procedury prewencyjno-edukacyjne aby potencjalny korzystający z sieci wiedział jak ma postępować aby nie stać się ofiarą cyberprzestępcy.

Artykuł ma charakter chronologiczno-problemowy. Pisząc go wykorzystano metody zarówno jakościowe jak i ilościowe. W szczególności oparto się na śledzeniu mechanizmów przyczynowości - *process tracing*, która jest stosowana w naukach o polityce a swoje źródło czerpie z psychologii. Pozwala ona badaczowi

zbliżyć się do potencjalnych mikrofundamentów, obserwowanych zjawisk związanych z działalnością aktorów cyberprzestrzeni.

## Cyberprzestrzeń i jej aktorzy

O tym że ataki w sieci stały się coraz bardziej prawdopodobne świadczą liczne publikacje a także wydarzenia, mające miejsce w Polsce czy innych krajach[1]. Fakt ten wynika z rozwoju społeczeństwa informacyjnego, połączonego z doskonaleniem i upowszechnieniem rozwiązań informatycznych, telekomunikacyjnych co powoduje, przenoszenie określonych obszarów ludzkiej działalności ze świata realnego w cyberprzestrzeń.

Główne cechy cyberprzestrzeni to globalny zasięg, wydajność, uniwersalność i w zasadzie taniość w dostępie. Czynniki te powodują że kolejne dziedziny życia społecznego są przenoszone do świata wirtualnego. Można przyjąć że obecnie bezpieczeństwo w tzw. cyberprzestrzeni stało się istotnym elementem aktywności polskich służb specjalnych. W świecie tak dynamicznych zmian, można zauważyć że wiele działań o charakterze destrukcyjnym czy wywiadowczym jest przenoszonych do świata wirtualnego. Obiektem ingerenci stają się sprzęt komputerowy czy elementy infrastruktury telekomunikacyjnej co ułatwia przejęcie danych niekiedy o charakterze wrażliwym. O tym że cyberprzestrzeń jest bardzo wrażliwa i jednocześnie podatna na wszelkiego rodzaju zagrożenia przekonują się zarówno organy państwa jak i przeciętni obywatele.

Niestety póki co świadomość tych ostatnich jest dosyć mglista o tym jakie mogą być konsekwencje bycia ofiarą w cyberprzestrzeni, zwłaszcza że ludzie nie wyobrażają sobie codziennego funkcjonowania bez korzystania z cyberprzestrzeni. Korzystają z portali społecznościowych[2], które pojawiły się w Polce w XXI wieku. Od początku zaczęły cieszyć się dość dużym uznaniem. Liczba odwiedzających z dnia na dzień radykalne zwiększała się. Szczególne zainteresowanie portali społecznościowych budziło u ludzi młodych, którzy zazwyczaj wybierają to, co nowe. W Polsce pierwszym portalem społecznościowym, który budził zainteresowanie była „NK"[3] a później Facebook i Twiterr.

[1] K. Rokiciński, *Wymagania w zakresie współpracy cywilno-wojskowej (CI-MIC) w czasie planowania i przygotowania działań w pasie nadmorskim RP*, II Konferencja „Zarządzanie Kryzysowe", Szczecin 18 czerwca 2004.

[2] Przykładem może być popularny Facebook.

[3] Obecne jako NK.

Portale te zaczęli również efektywnie wykorzystywać politycy. Co niektórzy prowadzili nawet kampanie wyborcze z wykorzystaniem technik interaktywnych na portalach społecznościowych. Na portalach społecznościowych istnieje wiele metod i form komunikacji, do których zalicza się przede wszystkim fora, blogi, fora dyskusyjne[4].

Ludzie korzystają także z poczty elektronicznej, różnych typów komunikatorów, cyfrowych bibliotek, łączności bezprzewodowej oraz wirtualnych środków finansowych. Zauważyć należy że możliwości cyberprzestrzeni ulegają ciągłemu rozwojowi i pojawia się coraz więcej bardziej doskonałych i innowacyjnych rozwiązań teleinformatycznych[5].

Oprócz pozytywnych aspektów związanych z cyberprzestrzenią można znaleźć także elementy negatywne. Możliwości jakie stwarza komunikacja elektroniczna oparta na zaawansowanych technologiach cyfrowych powoduje że pojawia się nowa grupa złodziei, chuliganów, terrorystów czy nawet szpiegów. Osoby te uważają że cyberprzestrzeń daje im poczucie anonimowości, co determinuje ich do podejmowania różnych działań bardzo często niezgodnych z porządkiem prawnym. Można zatem wyróżnić kilka kategorii osób, które stanowią swoiste zagrożenie dla cyberprzestrzeni. Są to:

- Cyber-chuligani - najczęściej to pojedyncze osoby lub niewielkie grupy prowadzące określone działania w celu sprawdzenia swoich umiejętności, dokonania jakiegoś czynu zabronionego czy odwetu na innych.
- Cyber-aktywiści - to grupy osób, które prowadzą działania w celu wsparcia jakiejś idei. Propagują ją poprzez rozpowszechnianie spektakularnych działań o dość dużym zasięgu i zakresie i najczęściej godzą w czyjś wizerunek.
- Cyber-przestępcy - pojedyncze osoby lub grupy osób, które prowadzą działania dla korzyści majątkowej lub osobistej, dokonują przeważnie klasycznych czynów przestępnych takich jak oszustwa, kradzieże, wyłudzenia z wykorzystaniem metod i narzędzi dostępnych w wirtualnym świecie.
- Cyber-terroryści - pojedyncze osoby, lub grupy osób lub organizacje polityczne prowadzące działania w cyberprzestrzeni dla wsparcia swoich egoistycznych często politycznych celów, dążą do ich osiągnięcia poprzez stosowanie różnych form zastraszania i wywoływania stanu zagrożenia.

[4] P. Frankowski, A. Juneja, *Serwisy społecznościowe. Budowa, administracja i moderacja*, Gliwice 2009, s. 23.
[5] *Ibidem*, s.25.

Osoby te wykorzystują cyberprzestrzeń jako narzędzie komunikacji, propagandy, gromadzenia środków finansowych oraz werbunku i prowadzenia różnych szkoleń.

- Cyber- szpiedzy -organizacje lub przedsiębiorstwa[6] pracujące na rzecz biznesu lub resortów siłowych prowadzące działania w cyberprzestrzeni głównie w celu skrytego pozyskania wiedzy lub wywarcia wpływu. Wiele państw[7] na szeroką skalę wykorzystuje cyberprzestrzeń do takich celów, bowiem jest to niezwykle tania, efektywna i łatwa do ukrycia forma działalności o charakterze wywiadowczym.
- Cyber - żołnierze - to najczęściej organizacje najemnicze lub oddziały wojskowe przeznaczone do prowadzenia działań zbrojnych w cyberprzestrzeni traktowanej jako arena działań wojennych[8].

Każdy w wymienionych aktorów może mieć swój zarówno pozytywny jak i negatywny udział w cyberprzestrzeni. Aby mówić o negatywnym udziale w cyberprzestrzeni należy przyjąć że osoby takie mogą dopuścić się popełnienia określonego przestępstwa - cybeprzestępstwa. Pojęcie to jest zamachem na bezpieczeństwo elektronicznie przetwarzanej informacji, czyli przestępstwem przeciwko poufności, integralności i dostępności danych i systemów informatycznych. W Polsce jak i w innych państwach Unii Europejskiej tego typu zachowania są ścigane przez odpowiednie organy.

## Kryminalizacja działań w cyberprzestrzeni

W polskim kodeksie karnym przestępstwa przeciwko informacji zostały stypizowane w rozdziale XXXIII - przestępstwa przeciwko ochronie informacji[9]. Przestępstwo takie można popełnić w zasadzie wyłącznie umyślnie, z kolei jeśli chodzi o stadialność przestępstwa to zarówno usiłowanie oraz dokonanie są karalne[10]. Karalnym nie jest stadium przygotowania[11]. Pierwszym typem przestępstwa jest hac-

[6] Niezależnie od formy prawnej.
[7] W tym szczególnie Chiny, USA , czy też Rosja.
[8] *Informacja o wynikach kontroli Realizacja przez podmioty państwowe zadań z zakresie ochrony cyberprzestrzeni RP*, Warszawa 2015, s. 20.
[9] M. Budyn-Kulik, *et al.*, red. M. Mozgawa , *Kodeks karny: komentarz*, Warszawa 2014.
[10] Art 14 *Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, Dz.U. 1997, Nr 88, poz. 553*; Karane są również współsprawstwo, sprawstwo kierownicze, podżeganie oraz pomocnictwo.
[11] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2010.

king, którego penalizacja została określona w art. 267 kodeksu karnego. Przestępstwo to polega na włamaniu się do systemu komputerowego, sieci komputerowej, pokonując tym samym zabezpieczenia[12]. Uzyskanie dostępu do informacji musi mieć charakter nielegalny a zatem osoba dokonująca tego przestępstwa musi działać nielegalnie. Drugą kwestią jest fakt że informacje do których włamuje się sprawca nie są z oczywistych względów dla niej przeznaczone. Penalizowane są zachowania polegające na nielegalnego podłączenia się do sieci telekomunikacyjnej a także stosowanie urządzeń podsłuchowych, wizualnych bądź innych[13]. Zabroniony jest w szczególności podsłuch transmisji w sieci tzw. sniffing oraz spoofing, czyli podszywanie się pod system uznany przez system atakowany za godny zaufania[14].

Kolejne przepisy sankcjonujące naruszenie porządku w cyberprzestrzeni dotycząc naruszenia integralności komputerowego zapisu informacji poprzez usunięcie, modyfikację lub uszkodzenie plików[15]. Obecnie znamiona wyczerpujące tego typu zachowanie zostały uregulowane w art. 268 i 268 a. Pierwszy z nich sankcjonuje niszczenie, uszkadzanie, usuwanie lub zmianę zapisu istotnej informacji lub udaremnianie bądź utrudnianie osobie uprawnionej do zapoznania się z informacją[16]. Za tego typu czyn ustawodawca przewiduje grzywnę, karę ograniczenia wolności lub karę pozbawienia wolności do lar dwóch. Z kolei jeśli czyn dotyczy zapisu na informatycznym nośniku danych, ustawodawca przewiduje karę pozbawiania wolności do lat trzech[17]. W przypadku kiedy sprawca dodatkowo swoim działaniem wyrządza szkodę majątkową może podlegać karze pozbawienia wolności od trzech miesięcy do lat pięciu[18].

[12] *Ibidem*; Przełamanie zabezpieczeń to każda czynność, która ma niejako „otworzyć" sprawcy dostęp do informacji; może polegać na usunięciu zabezpieczenia przez jego zniszczenie lub też na oddziaływaniu na zabezpieczenie w celu zniwelowania jego funkcji ochronnej, jednakże bez zniszczenia go.
[13] P. Kozłowska-Kalisz, *Komentarz do art. 267 kodeksu karnego*, [w:] M. Budyn-Kulik, *et al.*, red. M. Mozgawa, *Kodeks …*, s. 976 i n.
[14] A. Suchorzewska, *op. cit.*, s. 120-200.
[15] *Ibidem.*
[16] Art 268 § 1 *Ustawy z dnia 6 czerwca 1997 r. …*
[17] Art. 268 § 2 k.k. pośrednio chroni także integralność programów komputerowych, jednakże tylko wówczas, gdy następstwem nieuprawnionej ingerencji w kod programu jest udaremnienie lub znaczne utrudnienie dysponentowi informacji lub innej osobie uprawnionej zapoznania się z tą informacją Tym samym nie każde zawirusowanie systemu informatycznego lub jego nieuprawniona rekonfiguracja narusza dyspozycję tego artykułu.
[18] Art 268 § 3 *Ustawy z dnia 6 czerwca 1997 r. …*

Przestępstwo to ma charakter wnioskowy a zatem ścigane jest na wniosek pokrzywdzonego[19]. Reasumując przepis ten chroni integralność zapisu oraz dostępność informacji istotnej zatem nie każdej jakby się wydawało. Informacja musi być istotna w znaczeniu obiektywnym z tego względu ocena owej istotności uzasadnia określony interes dysponenta informacji a także interes podmiotu, którego dana informacja dotyczy[20].

Kolejnym artykułem który penalizuje integralność komputerowego zapisu informacji jest artykuł 268 a k.k. który mówi iż kto niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenia lub przekazywanie takich danych podlega karze pozbawienia wolności do lat trzech[21].Jeżeli sprawca dodatkowo wyrządza szkodę majątkową podlega karze pozbawienia wolności od trzech miesięcy do pięciu lat. Przestępstwo to jest również ścigane na wniosek pokrzywdzonego[22].

Reasumując zamachy na integralność komputerowego zapisu informacji mogą w istocie rzeczy powodować znaczące szkody zarówno o charakterze społecznym jak i finansowym. W związku z powyższym słusznie ustawodawca penalizuje tego typu czyny. Następnymi przepisami, które sankcjonują naruszenie cyberprzestrzeni jest zjawisko sabotażu komputerowego opisane w art. 269-269 a kodeksu karnego.

Pierwszy artykuł penalizuje niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej lub instytucji państwowej w tym samorządu terytorialnego. Sankcjonowane jest również zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych o istotnym znaczeniu dla państwa. W takiej sytuacji sprawa podlega karze pozbawienia wolności od sześciu miesięcy do ośmiu lat[23].

Drugi przepis penalizuje zachowanie osoby, która nie będąc do tego uprawniona, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych w znaczącym stopniu zakłócą pracę systemu lub sieci komputerowej[24]. W takim przypadku sprawca tego czynu podlega karze

[19] Art 268 § 4 *Ustawy z dnia 6 czerwca 1997 r. …*
[20] A. Suchorzewska, *op. cit.*, s. 120-200.
[21] Chodzi o osobę, która nie jest do tego uprawniona.
[22] Art 268 a § 2-3 *Ustawy z dnia 6 czerwca 1997 r. …*
[23] Art 269 § 1 *Ustawy z dnia 6 czerwca 1997 r. …*
[24] Ustawodawca nie penalizuje zachowań na przykład polegających na atakach DoS (*Denial of Service*) skierowanych nie przeciwko serwerom należącym do podmiotów ze sfery publicznej, lecz przeciwko podmiotom prawa prywatnego.

pozbawienia wolności od trzech miesięcy do pięciu lat[25]. Zaznaczyć należy że pod względem technicznym sabotaż komputerowy obejmuje również swoim zakresem takie zjawiska jak przesyłanie wirusów i robaków komputerowych, bomb logicznych i ataków DoS[26].Przepisy artykułów 268a i 269 kodeksu karnego są odzwierciedleniem regulacji zawartej w decyzji ramowej Unii Europejskiej, zmienionej dyrektywą[27], co jest wynikiem procesu europeizacji top-down w zakresie prawa karnego. Omawiane artykuły zawarte w polskim kodeksie karnym dotyczące sabotażu komputerowego są do siebie podobne, bowiem obydwa chronią dane informatyczne, ponadto penalizują ingerencję w systemem informatyczny[28] co jest tożsame w regulacjami międzynarodowymi w tym obszarze.

Polski ustawodawca sankcjonuje bezprawne wykorzystywanie programów i danych. Wprowadzenie tego przepisu jest konsekwencją dostosowania polskich przepisów do regulacji zwartych w konwencji Rady Europy o cyberprzestepczości[29]. Ustawodawca przyjmuje że kto wytwarza, zbywa, lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia określonego przestępstwa ponadto udostępnia hasła komputerowe, kody dostępu lub inne dane komputerowe, które umożliwiają dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej podlega karze pozbawienia wolności do trzech lat[30].

Wprowadzenie do porządku prawnego kryminalizacji tego typu zachowań ma zarówno pewne wady jak i zalety. Do wad zaliczyć można trudność z egzekwowaniem produkcji i rozpowszechniania narzędzi hackerskich, duże koszty związane z wprowadzeniem odpowiednich regulacji w życie oraz trudności z dokładnym określeniem zakresu dozwolonego użytku. Z kolei zaletami tego przepisu są podkreślenie wysokiej szkodliwości takich czynów, wpływ na zmniejszenie ilości ataków skierowanych przeciwko bezpieczeństwu informacji[31]. Przepis ten może również stanowić podstawę do skutecznego i sprawnego ścigania tego rodzaju przestępstw i osób dopuszczających się takowych czynów zabronionych. Kolejną grupę

[25] Art 269 a *Ustawy z dnia 6 czerwca 1997 r. …*
[26] A. Suchorzewska, *op. cit.*, s. 150-160.
[27] *Decyzja Ramowa 2005/222/WE Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dziennik Urzędowy Unii Europejskiej, L 218/8.*
[28] Por. *Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestepczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r.*
[29] *Ibidem*.
[30] Art 269 b *Ustawy z dnia 6 czerwca 1997 r. …*
[31] Por. A. Suchorzewska, *op. cit*., s. 200-202.

przestępstw popełnianych za pomocą komputerów, godzącą w cyberbezpieczeństwo stanowią: oszustwo z wykorzystaniem komputera, oszustwo telekomunikacyjne, przestępstwa przeciwko wiarygodności dokumentów z wykorzystaniem komputera, fałszerstwo komputerowe, nielegalne uzyskanie programu komputerowego, paserstwo programu komputerowego, szpiegostwo komputerowe oraz sprowadzenie niebezpieczeństwa o charakterze powszechnym na skutek zakłócenia procesów automatycznego przetwarzania danych[32].

Jednym z przepisów kodeksu karnego kryminalizującym przestępstwo sprowadzania niebezpieczeństwa dla życia lub zdrowia wielu osób albo mienia w wielkich rozmiarach poprzez zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych jest art. 165 k.k[33]. Ustawodawca w takiej sytuacji wprowadza podstawową sankcję w postaci kary pozbawienia wolności od sześciu miesięcy do ośmiu lat. W przypadku kiedy sprawca działa nieumyślnie, sankcja jest łagodniejsza w postaci kary pozbawienia wolności od lat trzech. Szczególne obostrzenie kary ma miejsce w przypadku kiedy następstwem czynu jest śmierć człowieka lub ciężki uszczerbek na zdrowiu wielu osób, kara może wynieść od 6 miesięcy do dwunastu lat pozbawienia wolności[34]. Ściganie tego typu przestępstwa następuje z oskarżenia publicznego, nie jest to więc przestępstwo wnioskowe.

Przestępstwa w sieci można dokonać również naruszając wiarygodność dokumentów. Choć pojęcie dokumentu jest bardzo szerokie i zazwyczaj pojęcie to jest często jak podają autorzy stosowane w życiu codziennym, to jest to dość szeroko znaczeniowo termin. W słowniku języka polskiego za dokument uważa się:

- wszelki przedmiot stwierdzający prawdziwość czegoś; pismo stwierdzające coś, skrypt; dowód[35],
- czynny dowód[36],
- zapewnienie, wyznanie[37].

[32] *Ibidem*, s. 200-230.

[33] Penalizuje on sprowadzanie niebezpieczeństwa, które powoduje zagrożenie epidemiologiczne, lub szerzenie się choroby zakaźnej, wprowadzanie do obrotu szkodliwych substancji, uszkodzenie lub unieruchomienie urządzeń użyteczności publicznej. Szczególnie Art. 165§ 1 pkt. 4 Ustawy z dnia 6 czerwca 1997 r. …

[34] Art 165 § 3-4 *Ustawy z dnia 6 czerwca 1997 r.* …

[35] Na przykład opierać się na dokumentach, składać nowe dokumenty.

[36] Na przykład już w młodości dawał wiarygodne dokumenty swojej bezduszności.

[37] J. Karłowicz, A. Kryński, W. Niedźwiecki (red), *Słownik Języka Polskiego*, t. 1, Warszawa 1900, s. 496: za K. Knoppek, *Dowód w procesie cywilnym*, Poznań 1993, s.11.

W minionym czasie jak podaje K. Knoppek w okresie dziejów języka polskiego dokumentami były wszelkie przedmioty i zachowania, które coś stwierdzały lub potwierdzały. W XX wieku w słownikach języka polskiego zamieszczano definicje dokumentu, które koncentrowały się na stwierdzeniu że dokumentem jest akt urzędowy, pismo urzędowe, lub dowód, świadectwo prawdziwości jakiegoś faktu[38]. Z kolei ten sam autor wskazuje że w Słowniku języka polskiego z 1978 roku, dokument to pismo urzędowe, akt spisany w celu stwierdzenia jakiejś okoliczności, dowód, świadectwo prawdziwości jakiegoś faktu, w liczbie mnogiej – dowód stwierdzający tożsamość, dowód osobisty, legitymacja, paszport[39].

W dzisiejszym słowniku języka polskiego za dokument uważa się:

- pismo urzędowe, akt spisany w celu stwierdzenia jakiejś okoliczności, np. nadania czegoś, zawarcia umowy o coś, zobowiązania do czegoś itp.,
- dokument notarialny.
- dokument erekcyjny szpitala,
- dowód, świadectwo prawdziwości jakiegoś faktu,
- złożenie, włączenie ważnego dokumentu do akt sprawy,
- przedstawienie dokumentów stwierdzających niewinność oskarżonego,
- przedstawienie czegoś co stanowi dokument naukowy,
- zabytki przedhistoryczne które są cennymi dokumentami naukowymi
- a nadto dokument epoki dzieło, fakt, wydarzenie charakterystyczne dla danej epoki
- w innym znaczeniu zwykle w licznie mnogiej dowód stwierdzający czyjąś tożsamość; dowód osobisty, legitymacja, paszport,
- ostatnie znaczenie to film dokumentalny, dokument pełnometrażowy, telewizyjny[40].

Od dokumentu w znaczeniu potocznym należy odróżnić dokument jako termin przyjęty w naukoznawstwie i informacji naukowej. W znaczeniu ogólno-naukowym dokument to materialnie utrwalony obraz myśli ludzkiej. Tak rozumiane dokumenty dzielą się na dokumenty graficzne, audialne, wizualne i audiowizualne. Wśród dokumentów graficznych wyróżnia się dokumenty piśmienne[41]. Z kolei wg innych dokumentem jest każdy przedmiot materialny , który wyraża myśl ludzką

[38] W. Doroszewski (red), *Słownik języka polskiego*, t. 2, Warszawa 1965, s. 221-222, za:K. Knoppek, *op. cit.*, s.11.
[39] M .Szymczak (red), *Słownik języka polskiego*, t. 1, Warszawa 1978, s. 418.
[40] *Słownik Języka Polskiego PWN*, Warszawa 2006, s. 132-133.
[41] M. Dembowska, *Słownik terminologiczny informacji naukowej*, Warszawa 1974, s. 158 za: K. Knoppek, *op. cit.*, s.12.

lub służy do udowodnienia prawdziwości twierdzeń sformułowanych w toku badań naukowych[42].

Jak zatem można zauważyć pojęcie dokumentu jest wieloznaczne. Występuje praktycznie w każdej dziedzinie naukowej stanowiąc w pewnym sensie dowód poznania naukowego. Również o czym dalej będzie wspominane dokument pełni szczególną rolę w prawie. Mimo tego każda ingerencja w treść dokumentu, w tym dokumentu elektronicznego polegająca na jego podrobieniu lub przerobieniu przez osobę do tego nieuprawnioną i działającą w zamiarze posłużenia się tym dokumentem wyczerpuje znamiona określone w kodeksie karnym. Przyjmuje on że osoba taka polega karze grzywny, ograniczenia wolności albo pozbawienia wolności od 3 miesięcy do lat pięciu[43].

Zaznaczyć należy że w prawie polskim brak jest ustawowej definicji dokumentu elektronicznego. Posiłkowo stosując jednak przepisy kodeksu karnego można przyjąć że dokumentem jest każdy przedmiot lub inny nośnik informacji, z którym związane jest określone prawo, albo który ze względu na zawarta w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mających znaczenie prawne[44].

Do przestępstw tej kategorii można również zaliczyć wyłudzanie numerów kart płatniczych, przechwytywanie ich numerów[45] w sposób oczywisty i nielegalny[46], czy wprowadzanie do obiegu fałszywych kart płatniczych[47]. Wśród przestępstw przeciwko wiarygodności dokumentów należy wymienić sytuacje w której osoba składa bezpieczny podpis elektroniczny za pomocą danych służących do składania podpisu elektronicznego, które zostały przeznaczone do innej osoby podlega grzywnie albo karze pozbawienia wolności do trzech lat lub łącznie obu karom[48]. Wydaje się że warunkiem złożenia skutecznie podpisu elektronicznego w imieniu innej osoby jest wejście w posiadanie jej klucza prywatnego. W związku z tym trzeba posiadać kartę kryptograficzną z zapisanym na niej kluczem prywatnym da-

[42] *Wielka Encyklopedia Powszechna*, t. 3, Warszawa 1983, s. 89.
[43] Art 270 § 1 *Ustawy z dnia 6 czerwca 1997 r.* … .
[44] Art. 115 § 14 *Ustawy z dnia 6 czerwca 1997 r.* … .
[45] Por. Art. 267 § 3 w związku z art. 310 § 1 i 2 *Ustawy z dnia 6 czerwca 1997 r.* … .
[46] Mam na myśli sytuację że następuje to wbrew woli posiadacza karty bankomatowej czy kredytowej.
[47] A. Suchorzewska, *op. cit*.
[48] Art 47 *Ustawy z dnia 18 września 2001 roku o podpisie elektronicznym, Dz.U. 2013, Nr 0, poz. 262.*

nej osoby oraz znać kod PIN. Przypadek takie jest szczególnie niebezpieczny, bowiem technicznie nie można stwierdzić przez kogo w konsekwencji był złożony podpis elektroniczny[49].

Równie istotnym jest przestępstwo oszustwa komputerowego. A. Marek twierdzi że nazwa tego przestępstwa nie jest zbyt trafna, bowiem w tym przypadku sprawca nie wprowadza w błąd ani nie wykorzystuje cudzego błędu, tylko ingeruje w urządzenie lub system przeznaczony do gromadzenia, przetwarzania lub przesyłania informacji[50].

Oszustwa komputerowego się może każdy kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych. W takiej sytuacji osoba ta podlega karze pozbawienia wolności od trzech miesięcy do pięciu lat[51]. W przypadku mniejszej wagi sankcja jest niższa[52]. Przykładem typowego oszustwa komputerowego może być włamanie się do sieci policyjnej, bankowej i wydanie określonych dyspozycji[53]. W ramach przestępstwa oszustwa komputerowego praktyka wyróżnia trzy rodzaje manipulacji: danymi, programem oraz wynikiem[54]. Pierwszy przypadek polega na wprowadzeniu do danego systemu nieprawdziwych danych w celu uzyskania określonych informacji[55], drugi przypadek obejmuje działania polegające na wprowadzeniu nowych bądź zmodyfikowanych poleceń programowanych, które spowodują samoczynne wykonanie danego zadanie

[49] Por. K. Szaniawski, T. Kościelny, *Ustawa o podpisie elektronicznym. Komentarz*, Kraków 2003, s. 40–41; M. Marucha-Jaworska, *Podpis elektroniczny*, Warszawa 2002, s. 35–36; J. Janowski, *Podpis elektroniczny w obrocie prawnym*, Warszawa 2007, s. 38.

[50] A. Marek, *Kodeks karny. Komentarz*, Kraków 2007, s. 527.

[51] Art 287§ 1 *Ustawy z dnia 6 czerwca 1997 r. … .*

[52] Jest to grzywa, kara ograniczenia wolności albo pozbawienia wolności do roku. Art 287§ 2 *Ustawy z dnia 6 czerwca 1997 r. … .*

[53] W przypadku banku najczęściej jest to dyspozycja przelewu na określone konto – zazwyczaj sprawcy. Por. A. Bógdał-Brzezińska, M. F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 31.

[54] Por. P. Kardas, *Oszustwo komputerowe w kodeksie karnym*, „Przegląd Sadowy" 2000, nr 11 – 12, s. 60; Zob. też; A. Suchorzewska, *op. cit.*

[55] Przykładem takich operacji mogą być: doprowadzenie do upadku firmy, podawanie nieprawdziwych informacji o świadczeniobiorcach.

na które wpływu nie będzie miał operator sieci[56]. Trzeci przypadek dotyczy manipulacji urządzeniami peryferyjno - systemowymi oraz urządzeniami wejścia-wyjścia[57].

Reasumując powszechny dostęp do sieci internetowej, umożliwił rozwój przestępczości komputerowej - cybeprzestępczości. Potencjalni przestępcy z racji tego iż są w większości anonimowi w sieci czują się praktycznie bezkarni a osoby poszkodowane bezradne. Dodatkowo oszustwo komputerowe w rekach terrorystów stanowi niebezpieczne narzędzie za pomocą którego mogą oni wpływać na określone obszary życia społecznego. Staje się to bardzo niebezpieczne kiedy uderzają w aparat państwowy. Cyberprzestrzeń stworzyła niebagatelne możliwości zarówno dla potencjalnych obywateli jak i do typowych przestępców. W związku z tym ważne staje się odpowiednie zabezpieczanie sprzętu, sieci i urządzeń peryferyjnych. W tym przypadku szeroko rozumiana profilaktyka jest wskazana i zarazem konieczna.

Osobnym przestępstwem związanym z ochroną cyberprzestrzeni będzie bezprawne przetwarzanie danych osobowych w wyniku którego dojdzie do kradzieży tożsamości. Przykładem może być sytuacja w której dane osoba szuka pracy. W odpowiedzi na CV, fałszywy pracodawca kontaktuje się w celu ustalenia rozmowy kwalifikacyjnej z prośba o wypełnienie bardzo szczegółowego kwestionariusza na stronie internetowej lub o przesłanie danych w pliku na określony adres internetowy[58]. Tak pozyskane dane mogą służyć do wyłudzenia kredytów czy innych środków. Równie osobliwe są ostatnio oszustwa nigeryjskie[59], kradzieże w sklepach internetowych, kradzieże z wykorzystaniem złośliwego oprogramowania, kopiowanie kart płatniczych, kradzieże związane z kartami zbliżeniowymi, kradzieże przy użyciu danych z kary płatniczej, kradzieży z telefonu na której jest zainstalowana aplikacja do dokonywania płatności mobilnych[60].

[56] Na przykład modyfikacja programu obliczającego salda na rachunkach bankowych w ten sposób, aby zaokrąglał salda zawsze "w dół", jednocześnie przelewając nadwyżki na ustalony rachunek bankowy sprawcy; Por. A. Suchorzewska, *op. cit.*

[57] Na przykład wyłudzenie wypłaty gotówki z bankomatu za pomocą skradzionej karty; Zob. A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 119-121.

[58] Zaznaczyć należy że na potrzeby procesu rekrutacji szczegółowe dane nie są potrzebne.

[59] Polega na przyjęciu pieniędzy niewiadomego pochodzenia na swój rachunek bankowy i przekazanie ich dalej co może być udziałem w większym oszustwie – praniu pieniędzy czy nawet finansowaniu terroryzmu. Bardzo często środki pieniężne przekazywane zgodnie z opisanym procederem mogą pochodzić z tzw. phisingu.

[60] Szerzej: M. Górnisiewicz, R. Obczyński, M. Pstruś, *Bezpieczeństwo finansowe w bankowości elektronicznej - przestępstwa finansowe związane z bankowością elektroniczną*, Warszawa 2014.

Za pomocą sieci można również rozpowszechniać pornografię dziecięcą[61], co podlega karze pozbawienia wolności od sześciu miesięcy do ośmiu lat. Jest to przestępstwo coraz bardziej powszechne. Osoby zajmujące się tym procederem prezentują dzieciom materiały pornograficzne, uwodzą za pomocą Internetu czy proponują tzw. wirtualny seks[62]. W tym przypadku należy wskazać że przestępstwo to jest szczególnie niebezpieczne dla dziecka bowiem wpływa na jego psychikę. Prezentowanie materiałów pornograficznych dzieciom w szczególności w sposób nachalny, jest przestępstwem które można popełnić w cyberprzestrzeni. W przypadku uwodzenia wykorzystywane są wszelkiego rodzaju komunikatory, za pomocą których anonimowi rozmówcy podają się za rówieśnika swojej ofiary, wykorzystują w ten sposób naiwność i łatwowierność małego dziecka, zdobywają cenne informacje, zaprzyjaźniają się i dążą do spotkania z dzieckiem a jeśli już do niego dojdzie dziecko może zostać wykorzystane seksualnie.

Wreszcie bardzo szkodliwy dla psychiki małego dziecka jest wirtualny seks. Polega on najczęściej na rozmowie on-line dotyczącej tematyki seksualnej przedstawionej w sposób bardzo agresywny i wulgarny. Proces uwikłania dziecka w tego typu rozmowę przebiega bardzo podobnie jak uwodzenie. Nie prowadzi on jednak do spotkania a jedynie aktywności on-line która ma doprowadzić do zaspokojenia seksualnego sprawcy.

Przepisy prawa karnego zabraniają publicznego znieważania[63] oraz nawoływania do nienawiści na tle narodowym, rasowym, etnicznym czy wyznaniowym[64]. Przestępstw tych można dopuścić się w sieci, co również jest kryminalizowane przez ustawodawcę. Czynem kryminalnym, który może zostać popełniony w cyberprzestrzeni jest przesyłanie niezamówionej informacji handlowej za pomocą środków komunikacji elektronicznej w tym za pomocą poczty elektronicznej[65].

Podmiotem ponoszącym odpowiedzialność za przekazywanie niezamawianych informacji handlowych jest nadawca czyli podmiot mający wpływ na jej treść. W sytuacji kiedy nadawca działa na zlecenie podmiotu, którego informacje dotyczą

[61] Art 203 § 2 *Ustawy z dnia 6 czerwca 1997 r. … .*
[62] Zob. M. Szmit, *Wybrane zagadnienia opiniowania sądowo-informatycznego,* Warszawa 2014.
[63] Art 256 *Ustawy z dnia 6 czerwca 1997 r. … .*
[64] *Ibidem*.
[65] Art 24 *Ustawy z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną, Dz. U. 2013, poz. 1422*. Otwarty katalog środków komunikacji oznacza, że zakaz przesyłania niezamówionej informacji handlowej stosuje się także do innych środków komunikacji elektronicznej, np. do wiadomości SMS. Por. A. Suchorzewska, *op. cit.*

to on ponosi odpowiedzialność za przekazywanie informacji w sposób nieprawidłowy, bowiem jest uprzednio zobowiązany do uzyskania zgody odbiorcy[66]. W sytuacji zagrożenia cyberterroryzmem jednym z ważniejszych aspektów ochrony jest bezpieczeństwo informacji. Chodzi o informacje, które powinny być w dyspozycji państwa i jego organów. Z tego względu w polskim systemie prawnym ważną rolę pełni ustawa o ochronie informacji niejawnych[67], którą można uznać za skuteczne narzędzie do walki z cyberterroryzmem.

Informacja niejawna jest w tym przypadku informacją, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczpospolitej Polskiej albo byłoby z punktu widzenia jej interesów szczególnie niekorzystne. W związku z powyższym informacja niejawna jest w polskim systemie prawnym otoczona szczególnym nadzorem, przez co zdobycie jej przez terrorystów jest znacznie utrudnione. Ochroną oprócz informacji niejawnych są również objęte dane osobowe, których przetwarzanie bez podstawy prawnej jest zabronione. W tym względzie odpowiednie zabezpieczenia musi posiadać sieć teleinformatyczna w której znajdują się określone dane osobowe. Sieć takowa może stać się celem ataków terrorystycznych, które w efekcie mogą doprowadzić do ujawnienia danych osobowych, co w konsekwencji prowadzi do destabilizacji systemu ochrony informacji w państwie a także stanowi bezpośrednie zagrożenie dla osób, których dane ujawniono. Przedstawione rodzaje i kategorie przestępstw odnoszą się do bezpośrednio do przestępczości w sieci Internetowej. Zadaniem każdego państwa jest zapewnienie bezpieczeństwa informacyjnego. Liczne zdarzenia mające miejsce w sieci mogą jednak sugerować że cyberataki mają miejsce praktycznie codziennie. Obecnie popularne są cyberataki przez cloud -computing czyli chmurę. To jedna z nowszych form korzystania z dobrodziejstw sieci, gdzie zarówno oprogramowania jak i inne dane mogą być przechowywane na serwerach operatora. Potencjalny cyberatak może zatem wyrządzić ogromne szkody. Wydaje się że przez każdym cyberatakiem można próbować się bronić, jednak nie zawsze obrona taka jest skuteczna, mimo wszystko minimalizuje straty jakie odnieść mogą potencjalni obywatele korzystający z dobrodziejstw sieci. O tym że cyberatatki są możliwe mogą świadczyć dane zawarte w Raporcie Fundacji Bezpieczna Cyberprzestrzeń. Analizując ów Raport,

[66] A. Monarcha-Matlak, *Obowiązki administracji w komunikacji elektronicznej*, Warszawa 2008, s. 101-120; K. Kowalik-Bańczyk, A. Majchrowska, M. Świerczyński, *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warszawa 2009, s. 234-236; A. Frań-Adamek, *Komentarz do art. 24 ustawy o świadczeniu usług drogą elektroniczną*, System informacji prawnej Lex 2002.

[67] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2010, Nr 182, poz. 1228.*

można dojść do wniosku iż na całym świecie w 2014 roku doszło do zainfekowania złośliwym programem na Android atakującym mobilne urządzenia w sieci TOR[68].

W kwietniu 2014 roku pojawił się wirus o nazwie Heartbleed. Umożliwiał on wykradanie różnych danych, w tym na przykład licznych kluczy prywatnych. W maju 2014 roku pojawił się szkodliwy botnet Zeus Gameover. W unieszkodliwianiu jego wzięło udział 11 państw a akcję tę nazwano Operacja tovar[69]. W lipcu tegoż roku pojawiła się informacja o kampanii szpiegostwa komputerowego wymierzonego w szereg firm, głównie z sektora energetycznego. Atakujący to grupa Dragonfly, której udało się złamać zabezpieczenia wielu organizacji i przeprowadzić szeroko zakrojone operacje szpiegowskie[70].W drugiej połowie września 2014 roku społeczność dobiegła wiadomość o nowej luce zwanej Shellshock, która pozwalała na zdalne wykonanie komend w systemie wykorzystującym powlokę Bash. Wirus ten polega na błędnym sposobie interpretacji funkcji przypisanych do zmiennych a błąd może nieść ze sobą poważne skutki społeczne i ekonomiczne.

W październiku 2014 roku wykryto kolejne operacje szpiegowskie o nazwach BlackEnergy i Sandworm. Można powiedzieć że to kolejne dowody na to, że trwający konflikt na wschodzie Europy odbywa się również w cyberprzestrzeni[71]. Również w tym samym miesiącu świat otrzymał informacje o długoterminowej kampanii szpiegowskiej o nazwie APT28. Za kampanią tą stała grupa rosyjskich cybeprzestepców a ich działania były skierowane między innymi na organizacje w Gruzji, Europie Wschodniej, członków NATO i OBWE. Wśród celów znalazła się również Polska.

W grudniu 2014 roku miały miejsce cyberataki na Sony Pictures Entertainment. Nie znana jest jej geneza, jednak wiele wskazuje na to że w jednym z filmie "*The Interview*" w negatywnym świetle przedstawiono przywódcę koreańskiego i to Korea Północna stoi za atakami na Sony[72]. Według przewidywań Fundacji Bezpieczna Cyberprzestrzeń w 2015 roku na czoło klasyfikacji przestępstw popełnianych w sieci wybijają się phishing z wykorzystaniem poczty elektronicznej

[68] To nowość i pierwszy przypadek tego typu – dotychczas sieć TOR nie była wykorzystywana w atakach na urządzenia mobilne.

[69] *Największe zagrożenia dla bezpieczeństwa w Internecie w 2015 roku. Głos polskich ekspertów*, Warszawa 2015, s 6.

[70] Większość ofiar miało swoje siedziby w Stanach Zjednoczonych, Hiszpanii, Francji, Włoszech, Niemczech, Turcji i Polsce

[71] W tym przypadku chodziło o złośliwe oprogramowanie, trojana o nazwie BlackEnergy, które skutecznie zaatakowało wiele organizacji na Ukrainie i w Polsce.

[72] *Największe zagrożenia…*, s 7.

i serwisów WWW, ataki DDoS na podmioty komercyjne oraz zagrożenia dla platformy Android[73]. Z raportu Najwyższej Izby Kontroli wynika, że cyberataki miały miejsce również w Polsce.

W 2012 roku najważniejsze strony administracji publicznej w domenie gov.pl stały się fragmentem kampanii protestu społecznego związanej z pracami mającymi na celu podpisanie przez Polskę międzynarodowego porozumienia dotyczącego walki z naruszaniem własności intelektualnej ACTA. Ataki miały miejsce na strony internetowe między innymi Kancelarii Sejmu RP, Kancelarii Prezydenta RP, Kancelarii Prezesa Rady Ministrów, Ministerstwa Spraw Zagranicznych, Ministerstwa Sprawiedliwości, Ministerstwa Edukacji Narodowej, Kancelarii Senatu RP, Ministerstwa Kultury, Ministerstwa Obrony Narodowej, Komendy Głównej Policji oraz Centralnego Biura Antykorupcyjnego. Miały one na celu przeciążenia serwerów udostępniających strony WWW tych instytucji. Ataki te pochodziły w większości polskich serwerów IP[74].

Podobne ataki miały miejsce na strony WWW Ministerstwa Gospodarki, a dotyczyły one wykradania określonych danych. Wykradzione dane zawierały kopie stron paszportów - głównie obcokrajowców, dane skrzynek pocztowych wraz z brzmieniem ich haseł oraz niektóre obrazy rządowych dokumentów[75]. Incydenty te spowodowały że administracja publiczna podjęła szereg cennych inicjatyw, których celem było zwiększenie bezpieczeństwa na stronach WWW. W lipcu i październiku 2014 roku miały miejsce cyberataki o znamionach terrorystycznych. Anonimowi nadawcy przesyłali informacje że ważnych instytucjach rządowych są podłożone ładunki wybuchowe. Po szczegółowym sprawdzeniu przez odpowiednie instytucje okazało się że informacje te były nieprawdziwe.

Również w październiku 2014 roku miała miejsce kradzież danych z systemów informatycznych Giełdy Papierów Wartościowych. Zostały one później udostępnione przez anonimowe osoby w Internecie. W listopadzie tego samego roku wykradzione z systemu informatycznego dane dotyczące pracowników Państwowej Komisji Wyborczej. Miało to miejsce w okresie w którym PKW borykała się z problemem związanym z oprogramowaniem do obliczenia wyników przeprowadzonych wyborów. Oprócz tych incydentów miały miejsce jeszcze inne takie jak

[73] *Ibidem*, s. 8.
[74] *Informacja o wynikach kontroli …*, s. 20.
[75] Były to w większości dane o mało istotnym znaczeniu dla bezpieczeństwa państwa.

udostępnienie w Internecie danych osobowych bliku 400 tys. abonentów firmy telefonicznej HYPERION oraz ORANGE[76].

Jak podaje Najwyższa Izba Kontroli nieznana jest ilość i skala ataków, w przypadku których nie ujawniono informacji o ich skutecznym przeprowadzeniu[77]. Zdarza się że bardzo często osoby poszkodowane nie są zainteresowane ściganiem tego typu przestępstw z różnych względów. Jednym z takich jest kwestia wizerunku na arenie publicznej czy względy osobiste.

Jak można zauważyć cyberbezpieczeństwo jest jednym z filarów sprawnie działającego państwa. O jego poziomie świadczy sprawność, wydajność i spójność działań podejmowanych w imieniu państwa przez odpowiednie służby, które na co dzień zajmują się monitorowaniem poziomu cyberbezpieczeństwa. Zagrożenie cyberprzestępczością, a także cyberterroryzmem jest realne i trudno mu przeciwdziałać. Aby jednak jej minimalizować państwa musi dysponować odpowiednimi służbami i stosownym sprzętem, który pośrednio wpływa na minimalizowanie cyberataków.

## Podsumowanie

Problematyka cyberbezpieczństwa jest niewątpliwie bardzo istotna zarówno z poznawczego jak i pragmatycznego punktu widzenia. Z poznawczego punktu widzenia stanowi ona nie do końca eksplorowany obszar badawczy. Publikacje które dotykają cyberbezpieczństwa pisane są z głównie z punktu widzenia nauk prawnych, na rynku brakuje publikacji które traktują to zagadnienie holistycznie a więc nie tylko z perspektywy prawa ale także innych dziedzin naukowych. Przedmiotowe opracowanie jest próbą połączenia spojrzenia prawniczego i politologicznego, subsydiarnie stosując dorobek nauk o bezpieczeństwie. Jeśli chodzi o pragmatyczny punkt widzenia należy wskazać że cyberbezpieczeństwo należy do kluczowych zagadnień państwa.

Dodatkowo z cybebezpieczeństwem łączą się dwa zjawiska cybeprzestepczość oraz cyberterroryzm. O ile z cybeprzestępczością można spotkać się na co dzień o tyle cyberterroryzm jest niewątpliwie zagrożeniem XXI wieku dla całego świata. Wynika to z faktu że cyberterroryzm jest najbardziej nieprzewidywalnym sposobem działania grup przestępczych o różnych konotacjach. Wpływa na stabilność instytucji państwa a także na system polityczny i gospodarczy.

[76] Były to takie dane jak imiona i nazwiska, nr telefonów, PESEL, NIP i dokumentów tożsamości oraz adresy tradycyjne i e-mail.
[77] *Informacja o wynikach kontroli* …, s. 21.

W związku z powyższym należy przyjąć że cyberterroryzm jest zjawiskiem wyjątkowo istotnym w problematyce cyberbezpieczństwa. Również ważna jest cyberprzestepczość, która wiąże się z wykorzystaniem środków komunikacji elektronicznej do popełniania czynów zabronionych. Również stanowi ono ogromne wyzwanie dla poszczególnych państw. Wynika to z tego że rozwój społeczeństwa informacyjnego doprowadził do pojawiania się zupełnie nowych typów czynów zabronionych, które dokonywane są w świecie wirtualnym. Wiążą się one z przetwarzaniem, gromadzeniem, przekazywaniem, przechowywaniem i wykorzystaniem informacji. Można zatem przyjąć że cyberbezpieczeństwo jest nową dziedziną bezpieczeństwa narodowego.

## Bibliografia

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

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

Budyn-Kulik M., *et al.*, *Kodeks karny: komentar,* red. M. Mozgawa, Warszawa 2014.

*Decyzja Ramowa 2005/222/WE Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dziennik Urzędowy Unii Europejskiej, L 218*

Dembowska M., *Słownik terminologiczny informacji naukowej*, Warszawa 1974.

Doroszewski W. (red), *Słownik języka polskiego*, t. 2, Warszawa 1965.

Frankowski P., Juneja A., *Serwisy społecznościowe. Budowa, administracja i moderacja*, Gliwice 2009.

Frań-Adamek A., *Komentarz do art. 24 ustawy o świadczeniu usług drogą elektroniczną*, System informacji prawnej Lex 2002.

Górnisiewicz M., Obczyński R., Pstruś M., *Bezpieczeństwo finansowe w bankowości elektronicznej - przestępstwa finansowe związane z bankowością elektroniczną*. Warszawa 2014.

*Informacja o wynikach kontroli Realizacja przez podmioty państwowe zadań z zakresie ochrony cyberprzestrzeni RP*, Warszawa 2015.

Janowski J., *Podpis elektroniczny w obrocie prawnym*, Warszawa 2007.

Kardas P., *Oszustwo komputerowe w kodeksie karnym*, „Przegląd Sadowy" 2000, nr 11 – 12.

Karłowicz J., Kryński A., Niedźwiecki W. (red), *Słownik Języka Polskiego*, t. 1, Warszawa 1900.

Knoppek K., *Dowód w procesie cywilnym*, Poznań 1993.

Kowalik-Bańczyk K., Majchrowska A., Świerczyński M., *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warszawa 2009.

Kozłowska-Kalisz P., *Komentarz do art. 267 kodeksu karnego*, [w:] Budyn-Kulik M. *et al*., *Kodeks karny: komentarz,* red. M. Mozgawa, Warszawa 2014.

Marek A., *Kodeks karny. Komentarz*, Kraków 2007.

Marucha-Jaworska M., *Podpis elektroniczny*, Warszawa 2002.

Monarcha-Matlak A., *Obowiązki administracji w komunikacji elektronicznej*, Warszawa 2008.

*Największe zagrożenia dla bezpieczeństwa w Internecie w 2015 roku*. *Głos polskich ekspertów*, Warszawa 2015.

Rokiciński K., *Wymagania w zakresie współpracy cywilno-wojskowej (CI-MIC) w czasie planowania i przygotowania działań w pasie nadmorskim RP*, II Konferencja „Zarządzanie Kryzysowe", Szczecin 18 czerwca 2004.

*Słownik Języka Polskiego PWN*, Warszawa 2006.

Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2010.

Szaniawski K., Kościelny T., *Ustawa o podpisie elektronicznym. Komentarz*, Kraków 2003.

Szmit M., *Wybrane zagadnienia opiniowania sądowo-informatycznego,* Warszawa 2014.

Szymczak M.(red), *Słownik języka polskiego*, t. 1, Warszawa 1978.

*Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r.*

*Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną, Dz. U. 2013, poz. 1422.*

*Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2010, Nr 182, poz. 1228.*

*Ustawy z dnia 18 września 2001 roku o podpisie elektronicznym, Dz.U. 2013, Nr 0, poz. 262.*

*Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, Dz.U. 1997, Nr 88, poz. 553.*

*Wielka Encyklopedia Powszechna*, t. 3, Warszawa 1983.

Marek Górka

Politechnika Koszalińska

# Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa

Słowa kluczowe: cyberwojna, cyberbezpieczeństwo, konflikt asymetryczny, cyberdemokracja, cyberatak

## Wstęp

W epoce informacji, wszystkie kluczowe sektory ludzkiej działalności jak: polityka, gospodarka, biznes, finanse, transport, infrastruktura, poczta, telekomunikacja, medycyna oraz nauka są ściśle zależne od technologii informacyjnych. Znaczącym przykładem tego są sieci społeczne, które mogą szybko wpłynąć na wartości, idee i zachowania dużych grup społecznych. Ze względu na swój globalny charakter, rządy praktycznie nie mają wpływu na treści pojawiające się w cyberprzestrzeni, a nakładana cenzura jest mocno ograniczona do określonego kraju, z wyjątkiem oczywiście całkowitego zakazu dostępu do sieci. W praktyce Internet daje nieograniczone możliwości dystrybucji różnych ideologii i poglądów związanych z demokratycznymi przemianami stosunków społecznych i praw człowieka.

Postęp technologii informacyjnych, a wraz z nim zależność codziennego życia od Internetu prowadzi do powstania wielu nowych wyzwań i zagrożeń w cyberprzestrzeni. Wszystko to jest idealną platformą dla nowych, tajnych wojen i konfliktów. Brak odpowiednich regulacji pozwala agresorom bez żadnych konsekwencji korzystać z anonimowości w cyberprzestrzeni. Tworzy ona bowiem możliwości prowadzenia działań przestępczych oraz ataków wymierzonych w interesy różnych organizacji publicznych oraz indywidualnych obywateli.

Rewolucja informacyjna oraz pojawiające się zagrożenia ustanowiły, odmienne od obecnych, wymagania dotyczące bezpieczeństwa państwa. Do tego zakresu zadań zaliczana jest kontrola i ochrona informacji w cyberprzestrzeni. Pozwala to przeciwdziałać atakom ze strony grup przestępczych oraz może zapobiec penetracji - ze strony wrogich podmiotów - systemów informacyjnych infrastruktury krytycznej państwa.

Cyberzagrożenia zagrażające infrastrukturze krytycznej państwa stanowią coraz poważniejszy problem dla decydentów i konsumentów. Technologia informacyjna i komunikacyjna (ICT) jest wszechobecna na wielu urządzeniach teleinformatycznych, które są współzależnymi od siebie elementami. Dlatego też zaburzenie jednego składnika może mieć negatywny wpływ na inne urządzenia. Cyberataki mogą obejmować odmowę usługi, kradzież lub manipulację danymi. Uszkodzenia infrastruktury krytycznej przez atak cybernetyczny może mieć istotny wpływ na bezpieczeństwo narodowe, gospodarkę i warunki życia oraz bezpieczeństwo wielu indywidualnych obywateli. Tradycyjnie cyberbezpieczeństwo postrzegane jest na poziomie zagrożenia dla systemu komunikacji czy też władzy państwowej.

Temat funkcjonowania cyberprzestrzeni w kontekście zarówno nauk politycznych, socjologii czy też w perspektywie bezpieczeństwa narodowego stanowi obszar badawczy wielu prac. Badacze podkreślają negatywne skutki dla funkcjonowania społeczeństwa coraz bardziej uzależnionego od tzw. aplikacji sieciowych. W tym obszarze istotna dla opisu wybranych zagadnień w artykule jest praca Petera Trima, Davida Uptona *Cyber Security Culture. Counteracting Cyber Threats through Organizational Learning and Training*[1].

Pomimo wszechobecności Internetu i jego znaczenia dla szerokiego zakresu funkcji państwa, istnieje jeszcze wiele procesów i zjawisk do zrozumienia, szczególnie w kontekście stosunków międzynarodowych czy też władzy państwowej w erze informacyjnej. Ten zakres tematyczny systematyzuje m.in. Madeline Carr w swej pracy *US Power and the Internet in International Relations.The Irony of the Information Age*[2].

Trzecią kluczową pracą dla dokonanej analizy w artykule jest praca Juliana Richardsa *Cyber-War. The Anatomy of the Global Security Threat*[3]. Książka przed-

[1] P. Trim, D. Upton, *Cyber Security Culture. Counteracting Cyber Threats through Organizational Learning and Training*, New York 2016.
[2] M. Carr, *US Power and the Internet in International Relations. The Irony of the Information Age*, Palgrave Macmillan 2016.
[3] J. Richards, *Cyber-War.The Anatomy of the Global Security Threat*, Palgrave Macmillan 2016.

stawia krytyczną ocenę aktualnych debatach wokół prawdopodobieństwa zaistnienia i wpływu cyberwojny. Zbliżając się do tematu z perspektywy społeczno-politycznej, twierdzi, że destrukcyjnego charakteru cyberwojny jeszcze nie widać, ale może być ona cechą przyszłego konfliktu.

Dalszą kontynuacją tematu jest praca *Deterring Cyber Warfare. Bolstering Strategic Stability in Cyberspace*[4]. Jej autorzy Brian Mazanec i Bradley Thayer wskazują, że powstrzymanie ataków internetowych jest jedną z najważniejszych kwestii poruszanych wśród wielu krajów, jednak zastosowanie środków odstraszania przed cyberatakiem - jak wskazują badacze - jest problematyczne.

Artykuł ma na celu przybliżenie pojawiających się zjawisk w zakresie praktyk związanych z operacjami sieciowymi prowadzonymi przez państwa i podmioty niepaństwowe. Opisuje także charakter i dynamikę konfliktów w cyberprzestrzeni. Praca oferuje także kilka refleksji na temat funkcjonowania współczesnego państwa oraz jego obywateli w cyberprzestrzeni. Stara się także uporządkować wybrane wątpliwości pojawiające się często w literaturze przedmiotu, dotyczące szczególnie wartościowania i kategoryzowania cyberzagrożeń.

## 1. Cyberprzestrzeń

Ponad połowa obecnej populacji ludzkiej prowadzi swą działalność polityczną, ekonomiczną czy też kulturową w przestrzeni cyfrowej. Domena ta stała się jednym z podstawowych obszarów funkcjonowania współczesnego społeczeństwa. Pomimo że, cyberprzestrzeń nie jest już tak zupełnie nową przestrzenią życia, to wciąż aktualnym wyzwaniem stojącym przed rządami wielu krajów jest potrzeba przeorganizowania istniejących instytucji wobec wystąpienia możliwych zagrożenia cybernetycznych. W odróżnieniu od naturalnych obszarów, takich jak: powietrze, woda, ląd, czy też kosmos, cyberprzestrzeń jest zjawiskiem stworzonym przez człowieka i w wyniku sprzężonej ze sobą infrastruktury informacyjnej, posiada charakter globalny.

Zakres pojęciowy cyberprzestrzeni jest bardzo szeroko zrozumiany. Okazuje się także, że termin ten może być największym wyzwaniem zarówno dla analizy badawczej, jak i interpretacji. Przydomek „cyber" odwołuje sie do wykorzystania nowych technologii informacyjnych i komunikacyjnych, a także do opartych na tych technologiach rozwoju, jak gospodarka, społeczeństwo, edukacja, kultura,

[4] B.M. Mazanec, B. Thayer, *Deterring Cyber Warfare. Bolstering Strategic Stability in Cyberspace*, Palgrave Macmillan 2016.

rozrywka, a przede wszystkim wiedza. To także przestrzeń, która wciąż się poszerza i ewoluuje na skutek ciągłych zmian w oparciu o pomysłowość i udziału samych użytkowników[5].

Kluczową definicją dla terminu cyberprzestrzeń jest dyrektywa numer 54 *National Security Presidential*, według której pojęcie to rozumiane jest jako wirtualne środowisko informacji i interakcji między ludźmi[6]. Idąc tym tropem można zauważyć potrzebę zaakcentowania znaczenia relacji międzyludzkich. Cyberprzestrzeń, wymaga nie tylko sprzętu, oprogramowania i systemów informacyjnych, ale ludzkich zachowań uchwyconych za pośrednictwem sieci cyfrowych. Owe interakcje to bogaty zbiór odzwierciedlający pozytywne, jak i negatywne strony ludzkiej natury, wahających się od cyber autokreacji i autoekspresji do działań przestępczych, prowadzących również do aktów terrorystycznych oraz możliwych konfliktów cybernetycznych. Główne cechy cyberprzestrzeni to brak granic, dynamiczne procesy i zjawiska oraz anonimowość użytkowników.

Instytucje publiczne mające swoją domenę w cyberprzestrzeni podatne są na włamania, zarówno ze strony pojedynczych osób, zorganizowanych grup czy też wrogich państw. A zatem ze względu na transgraniczny charakter cyberprzestrzeni, cyberagresorem mogą być jednostki, grupy czy wrogie rządy.

## 2. Państwo w cyberprzestrzeni

W zglobalizowanym świecie szybka i bezpieczna łączność nie jest luksusem, lecz czynnikiem warunkującym konkurencyjności. Wiele państw czyni znaczne inwestycje, aby poszerzyć swoją infrastrukturę cyfrową, a obywatele przyjmują te nowe technologie z entuzjazmem. Instytucje rządowe coraz częściej korzystają z cyfrowych mediów do komunikowania się z obywatelami. Problemem jednak jest, jak to zrobić bez narażania się na niebezpieczeństwa związane z cyberprzestępczością? Potencjalne zagrożenia rosną wraz ze wzrostem społecznego uzależnienia od tej nowej infrastruktury. Jest to palący problem, zwłaszcza w rzeczywistości, w której większość zamówień publicznych realizowanych jest drogą elektroniczną.

[5] U. Soler, *Cyberculture in the City on the Example of Lublin,* [w:] *Peripheral Metropolitan Areas in the European Union. The Case of Lublin*, red. Z. Pastuszak, M. Sagan, K. Żuk, Bangkok- Celje-Lublin 2015, s.253-261; R. J. Deibert, R. Rohozinski, *Risking Security: Policies and Paradoxes of Cyberspace Security*, „International Political Sociology" 2010, vol. 4/1, s.15-32.

[6] *National Security Presidential Directives [NSPD] George W. Bush Administration, NSPD 54: Cybersecurity Policy*, źródło: https://fas.org (dostęp: 12.08.2016).

Cyberzagrożenia w ostatnich latach stały się coraz bardziej poważne. Niektóre kraje i organizacje międzynarodowe mają świadomość konieczności przyjęcia strategii i polityki w dziedzinie bezpieczeństwa cybernetycznego. Sama natura pojawiających się treści w cyberprzestrzeni może rzucić światło na czyhające zagrożenia.

Problemy mnożą się w takim samym tempie, w jakim pojawiają się możliwości zaistnienia realnego cyberataku, który może siać spustoszenie np. w systemie finansowym określonej organizacji. Tego typu działania dokonywane są w celu wymuszenia na firmie zapłacenia okupu, aby nie utracić swoje bazy danych bądź aby odzyskać dostęp do swoich informacji cyfrowych.

W niektórych przypadkach, świat wprowadza technologie cyfrowe szybciej niż ludzka zdolność jest w stanie zrozumieć skutki, jakie mogą z nich wyniknąć dla bezpieczeństwa publicznego. Cyberbezpieczeństwo stało się więc priorytetem dla większości państw na świecie.

Zagrożenia cybernetyczne osłabiły tradycyjne formy władzy politycznej. W odpowiedzi na to zjawisko państwa narodowe starają się coraz bardziej zapanować nad procesami przebiegającymi w cyberprzestrzeni[7]. Te wzmożone wysiłki zmierzają w kierunku coraz większego zintegrowania cyberbezpieczeństwa w ramach szerszych ram bezpieczeństwa narodowego i obrony państwa. Oznacza to tworzenie współpracy między organami państwowymi a pozostałymi podmiotami, zyskując w ten sposób zdolność do przystosowywania się do dynamicznych zmian technologicznych w coraz bardziej zintegrowanym komunikacyjnie świecie[8].

Sporym wyzwaniem dla obszaru cyberbezpieczeństwa jest przekształcenie dotychczasowego modelu uprawiania polityki, tak aby agencje rządowe dzieliły się częścią władzy z poszczególnymi podmiotami[9]. Polityka bezpieczeństwa, w tym także cyberprzestrzeni, obejmuje bowiem wszystkie podmioty, które korzystają z globalnej infrastruktury technologii informacyjnej. Dzisiaj współpraca między państwem a prywatnym sektorem przedsiębiorstw nie jest już jedną z wielu możliwości, ale można ją potratować jako swego rodzaju podstawę do funkcjonowania w przestrzeni publicznej, dającą także możliwości innowacji - również w zakresie bezpieczeństwa publicznego. W wyniku rosnącego znaczenia sektora prywatnego w dziedzinie cyberprzestępczości, coraz ważniejsza staje się współpraca tego sektora z podmiotami publicznymi.

[7] W. A. Vacca, *Military Culture and Cyber Security*, „Survival .Global Politics and Strategy" 2011, vol. 53/6, s.159-176.
[8] T. Borandi, *Introduction to Secure Global Collaboration*, „Information Security Journal: A Global Perspective" 2009, vol. 18/2, s. 51-56.
[9] A. F. Brantly, *The Cyber Losers*, „Democracy and Security" 2014, vol. 10/2, s. 132-155.

Innymi słowy poziom cyberbezpieczeństwa zależy od stopnia, w jakim rząd mobilizuje podmioty prywatne do udziału w inicjatywach bezpieczeństwa wobec wspólnych zagrożeń oraz od elastyczności w stosunku do oczekiwań ze strony podmiotów publicznych i prywatnych.

Zarządzanie cyberbezpieczeństwem może być interpretowane jako forma dialogu między organizacjami i w dużej mierze może pomóc w ochronie przed zagrożeniami cybernetycznymi, jednak taki model współpracy wewnątrz podmiotów rządowych jak i między agencjami rządowymi a sektorem publicznym do tej pory nie jest wystarczająco rozpropagowany wśród decydentów.

Podsumowując, cyberbezpieczeństwo jest wyzwaniem w ramach współpracy pomiędzy różnymi podmiotami krajowymi i instytucjami, firmami prywatnymi i organizacjami pozarządowymi, a także na poziomie międzynarodowym poprzez współpracę między państwami, organizacjami regionalnymi i globalnymi. Kwestia bezpieczeństwa cybernetycznego stała się priorytetem dla Unii Europejskiej (UE) i NATO, która prowadzi czynności prawne niezbędnych do opracowania cyber mechanizmów obronnych.

### 2.1. Polityka - władza

Świat w XXI wieku stał się coraz bardziej zależny od informacji, technologii informacyjnych i komunikacyjnych. Większość współczesnych rządów stara się podejmować działania po to, aby być przygotowanym do stawienia czoła nowym wyzwaniom, jakie może przynieść cyberprzestrzeń. Codzienne życie każdego obywatela, gospodarki narodowej i każdego państwa zależy obecnie od stabilności i bezpieczeństwa cyberprzestrzeni. Okazuje się, że łatwy dostęp do technologii informacyjnych i komunikacyjnych jest jednym z warunków prawidłowego funkcjonowania współczesnego społeczeństwa.

Popularność cyberprzestrzeni jest na tyle znacząca, że zmienia rzeczywistość, a także w pewien sposób determinuje i kształtuje dotychczasowe modele władzy. Stąd zapewne pojawienie się takiego terminu jak *cyberdemokracja*. Pojęcie to rozumiane jest przez autorów jako podstawowa zasada obejmująca większość zagadnień związanych z połączeniami między technologią informatyczną a procesami demokracji odnoszącymi się m.in. do udziału ludzi w państwie, funkcjonowania administracji, czy też procesu wyborczego[10].

[10] M. J. Jensen , J.s N. Danziger, A. Venkatesh, *Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics*, „The Information Society" 2007, vol. 23/1, s. 39-50.

Warto zastanowić się zatem nad wpływem technologii informacyjnej na jakość demokracji. Okazuje się bowiem, że cyberprzestrzeń umożliwia powstanie ponadnarodowej i globalnej przestrzeni publicznej, w której dokonuje się dyskusja oraz refleksja na temat praw i wolności obywatelskich.

W tej kwestii szczególną rolę odgrywają media społecznościowe, które aktywizują oraz konsolidują grupy społeczne czy też ruchy protestacyjne, w ten sposób dając impuls dla procesów demokratyzacji, tak jak to miało miejsce w przypadku krajów Bliskiego Wschodu i Afryki Północnej. Zasadniczo więc szanse związane z cyberdemokracją stwarzają możliwości większego udziału społecznego oraz przejrzystości w procesach politycznych. Nowe technologie stawiają jednak przed władzą także wyzwania, w postaci choćby cyberprzestępczości i cyberterrroryzmu.

W coraz bardziej zglobalizowanej i ujednoliconej rzeczywistości, polityka czy gospodarka uzależniona jest od technologii. I to nie tylko w znaczeniu komunikacyjnym, jak i wizerunkowym, ale także i finansowym. Widocznym tego przykładem jest kampania wyborcza w Stanach Zjednoczonych, w której wszyscy kandydaci na prezydenta, aby zebrać pieniądze, odwiedzają Dolinę Krzemową oraz inne centra technologiczne. Znaczenie technologii informacyjnej oraz środków i możliwości jakie ona generuje jest znaczące dla współczesnej demokracji.

## 2.2. Cyberinwigilacja

Wartości demokratyczne stają się w pewnych okolicznościach przeszkodą dla zapewnienia bezpieczeństwa cybernetycznego. W skrajnym przypadku w procesie zarządzania bezpieczeństwem cybernetycznym znajdują się autorytarne państwa kontrolujące dostęp do Internetu, w celu m.in. ograniczenia dostępu użytkowników do wybranych i akceptowanych przez władze stron internetowych[11]. Sposób, w jaki elementy cyber zarządzania bezpieczeństwem współdziałają ze sobą, głównie na linii rząd a osoby prywatne, coraz bardziej determinuje model władzy w państwie. Pluralistyczny charakter cyberprzestrzeni daje swobodę indywidualnej i nieskrępowanej wypowiedzi, jeśli jednak wartości demokratyczne zostaną ograniczone w tym obszarze, to równowaga między demokracją i bezpieczeństwem zostanie zachwiana na rzecz bezpieczeństwa. Dowodem na nieetyczne oraz nieuprawnione działania są dokumenty, które wyciekły dzięki byłemu pracownikowi NSA -

[11] B. Simpson, M. Murphy, *Cyber-privacy or cyber-surveillance? Legal responses to fear in cyberspace*, „Information & Communications Technology Law" 2014, vol. 23/3, s.189-191; C. J. Bennett, A. Clement, K. Milberry, *Introduction to Cyber-Surveillance*, „Surveillance & Society" 2012, vol. 9/4, s. 339-347.

Edwardowi Snowdenowi. Ujawniają one m.in. ogrom cyberinwigilacji zastosowanej przez służby wywiadowcze oraz ich działania penetrujące prywatny obszar w sieciach łączności.

W odpowiedzi na konflikty cybernetyczne na szczeblu władzy może wystąpić szereg negatywnych konsekwencji, takich jak chęć wprowadzenia regulacji prawnych ograniczających prawa i swobody obywatelskie, które w następnym etapie mogą prowokować do stosowania przemocy. Poza ogromnymi szkodami fizycznymi i bezpośrednimi stratami finansowymi, sama możliwość wystąpienia przyszłych cyberzagrożeń prowadzić może do społecznej nieufności i niechęci do pracy z nowymi technologiami. Innymi słowy awarie bądź paraliż systemów komunikacji rodzi negatywne konsekwencje i przekonania opinii publicznej dotyczace wiarygodności elektronicznej obsługi zasobów, finansów czy też usług medycznych. Nawet utrata samego zaufania może prowadzić do ogromnych zakłóceń społecznych i gospodarczych we współczesnym państwie.

### 2.3. Społeczeństwo

Szybki rozwój technologii informacyjnych i komunikacyjnych oraz ich obecność w każdym aspekcie ludzkiego życia oraz wysoki stopień uzależnienia od cyberprzestrzeni ukształtowało współczesne funkcjonowanie społeczeństwa i przyczyniło się do wzrostu jego dobrego samopoczucia.

Społeczeństwo buduje przyszłość w oparciu o technologię, której tak naprawdę nie jest w stanie chronić. Globalna ekspansja sieci społecznych, takich jak Facebook czy Twitter zdominowały codzienne życie, ale równocześnie stworzyły problem, który grozi wymknięciem się spod kontroli. Trojany, robaki i wirusy są instalowane na komputerach oraz urządzeniach przenośnych w celu przejęcia kontroli i zdobycia hasła do m.in.: rachunków bankowych, danych Facebooka, zdjęć lub adresów e-mail. Jednak, aby doszło do włamania nie zawsze wymagana jest obecność tylko usterki w systemie czy też tylko błędu po stronie użytkownika. Kradzież kart kredytowych, danych lub tożsamości, oszustwa bankowe, masywny spam i szantaż to tylko kilka przykładów, które świadczą o szerokim wachlarzu przestępstw. Aby do takich sytuacji doszło wymagane jest zaistnienie obu - wyżej wspomnianych czynników - jednocześnie. Innymi słowy luka techniczna oraz naiwność bądź nieostrożność często prowadzi do np. otwarcia wiadomości z zainfekowanym załącznikiem. Dziś, powstanie sieci społecznych i bogactwo informacji, które eksponowane są na widok publiczny, prowadzą do tego, że ludzka natura jest

słabsza niż kiedykolwiek i bardziej skłonna na poddawanie się pokusom. Przez Internet każdy przestępca, który poświęci trochę czasu może wiedzieć wiele o każdym niemal użytkowniku i może te informacje wykorzystać. Logiką takiego oszustwa jest stworzenie wiarygodnej wiadomości, która w przekonaniu ofiary ma pochodzić od osób, którym ufa, czyli od członka rodziny bądź przyjaciela lub kolegi. Celem jest budowanie zaufania, a następnie kradzież danych[12].

Budowa własnego wizerunku publicznego przed epoką Internetu zajmowała miesiące lub lata i wymagała ogromnych nakładów pracy i energii. Dziś w ciągu kilku godzin można stworzyć na nowo wiarygodną postać, nie mającą odpowiednika w rzeczywistości[13]. Niesamowite jest zatem to, jaką ilość informacji ludzie są w stanie umieścić w Internecie. Wpływ inżynierii społecznej jest katastrofalny, ponieważ można tworzyć dobre relacje i budować zaufanie bez pozostawienia jakiegokolwiek śladu. I nie chodzi tu o atakowanie systemów informatycznych, ale o agresję wobec ludzi.

Informacje, które są zbierane za pośrednictwem aplikacji i ze wszystkich portali społecznościowych, stanowią źródło wiedzy na temat rodzin, przyjaciół i współpracowników ofiary. Taki zasób danych jest nieoceniony i może mieć nieprzewidywalne konsekwencje, kiedy trafi w ręce napastników, którzy mogą one prowadzić do spersonalizowanych ataków.

## 3. Cyberwojna

Porównując cyberkonflikt do konwencjonalnych działań wojennych okazuje się, że jest to dość tania forma prowadzenia konfrontacji między państwami. Ponadto działania w cyberprzestrzeni mogą być zainicjowane z dowolnego miejsca i nie wymagają dużej ilości wojsk oraz broni, ale tylko dostępu do komputera i Internetu. Możliwość zaistnienia cyberkonfliktu należy do największych współczesnych wyzwań w obszarze bezpieczeństwa nie tylko militarnego, ale i politycznego, gospodarczego oraz społecznego państwa.

Chociaż dokładne granice zjawiska cyberwojny nie zostały jeszcze zidentyfikowane i są kwestionowane w kręgach naukowych, bardziej ogólna definicja tego pojęcia może być sformułowana jako konflikt toczący się w cyberprzestrzeni, z wykorzystaniem technologii informacyjnych i komunikacyjnych w celu zniszczenia

[12] B. Oates, *Cyber Crime: How Technology Makes it Easy and What to do About it*, „Information Systems Management" 2001, vol. 18/3, s. 92-96.
[13] L. D. Roberts, D. Indermaur, C. Spiranovic, *Fear of Cyber-Identity Theft and Related Fraudulent Activity*, „Psychiatry, Psychology and Law" 2013, vol. 20/3, s. 315-328.

zasobów oraz infrastruktury technologicznej i informacyjno-komunikacyjnej przeciwnika[14].

Richard Clarke w swojej książce „Cyber Warfare" pojęcie cyberwojny definiuje jako włamanie do komputerów lub sieci innego państwa narodowego, w celu osiągnięcia takich celów jak utrata lub zniszczenie zasobów przeciwnika[15]. Brytyjski magazyn „The Economist" opisuje cyberwojnę jako piąty obszar wojny, po ziemi, morzu, powietrzu i przestrzeni kosmicznej[16] .

Zakładając, że cyberprzestrzeń jest alternatywnym środowiskiem rywalizacji państw i zorganizowanych grup, często też zastępującym działania w rzeczywistości, można przypuszczać, że eskalacja konfliktów na tym poziomie prowadzi do poważnych strat w niemal we wszystkich dziedzinach życia publicznego. Fakt ten pozwala więc na zastosowanie pojęcia „cyberwojny".

Środowisko informacyjne stwarza nowe możliwości oddziaływania militarnego. Zmiany zachodzą na bardzo wysokim stopniu przygotowania. Nowe technologie pozwoliły zwiększyć skuteczność broni. Znaczącej poprawie uległy środki wywiadowcze, których posiadanie gwarantuje przewagę walczącym stronom na polu bitwy. Cyberprzestrzeń zatem stała się także źródłem informacji o strategicznym znaczeniu[17]. Wśród głównych celów walki w pierwszych fazach wojny jest uzyskanie dokładnych i precyzyjnych informacji. A zatem, aby uzyskać przewagę w starciu militarnym, trzeba najpierw wygrać rywalizację o informację. Dziś zdolność do gromadzenia, wykorzystywania, przetwarzania i przechowywania informacji jest najważniejszym wyznacznikiem potęgi militarnej[18].

Technologie komunikacyjne, informacyjne przyjęte i dostosowane przez wojsko oraz organizacje paramilitarne prowadzą do rewolucyjnych zmian w działaniach wojennych. Nowe technologie informatyczne pozwalają na wielokrotny wzrost szybkości przetwarzania dużych ilości danych, co ułatwia podejmowania złożonych decyzji operacyjnych i zasadniczo tworzy nowe metody taktyczne walki zbrojnej. Znacznie zwiększają one potencjał bojowy systemów elektronicznych,

[14] T. Rid, *Cyber War Will Not Take Place*, „Journal of Strategic Studies" 2012, vol. 35/1, s.5-32.
[15] R. A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It*, New York 2012, s.33-68.
[16] *Cyberwar.The threat from the internet*, „The Economist", źródło: http://www.economist.com (dostęp: 12.08.2016).
[17] T. Thomas, *Creating Cyber Strategists: Escaping the 'DIME' Mnemonic*, „Defence Studies" 2014, vol. 14/4, s.370-393.
[18] D. Ormrod, B. Turnbull, *The cyber conceptual framework for developing military doctrine*, „Defence Studies" 2016, vol. 16/3, s. 270-298.

który włącza je do nowego rodzaju broni informacyjnej, mającej na celu unieszkodliwienie wojskowej i cywilnej infrastruktury wroga poprzez uszkodzenie lub zniszczenie sieci komputerowych. W opinii niektórych ekspertów niewidzialna broń jest w stanie zakończyć konflikt przed rozpoczęciem fizycznej walki, ponieważ dalsze kontynuowanie walki cybernetycznej może prowadzić do katastrofy dla jednej z rywalizujących stron. W tym sensie można stwierdzić, że posiadanie broni w postaci technologii informacyjnej zapewnia korzyści militarne i prawdopodobnie już dziś jej wykorzystanie może skutecznie konkurować z użyciem konwencjonalnych środków militarnych. Te dwa rodzaje broni są obecnie potężnym czynnikiem presji politycznej. Broń informatyczna stopniowo staje się jednym z głównych składników potencjału militarnego nowoczesnych państw. Obecnie wiele krajów, szczególnie wysoko rozwiniętych jak USA, Chiny, Federacja Rosyjska, konsekwentnie i wytrwale przygotowuje się do brania udziału w wojnach informacyjnych[19].

Można przypuszczać, że mniej zaawansowane technologicznie kraje również dążą do nabycia umiejętności pozwalających prowadzić wojny informacyjne. Jest to całkiem możliwe, ponieważ broń informacyjna posiada określone zalety dla rywalizujących stron. Po pierwsze jej stosowanie i rozprzestrzenianie jest szybkie, dodatkowo ma stosunkowo niskie koszta, a to sprawia, że jest ona dostępna dla różnych wrogo nastawionych podmiotów. Ponadto może być opracowana, zbudowana, wdrożona i używana w ukryciu przed opinią publiczną. A zatem trudno jest przypisać autorstwo i odpowiedzialność określonemu podmiotowi, którym jest zazwyczaj obcy reżim polityczny, a którego celem jest wywołanie problemów na skalę regionalną lub globalną[20].

Reasumując, cyberwojna oznacza używanie komputerów w celu zakłócania działalności określonego - zazwyczaj wrogiego lub konkurencyjnego - państwa poprzez celowe ataki na systemy komunikacyjne. Wśród głównych czynników określających pojęcie cyberwojny, można wyróżnić, po pierwsze: asymetryczny charakter konfliktu, a zatem jej tani i destrukcyjny czynnik, który może zachęcić słabsze podmioty do zaangażowania się w konflikty z silniejszym państwem. Po drugie, cyberataki są bardzo trudne do wykrycia, dlatego ich autorzy nie muszą obawiać się natychmiastowego odwetu i zachowują się bardziej agresywnie niż zwykle. Po trzecie, trudno jest bronić się przed atakami cybernetycznymi, więc większość pań-

[19] U. Soler, *Rola nowoczesnych technologii w cyberwojnie*, [w:] *E-gospodarka w Europie Środkowej i Wschodniej. Teraźniejszość i perspektywy rozwoju*, red. R. Sobiecki, Lublin 2015, s. 373-382.

[20] D. Peterson, *Offensive Cyber Weapons: Construction, Development, and Employment*, „Journal of Strategic Studies" 2013, vol. , 36/1, s. 120-124.

stw, działając logicznie, woli zaatakować jako pierwsze. Po czwarte, środki prowadzenia cyberwojny otoczone są tajemnicą, a porozumienia dotyczące kontroli zbrojeń są trudne do wdrożenia. Innymi słowy, cyberwojna oznacza poszerzenie wachlarza i możliwości działań militarnych[21].

Wysoki stopień rywalizacji oraz sprzeczne i wykluczające się wzajemnie interesy wielu podmiotów oraz grup stanowią poważne utrudnienia w ustanowieniu skutecznego systemu prawnego w przestrzeni międzynarodowej, który definiowałby jakie działania i jakie zachowania mogą być klasyfikowane jako cyberprzestępczość. Oczywiście, istnieją również inne okoliczności utrudniające współpracę międzynarodową w wykrywaniu przestępstw w cyberprzestrzeni. Kraje rozwinięte technologicznie prowadzą szereg korzystnych dla siebie interesów w przestrzeni informacyjnej i z pewnością nie chciałyby ich stracić w tak wysoce konkurencyjnym i dynamicznie rozwijającym się środowisku informacyjnym.

Jednym z najpoważniejszych problemów jest brak znaczących umów i porozumień międzynarodowych dotyczących zasad rozwoju, upowszechniania i stosowania cyberbroni, jak również porozumienia regulujące wykorzystanie złośliwego oprogramowania do celów wojskowych. Pojawiają się więc w kręgach władzy, ale i także wśród opinii publicznej pytania typu: kiedy i w jakim zakresie można zastosować cyberbroń? W jakich okolicznościach jej zastosowanie jest uzasadnione?

Stosowanie cyberbroni budzi także szereg wątpliwości typu, jak stosować niezwykle niebezpieczne wirusy atakujące strony infrastruktury krytycznej, które mogą wywołać regionalną bądź globalną katastrofę ekologiczną lub społeczno-gospodarczą? Jak ich używać, aby samemu nie zostać ofiarą cyberataku? Czy użycie broni cybernetycznej może sprowokować klasyczny konflikt zbrojny? Na ile cyberatak może stanowić usprawiedliwienie bądź odpowiedź na atak wojskowy innego kraju?

Częściową odpowiedzią na powyżej postawione pytania może być ustanowienie norm i zasad regulujących stosowanie cyberbroni, a także integracja uzgodnionych wcześniej porozumień między państwami, które będą tworzyć ramy dla funkcjonowania podmiotów politycznych.

Z instytucjonalnego oraz technicznego punktu widzenia, istnieje wiele trudności, w zakresie stosowania zasad prawa międzynarodowego podczas operacji cybernetycznych. W rzeczywistości, społeczność międzynarodowa wymaga czegoś

[21] T. J. Junio, *How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate*, „Journal of Strategic Studies" 2013, vol. 36/1, s.125-133; J. Stone, *Cyber War Will Take Place!,* „Journal of Strategic Studies" 2012, vol. 36/1, s. 101-108.

więcej niż umowy dwustronne, które nie powodują żadnych sankcji w przypadku nieprzestrzegania przepisów. Niektóre państwa przyjęły środki o charakterze wiążącym na poziomie organizacyjnym, jak np. utworzenie krajowej strategii cyberbezpieczeństwa po to, aby zmniejszyć skutki cyberataków. Środki te jednak mają ograniczony zakres.

Nie istnieją umowy lub wielostronne porozumienia międzynarodowe, w których przewidziana byłaby prosta definicja, czym jest cyberatak i jakie powinien on pociągać za sobą sankcje ekonomiczne czy też polityczne. Zauważalny jest także brak w umowach współpracy między podmiotami w zakresie kontroli, przetwarzania oraz udostępniania informacji, które mogą być pomocne w trakcie identyfikacji i śledzenia cyberagresorów[22].

Innym komplikującym faktem jest sytuacja, w której działania niektórych państw, jak USA czy Federacja Rosyjska, często nie mogą być odróżnione od działań podmiotów niepaństwowych, takich jak: organizacje terrorystyczne czy grupy cyberprzestępcze. W takim przypadku wybór działań, będących odpowiedzią na takie cyberataki staje się skomplikowany i niezwykle ryzykowny.

Połączenie anonimowości i działań przeprowadzanych równolegle z obu państw czy podmiotów niepaństwowych oraz trudności w rozróżnieniu działań militarnych od działań przestępczych sprawia, że zarządzanie tego typu konfliktami staje się niezwykle problematyczne. Każdy cyber incydent jest dość trudny do określenia; a zatem, nie można z całą pewnością przypisać za niego odpowiedzialności określonemu podmiotowi.

Ponadto, niepewność dotycząca przypisania, wraz z brakiem wspólnego porozumienia między aktorami politycznymi, stwarza ryzyko niestabilności i błędnego postrzegania sytuacji. W związku z tym, ze strategicznego punktu widzenia, klasyfikacja cyberkonfliktów staje się dość trudna z powodu zarówno ich złożonej natury oraz występowania wielu sposobów interpretacji tego zjawiska. Jak się więc okazuje, identyfikacja motywacji sprawcy, choć bardzo trudna, jest konieczna dla dokonania rozróżnienia pomiędzy zjawiskiem cyberprzestępczości, cyberterroryzmu i cyber wojny. Dodatkowo trzeba brać pod uwagę, że za atakiem może ukrywać się pojedyncza osoba lub określona organizacja albo określony podmiot polityczny.

[22] N. Choucri, S. Madnick, J. Ferwerda, *Institutions for Cyber Security: International Responses and Global Imperatives*, „Information Technology for Development" 2013, vol. 20/2, s. 96-121.

### 3.1. Konflikt asymetryczny

Tocząca się w cyberprzestrzeni rywalizacja ma charakter asymetryczny. Okazuje się bowiem, że osiągnięcia technologiczne stwarzają nieupoważnionym użytkownikom możliwości przejęcia kontroli np. nad systemem zarządzania odpowiedzialnym za określony obszar publiczny. W rezultacie systemy finansowe, gospodarcze czy też polityczne pozostają w zagrożeniu. W tym przypadku podmioty bądź organizacje wrogo nastawione do wybranego państwa uzyskują nad jego instytucjami publicznymi przewagę[23].

Ilustracją tego zjawiska jest cyberatak przeprowadzony przez hakerską grupę Anonymous na około 400 tysięcy tureckich stron internetowych z domeną kończącą się na „.tr". Akcja przeprowadzona została na skutek oskarżeń wysuniętych w stronę tureckiego rządu jakoby, kupując ropę naftową, wspierał on Państwo Islamskie. Anonymous zagroziła zainicjowaniem większej fali cyberataków przeciwko Turcji, dopóki jej władze nie przestaną wspierać logistycznie i finansowo ISIS[24]. Poprzez podobnie organizowane działania tego typu podmioty mogą determinować kształt polityki państwa.

Gwałtowny rozwój technologiczny zatarł granice między celami publicznymi i prywatnymi w Internecie. Przeciwnik może sparaliżować kraj, na przykład utrudniając funkcjonowanie rynków finansowych, nie biorąc przy tym za główny cel organizacji rządowych lub systemów wojskowych. Żaden kraj nie jest więc wolny od zagrożeń. Głównym więc zadaniem państwa jest zapewnienie zarówno bezpieczeństwa dla swych żywotnych interesów, jak i własnych obywateli.

### 3.2. Cyberataki wirusy

Rozwój wirusów komputerowych, jak i ochrona przed nimi stanowi, w metaforycznym ujęciu, kolejny wyścig zbrojeń pomiędzy podmiotami politycznymi. Informacje medialne dotyczące superwirusów jak „Stuxnet" i „Płomień" pokazują poziom zaawansowania i złożoności obu programów. Bez wątpienia wskazują także na autorów w postaci agencji wywiadowczych, pochodzących z zaawansowanych technologicznie krajów. Wirusy te, które najwyraźniej zostały opracowane przez

[23] J. Schroefl, S. J. Kaufman, *Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War*, „Studies in Conflict & Terrorism" 2014, vol. 37/10, s. 862-880; E. Ahrari, *Transformation of America's Military and Asymmetric War*, „Comparative Strategy" 2010, vol. 29/3, s.223-244.

[24] Ch. Summers, *Hacking group Anonymous declares 'cyber war' on Turkey for 'supporting ISIS'*, „Daily Star" 2015, 23 grudnia; *Stop supporting IS': Anonymous declares cyber war on Turkey*, „Daily Times" 2015, 23 grudnia.

USA i Izrael w celu udaremnienia programu jądrowego Iranu, uosabiają poziom zaawansowania, który znacznie przewyższa każdy inny szkodliwy do te pory program. Oba wirusy są zaszyfrowane i są trudne do wykrycia, gdy znajdą się w komputerze. Wirus „Płomień" ma możliwość przejęcia urządzenia peryferyjnego, nagrywania rozmów Skype, robienia zdjęć za pomocą aparatu z komputera oraz przesyłania informacji przez Bluetooth do dowolnego urządzenia[25].

W sytuacji, kiedy jedne z najsilniejszych krajów na świecie rozwijają wirusy komputerowe, warto zastanowić się jaką gwarancję bezpieczeństwa posiadają ich twórcy? Czy te szkodliwe programy nie będą wstanie przedostać się i zainfekować znacznie szerszej gamy systemów lub czy w przyszłości organizacje terrorystyczne nie wejdą w ich posiadanie po to, aby ich użyć wobec swoich twórców?

### 3.3. Stereotypizacja cyberkonfliktu

W literaturze przedmiotu często spotykanym sformułowaniem jest stwierdzenie, że cyberwojna ma asymetryczną naturę, bowiem cybernarzędzia, które używane są do jej prowadzenia są tanie i łatwo dostępne. Okazuje się to jednak nie do końca prawdą. Ich opracowanie wymaga dużo zasobów, czasu i tajemnicy operacyjnej. Słabe i niestaranne przygotowanie do przeprowadzania ataków, może w przypadku dobrze zabezpieczonego systemu, zakończyć się niepowodzeniem dla cyberagresora[26].

Ponadto cyberataki mają sens tylko wtedy, jeśli współgrają z użyciem broni konwencjonalnej. Taka ofensywa państwa lub grupy słabszych podmiotów ma sens jedynie, jeśli mogą one wspierać stosowanie broni konwencjonalnej. Ale nawet gdyby w planach cyber broń miałaby być zastosowana, to i tak mało prawdopodobny jest scenariusz jej użycia. A to dlatego, że w odpowiedzi na taki cyberatak, użyte zostałyby konwencjonalne środki wojskowe silniejszego państwa niszcząc w ten sposób infrastrukturę przeciwnika. To wyjaśnia, dlaczego mało prawdopodobne jest, aby takie państwa jak Somalia czy Tadżykistan podjęły się w najbliższej przyszłości cyberwojny przeciwko Stanom Zjednoczonym. Bez względu na szkody, które wyrządziłby cyberatak, szybka i zdecydowana represja przy pomocy broni konwencjonalnej byłaby miażdżąca dla tych państw.

[25] E. Messmer, *Stuxnet and Flame share code, development teams: Kaspersky Lab says early version of Stuxnet has a Flame module*, „Network World" 2012, 11 czerwca; B. Bencsath, G. Pek, L. Buttyan, M. Felegyhazi, *The Cousins of Stuxnet: Duqu, Flame, and Gauss*, „Future Internet" 2012, vol. 4/4, s. 971-1003.

[26] T. Rid, P. McBurney, *Cyber-Weapons*, „The RUSI Journal" 2012, vol. 157/1, s. 6-13.

Przy rozpoczęciu cyberwojny, ich potencjalni agresorzy, muszą posiadać wiedzę na temat rzeczywistych skutków własnych cyberataków. Nawet potęga militarna, stosująca również zaawansowane cybernarzędzia nie może być do końca pewna co do szans powodzenia takich ataków; ryzyko samookaleczenia jest bowiem wysokie. Taka obawa o własne bezpieczeństwo może być najlepszym środkiem odstraszającym.

Niektóre państwa bądź organizacje wolą skorzystać z cyber luki i nie podejmować kosztownych działań na rzecz tańszych sposobów, aby rozwiązać konflikt. Pod tym względem dostępność cyberbroni, bez względu na rzeczywisty potencjał destrukcyjny, może rzeczywiście pozwolić słabszym państwom na więcej możliwości, wobec silniejszych przeciwników. Ponadto, w pewnych okolicznościach możliwość zaistnienia cyberwojny paradoksalnie może być bardziej przydatna jako środek odstraszający wobec tradycyjnych przeciwników, zmniejszając tym samym prawdopodobieństwo otwartego konfliktu. Zjawisko to jest analogiczne do możliwości użycia broni atomowej, której prawdopodobieństwo zastosowania było wystarczającym argumentem do zaniechania eskalacji konfliktów militarnych w okresie zimnej wojny oraz czynnikiem wspomagającym negocjacje pokojowe, w trakcie np. kryzysu kubańskiego w 1962 roku.

Na marginesie warto zauważyć, że wiedza na temat cyberprzestrzeni często ulega silnej stereotypizacji. O ile więc można zgodzić się ze stwierdzeniem, że cyberwojna jest z natury szkodliwa dla międzynarodowego bezpieczeństwa i pokoju na świecie, to jednak trudno w pełni zaakceptować słuszność tezy, że sieci społeczne są z natury szkodliwe dla dyktatorów. Okazuje się, że ściśle kontrolowane i będące w rękach reżimu autorytarnego technologie informacyjne, mogą być kolejnym środkiem upowszechniającym określone idee.

Przeprowadzenie cyberataków nie jest takie proste, gdyż zazwyczaj nie wiadomo skąd pochodzą. To sprawia, że niezwykle trudno jest ukierunkować metody odstraszania. Ponadto, dobry środek odstraszający musi być wiarygodny. Joseph S. Nye, strateg w Harvard University stwierdza, że głównym środkiem zniechęcającym do zastosowania cyberataku są wysokie koszty, które musi ponieść cyberagresor. Takim czynnikiem dla atakującego może być podanie do publicznej wiadomości informacji o tym, kto jest autorem ataku. Odstraszanie może również zależeć

od tego, jak zaatakowane mocarstwo użyje swojej broni cybernetycznej w przyszłości. Byłoby to wyraźne ostrzeżenie, że określone państwo jest gotowe i chętne do działania[27].

## Zakończenie

Trudno przecenić, jaką rolę spełniają systemy komputerowe w utrzymaniu nowoczesnych gospodarek. Jednak łatwo sobie wyobrazić, co by się stało, gdyby awarii uległy satelity komunikacyjne, czy też bazy danych głównych systemów finansowych. Chociaż większość cyberzagrożeń pochodzi ze strony państw, które mają zdolność do tworzenia i rozwijania niezwykle wyrafinowanych wirusów, to zaznaczyć należy, że zagrożenia pochodzą także ze strony grup i organizacji anarchistycznych czy terrorystycznych.

W środowisku ekspertów z zakresu cyberbezpieczeństwa można zauważyć dwa przeciwstawne stanowiska - jedna strona twierdzi, że przy rozsądnych i tanich środkach profilaktycznych ogromne cyberkatastrofy są mało prawdopodobne[28], druga strona zaś stwierdza, że cyberterroryści są w stanie pociągnąć światową gospodarkę na skraj katastrofy[29]. Trudno ocenić, kto ma w tej debacie rację, wydaje się jednak, że oba scenariusze są możliwe do zrealizowania. Wszystko - jak należy sądzić - zależy od edukacji społecznej w zakresie cyberbezpieczeństwa, a także zachowania umiejętności - w przypadku awarii - używania i korzystania z analogowych czy też tradycyjnych narzędzi.

Warto jednak podkreślić, że zarówno cyberbezpieczeństwo, jak i stabilność ekonomiczna państwa są bardzo delikatną i skomplikowaną materią, a wiele instytucji publicznych, odpowiedzialnych za ich sprawne funkcjonowanie, nie zawsze nadąża nad dynamicznymi zmianami w tym obszarze.

[27] J. S. Nye, *The Future of Power*, New York 2011, s. 25-50.

[28] D. Isenberg, *A cyber Pearl Harbor? More hype than threat*, „Journal of Commerce", 28 grudnia 1999, s. 7; R. Abott, *Harvard Brief Says U.S. Exaggerates Chinese Cyber Capabilities*, *Causes Dangerous Mistrust*, „Defense Daily" 2015, 14 maja.

[29] J. Burton, *NATO's cyber defence: strategic challenges and institutional adaptation*, „Defence Studies" 2015, vol. 15/4, s. 297-319; M. Clayton, *Cyber Pearl Harbor': Could future cyberattack really be that devastating?,* „The Christian Science Monitor" 2012, 07 grudnia.

## BIBLIOGRAFIA

Abott R., *Harvard Brief Says U.S. Exaggerates Chinese Cyber Capabilities, Causes Dangerous Mistrust*, „Defense Daily" 2015, 14 maja.

Ahrari E., *Transformation of America's Military and Asymmetric War*, „Comparative Strategy" 2010, vol. 29/3.

Bencsath B., Pek G., Buttyan L., Felegyhazi M., *The Cousins of Stuxnet: Duqu, Flame, and Gauss*, „Future Internet" 2012, vol. 4/4.

Bennett C. J., Clement A., Milberry K., *Introduction to Cyber-Surveillance*, „Surveillance & Society" 2012, vol. 9/4.

Borandi T., *Introduction to Secure Global Collaboration*, „Information Security Journal: A Global Perspective" 2009, vol. 18/2.

Brantly A. F., *The Cyber Losers*, „Democracy and Security" 2014, vol. 10/2.

Burton J., *NATO's cyber defence: strategic challenges and institutional adaptation*, „Defence Studies" 2015, vol. 15/4.

Carr M., *US Power and the Internet in International Relations. The Irony of the Information Age*, Palgrave Macmillan 2016.

Choucri N., Madnick S., Ferwerda J., *Institutions for Cyber Security: International Responses and Global Imperatives*, „Information Technology for Development" 2013, vol. 20/2.

Clarke R. A., *Cyber War: The Next Threat to National Security and What to Do About It*, New York 2012.

Clayton M., *Cyber Pearl Harbor': Could future cyberattack really be that devastating?,* „The Christian Science Monitor" 2012, 07 grudnia.

*Cyberwar. The threat from the internet*, „The Economist", źródło: http://www.economist.com (dostęp: 12.08.2016).

Deibert R. J., Rohozinski R., *Risking Security: Policies and Paradoxes of Cyberspace Security*, „International Political Sociology" 2010, vol. 4/1.

Isenberg D., *A cyber Pearl Harbor? More hype than threat*, „Journal of Commerce", 28 grudnia 1999.

J. Stone, *Cyber War Will Take Place!,* „Journal of Strategic Studies" 2012, vol. 36/1.

Jensen M. J., Danziger J. N, Venkatesh A., *Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics*, „The Information Society" 2007, vol. 23/1.

Junio T. J., *How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate*, „Journal of Strategic Studies" 2013, vol. 36/1.

Mazanec B. M., Thayer B., *Deterring Cyber Warfare. Bolstering Strategic Stability in Cyberspace*, Palgrave Macmillan 2016.

Messmer E., *Stuxnet and Flame share code, development teams: Kaspersky Lab says early version of Stuxnet has a Flame module*, „Network World" 2012, 11 czerwca;

*National Security Presidential Directives [NSPD] George W. Bush Administration, NSPD 54: Cybersecurity Policy*, źródło: https://fas.org (dostęp: 12.08.2016).

Nye J. S., *The Future of Power*, New York 2011.

Oates B., *Cyber Crime: How Technology Makes it Easy and What to do About it*, „Information Systems Management" 2001, vol. 18/3.

Ormrod D., Turnbull B., *The cyber conceptual framework for developing military doctrine*, „Defence Studies" 2016, vol. 16/3.

Peterson D., *Offensive Cyber Weapons: Construction, Development, and Employment*, „Journal of Strategic Studies" 2013, vol. , 36/1.

Richards J., *Cyber-War.The Anatomy of the Global Security Threat*, Palgrave Macmillan 2016.

Rid T., *Cyber War Will Not Take Place*, „Journal of Strategic Studies" 2012, vol. 35/1.

Rid T., McBurney P., *Cyber-Weapons*, „The RUSI Journal" 2012, vol. 157/1.

Roberts L. D., Indermaur D., Spiranovic C., *Fear of Cyber-Identity Theft and Related Fraudulent Activity*, „Psychiatry, Psychology and Law" 2013, vol. 20/3.

Schroefl J., Kaufman S. J., *Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War*, „Studies in Conflict & Terrorism" 2014, vol. 37/10.

Simpson B., Murphy M., *Cyber-privacy or cyber-surveillance? Legal responses to fear in cyberspace*, „Information & Communications Technology Law" 2014, vol. 23/3.

Soler U., *Cyberculture in the City on the Example of Lublin,* [w:] *Peripheral Metropolitan Areas in the European Union. The Case of Lublin*, red. Z. Pastuszak, M. Sagan, K. Żuk, Bangkok- Celje-Lublin 2015.

Soler U., *Rola nowoczesnych technologii w cyberwojnie*, [w:] *E-gospodarka w Europie Środkowej i Wschodniej. Teraźniejszość i perspektywy rozwoju*, red. R. Sobiecki, Lublin 2015.

*Stop supporting IS': Anonymous declares cyber war on Turkey*, „Daily Times" 2015, 23 grudnia.

Summers Ch., *Hacking group Anonymous declares 'cyber war' on Turkey for 'supporting ISIS'*, „Daily Star" 2015, 23 grudnia.

Thomas T., *Creating Cyber Strategists: Escaping the 'DIME' Mnemonic*, „Defence Studies" 2014, vol. 14/4.

Trim P., Upton D., *Cyber Security Culture. Counteracting Cyber Threats through Organizational Learning and Training*, New York 2016.

Vacca W. A, *Military Culture and Cyber Security*, „Survival .Global Politics and Strategy" 2011, vol. 53/6.

**Bogusław Węgliński**

Dolnośląska Szkoła Wyższa

# Cyberterroryści w cyfrowych czasach – profesjonalizacja i digitalizacja współczesnych organizacji terrorystycznych

Słowa kluczowe: Al-Kaida, Państwo Islamskie, cyberterroryzm; terroryzm, Internet, media cyfrowe, ustawa antyterrorystyczna, drony.

## Wprowadzenie: ewolucja instrumentarium terrorystycznego

Terroryści i przestępcy zawsze korzystali ze zdobyczy cywilizacji, także tych technicznych. Przejawem technologicznego zaawansowania terrorystów był choćby atak za pomocą gazu sarin w tokijskim metrze. Z drugiej strony możemy znaleźć mnóstwo przykładów na to, iż pomimo znaczących przeobrażeń współczesnego świata i rewolucji technologicznej oręż terrorystów nie zmienił się praktycznie w przeciągu ostatnich 150 lat. Pistolety, czy ładunki wybuchowe w dalszym ciągu stanowią groźny oręż w rękach terrorystów XXI w. i są dla społeczeństwa takim samym zagrożeniem jak dla pokoleń o wiek przynajmniej wcześniejszych. Zwracał na to uwagę w 1998 roku Zbigniew Brzeziński[1]. Niewiele później terroryści zrealizowali scenariusz użycia samolotów komunikacyjnych jako latających bomb. 11 września 2001 roku. Stał się on ponurą cezurą w historii ludzkości a widok walących się wież WTC w dalszym ciągu spędza sen z powiek służbom bezpieczeństwa na całym świecie. Jak na ironię, głównym zagrożeniem dla załóg porywanych w tym dniu samolotów były użyte przez terrorystów plastikowe noże do papieru oraz atrapy bomb. Renesans użycia broni białej widać także w serii palestyńskich ataków nożowników w Izraelu na przełomie ubiegłego i bieżącego roku. Alternatywną metodą ataków stało się jednak użycie samochodów i innych

[1] Z. Brzeziński, *Kłopoty dobrego hegemona*, źródło: http://szukaj.wyborcza.pl (dostęp: 06.05.2016).

pojazdów (używano także ładowarek) jako narzędzi do „rozjeżdżania" przystanków i grup przechodniów. Potwierdzeniem tej tezy stał się niestety atak z Nicei, gdzie niezależnie od inspiracji zamachowca, rozpędzona ciężarówka służyła jako narzędzie mordu[2]. Warto przy tym przypomnieć, że Francja była już celem tego typu ataków w grudniu 2014 roku, kiedy na szczęście skończyło się tylko na osobach rannych[3]. Obawiam się, że prostota działania i przerażająca „skuteczność" akcji może stać się inspiracją do przeprowadzania podobnych zamachów w przyszłości. Widać na tej podstawie, że działalność współczesnych organizacji terrorystycznych może się rozwijać wielotorowo. W dalszych fragmentach artykułu postaram się przybliżyć, te bardziej wyrafinowane technologicznie metody działań związanych z użyciem cyberprzestrzeni oraz pozwiązane z nimi wybrane rozwiązania ustawodawcze.

## Technologie cyfrowe w służbie terrorystów

To nie wyposażenie, ale istota podejmowanych działań, która nie uległa zmianie świadczy o zagrożeniu jakie stwarzają współcześni terroryści. Trafnie zwraca na to uwagę Bartosz Bolechów[4].

W artykule postawiłem hipotezę, że współcześni terroryści wzorem swoich poprzedników wykorzystują instrumentarium swojej epoki, korzystając ze współcześnie dostępnych nowoczesnych technologii. Oprócz wyposażenia, czerpią oni także know how, czyli adaptują to co skuteczne w dzisiejszych metodach pracy i organizacji do funkcjonowania ugrupowań terrorystycznych. Hipotezie towarzyszy zestaw pytań badawczych:

[2] 14 lipca w godzinach wieczornych dokonano dwukilometrowego rajdu przez zatłoczoną promenadę nadmorską w Nicei. W jej wyniku 84 osoby zmarły, a ok. 200 odniosło różnego rodzaju obrażenia. Liczba ofiar nie musi być zamknięta, ponieważ część rannych w dalszym ciągu przebywa w stanie krytycznym. O ile władze francuskie sugerują powiązania sprawcy z islamskimi bojownikami, a ISIS „przyznało się" do przeprowadzenia zamachu, nie jest oczywiste, czy sprawca – 31-letni Mohamed Lahoualej Bouhlel, Tunezyjczyk, z prawem stałego pobytu we Francji rzeczywiście dokonał swego czynu w imię walki z „niewiernymi", czy po prostu przeszedł ostre załamanie psychiczne. Nie zmienia to faktu, że było to najkrwawsze dotychczas wykorzystanie samochodu jako narzędzia terroru; por. także *Zamach w Nicei. Francuska policja zatrzymała trzy osoby*, http://wiadomosci.gazeta.pl (dostęp: 17.07.2016).

[3] W grudniu 2014 odnotowano zamachy w Dijon i Nantes. Obaj sprawcy użyli samochodów do wjechania w tłum, wznosząc przy tym okrzyki związane z islamem. W Dijon rany odniosło 13 a w Nantes 10 osób. (*Francja: kolejny atak islamskiego radykała? Auto wjeżdża w tłum przechodniów w Nantes*, www.polskieradio.pl <<dostęp: 17.07.2016>>).

[4] B. Bolechów, *Terroryzm w świecie podwubiegunowym*, Toruń, 2002, s. 496-497.

1. Czy dzisiejsze organizacje terrorystyczne korzystają ze współczesnych osiągnięć technologicznych i organizacyjnych ?

2. Jak wygląda obecność organizacji terrorystycznych we współczesnych mediach cyfrowych? Na ile profesjonalna jest ich zawartość?

3. Czy współczesne państwa, w tym Polska są przygotowane na użycie nowoczesnych technologii, w tym dronów przez terrorystów?

Dzięki możliwościom, jakie stwarza jednak dzisiejsza technologia, użycie przez islamskich terrorystów miecza lub sztyletu, którym przed okiem kamery służącej do transmisji wydarzenia w sieci WWW dokonują oni egzekucji przedstawiciela naszej cywilizacji, nawet wydawałoby się przestarzała technologicznie biała broń może w dalszym ciągu służyć do zastraszania szerokich rzesz „niewiernych" odbiorców. Ten sam film oglądany przez inną grupę odbiorców wywoła euforyczne uniesienie dla toczonej przez nią walki, a niezdecydowanych może przekonać do wstąpienia w szeregi bojowników lub choćby sprowokować do wsparcia finansowego dzieła (oczywiście też przy pomocy nowoczesnych technologii bankowych). Niezależnie od etycznej wartości działań użyć możemy tych samych narzędzi. Tak krytykowany przecież za możliwość jego użycia w złych celach Internet może przecież służyć do propagowania idei demokratycznych w społeczeństwach zamkniętych[5], a nowe, cyfrowe technologie w rękach dyktatorów wydają się zagrożeniem porównywalnym z wykorzystaniem ich przez terrorystów[6].

Bruce Hoffman zauważa: „Narzędziami terrorystów są dzisiaj nie tylko bomby i rewolwery. Nowoczesny arsenał terrorysty obejmuje komputery i laptopy, nagrywarki CD i DVD, konta e-mailowe, Internet i sieć WWW. Terroryści dzięki nowym mediom mogą nie tylko kontrolować treść i kontekst przekazów, ale także środki, jakimi docierają do cyberprzestrzeni, i dobierać je stosownie do specyficznych grup odbiorców"[7].

Gabriel Weimann wyodrębnił typologię zastosowań Internetu przez grupy terrorystyczne. Najczęściej pełnione przez Internet role to :

1. sieć używana jako baza danych,
2. utrzymywanie kontaktu przez sieć WWW pomiędzy komórkami organizacyjnymi terrorystów,
3. internetowa rekrutacja i poszukiwania specjalistów,

[5] T. Danitz, W. P. Strobel, *Networking dissent: Cyber activists use the Internet to promote Democracy in Burma*, [w:] *Networks and Netwars*. red. Arquila J., Ronfeldt D, Santa Monica 2001, s. 129-169.
[6] D. Ronfeldt, J. Arquilla, *What next for networks and netwars?*, [w:] *Ibidem*, s. 314.
[7] B. Hoffman, *Foreword*, [w:] G. Weimann, *Terror on the Internet. The New Arena, the New Challenges*, Washington 2006, s. 9.

4. sieć jako miejsce przesyłania (zamieszczania) instrukcji i poradników,
5. sieć WWW jako narzędzie planowania i koordynacji działań,
6. miejsce zdobywania funduszy i zasobów,
7. internet jako miejsce walki z innymi organizacjami terrorystycznymi.[8]

Z zasobów i możliwości oferowanych przez wirtualną przestrzeń sieci chętnie korzystają obie strony konfliktu. W roku 2011, swoje konta na Twitterze uruchomili zarówno talibowie (@alemerahweb) jak i somalijskie Al-Shabaab (@HSM-Press). Jednocześnie konta utworzyli ich oponenci, kontyngent sił stabilizacyjnych NATO – (@ISAFmedia), czy mjr Emmanuel Chirchir (@MajorEChirchir), rzecznik kenijskiej armii w trakcie interwencji w Somalii[9]. Biorąc pod uwagę różnorodność proponowanych zastosowań, niewiele z dzisiejszych grup terrorystycznych może sobie pozwolić w kontekście ewolucji struktury, metod i celów działania na niekorzystanie z zaawansowanych technologii. Al-Kaida, czy jej współczesny sojusznik, a czasami konkurent - ISIS sprawnie wykorzystywały możliwości oferowane w wirtualnej przestrzeni. Obie organizacje nie stronią także od prowadzenia własnej polityki informacyjnej z wykorzystaniem mediów głównego nurtu. O ile Osama bin Laden chętnie przekazywał swoje przesłania telewizji Al Jazeera, o tyle wypowiedzi kalifa ISIS bez problemu można ściągnąć z sieci. Jak zauważa Patryk Cockburn „połowa świętej wojny toczy się w mediach. [...] Facebook, Twitter, YouTube oraz stacje telewizyjne codziennie przynoszą nowe informacje dotyczące idei, działań i celów sunnickich fundamentalistów. Mając dostęp do tak potężnych narzędzi propagandowych, ugrupowania w rodzaju Al-Kaidy nie muszą martwić się o napływ funduszy i ochotników”[10]. Nic dziwnego, że terroryści tak chętnie korzystają z Internetu skoro narzędzie to charakteryzuje:

- łatwy dostęp,
- niewielka (lub żadna) regulacja, cenzura albo inne formy kontroli państwowej,
- potencjalne wielkie audytoria rozproszone na całym świecie,
- anonimowość komunikowania,

[8] G. Weimann, *Terror on the Internet. The New Arena, the New Challenges*, Washington 2006, s. 111-146.
[9] D. Bennett, *Exploring the impact of an evolving war and terror blogosphere on traditional media coverage of conflict*, „Media, War & Conflict ” 2013, vol. 6, issue 1, s. 48.
[10] P. Cockburn, *Państwo Islamskie*, Warszawa 2015, s.168.

- szybki przepływ informacji,
- niezbyt kosztowne przygotowanie i utrzymanie portalu,
- multimedialność (możliwość łączenia tekstu, grafiki, słowa, muzyki filmu) oraz wymiana i ściąganie z sieci plików wideo, muzycznych itd.,
- zdolność podsuwania tematów tradycyjnym mass mediom, które coraz częściej traktują Internet jako źródło wiadomości[11].

Zachęcone możliwościami tkwiącymi w tym prostym narzędziu, organizacje terrorystyczne adaptują się do wymogów współczesnego świata. Al-Kaida, obecna w sieci od późnych lat 90-tych[12] ubiegłego wieku, dysponowała przez lata systemem informatycznym określanym przez służby jako Obelisk[13]. Do 2007 roku działał on na trzech, różnych płaszczyznach. Amerykańskie służby specjalne złamały

w pewnym momencie zabezpieczenia go chroniące, jednak przeciek medialny dotyczący nieujawnionego jeszcze przez organizację wystąpienia Bin Ladena musiał spowodować konsternację i potrzeby zmian w sieciowych zasobach i narzędziach organizacji[14]. Trzy poziomy zastosowań Internetu w Al-Kaidzie miały wyglądać następująco:

- na poziomie ścisłego kierownictwa organizacji funkcjonowała sieć do której dostęp miało tylko ok. 20 osób,
- na kolejnym stopniu, który obejmował krąg użytkowników średniego

  i niższego stopnia mogli się oni do niego dostać po wpisaniu haseł dostępu. Sam system pozostawał stosunkowo mobilny, co zabezpieczało go przed atakami służb na serwery go obsługujące,
- organizacja dysponowała także szeroką gamą, (ich liczba dynamicznie się zmieniała, jednak można mówić o 4-6 tys.) ogólnodostępnych stron internetowych skierowanych do sympatyków i osób „niezrzeszonych" pełniących funkcję propagandową, szkoleniową i rekrutacyjną[15].

[11] B. Hoffman*, op.cit.*, s. 9-11.
[12] D. E. Denning, *Terror`s Web: How the Internet Is Transforming Terrorism*, [w:] *Handbook of Internet Crime*, red. Y. Jewkes, M. Yar, London 2010, s. 195-196.
[13] B. Bolechów, *„Baza" w sieci. Wykorzystanie Internetu przez Al-Kaidę i jej zwolenników*, [w:] *Terroryzm w medialnym obrazie świata*, red. K. Liedel i S. Mocek, Warszawa 2010, s. 146-147.
[14] E. Lake, *Al Qaeda Breach Called 'Serious' but 'Reparable'*, źródło: www.nysun.com (dostęp: 19.07.2016).
[15] B. Bolechów, *„Baza" w sieci*… , s. 146-147.

Celem bojowników była także walka z infrastrukturą sieciowa i zawartością stron „niewiernych". Już w 2003 roku powstał Arabski Zespół Dżihadu Elektronicznego. Na szczęście główny, założony wtedy cel[16], którym było zniszczenie wszystkich izraelskich i amerykańskich witryn nie został dotychczas zrealizowany. Przedsięwzięcie wykraczało poza ramy Al-Kaidy, jednocząc wszystkich wokół wyznawanej idei. W ciągu zaledwie 7 lat od momentu kiedy meksykańscy zapatyści po raz pierwszy użyli Internetu do świadomej promocji i informowania o swoich działaniach[17] ten aspekt funkcjonowania organizacji terrorystycznej przeszedł gruntowną ewolucję. Cele działania e-dżihadystów zostały rozbudowane i obejmowały miedzy innymi:

- likwidację internetowych stron, które w jakikolwiek sposób obrażały muzułmanów,
- godne pomszczenie męczenników, którzy oddali swoje życie za Allaha a także innych prześladowanych jego wyznawców,
- ekonomiczne i moralne osłabienie użytkowników sieci WWW na Zachodzie,
- całkowity paraliż działalności infrastruktury komputerowej Zachodu doprowadzić ma do jego upadku[18].

Wobec prezentowanej, niewzruszonej postawy etycznej bojowników zaskakujące mogą być informacje jednego z byłych decydentów amerykańskiego wywiadu, który twierdzi, że komputery bojowników ISIS w większości wypełnione są treściami pornograficznymi[19]. Badający aktywność sieciowych bojowników Eli Alshech zauważa, że w początkowym okresie działania` w sieci (do roku 2006) ataki kierowano przeciwko trzem typom celów:

1. Atrakcyjnym celem były strony WWW propagujące niemuzułmańskie (w rozumieniu bojowników) ideologie: chrześcijaństwo, syjonizm, szyityzm(!).
2. Atakowano także strony promujące zakazane dla wyznawców Allaha aktywności (np. sportowe zaangażowanie kobiet).

[16] *Ibidem*, s. 147.
[17] D. E. Denning, *op. cit.*, s. 194-195; O zapatystach i ich działalności w sieci pisał także Michał Bogusz, por. M. Bogusz, *Ejército Zapatista de Liberación Nacional - wirtualna partyzantka*, [w:] *Terroryzm w medialnym obrazie świata*, red. K. Liedel i S. Mocek, Warszawa 2010, s. 162-172.
[18] B. Bolechów, *„Baza" w sieci* …, s. 150.
[19] L. Ferran, E. Brown, J.G. Meek, J. Fishel, *Jihadists' Computers '80 Percent' Full of Porn, Ex-Official Says*, źródło: http://abcnews.go.com (dostęp: 21.07.2016).

3. Na celowniku bojowników były także internetowe witryny, fora dyskusyjne i inne formy sieciowej aktywności, które urażały lub obrażały muzułmanów[20].

Al-Kaida wykorzystywała w swojej medialnej aktywności całą sieć mniej lub bardziej profesjonalnych producentów. Materiały ich produkcji zawierały zarówno logo wytwórcy, jak i zbrojnej grupy, którą promowały[21]. Interesującymi z punktu widzenia badacza było rozesłanie w maju 2008 roku przez Brygady Cyberdżihadu ponad 26 tys. maili do mieszkańców rejonu Zatoki Perskiej z informacją o celach działania organizacji, czy użycie do własnych celów neutralnych stron internetowych - znamienne było tu użycie arabskiej mutacji Wikipedii, na której umieszczano orędzia współpracującego jeszcze wtedy a Al-Kaidą Omara al-Baghdadiego[22]. Późniejsze dokonania cyfrowych mudżahedinów co pewien czas przykuwają uwagę światowych mediów. W 2015 roku skutecznie zakłócili oni funkcjonowanie stron francuskiej telewizji TV5[23]. Należy się spodziewać, że aktywność dżihadystów w sieci będzie narastała, choć oczywiście zdarzają się tez grupy hakerów, którzy atakują infrastrukturę sieciową bojowników[24].

W cyfrowy świat wpisują się także twórcy gier, w których gracze mogą się wcielać zarówno w przedstawicieli służb zwalczających terrorystów, jak i bojowników[25]. Widać w tym segmencie rynku zwiększającą się podaż produktów umożliwiających destrukcję świata, a nie jego obronę. Negatywni bohaterowie nie umierają w nich, lecz szybko wracają do kreowanej w grze rzeczywistości[26] Co więcej, możliwość szybkiego „odrodzenia" gracza po wirtualnej śmierci może wprowadzać zamieszanie w psychice młodych ludzi, co skutkuje atakami szalonych strzelców w Stanach Zjednoczonych i innych krajach, jak i terrorystycznymi atakami tzw. „samotnych wilków". Wpływ brutalnych gier komputerowych niewykluczony jest także w przypadku 18-letniego Niemca irańskiego pochodzenia, który 22 lipca

[20] E. Alshech, *Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad*, „Inquiry & Analysis Series Report" 2007, No. 329, s. 4-6.
[21] D. E. Denning, *op.cit*. s. 197-198.
[22] *Ibidem*, s. 198.
[23] *Francuska telewizja ofiarą cyberataku. Hakerzy podają się za dżihadystów*, źródło: http://www.newsweek.pl (dostęp: 22.07.2016).
[24] *Dżihadysta-gej? Zemsta hakera robi furorę*, źródło: http://tvn24bis.pl ( dostęp: 22.07.2016).
[25] M. Schulzke, *Being a terrorist: Video game simulations of the other side of the War on Terror*, „Media, War & Conflict" 2013, vol. 6, issue 3, s, 218.
[26] M. Babecki M., *Funkcje epizodycznych gier internetowych w procesach modelowania wirtualnego wizerunku terrorysty i terroryzmu. Analiza aspektowa*, „Media – Kultura – Komunikacja Społeczna" 2013, nr 9, s. 49.

2016 zastrzelił w Monachium 9 osób i zranił kolejne 30, popełniając potem samobójstwo[27]. Argumenty przytoczone w podrozdziale wydają się potwierdzać hipotezę postawioną wcześniej, dając jednocześnie odpowiedź na część pytań badawczych tam zadanych.

## Zastosowanie dronów – szanse i zagrożenia

Drony i BSL wykorzystywane są często do zwalczania organizacji terrorystycznych[28], z drugiej strony zagrożenie, jakie mogą one stanowić w rękach tych ugrupowań jawi się jako bardzo realne. Dobrze, że świadomość niebezpieczeństw jakie użycie dronów stwarza jest wśród przedstawicieli organów i służb odpowiedzialnych za utrzymanie naszego bezpieczeństwa w miarę wysoka, co przekłada sie na rozwiązania jakie zostały zawarte w nowej tzw. ustawie antyterrorystycznej. Dokument ten zakłada między innymi zmiany w dotychczas obowiązującym prawie lotniczym[29]:

Art. 126a. 1. Bezzałogowy statek powietrzny, w tym model latający, może zostać zniszczony, unieruchomiony albo nad jego lotem może zostać przejęta kontrola, w przypadku gdy:

1) przebieg lotu lub działanie bezzałogowego statku powietrznego: a) zagraża życiu lub zdrowiu osoby, b) stwarza zagrożenie dla chronionych obiektów, urządzeń lub obszarów, c) zakłóca przebieg imprezy masowej albo zagraża bezpieczeństwu jej uczestników, d) stwarza uzasadnione podejrzenie, że może zostać użyty jako środek ataku terrorystycznego;

2) bezzałogowy statek powietrzny wykonuje lot w przestrzeni powietrznej w części której państwowy organ zarządzania ruchem lotniczym wprowadził ograniczenia lotów albo znajdującej się nad terytorium Rzeczypospolitej Polskiej, w której lot statku powietrznego jest zakazany od poziomu terenu do określonej wysokości[30].

[27] *„Nienawiść do ludzi". Kolega ze szpitala psychiatrycznego o zamachowcu* . źródło: http://www.tvn 24.pl (dostęp: 25.07.2016).

[28] Pomimo tego, iż drony coraz częściej używane są zarówno przez siły porządkowe jak i regularną armię pozostaje cały wachlarz wątpliwości etycznych i prawnych towarzyszących tego typu działaniom. Zob. E. Schwarz, *Prescription drones: On the techno-biopolitical regimes of contemporary 'ethical killing'*, „Security Dialogue" 2016, vol. 47(I) , s. 56 i n.; P. Sheets, C.M. Rowling, T. M. Jones, *The view from above (and below): A comparison of American, British, and Arab news coverage of US drones*, „Media, War & Conflict" 2015. vol. 8, issue 3, s. 1-23 .

[29] *Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze, Dz.U. 2002, Nr 130, poz. 1112.*

[30] Art. 39, *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz.U. 2016, poz. 904.*

Ten sam projekt dokumentu określa katalog służb i formacji, które mogłyby nadzorować egzekwowanie prawa w przypadku jego łamania. Zniszczyć, unieruchomić bądź przejąć kontrolę nad lotem BSP może:

- Policja,
- Straż Graniczna,
- Biuro Ochrony Rządu,
- Agencja Bezpieczeństwa Wewnętrznego,
- Agencja Wywiadu,
- Centralne Biuro Antykorupcyjne,
- Służba Kontrwywiadu Wojskowego,
- Służba Wywiadu Wojskowego,
- Służba Celna,
- Służba Więzienna
- żołnierze Żandarmerii Wojskowej i Sił Zbrojnych
- pracownicy specjalistycznych uzbrojonych formacji ochronnych[31].

Lista ta jest nieznacznie mniejsza w przypadku imprez masowych, a siły zbrojne RP maja prawo do działań tego typu w przypadku naruszania przez urządzenie i jego operatora stref zastrzeżonych. Wszystko zależy oczywiście od tzw. zimnej krwi funkcjonariuszy, ale istnieją duże szanse na pełne dramatyzmu artykuły w tabloidach piętnujące „nadgorliwych" obrońców prawa niszczących zabawki dzieciom. Jest to tym bardziej prawdopodobne, iż lot drona kierowanego przez niewprawnego operatora może budzić wątpliwości u postronnych obserwatorów. W kontekście powtarzających się jednak incydentów w okolicach lotnisk oraz zgłaszanych naruszeń stref zakazanych dotyczących najważniejszych osób i instytucji w państwie działania tego typu należy uznać za uprawnione. Nie dotarłem do tej pory do opisu użycia drona jako narzędzia zamachu, ale poprawiające się szybko charakterystyki osiągów tych urządzeń predestynują je do zastosowań terrorystycznych. Wydawało sie przez chwilę, że to siły porządkowe użyły sterowanej, latającej bomby do unieszkodliwienia „snajpera" w Dallas[32], ale okazało się, że wykorzystano urządzenie naziemne, które pozwoliło dostarczyć ładunek wybuchowy

[31] *Ibidem*.

[32] W nocy 8 lipca, doszło przy okazji demonstracji potępiającej brutalność białych funkcjonariuszy policji wobec czarnoskórych zatrzymanych do ataku na funkcjonariuszy policji w Dallas. Snajper (lub kilku sprawców) zabił 5 i ranił kolejnych kilku ( od 6 do 9) policjantów. Po wymianie ognia z policjantami sprawca został zabity. por. *Snajperski ostrzał w Dallas. Napastnik chciał wymordować białych policjantów*, http://www.rmf24.pl (dostęp: 12.07.2016).

blisko przestępcy[33]. Jak bardzo wrażliwy na wszelkie, nawet niezamierzone zakłócenia jest cały funkcjonujący dzisiaj system lotnictwa cywilnego świadczyć może „współzawiniona" przez obce oprogramowanie katastrofa lotnicza w Madrycie w 2008. Osłabiony przez działanie tzw. trojana system bezpieczeństwa nie zareagował na wysyłane z samolotu informacje o awarii, co doprowadziło do śmierci 154 osób[34]. Zamach w Dallas po raz kolejny pokazuje użyteczność nowoczesnych technologii w zwalczaniu zagrożeń dla porządku publicznego. W tej części artykułu udało się odpowiedzieć na zadane wcześniej kolejne z pytań badawczych. Polskie państwo zauważyło potencjał zagrożeń, jaki niesie ze sobą użycie dronów w celach terrorystycznych. Przygotowane na tą okoliczność prawodawstwo umożliwia sprawne reagowanie przez przeznaczone do tego agendy państwa, dając obywatelom większe poczucie bezpieczeństwa.

## Zakończenie

Jeszcze niecałe 200 lat temu, informacje Europy do obu Ameryk płynęły ok. 6 tygodni. Transmisje z zamachu na WTC 11 czerwca 2001 roku zaczęły się ok. 15 minut po uderzeniu pierwszego samolotu, a atak na drugą wieżę można już było oglądać na niemal całym świecie „na żywo"[35]. Nie inaczej jest dzisiaj. Liczne telewizje informacyjne rywalizują ze sobą, o to która z nich przekaże informację o zamachach, wypadkach i katastrofach najszybciej, najdrastyczniej i najskuteczniej. W obliczu wyścigu z czasem i konkurencją we współczesnych mediach często brakuje weryfikacji doniesień, czy też innych elementów właściwych dla profesjonalnego i odpowiedzialnego dziennikarstwa. Sensacyjne informacje wypierają inne przekazy, ponieważ audytorium odbiorców oczekuje „prawdziwego" obrazu rzeczywistości. Nic więc dziwnego, że we współczesnym świecie o wiele więcej uwagi przywiązujemy do nie tak popularnego w końcu zjawiska cyberterroryzmu, co do mogącego nas statystycznie spotkać o wiele bardziej prawdopodobnie przestępstwa w Internecie[36]. To przecież tam odbywa się nieustanne polowanie na nasze hasła

[33] D. Beres *This Is The Robot Dallas Police Used To Kill Shooting Suspect*, źródło: http://www.huffingtonpost.com (dostęp: 12.07.2016).

[34] R. Heickerö, *Cyber Terrorism: Electronic Jihad*, „Strategic Analysis" 2014, vol. 38, no.4, s 556.

[35] P. Wojtunik, J. Bartoszek, G. Biskupska, *Strategie i cele wykorzystywania mediów przez organizacje terrorystyczne*, [w:] *Polityka medialna instytucji państwowych w obszarze zagrożeń terrorystycznych. Materiały z II edycji międzynarodowej konferencji z cyklu Przeciwdziałanie terroryzmowi. Warszawa, 18 listopada 2008 r.*, Warszawa 2009, s. 10.

[36] por. Y. Jewkes , M. Yar , *Introduction: the Internet, cybercrime and the challenges of the twentyfirst century*, [w:] *Handbook of Internet Crime*, red. Y. Jewkes , M. Yar , London 2010, s. 4-7.

dostępu, dane osobowe, czy choćby informacje o naszych internetowych preferencjach zakupowych. ONZ prognozuje, że już w 2020 roku trudno będzie o przestępstwo nie powiązane w żaden sposób ze sferą Internetu[37].

Przerażeni cyberdżihadystami zapominamy też o terrorystach działających w imieniu, czy też na zamówienie legalnych rządów. Potwierdzono tego typu aktywność Północnej Korei[38], Chin, a tajemnicą poliszynela są działający na zlecenie Rosji sprawcy ataków na infrastrukturę krytyczną Ukrainy[39]. Również do Rosji prowadzą ślady najnowszej afery związanej z ujawnieniem potencjalnych nadużyć w sztabie Partii Demokratycznej w USA[40]. Ta sama cyberprzestrzeń stwarza zagrożenia dla krajów niedemokratycznych, które nie zawsze są w stanie zapanować nad jej zawartością. Satelity i Facebook jawią się notablom w Iranie jako narzędzia „miękkiej wojny"[41] Epatowani na co dzień mrożącymi krew w żyłach obrazami i relacjami przejmujemy wizję świata złego i zagrażającego nam, nie zauważając, że przyjmujemy tylko jedną z jego sztucznych kreacji, która przywiąże nas do nadawców informacji i ew. sprzedawców/promotorów kolejnych metod na zapewnienie nam bezpieczeństwa. Te same media utrudniają czasami działania służb ujawniając zbyt wiele szczegółów ich działań, a czasem same biorą na siebie rolę śledczych[42].

Dostosowanie miast do zagrożeń terrorystycznych otwiera także szeroką drogę do zleceń dla szeroko rozumianego sektora budowlanego, z którego niewątpliwie wygeneruje się specjalistyczna odnoga budownictwa (dla) bezpieczeństwa. Takie są nasze czasy i zagrożenia im towarzyszące, co zmusza nas do uwzględniania ich

[37] *Comprehensive Study on Cybercrime, Draft, February 2013*, United Nations Office on Drugs and Crime, New York 2013, s. 4-50, por także S. Tripathi, *Cyber: Also a Domain of War and Terror*, „Strategic Analysis" 2015, vol. 39, issue1, s. 1-2.

[38] R. Heickerö, *Cyber Terrorism…*, s 556.

[39] Taką informację udostępniła telewizja CNN powołując się na wypowiedź wiceszefowej Departamentu Energii USA Elizabeth Sherwood-Randall. Por także: *USA unikają oficjalnego oskarżenia Rosji o atak hakerski na Ukrainę*, źródło: http://biznesalert.pl (dostęp: 21.07.2016).

[40] A. Phillips, *Clinton campaign manager: Russians leaked Democrats' emails to help Donald Trump*, źródło: https://www.washingtonpost.com (dostęp: 25.07.2016).

[41] Tak wypowiadał się Minister Spraw Wewnętrznych Iranu –Mostafa Najjar, a szef Irańskich Strażników Rewolucji - Abdollah Araghi zapewniał, że jego formacja posiada juz narzędzia do walki z tego typu zagrożeniami , które mogą być groźniejsze niż wojna fizyczna. Zob. J.A. Lewis, *National Perception of Cyber Threats,* „Strategic Analysis" 2014, vol. 38, issue 4, s.574.

[42] Po zamachu w Bostonie w 2013 roku internauci i media ochoczo typowali potencjalnych sprawców, publikując ich wizerunki w ogólnokrajowych/globalnych (?) mediach. zob. także B. Węgliński, *Analiza wybranych aktów terrorystycznych w roku 2013. Odrodzenie Al-Kaidy?*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, vol.8, nr 1, s.186-187.

w codziennych przedsięwzięciach, jakie podejmujemy, a listy gończe z podobiznami domniemanych terrorystów możemy zobaczyć w mediach, czy na słupach i wystawach sklepowych.

Podsumowując, udało mi się potwierdzić postawioną w tekście hipotezę. Współcześni terroryści zarówno korzystają z nowoczesnych rozwiązań technologicznych jak i organizacyjnych. W profesjonalny sposób prowadzone media społecznościowe, a także inne cyfrowe kanały przekazu to potwierdzają. Obecność w strukturach organizacji terrorystycznych wykwalifikowanych specjalistów z zakresu dziennikarstwa cyfrowego, logistyki czy choćby budowy ładunków i planowania nie dają cienia wątpliwości, co do procesu profesjonalizacji we współczesnym terroryzmie. Można mówić wręcz o ich korporacyjnym modelu działania. Zaskakujący jest jednoczesny, zauważalny w ostatnich latach trend do delegowania części działań na poziom jak najbardziej "amatorski" - przykładem tego będzie aktywność "samotnych wilków". Nie zmienia to faktu, że "amatorów" motywuje do akcji działalność profesjonalistów. Pozytywna jest także odpowiedź na pytanie o stopień przygotowania do użycia przez terrorystów dronów i innych BSL. Na poziomie prawodawstwa problem jest rozstrzygnięty, a rozwojowi tej technologii towarzyszą badania nad wytworzeniem urządzeń je neutralizujących.

Należy oczywiście założyć, że wraz z dalszym rozwojem cywilizacji i technologii, terroryści będą je adaptowali do swoich celów na podobnych zasadach, jak robią to już dziś. Ważne jest jedynie to, aby służbom zwalczającym terrorystów udawało się być zawsze krok przed nimi.

## Bibliografia

*„Nienawiść do ludzi". Kolega ze szpitala psychiatrycznego o zamachowcu*, źródło: http://www.tvn24.pl (dostęp: 25.07.2016).

Alshech E., *Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad*, „Inquiry & Analysis Series Report" 2007, No. 329.

Babecki M., *Funkcje epizodycznych gier internetowych w procesach modelowania wirtualnego wizerunku terrorysty i terroryzmu. Analiza aspektowa*, „Media – Kultura – Komunikacja Społeczna" 2013, nr 9.

Bennett D., *Exploring the impact of an evolving war and terror blogosphere on traditional media coverage of conflict*, „Media, War & Conflict " 2013, vol. 6, issue 1.

Beres D., *This Is The Robot Dallas Police Used To Kill Shooting Suspect*, źródło: http://www.huffingtonpost.com (dostęp: 12.07.2016).

Bogusz M., *Ejército Zapatista de Liberación Nacional - wirtualna partyzantka*, [w:] *Terroryzm w medialnym obrazie świata*, red. K. Liedel, S. Mocek, Warszawa 2010.

Bolechów B., *„Baza" w sieci. Wykorzystanie Internetu przez Al-Kaidę i jej zwolenników*, [w:] *Terroryzm w medialnym obrazie świata*, pod red. K. Liedel i S. Mocek, Warszawa 2010.

Bolechów B., *Terroryzm w świecie podwubiegunowym*, Toruń, 2002.

Brzeziński Z., *Kłopoty dobrego hegemona*, źródło: http://szukaj.wyborcza.pl (dostęp: 06.05.2016).

Cockburn P., *Państwo Islamskie*, Warszawa 2015.

*Comprehensive Study on Cybercrime, Draft, February 2013*, United Nations Office on Drugs and Crime, New York 2013

Danitz T., Strobel W. P., *Networking dissent: Cyber activists use the Internet to promote Democracy in Burma*, [w:] *Networks and Netwars*. red. Arquila J., Ronfeldt D., Santa Monica 2001.

Denning D. E., *Terror`s Web: How the Internet Is Transforming Terrorism*, [w:] *Handbook of Internet Crime*, red. Y. Jewkes, M. Yar, London 2010.

*Dżihadysta-gej? Zemsta hakera robi furorę*, źródło: http://tvn24bis.pl ( dostęp: 22. 07.2016).

Ferran L., Brown E., Meek J. G., Fishel J., *Jihadists' Computers '80 Percent' Full of Porn, Ex-Official Says*, źródło: http://abcnews.go.com (dostęp: 21.07.2016).

*Francja: kolejny atak islamskiego radykała? Auto wjeżdża w tłum przechodniów w Nantes*, źródło: www.polskieradio.pl (dostęp: 17.07.2016).

*Francuska telewizja ofiarą cyberataku. Hakerzy podają się za dżihadystów*, źródło: http://www.newsweek.pl (dostęp: 22.07.2016).

Heickerö R., *Cyber Terrorism: Electronic Jihad*, „Strategic Analysis" 2014, vol. 38, no.4.

Hoffman B., *Foreword*, [w:] G. Weimann, *Terror on the Internet. The New Arena, the New Challenges*, Washington 2006.

Jewkes Y., Yar M., *Introduction: the Internet, cybercrime and the challenges of the twentyfirst century*, [w:] *Handbook of Internet Crime*, red. Y. Jewkes, M. Yar , London 2010.

Lake E., *Al Qaeda Breach Called 'Serious' but 'Reparable'*, źródło: www.nysun.com (dostęp: 19.07.2016).

Lewis J. A., *National Perception of Cyber Threats,* „Strategic Analysis" 2014, vol. 38, issue 4.

Phillips A., *Clinton campaign manager: Russians leaked Democrats' emails to help Donald Trump*, źródło: https://www.washingtonpost.com (dostęp: 25.07.2016).

Ronfeldt D., Arquilla J., *What next for networks and netwars?*, [w:] *Networks and Netwars*. red. Arquila J., Ronfeldt D, Santa Monica 2001.

Schulzke M., *Being a terrorist: Video game simulations of the other side of the War on Terror*, „Media, War & Conflict" 2013, vol. 6, issue 3.

Schwarz E., *Prescription drones: On the techno-biopolitical regimes of contemporary 'ethical killing'*, „Security Dialogue" 2016, vol. 47(I).

Sheets P., Rowling C. M., Jones T. M., *The view from above (and below): A comparison of American, British, and Arab news coverage of US drones*, „Media, War & Conflict" 2015. vol. 8, issue 3.

*Snajperski ostrzał w Dallas. Napastnik chciał wymordować białych policjantów*, http://www.rmf24.pl (dostęp: 12.07.2016).

Tripathi S., *Cyber: Also a Domain of War and Terror*, „Strategic Analysis" 2015, vol. 39, issue1

*USA unikają oficjalnego oskarżenia Rosji o atak hakerski na Ukrainę*, źródło: http://biznesalert.pl (dostęp: 21.07.2016).

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

*Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze, Dz.U. 2002, Nr 130, poz. 1112.*

Weimann G., *Terror on the Internet. The New Arena, the New Challenges*, Washington 2006.

Węgliński B., *Analiza wybranych aktów terrorystycznych w roku 2013. Odrodzenie Al-Kaidy?,* „Rocznik Bezpieczeństwa Międzynarodowego" 2014, vol.8, nr 1.

Wojtunik P., Bartoszek J., Biskupska G., *Strategie i cele wykorzystywania mediów przez organizacje terrorystyczne*, [w:] *Polityka medialna instytucji państwowych w obszarze zagrożeń terrorystycznych. Materiały z II edycji międzynarodowej konferencji z cyklu Przeciwdziałanie terroryzmowi. Warszawa, 18 listopada 2008 r.*, Warszawa 2009.

*Zamach w Nicei. Francuska policja zatrzymała trzy osoby*, źródło: http://wiadomosci.gazeta.pl (dostęp: 17.07.2016).

**Bogusław Olszewski**
Uniwersytet Wrocławski

# Ataki cyber-fizyczne a system bezpieczeństwa narodowego

Słowa kluczowe: system cyber-fizyczny, bezpieczeństwo międzynarodowe, cyberprzestrzeń

## Uwagi wstępne

Klasyczne cyberataki skupiają się głównie na zawartości informacyjnej, obierając jako cel zarówno urządzenia umożliwiające wymianę danych w obrębie Sieci, jak i przechowywane na nich zasoby, naruszając integralność, poufność i dostępność danych (tzw. triada CIA). Powszechność i dynamiczny rozwój systemów obliczeniowych oraz rozległość łączącej ich infrastruktury telekomunikacyjnej poszerzyły zakres możliwych podatności na atak daleko poza zakłócenie i ograniczenie funkcji urządzeń będących elementami globalnej sieci informacyjnej, realizowanych zwłaszcza w warstwie World Wide Web. Technologie telekomunikacyjne (*information and communication technologies*, ICT) umożliwiają współcześnie nie tylko oddziaływanie na poziomie cyfrowym (logicznym) dla uzyskania pożądanych zdarzeń w dowolnym punkcie cyberprzestrzeni, ale dzięki systemom cyber-fizycznym (*cyber-physical systems*, dalej C-F) stanowią o zaistnieniu tychże w świecie rzeczywistym. Systemy te łączą świat fizyczny i cyberprzestrzeń, umożliwiając wpływanie na rzeczywistość materialną z poziomu warstwy cyfrowej. Pozwalają na ingerencję z jednej lokacji fizycznej w drugą, z wykorzystaniem Internetu jako medium transmisyjnego generującego zamierzone efekty kinetyczne. Dotychczasowy paradygmat charakterystyczny dla świata ery preindustrialnej, kiedy oddziaływanie na elementy świata materialnego wymagało podjęcia adekwatnych działań w obrębie tej samej płaszczyzny, uległ zmianie.

Współcześnie, w efekcie trzeciego etapu rewolucji naukowo-przemysłowej związanego z informatyzacją, systemy automatyki występują powszechnie w połączeniu z urządzeniami IT. Wielorakie konfiguracje umożliwiają ich nadzór z dowolnego miejsca globu, podobnie odczyt i modyfikację parametrów procesów produkcyjnych czy sterowanie elementami układów hydroinżynieryjnych. Na potrzeby niniejszego artykułu przyjęto definicję Helen Gill z National Science Foundation, w myśl której systemy C-F są: „Fizycznymi, biologicznymi i inżynierskimi systemami, których operacje są zintegrowane, monitorowane i/lub kontrolowane przez centrum [rdzeń] obliczeniowe. Komponenty są w każdej skali usieciowione. przetwarzanie danych jest głęboko osadzone w każdym komponencie […] system wbudowany stanowi rdzeń obliczeniowy, zwykle wymaga natychmiastowej odpowiedzi, a sam system jest najczęściej rozproszony”[1].

Ataki cyber-fizyczne stanowią naruszenie bezpieczeństwa cyberprzestrzeni, oddziałują w sposób niepożądany na przestrzeń materialną, skutkując przejęciem kontroli nad kluczowymi aspektami systemu C-F oraz posiadają rozprzestrzeniający się efekt fizyczny. Stały się immanentną częścią współczesnego systemu bezpieczeństwa międzynarodowego, o którym Tomasz Aleksandrowicz pisze: „widoczne jest dążenie do zacierania granic pomiędzy bezpieczeństwem wewnętrznym i zewnętrznym”[2]. Ataki C-F mogą naruszyć (bezpośrednio lub pośrednio) stabilność systemu bezpieczeństwa narodowego oraz międzynarodowego. Wpływając na zachowania podmiotów państwowych i niepaństwowych zmieniają jego strukturę i dynamikę. Już kilka dekad temu Richard Ullman, mówiąc o koncepcji bezpieczeństwa i katalogu zagrożeń, zauważał ich ekspansję – obecnie coraz częściej podkreśla się znaczenie bezpieczeństwa ludzkiego (indywidualnego)[3]. Ten ostatni wymiar staje się nad wyraz istotny w kontekście systemów cyber-fizycznych, tym bardziej że „bezpieczeństwo splata się tymczasem również w zasadniczych swych wymiarach: jednostkowym, narodowym i międzynarodowym”[4].

[1] H. Gill, *A Continuing Vision: Cyber-Physical Systems*, Arlington 2008, s. 3, źródło: https://www.ece.cmu.edu (dostęp: 27.07.2016).
[2] T. R. Aleksandrowicz, *Świat w sieci. Państwa, społeczeństwa ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014, s. 206.
[3] R.H. Ullman, *Redefining Security*, „International Security” 1983, vol. 8, no. 1, ss. 129-153.
[4] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, s. 47.

## Elementy systemów cyber-fizycznych

Komponenty otoczenia cyber-fizycznego można podzielić na kilka podstawowych grup: przetworniki (czujniki oraz aktuatory – urządzenia wykonawcze), kontrolery – w tym programowalne kontrolery logiczne PLC (*Programmable Logic Controler*), systemy wbudowane (osadzone, *embedded systems*), rozproszone systemy sterowania DCS (*Distributed Control Systems*), SCADA (*Supervisory Control And Data Acquisition)* oraz tzw. Internet rzeczy (*Internet of Things*, dalej IoT).

Przetworniki (*transducers*) pozwalają na wymianę i translację stanów energetycznych z informacyjnych na fizyczne i odwrotnie. Wśród nich można wyróżnić czujniki (*sensors*) mierzące wilgotność, ciśnienie atmosferyczne, dystans, ruch, temperaturę, promieniowanie, stan danych funkcji organizmu itp., przesyłające odczyty stanów fizycznych w postaci sygnałów elektrycznych interpretowanych następnie przez system komputerowy. Kontrolery monitorują i korygują zadane warunki działania systemów pod wpływem sygnałów napływających ze zmieniającego się, otaczającego środowiska; aktuatory z kolei zamieniają sygnał elektryczny na ruch mechaniczny, umożliwiając zwrotne oddziaływanie kinetyczne. Systemy osadzone są najczęściej układami elektronicznymi opartymi na mikroprocesorze, są preprogamowane i posiadają ograniczoną funkcjonalność wynikającą z przeznaczenia danego urządzenia, zaś ich oprogramowanie jest, zgodnie z tzw. modelem Berkeley, „ściśle zintegrowane z zarządzanymi procesami fizycznymi”[5]. Typowy system osadzony składa się z interfejsu użytkownika, pamięci, procesora, konwerterów, czujników, portów diagnostycznych, programowalnych układów logicznych, układu wejścia/wyjścia i zasilania.

Sterowniki PLC są kontrolerami pozwalającymi organizować działania logiczne na poziomie urządzenia za pomocą tzw. drabinkowego języka programowania. Automatyzują nadzór nad maszyną, są dedykowaną stacją zdolną obsługiwać wiele rodzajów czujników i aktuatorów. Coraz częściej połączone z rozproszonymi systemami sterowania DCS, które należą do przemysłowych narzędzi kontroli, są zorientowane głównie na procesy produkcyjne przedsiębiorstwa. Stanowią swego rodzaju etap pośredni w łańcuchu kontroli i sterowania agregatami w rodzaju linii produkcyjnych, pozostają najczęściej długookresowo włączone do Sieci. Z kolei systemy SCADA są zorientowane na dane rozproszone geograficznie, a ich istotą jest możliwość odczytu i modyfikacji żądanej informacji (parametrów) w czasie

[5] E. A. Lee, *The Future of Embedded Systems*, źródło: https://chess.eecs.berkeley.edu (dostęp: 28.07. 2016).

rzeczywistym. Jako takie „pozwalają na uzyskanie szybkiego wglądu w faktyczny stan urządzeń produkcyjnych i wykonawczych […] umożliwiają szybką lokalizację alarmów, podstawowe logowanie danych czy też automatyczną reakcję na określone sygnały pochodzące z urządzeń”[6]. System SCADA w warstwie graficznej odpowiada za jednoznaczne zaprezentowanie dynamicznie zmieniającej się informacji. W systemie tego typu „zdefiniowane przez użytkownika algorytmy logiczne przyspieszają i wspomagają operatora w jego pracy”[7], a w szerszej perspektywie system SCADA jest „podstawowym źródłem danych dla systemów nadrzędnych i przemysłowych baz danych”[8]. Dostęp do odległych lokacji, które mogą być monitorowane i zarządzane przez operatora bezpośrednio lub zdalnie poprzez dedykowane urządzenia dostępowe, odbywa się przez transmisję danych telemetrycznych realizowaną za pomocą interfejsu RTU (*Remote Terminal Unit*)[9]. Systemy SCADA posiadają formę specjalistycznego oprogramowania uruchamianego na komputerach produkowanych seryjnie lub występują w postaci urządzeń z preinstalowanym oprogramowaniem, działającym wyłącznie na danej platformie fizycznej.

Ostatnią grupę, Internet rzeczy (*Internet of Things*), nazywany także Internetem wszystkiego, stanowi globalna infrastruktura fizycznych obiektów pozostających online, „to wzajemne połączenie unikatowych wbudowanych urządzeń komputerowych”[10]. W ramach Internetu, głównie na gruncie sieci dedykowanych wyłącznie dla IoT (Ethernet, a przede wszystkim bezprzewodowe: WiFi i Bluetooth), urządzenia wymieniają dane zebrane z otoczenia za pośrednictwem czujników. Ten typ komunikacji *machine-to-machine* (M2M) umożliwia współdzielenie danych w kierunku pełnej automatyzacji ich funkcji. Sprzęt AGD i RTV, aparatura medyczna, pojazdy, a w konsekwencji całe obszary fizyczne są traktowane jako inteligentne węzły (domy, dzielnice, miasta, państwa) i mogą stać się częścią sieci złożonej z miliardów elementów, tworzących w efekcie inteligentne otoczenie. Interpretacji i dalszej implementacji pozyskanych danych ma służyć koncepcja Big Data[11],

[6] *Systemy SCADA*, http://www.astor.com.pl (dostęp: 28.07.2016).
[7] *Ibidem*.
[8] *Ibidem*.
[9] Szerzej na ten temat: *Remote Terminal Unit (RTU)*, http://www.wbsetcl.in (dostęp: 28.07.2016).
[10] M. Miller, *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa 2016, s. 23.
[11] Szerzej na ten temat: S. Mukherjee, R. Shaw, *Big Data – Concepts, Applications, Challenges and Future Scope*, „International Journal of Advanced Research in Computer and Communication Engineering” 2016, vol. 5, issue 2.

jako że tzw. inteligencja IoT jest wynikiem analizy i ekstrapolacji informacji przepływającej w postaci olbrzymiej ilości danych. Jakkolwiek pojęcie inteligencji jest nadużywane w celach marketingowych, to faktycznie - z uwagi na aspekty technologiczne i finansowe – koncepcja znajduje się w swoim początkowym stadium i „mówimy o dziesięcioleciach, które muszą upłynąć, nim większość urządzeń i systemów stanie się kompatybilna i skomunikowana z IoT"[12]. Według prognozy światowego lidera rozwiązań sieciowych Cisco, do 2020 roku liczba urządzeń w ramach Internetu rzeczy osiągnie 50 mld[13]. Jak dotychczas, IoT posiada przede wszystkim wymiar komercyjny i jako taki stanowi nową ofertę na stosunkowo niedużym rynku urządzeń tego typu. Brak spójnej polityki cyberbezpieczeństwa czyni je jednak już teraz łatwym celem dla wszystkich zainteresowanych wykorzystaniem ich podatności. IoT umożliwia penetrację Sieci jako jej stosunkowo najsłabiej zabezpieczony komponent, zwłaszcza że dostawcy tych rozwiązań operują szerokimi kontekstami – taki stan rzeczy czyni zagadnienie bezpieczeństwa międzynarodowego jeszcze bardziej nieostrym.

## Systemy C-F a bezpieczeństwo międzynarodowe

Systemowe ujęcie bezpieczeństwa międzynarodowego wciąż lokuje państwa jako jego najistotniejsze i immanentne elementy, jednak nie są już one odizolowane ponieważ „inne podmioty społeczne występujące w stosunkach międzynarodowych oddziałują na państwa w takim wymiarze, który wynika ze stopnia współzależności i oddziaływań państw oraz stosunków, które posiadają w środowisku międzynarodowym"[14]. Instytucjonalne formy współpracy kreują i ustanawiają między państwami związki o charakterze systemowym, będące ostatecznie podstawą bezpieczeństwa międzynarodowego. Transformujący charakter *modus operandi* związanego z globalizacją bezpieczeństwa sprawia, że „systemowa postać stosunków międzynarodowych tworzy systemową postać bezpieczeństwa państwa"[15]. Uniwersalność modelu sieciowego pozwala określić ów kształtujący się paradygmat bezpieczeństwa narodowego takim samym mianem: „Sieciowy paradygmat bezpieczeństwa państwa zakłada zatem istnienie i funkcjonowanie stosunków międzyna-

[12] M. Miller, *op. cit.,* s. 29.
[13] D. Evans, *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*, „Cisco White Paper" 2014, s. 3.
[14] J. Gryz, *Państwo w systemie bezpieczeństwa międzynarodowego*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, vol. 8, nr 2, s. 111.
[15] *Ibidem*.

rodowych w postaci sieci […] państwa stanowią węzły o charakterze stałym i zajmują pozycję *hubów*"[16]. Nie są one także monolityczne, jak chociażby w teoretycznym ujęciu realizmu, ale same stanowią konglomerat złożonych systemów – w tym systemów cyber-fizycznych. Przyjęcie tej optyki oznacza przejście na coraz niższe warstwy systemu, obejmując elementy dotychczas zupełnie pomijane w kontekście bezpieczeństwa międzynarodowego. Jest to naturalna konsekwencja i cecha charakterystyczna paradygmatu sieciowego, który „powoduje spadek znaczenia czynnika geograficznego i czynnika czasu przy równoczesnym wzroście roli czynnika technologicznego"[17] i w obrębie którego „wzrasta wrażliwość podmiotów na zagrożenia związane z wykorzystywaniem wysoko rozwiniętych technologii komunikacyjnych"[18].

Kooperacja na płaszczyźnie instytucjonalnej sprawia, że relacje systemowe pojawiają się nie tylko między państwami czy dużymi graczami na polu współczesnych stosunków międzynarodowych (korporacje, organizacje międzyrządowe, NGOs itp.). Globalny system bezpieczeństwa ulega postępującej fragmentacji, czego efektem jest sektorowa analiza bezpieczeństwa, której to zasadność jest obecnie z ww. względów dyskutowana. Jednocześnie, państwo jako wciąż najistotniejszy podmiot SM oddziałuje na swoje otoczenie, w którym „występują również inne podmioty pozapaństwowe, których zachowania stanowią o środowisku bezpieczeństwa międzynarodowego, występujących w nim strukturach i charakterze"[19]. System bezpieczeństwa państwa staje się z tego powodu konstruktem o nieostrych granicach, jako że „relacje międzynarodowe, jak i wewnętrzne przyjmują charakter sieciowy"[20]. A zatem, w jego zapewnieniu partycypują nie tylko znane dotychczas podmioty, ale i same komponenty ICT. W konsekwencji dychotomia: makroskalowa fragmentacja (dyfuzja bezpieczeństwa) – niskopoziomowa agregacja (IoT) staje się źródłem nowych napięć w systemie i czyni go dalece niespójnym. W kreowaniu polityki bezpieczeństwa coraz większą rolę odgrywają podsystemy tworzące jej dotychczasowe sektory, zaś „transformacja systemu bezpieczeństwa państwa, wynikająca z jego zachowań, identyfikowanych z podejmowanymi i niepodejmowanymi działaniami, wyrażana jest pod postacią zmiennych, których wpływ przekształca system bezpieczeństwa międzynarodowego"[21]. Wśród owych zmiennych

[16] *Ibidem*.
[17] *Ibidem*.
[18] *Ibidem*.
[19] J. Gryz, *op. cit.*, s. 112.
[20] T. R. Aleksandrowicz, *op. cit.*, s. 201.
[21] J. Gryz, *op. cit.*, s. 111.

(zależnych i niezależnych) znajdują się podatności generowane przez systemy C-F i posiadające charakter strukturalny.

## Ataki z wykorzystaniem systemów C-F

W przypadku systemów cyber-fizycznych, których wspólnym mianownikiem pozostaje wszechobecna infrastruktura teleinformatyczna, zdolność negatywnego oddziaływania obejmuje niemal cały zakres przedmiotowy związany z bezpieczeństwem. Podział na sektory (industrialny, militarny, społeczny etc.) jako płaszczyzny oddziaływania staje się coraz bardziej efemeryczny ponieważ można do nich dotrzeć z innego, pozornie niezwiązanego poziomu. Do ingerencji w system bezpieczeństwa militarnego można chociażby wykorzystać elementy związane z IoT, podobnie podsystem bezpieczeństwa politycznego nie jest już ograniczony wyłącznie do sfery publicznej, ale interferuje np. z płaszczyzną bezpieczeństwa ludzkiego. Bezpieczeństwo państwa i polityka jego kształtowania w otoczeniu międzynarodowym znajduje odzwierciedlenie w uwzględnianiu takich koncepcji, jak tzw. regiony uczące się[22] czy inteligentne miasta (*smart cities*)[23]. W obliczu wielowymiarowych zagrożeń generowanych przez usieciowiony system bezpieczeństwa międzynarodowego warto przytoczyć kilka przykładów podatności związanych z systemami C-F, możliwych do wykorzystania w procesie jego destabilizacji.

Inteligentne miasta stają się węzłami (*hubami*) funkcjonującymi w oparciu o zasady determinowane przez paradygmat sieciowy. Zarówno zmodyfikowana istniejąca infrastruktura miejska, jak i aglomeracje tworzone od podstaw zawierają komponenty realizujące swoje funkcje w oparciu o systemy C-F[24]. Np. w ramach projektu EMPHASIS rząd Szwecji stworzył sieć sensorów w kanalizacji miejskiej, monitorujących ścieki pod kątem obecności substancji chemicznych wykorzystywanych do produkcji IEDs[25]; takie podejście wpływa na zachowania potencjalnych terrorystów, którzy będą zmuszeni konstruować ładunki poza monitorowanymi obszarami miejskimi, pozbywać się odpadów w inny sposób lub ostatecznie – mo-

[22] Zob. M. Godowska, *Region uczący się – uwarunkowania i determinanty rozwoju na przykładzie województwa małopolskiego*, „Przedsiębiorczość – Edukacja" 2012, vol. 8, ss. 278-286.
[23] Szerzej na ten temat: D. Szymańska, M. Korolko, *Inteligentne miasta – idea, koncepcje i wdrożenia*, Toruń 2015.
[24] Np. miasto Masdar w Zjednoczonych Emiratach Arabskich, zob. *About Masdar City*, źródło: http://www.masdar.ae (dostęp: 29.07.2016). Także Fujisawa SST w prefekturze Kanagawa na wyspie Honsiu – eksperymentalna dzielnica stworzona przez firmę Panasonic, zob. http://fujisawasst.com.
[25] Szerzej na ten temat: *EMPHASIS*, http://www.foi.se (dostęp: 30.07.2016).

dyfikować odczyty sensorów. Koncepcja *smart city* obejmuje m.in. monitoring środowiska (tutaj czujniki kontrolujące skład atmosfery mogą zostać przejęte tuż przed atakiem chemicznym), inteligentne oświetlenie (np. w amsterdamskiej dzielnicy Westergasfabriek) pozwalające pogrążyć w mroku dzielnice stanowiące cel akcji terrorystycznej lub operacji antyterrorystycznej, powszechnie tworzone są inteligentne systemy zarządzania odpadami[26], w których dostęp do sieci jest realizowany przez pojemniki występujące w roli punktów dostępowych (*hot spots*). Ponadto, inteligentne sieci energetyczne (*smart grid*) stanowiące część infrastruktury krytycznej i zasilające miasta generują wiele nowych wektorów ataku C-F: identyfikacja przed planowaną kradzieżą aktywności domowników w oparciu o odczyty dobowego poboru energii, włamanie do sieci domowej i modyfikacja parametrów urządzeń AGD w celu dokonania zniszczeń itp.

Podobne możliwości generuje system inteligentnego zarządzania transportem, jako że kolejne centra miejskie wdrażają w praktyce ideę inteligentnej organizacji ruchu (*smart traffic lights*). Elektryfikacja stanowiła pierwszy etap procesu zapowiadającego ten stan rzeczy, umożliwiając pośrednie manipulowanie przez dezinformację (telegraf)[27], zaś po wprowadzeniu elektromechanicznych urządzeń sterujących w postaci sprzęgła sygnałowego, a później zwrotnicy, także zdalne fizyczne oddziaływanie na ruch kolejowy[28]; podobnie zastosowanie czujnika sankowego było krokiem w kierunku automatyzacji w torowym ruchu miejskim. Obecnie szeroko rozumiana ingerencja w zautomatyzowany system sygnalizacji świetlnej może być na różne sposoby wykorzystana jako atak główny lub dodatkowa zmienna sprzyjająca jego przeprowadzeniu. Także tramwaje są wyposażone w układy zdalnego sterowania w paśmie promieniowania podczerwonego lub radiowym i stanowią kolejną podatność w obszarze inteligentnej komunikacji miejskiej[29].

Inteligentny transport obejmuje zatem nie tylko zautomatyzowane systemy organizacji ruchu, ale same pojazdy, które z punktu widzenia inżynierii systemów

[26] *Optimising Waste Collection*, http://www.enevo.com (dostęp: 30.07.2016).

[27] Zob. H. Hickson, *Wild, Wild West: Act One, Scene One*, http://www.gbcnv.edu (dostęp: 28. 07.2016); 7 kwietnia 1880 w Elko (Nevada) na podstawie sfałszowanego telegramu wprowadzono w błąd obsługę i pasażerów przejeżdżającego pociągu, prowokując dłuższe zatrzymanie maszyny oraz napiętą sytuację.

[28] Spektakularne efekty można uzyskać obierając za cel szybkie pociągi w rodzaju japońskiego *Shinkansen* (tzw. *Bullet Train*, jadący 160 km/h) czy francuskiego TGV.

[29] W 2007 roku nastolatek za pomocą samodzielnie skonstruowanego nadajnika doprowadził do kolizji tramwajów w Łodzi, zob. T. Jabłoński, M. Jach, *Jak 14-latek spowodował katastrofę*, http://lodz.naszemiasto.pl (dostęp: 30.07.2016).

C-F stanowią zestaw wielu czujników dostarczających dane do komputera pokładowego, interpretującego odbierane sygnały i sterującego kontrolerami drzwi, układu hamulcowego, silnika, układami kontroli prędkości pojazdu, dyszami, rotorami etc. Możliwy staje się cyberatak na podzespoły i elementy krytyczne dla bezpieczeństwa pasażerów – układ hamulcowy i kierowania (zwłaszcza zdalnego, tzw. technologia X-by-Wire[30]) czy poduszki powietrzne, podobnie jak przejęcie sygnału GPS takiego pojazdu w celu śledzenia trasy, a nieuprawniona transmisja danych może posłużyć do jego unieruchomienia, zafałszowania odczytów wpływających na bezpieczeństwo pasażerów czy doprowadzenia do kolizji (tzw. *car hacking*)[31]. Ingerencja może nastąpić wskutek włamania przez system rozrywki (*car audio*, Internet pokładowy) z wykorzystaniem *malware* zapisanego na nośnikach zewnętrznych (pamięci masowe), jak i urządzenia dostępowe, chociażby smartfony (WiFi, Bluetooth). Firma vol.vo wykorzystuje w swoich samochodach system typu *infotainment* o nazwie Sensus Connect, magazynujący wszelkie dane używane przez kierowcę w chmurze obliczeniowej[32]; jednocześnie pojazd tworzy punkt dostępu WiFi a system wykorzystuje kartę SIM właściciela. W tym kontekście możliwa jest modyfikacja zadanej trasy dojazdowej przez moduł GPS (*hijack*) lub przejęcie kontroli nad całym pojazdem[33]. W efekcie technologia C-F tworzy nowe drogi dostępu do spersonalizowanego celu ataku, jak podszycie się pod pracownika firmy ubezpieczeniowej – system pokładowy wysyła bowiem dane zebrane w trakcie jazdy do ubezpieczyciela pojazdu. Ewentualne upowszechnienie komunikacji *vehicle-to-vehicle* zachodzącej bezpośrednio między samochodami oznacza możliwość łatwiejszego ataku na polityków i innych decydentów realizowanego na gruncie prywatnym. Koncepcja inteligentnego transportu otwiera również drogę do skutecznego przejmowania dronów cywilnych i wojskowych (o czym świadczy przykład amerykańskiego Sentinela RQ-170 zhakowanego w 2011 r. w Iranie)[34]. Na obecnym etapie rozwoju systemów C-F ma miejsce dyskusja nad ww. zagadnieniami, których ważność podkreślają świadomi problemu politycy, jak chociażby senator

[30] Zob. R. Frank, *X-By-Wire: For Power, X Marks the Spot*, http://electronicdesign.com (dostęp: 31.07.2016).

[31] Zob. C. Miller, Ch.Valasek, *Adventures in Automotive Networks and Control Units*, http://illmatics.com (dostęp: 30.07.2016); J. Frank, *Keeping Cars Secure: Solutions for Implementing in the Era of the Connected Vehicle*, Munich 2013, http://www.nxp.com/ (dostęp: 30.07.2016).

[32] *Sensus Connect*, http://support.volvocars.com (dostęp: 30.07.2016).

[33] G. Templeton, *Hackers Hijack a Super Yacht With Simple GPS Spoofing, and Planes Could Be Next*, http://www.extremetech.com (dostęp: 30. 07.2016).

[34] A. Rawnsley, *Iran's Alleged Drone Hack: Tough, but Possible*, źródło: https://www.wired.com (dostęp: 30.07.2016).

Edward E. Markey[35], a także przedsiębiorstwa (np. IBM)[36]. Z drugiej strony nie brakuje głosów, że nie należy nadmiernie akcentować kwestii ataków C-F na samochody ponieważ producenci pracują nad adekwatnymi zabezpieczeniami[37].

W przypadku inteligentnych domów i budynków (*smart houses*, *smart buildings*) nowe podatności są generowane przez ich systemy ogrzewania, wentylacji i klimatyzacji (*heating, venting, and air conditioning*, HVAC). W razie przejęcia systemu kontrolnego tego typu w budynkach użyteczności publicznej, siedzibach administracji rządowej, resortów siłowych i organizacji międzynarodowych oznacza to nie tylko zablokowanie wyjść z pomieszczeń czy sterowanie temperaturą. Podanie prądu o wysokim natężeniu (w przypadku dostępu do Internetu funkcjonującego w oparciu o sieć energetyczną, PowerLine Ethernet) na transmiter sieciowy może spowodować uszkodzenie sprzętu lub porażenie jego użytkownika. Przejęcie routera obsługującego *smart house* lub *smart building* oznacza nie tylko potencjalny dostęp do danych przechowywanych na wszystkich przyłączonych urządzeniach (komputerach, tabletach, smartfonach, implantach, rozrusznikach serca), ale oddziaływanie za ich pomocą na zachowanie użytkowników, chociażby poprzez wprowadzanie zmian w terminarzach spotkań i kinetyczne, destrukcyjne oddziaływanie na sprzęt IT. W przypadku kombinowanego ataku C-F jest możliwe powiązanie danych z monitoringu implantów medycznych z daną osobą i zmiana warunków w zajmowanym przez nią pomieszczeniu prowadząca do utraty świadomości i śmierci. Inną drogę zapewnia sprzęt codziennego użytku pozostający na wyposażeniu inteligentnych domów.

Tzw. inteligentny telewizor pozostający *online* dysponuje wbudowaną kamerą i mikrofonem (wykorzystywanymi do sterowania systemem operacyjnym i aplikacjami), które mogą zostać aktywowane bez wiedzy mieszkańców. Podobnie jak w przypadku kamer komputerowych[38], umożliwia podgląd codziennej aktywności, w tym rejestrację wizerunku i głosu mieszkańców, członków dalszej rodziny czy odwiedzających[39], a ponadto przechwycenie prywatnych plików przeglądanych

[35] *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, źródło: https://www.markey.senate.gov (dostęp: 30.07.2016).

[36] M. Borrett, G. Serio, *Code Is My Co-pilot: Security & Privacy in Connected Vehicles*, źródło: https://www-304.ibm.com (dostęp: 31.07.2016).

[37] L. Walford, *Why You Don"t Have to Worry About Your Connected Car Being Hacked*, http://www.autoconnectedcar.com (dostęp: 31.07.2016).

[38] Na gruncie prywatnym podobne zagrożenie stanowią konsole do gier podłączone do Sieci. Zarówno SmartTV, jak i konsole pozwalają powiązać ich hasła dostępowe z kontami poczty elektronicznej użytkowników.

[39] Nawet kiedy odbiornik jest wyłączony, co podczas konwentu Black Hat 2013 zademonstrował Seung Jin Lee z Uniwersytetu Koreańskiego, zob. D. Pauli, *Smart TVs a Spying Portal for Hackers,*

w s*mart tv* oraz wszelkich rozmów prowadzonych *online*[40]. Takie zagrożenie miałoby rację bytu np. w trakcie nieformalnych spotkań polityków w pokojach hotelowych lub salach konferencyjnych biur wyposażonych w podobne odbiorniki. Dodatkowo, inteligentne telewizory umożliwiają służbom specjalnym czy potencjalnym terrorystom zdobycie wielu bezpośrednich danych, pozwalając na skuteczne rozpoznanie miejsca operacji lub psychologiczne profilowanie obranych celów osobowych, nie wspominając o próbach nawiązania bezpośredniej łączności i szantażu. Inteligentny sprzęt AGD dostarcza podobnych możliwości, nawet jeśli zostałyby one ograniczone wyłącznie do rejestrowania obecności lokatorów w miejscu zamieszkania.

Podobnie, obecność intruza w sieci lub siedzibie korporacji może okazać się faktem dzięki systemom zarządzania infrastrukturą, wideokonferencji i nadzoru CCTV[41]. Instytucje mogą paść ofiarą własnej polityki zarządzania np. w przypadku urządzeń pracujących w technologii *Instant Ink*[42] – sukcesywne, bezpodstawne zamówienia tuszu po zhakowaniu drukarek online byłoby odczuwalne w skali przedsiębiorstwa tuż po automatycznym przelaniu należności z konta, podobnie jak wydruk kompromitujących materiałów bezpośrednio w biurze doprowadziłby do zmian personalnych (np. w przypadku ataku na CEO organizacji). Kolejne zagrożenia generuje druk 3D, zwłaszcza kiedy dzięki tej technologii powstają całe budynki i mosty – modyfikacja planów konstrukcyjnych przechowywanych w chmurze danych lub wpłynięcie na proces drukowania w trakcie jego trwania znalazłyby odzwierciedlenie w parametrach fizycznych takich elementów. Podobnie jak w przypadku samochodów, także na tym polu pojawiają się opinie bagatelizujące zagadnienia bezpieczeństwa systemów C-F[43].

Internet rzeczy staje się na wiele sposobów związany z dziedziną bezpieczeństwa na gruncie międzynarodowym, przede wszystkim ludzkiego (*human security*).

---

*Researcher Finds*, http://www.itnews.com.au (dostęp: 29.07.2016).

[40] D. Pauli, *Attackers Can Read USB Storage Attached to Samsung TVs*, http://www.itnews.com.au (dostęp: 31.07.2016).

[41] K. Zetter, *Most Popular Surveillance Cameras Can Be Hacked*, http://gizmodo.com (dostęp: 31. 07.2016); CCTV umożliwia np. monitoring fizycznej ochrony w celu uzyskania bezprzewodowego dostępu do SCADA.

[42] *HP Instant Ink - What Is HP Instant Ink?*, http://support.hp.com (dostęp: 31.07.2016).

[43] L. Fernandes, *Exploiting the „Printernet" of Things*, http://www.louellafernandes.com (dostęp: 31. 07.2016); A. Williams, *World's First 3D-printed Office Building Completed in Dubai*, http://newatlas.com (dostęp: 31.07.2016); M. Molitch-Hou, *Construction of World's 1st 3D Printed Bridge Begins in Amsterdam*, http://3dprintingindustry.com (dostęp: 31.07.2016); D. S. Maldow, *How to Defend Your Boardroom Against „Videoconferencing Hackers" and Other Mythical Creatures*, http://www.telepresenceoptions.com (dostęp: 31.07.2016).

Wśród nich na szczególną uwagę zasługują potencjalne ataki wymierzone w polityków i inne osoby decyzyjne w państwie lub organizacji międzynarodowej, których powodzenie może skutkować zmianą globalnego układu sił lub konfliktem zbrojnym. Środkiem prowadzącym do tego celu, poza klasycznym naruszeniem prywatności (poufności danych), jest w tym przypadku o wiele groźniejsze oddziaływanie cyber-fizyczne. Np. bezpośrednio na organizm biologiczny poprzez wspomniane już implanty bezprzewodowe[44], co stanowi obecnie na tyle realny problem, że były wiceprezydent USA, Dick Cheney, wyłączył w swoim rozruszniku serca funkcję monitorowania online[45]. Jak istotna jest to kwestia, niech świadczy niewyjaśniona śmierć hakera z firmy IOActive (Barnaby Jack)[46], który podczas konwencji Black Hat w Las Vegas (2013) miał publicznie udowodnić, że jest możliwa nie tylko modyfikacja oprogramowania rozruszników serca czy implantów, ale zabójstwo bezpośrednim, zdalnie indukowanym impulsem elektrycznym o napięciu kilkuset woltów[47]. Hacker zaznaczył, że może to posłużyć nie tylko do aktów cyfrowego skrytobójstwa, ale zostać wykorzystane w aktach cyberterroryzmu[48]. Hipotetycznie możliwe jest także wykorzystanie wszczepionego *chipa*, jako źródła infekcji nie tylko dla innych implantów w jego najbliższym otoczeniu, ale innych docelowych urządzeń niemedycznych (wirusem, *spyware* lub *malware*). Sprzyjają temu innowacje w dziedzinie *smart building*: pracownicy szwedzkiego biura używają *chipów* w codziennej pracy, co umożliwia ich ewentualne skopiowanie (sklonowanie), kradzież tożsamości i wejście nieuprawnionej osoby do budynku[49]. Nieautoryzowany dostęp do implantów medycznych oznacza nie tylko monitoring stanu zdrowia danego pacjenta, ale odkrycie nowych schorzeń bez jego wiedzy; podobnie można łatwo stwierdzić, że posiadacz danego smartfona (numeru telefonu) używającego glukometru iBGStar choruje na cukrzycę.

[44] Charakterystyka przykładowego rozrusznika pozostającego w trybie online firmy Etrinsa zob. *Etrinsa Pacemaker Family Technical Manual*, http://www.biotronikusa.com (dostęp: 31.07.2016).
[45] C. Franzen, *Dick Cheney Had the Wireless Disabled on His Pacemaker to Avoid Risk of Terrorist Tampering*, http://www.theverge.com (dostęp: 31.07.2016).
[46] X. Jardin, *Hacker Barnaby Jack Dies Just Before Black Hat Presentation on Lethal Pacemaker Hacks*, http://boingboing.net (dostęp: 31.07.2016).
[47] R. Boyle, *Hackers Could Access Pacemakers From A Distance And Deliver Deadly Shocks*, http://www.popsci.com (dostęp: 31.07.2016).
[48] D. Pauli, *Hacked Terminals Capable of Causing Pacemaker Deaths*, http://www.itnews.com.au (dostęp: 31.07.2016).
[49] T. Buchanan, *Swedish Firm Microchips Employees*, http://www.independent.co.uk (dostęp: 31.07.2016).

Szpitale jako funkcjonalna całość także stały się poważnym źródłem zagrożeń ze strony systemów C-F[50]. Ich przykładem jest potencjalna intencjonalna modyfikacja oprogramowania urządzeń medycznych wpiętych do Sieci (ewentualnie dokonanie zmian jeszcze na etapie ich produkcji)[51]. Na polu medycyny pojawiły się urządzenia i systemy C-F generujące bezpośrednie ścieżki prowadzące do danej osoby pełniącej funkcje publiczne, a komponenty medyczne typu *smart* stanowią obecnie dużą grupę produktów konstytuujących *Internet of Things*. Urządzenia online monitorujące i wspomagające funkcje organizmu (pulsometry, implanty), inteligentne tabletki, które po połknięciu zbiorą dane na temat stanu organizmu i nadchodzące zautomatyzowane systemy podawania leków w czasie rzeczywistym jeszcze bardziej skomplikuje powyższy obraz, umożliwiając nieautoryzowaną ingerencję[52]. Uzupełniają go coraz powszechniejsze inteligentne ubrania, koszulki biometryczne zawierające komponenty elektroniczne przyspieszające spalanie tkanki tłuszczowej, gromadzące dane na temat organizmu w zintegrowanej pamięci etc[53].

## Uwagi końcowe

Jakkolwiek ww. metody destabilizacji bezpieczeństwa państwa i systemu międzynarodowego za pośrednictwem systemów C-F wydają się być w pewnej mierze czysto hipotetyczne, ich rosnąca rola czyni podobne zagrożenia coraz bardziej realnymi. Konfliktogenny charakter otoczenia międzynarodowego i systemu jego bezpieczeństwa sprzyja poszukiwaniu nowych dróg negatywnego oddziaływania w celu uzyskania założonych sekwencji zdarzeń. W miarę dalszego upowszechniania systemów cyber-fizycznych, opracowanie nowych metod pożądanego oddziaływania zwrotnego w skali makro i mikro jest tylko kwestią czasu. Tym bardziej,

[50] W Stanach Zjednoczonych stanowią element infrastruktury krytycznej, zob. M. E. Callahan, *Cybersecurity*
*and Hospitals. What Hospital Trustees Need to Know About Managing Cybersecurity Risk and Response*, http://www.aha.org (dostęp: 31.07.2016).

[51] W latach osiemdziesiątych XX wieku błąd w oprogramowaniu aparatu do radioterapii Therac-25 doprowadził do śmierci kilku pacjentów chorych na nowotwór, zob. A. Fabio, *Killed by a Machine: The Therac-25*, http://hackaday.com (dostęp: 31.07.2016).

[52] S. Mitchell, N. Villa, M. Stewart-Weeks, A. Lange, *The Internet of Everything for Cities . Connecting People, Process, Data, and Things To Improve the 'Livability' of Cities and Communities*, http://www.cisco.com (dostęp: 30.07.2016).

[53] M. Sawh, *Thin Ice Smart Vest Cools Your Body Down to Burn Fat*, http://www.wareable.com (dostęp: 31.07.2016); D. Thompson, *Under Armour's Best Idea: A Smart Shirt That Measures Heart Rate and G-Force*, http://www.theatlantic.com (dostęp: 31.07.2016). Podobnie obuwie sportowe, zob. J. Beverly, *First Run: Under Armour's Smart Shoes*, http://www.runnersworld.com (dostęp: 31.07.2016).

że historia cyberbezpieczeństwa systemów C-F zna już co najmniej kilkadziesiąt przypadków ich wykorzystania w procesie oddziaływania na bezpieczeństwo narodowe i międzynarodowe (np. Arizona Salt River Project w 1994 r., australijski atak w Maroochy w 2000 r., elektrownia jądrowa Davis Besse w Ohio 20 sierpnia 2003 r.)[54].

Ewolucja systemów cyber-fizycznych oznacza dalsze odejście od paradygmatu akcentującego centralną rolą aparatu państwowego w kierunku celowanych ataków wymierzonych w bezpieczeństwo ludzkie (tak w szerokim kontekście społecznym, jak i w przypadku członków władz), a ich ich zdolność oddziaływania na przestrzeń materialną poszerza zakres bezpieczeństwa militarnego. Chociaż na obecnym etapie wiele możliwości oferowanych przez systemy C-F pozostaje w sferze fikcji lub jawi się jako zupełnie nieprzydatne lub nieszkodliwe, ich stosunkowo łatwa dostępność sprawi, że akty cyber-fizycznej przemocy staną się najprawdopodobniej coraz częstsze[55]. Sprzyja temu wspomniana dyfuzja systemów bezpieczeństwa (wewnętrznego i międzynarodowego).

System bezpieczeństwa międzynarodowego jest wypadkową systemów bezpieczeństwa państw, relacji i oddziaływań (tzw. miękkich i twardych) zachodzących pomiędzy nimi. Systemy C-F stanowią materialno-wirtualną płaszczyznę znoszącą granice pomiędzy bezpieczeństwem wewnętrznym, narodowym i międzynarodowym czyniąc je coraz bardziej umownymi, a wektory ataków informatycznych ulegają kategoryzacji w zależności od charakteru obiektu referencyjnego. Rosnąca współzależność podmiotów stosunków międzynarodowych, która w perspektywie miała położyć kres siłowym metodom rozwiązywania konfliktów, staje się w istocie przyczyną dywersyfikacji sposobów osiągania tych samych celów, czyniąc je coraz bardziej wyrafinowanymi. W tej nowej rzeczywistości zagrożenia generowane przez systemy C-F mają charakter strukturalny i pod przykrywką *smart power* grawitują zdecydowanie w kierunku „twardych" oddziaływań.

[54] Zob. G. Loukas, *Cyber-Physical Attacks. A Growing Invisible Threat*, Amsterdam 2015, Fig. 2.3, s. 55.

[55] E. A. Lee, *The Past, Present and Future of Cyber-Physical Systems: A Focus on Models*, „Sensors" 2015, vol. 15, no. 3, ss. 4837-4869.

## BIBLIOGRAFIA

*About Masdar City*, źródło: http://www.masdar.ae (dostęp: 29.07.2016).

Aleksandrowicz T. R., *Świat w sieci. Państwa, społeczeństwa ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014.

Beverly J., *First Run: Under Armour's Smart Shoes*, http://www.runnersworld.com (dostęp: 31.07.2016).

Borrett M., Serio G., *Code Is My Co-pilot: Security & Privacy in Connected Vehicles*, źródło: https://www-304.ibm.com (dostęp: 31.07.2016).

Boyle R., *Hackers Could Access Pacemakers From A Distance And Deliver Deadly Shocks*, źródło: http://www.popsci.com (dostęp: 31.07.2016).

Buchanan T., *Swedish Firm Microchips Employees*, źródło: http://www.independent.co.uk (dostęp: 31.07.2016).

Callahan M. E., *Cybersecurity and Hospitals. What Hospital Trustees Need to Know About Managing Cybersecurity Risk and Response*, źródło: http://www.aha.org (dostęp: 31.07.2016).

*EMPHASIS*, źródło: http://www.foi.se (dostęp: 30.07.2016).

*Etrinsa Pacemaker Family Technical Manual*, źródło: http://www.biotronikusa.com (dostęp: 31.07.2016).

Evans D., *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*, „Cisco White Paper" 2014.

Fabio A., *Killed by a Machine: The Therac-25*, http://hackaday.com (dostęp: 31.07.2016).

Fernandes L., *Exploiting the „Printernet" of Things*, źródło: http://www.louellafernandes.com (dostęp: 31.07.2016);

Frank J., *Keeping Cars Secure: Solutions for Implementing in the Era of the Connected Vehicle*, Munich 2013, http://www.nxp.com/ (dostęp: 30.07.2016).

Frank R., *X-By-Wire: For Power, X Marks the Spot*, źródło: http://electronicdesign.com (dostęp: 31.07.2016).

Franzen C., *Dick Cheney Had the Wireless Disabled on His Pacemaker to Avoid Risk of Terrorist Tampering*, źródło: http://www.theverge.com (dostęp: 31.07. 2016).

Gill H., *A Continuing Vision: Cyber-Physical Systems*, Arlington 2008, źródło: https://www.ece.cmu.edu (dostęp: 27.07.2016).

Godowska M., *Region uczący się – uwarunkowania i determinanty rozwoju na przykładzie województwa małopolskiego*, „Przedsiębiorczość – Edukacja" 2012, vol. 8.

Gryz J., *Państwo w systemie bezpieczeństwa międzynarodowego*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, vol. 8, nr 2.

Hickson H., *Wild, Wild West: Act One, Scene One*, źródło: http://www.gbcnv.edu (dostęp: 28.07.2016);

*HP Instant Ink - What Is HP Instant Ink?*, źródło: http://support.hp.com (dostęp: 31.07.2016).

http://fujisawasst.com.

Jabłoński T., Jach M., *Jak 14-latek spowodował katastrofę*, źródło: http://lodz.naszemiasto.pl (dostęp: 30.07.2016).

Jardin X., *Hacker Barnaby Jack Dies Just Before Black Hat Presentation on Lethal Pacemaker Hacks*, źródło: http://boingboing.net (dostęp: 31.07.2016).

Lee E. A., *The Future of Embedded Systems*, źródło: https://chess.eecs.berkeley.edu (dostęp: 28.07.2016).

Lee E. A., *The Past, Present and Future of Cyber-Physical Systems: A Focus on Models*, „Sensors" 2015, vol. 15, no. 3.

Loukas G., *Cyber-Physical Attacks. A Growing Invisible Threat*, Amsterdam 2015.

Maldow D. S, *How to Defend Your Boardroom Against „Videoconferencing Hackers" and Other Mythical Creatures*, źródło: http://www.telepresenceoptions.com (dostęp: 31.07.2016).

Miller C., Valasek Ch., *Adventures in Automotive Networks and Control Units*, źródło: http://illmatics.com (dostęp: 30.07.2016).

Miller M., *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa 2016.

Mitchell S., Villa N., Stewart-Weeks M., Lange A., *The Internet of Everything for Cities . Connecting People, Process, Data, and Things To Improve the 'Livability' of Cities and Communities*, źródło: http://www.cisco.com (dostęp: 30.07.2016).

Molitch-Hou M., *Construction of World's 1st 3D Printed Bridge Begins in Amsterdam*, źródło: http://3dprintingindustry.com (dostęp: 31.07.2016);

Mukherjee S., Shaw R., *Big Data – Concepts, Applications, Challenges and Future Scope*, „International Journal of Advanced Research in Computer and Communication Engineering" 2016, vol. 5, issue 2.

*Optimising Waste Collection*, źródło: http://www.enevo.com (dostęp: 30.07.2016).

Pauli D., *Attackers Can Read USB Storage Attached to Samsung TVs*, źródło: http://www.itnews.com.au (dostęp: 31.07.2016).

Pauli D., *Hacked Terminals Capable of Causing Pacemaker Deaths*, źródło: http://www.itnews.com.au (dostęp: 31.07.2016).

Pauli D., *Smart TVs a Spying Portal for Hackers, Researcher Finds*, źródło: http://www.itnews.com.au (dostęp: 29.07.2016).

Rawnsley A., *Iran's Alleged Drone Hack: Tough, but Possible*, źródło: https://www.wired.com (dostęp: 30.07.2016).

*Remote Terminal Unit (RTU)*, źródło: http://www.wbsetcl.in (dostęp: 28.07.2016).

Sawh M., *Thin Ice Smart Vest Cools Your Body Down to Burn Fat*, źródło: http://www.wareable.com (dostęp: 31.07.2016).

*Sensus Connect*, źródło: http://support.volvocars.com (dostęp: 30.07.2016).

Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996.

*Systemy SCADA*, źródło: http://www.astor.com.pl (dostęp: 28.07.2016).

Szymańska D., Korolko M., *Inteligentne miasta – idea, koncepcje i wdrożenia*, Toruń 2015.

Templeton G., *Hackers Hijack a Super Yacht With Simple GPS Spoofing, and Planes*

*Could Be Next*, źródło: http://www.extremetech.com (dostęp: 30. 07.2016).

Thompson D., *Under Armour's Best Idea: A Smart Shirt That Measures Heart Rate and G-Force*, http://www.theatlantic.com (dostęp: 31.07.2016).

*Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, źródło: https://www.markey.senate.gov (dostęp: 30.07.2016).

Ullman R. H., *Redefining Security*, „International Security" 1983, vol. 8, no. 1.

Walford L., *Why You Don"t Have to Worry About Your Connected Car Being Hacked*, źródło: http://www.autoconnectedcar.com (dostęp: 31.07.2016).

Williams A., *World's First 3D-printed Office Building Completed in Dubai*, źródło: http://newatlas.com (dostęp: 31.07.2016);

Zetter K., *Most Popular Surveillance Cameras Can Be Hacked*, źródło: http://giz modo.com (dostęp: 31.07.2016)

**Marcin Adamczyk**

Uniwersytet Wrocławski

# Cyberszpiegostwo w relacjach chińsko-amerykańskich w kontekście potencjalnej zmiany światowego hegemona

Słowa kluczowe: USA, Chiny, cyberszpiegostwo, hegemonia

Chińska Republika Ludowa od momentu przejęcia sterów władzy przez Deng Xiaopinga w końcu lat 70., wkroczyła na ścieżkę dynamicznego rozwoju ekonomicznego. W efekcie kraj będący niecałe 40 lat temu dziesiątą gospodarką świata, dziś osiągnął pozycję wicelidera[1] lub nawet lidera[2]. Warto podkreślić, iż w latach 1979-2010 średnia roczna stopa wzrostu PKB w Chinach wynosiła blisko 10%, natomiast w Stanach Zjednoczonych, Japonii i Niemczech oscylowała w okolicach 2%[3]. Przy czym w rekordowych latach (1984, 1992 i 2007) chińska gospodarka rosła o blisko 15% r/r[4]. Jak wskazują ekonomiści, dotychczas wiodącym czynnikiem odpowiadającym za dynamiczny wzrost gospodarki tego kraju były inwestycje[5]. W ostatnich kilkunastu miesiącach tempo rozwoju gospo-

[1] *World Development Indicators*, źródło: http://data.worldbank.org (dostęp: 10.01.2018); *World Economic Outlook Database April 2017*, źródło: https://www.imf.org (dostęp: 10.01.2018).

[2] Różnica jest spowodowana utrzymywaniem przez ChRL drastycznie zaniżonego kursu juana – stąd PKB według parytetu siły nabywczej jest w Chinach blisko dwukrotnie wyższy od nominalnego.

[3] M.A. Kolka, *Czynniki wzrostu PKB i perspektywy rozwoju gospodarczego Chin do 2015 roku*, „Międzynarodowe stosunki gospodarcze - wybrane podmioty i procesy gospodarki światowej" 2012, nr 122, s. 140.

[4] *Ibidem*, s. 141.

[5] T. Białowąs, *Inwestycje a wzrost gospodarczy Chin w latach 1980-2012*, „Annales Universitatis Mariae Curie-Skłodowska. Sectio H, Oeconomia" 2014, t. 48, nr 2, s. 19.

darczego Państwa Środka zmniejszyło się (roczny wzrost PKB obniżył się do poziomu ok. 7%)[6], w efekcie czego większy nacisk położono na konsumpcję, jako koło zamachowe gospodarki[7]. Pomimo niewielkiego spowolnienia dotychczasowej dynamiki wzrostu siły ekonomicznej, ChRL wciąż rozwija się znaczniej szybciej niż np. kraje szeroko pojętego Zachodu. Fakt ten wraz z rosnącym zaangażowaniem Chin na świecie[8] oraz rozwojem ich potencjału militarnego[9] zdaniem wielu naukowców i komentatorów (jak również autora niniejszego opracowania) świadczy o dążeniu Pekinu do podważenia istniejącego *Pax Americana* i zastąpienia go kolejną w historii odsłoną *Pax Sinica*[10]. Warto podkreślić, iż na początku 2017 roku chińskie MSZ ustami swojego dyrektora generalnego w departamencie międzynarodowych stosunków gospodarczych Zhanga Juna zadeklarowało, iż Chińska Republika Ludowa jest przygotowana na podjęcie się roli światowego

[6] P. Ciszak, *Gospodarka Chin zwalnia. Niższe tempo wzrostu gospodarczego wpłynie na Europę,* źródło: https://www.money.pl (dostęp: 10.01.2018); S. Stodolak, *Na spowolnienie w Chinach nie ma sprawdzonych recept*, źródło: https://www.obserwatorfinansowy.pl (dostęp: 10.01.2018).

[7] *Kolejny znak spowolnienia chińskiej gospodarki. Eksport w styczniu spadł o 11,2 proc. rdr*, źródło: http://www.polskieradio.pl (dostęp: 10.01.2018); A. Kaliński, *W Chinach wyhamowała konsumpcja*, źródło: https://www.obserwatorfinansowy.pl (dostęp: 10.01.2018); *Chiny mogą zaszkodzić surowcom, ale wesprzeć konsumpcję*, źródło: http://www.bankier.pl (dostęp: 10.01.2018).

[8] Zob. m. in. K. Andrijauskas, *China's Economic Penetration into Post-Soviet Central Asia and Eastern Europe*, „Lithuanian Foreign Policy Review" 2013, nr 30, s. 113-131; R. Rousseau, *China's Growing Economic Presence in Ukraine and Belarus*, „Strategic Analysis" 2012, nr 1 (36), s. 18-22; H. Campbell, *China in Africa: challenging US global hegemony*, „Third World Quarterly" 2008, nr 29, t. 1, 89-105; D. Kopiński, *Ekspansja gospodarcza Chin w Afryce – szansa na rozwój czy początek neokolonizacji?*, [w:] *Afryka na progu XXI wieku Polityka. Kwestie społeczne i gospodarcze*, red. D. Kopiński, A. Żukowskiego, Warszawa 2009, s. 221-233; B. Liberska, *System powiązań Ameryki Łacińskiej z Indiami i Chinami we współczesnej gospodarce światowej*, „International Journal of Management and Economics" 2008, nr 23, s. 66-83; M. Mencel, *Strategia Chin wobec państw Ameryki Łacińskiej*, „Studia Gdańskie. Wizje i rzeczywistość" 2013, nr 10, s. 302-327; T. Kamiński, *Sypiając ze smokiem. Polityka Unii Europejskiej wobec Chin*, Łódź 2015, *passim*;K. Żodź – Kuźnia, J. Wiśniewski, *Dynamika wzajemnych relacji między Unią Europejską a Chińską Republiką Ludową na początku XXI wieku,* „Przegląd Politologiczny" 2012, nr 2, s. 65-84.

[9] Zob. M. Adamczyk, *Porównanie zmiany potencjału militarnego Chin na tle Rosji, Indii, Stanów Zjednoczonych oraz Japonii w okresie od 1989 do 2013 roku*, [w:] *Aspekty bezpieczeństwa w życiu publicznym*, red. D. Magierek, M. Pogonowski, Koszalin 2015, s. 123-140.

[10] Zob. m. in. A. Brunet, J. P. Guichard, *Chiny światowym hegemonem?*, Warszawa 2011, *passim*; R. Kagan, *Powrót historii i koniec marzeń,* Poznań 2009, s. s. 31-42; S.W. Mosher, *Hegemon: China's plan to dominate Asia and the world*, San Francisco 2002, *passim*; D. Roy, *Hegemon on the Horizon? China's Threat to East Asian Security*, „International Security" 1994, Nr 19, t. 1, s. 149-168; R. Bernstein, Munro R. H, *The coming conflict with China*, Nowy Jork 1998, *passim*.

lidera w obliczu osłabienia dotychczasowych przywódców[11]. Chęć uzyskania statusu państwa hegemonicznego[12] poprzez zmianę dotychczasowego porządku wymaga od Chin m. in. podjęcia odpowiednich działań w polityce wewnętrznej i międzynarodowej. Zdaniem autora Pekin powinien nie tylko skonsolidować wokół siebie koalicję państw wspierających go na arenie światowej, ale przede wszystkim zmniejszyć dystans ekonomiczny i militarny[13] jaki dzieli go od wciąż „urzędującego" hegemona – Stanów Zjednoczonych.

Niniejsze opracowanie poświęcone jest rozpoznanym działaniom ChRL w cyberprzestrzeni (traktowanej przez autora jako „wszechogarniająca świat domena informacyjna"[14]), ukierunkowanych na pozyskanie technologii wojskowych i cywilnych ze Stanów Zjednoczonych. Spośród wszystkich krajów na świecie, to prawdopodobnie Chiny dysponują największymi możliwościami w tym zakresie[15]. Impulsem do powstania niniejszej pracy były prowadzone przez autora badania nad powstawaniem państw hegemonicznych – Chiny mogą stać się pierwszym dominującym mocarstwem, które o swoją supremację walczyć będzie również w cyberprzestrzeni. Niniejsze opracowanie jest ponadto rozwinięciem wcześniejszych badań dotyczących funkcjonowaniu chińskiego wywiadu[16]. Państwo Środka jest aktualnie jedynym liczącym się krajem, który potencjalnie mógłby rzucić wyzwanie dominacji Stanów Zjednoczonych, stąd jego wybór jako obiektu badań. Implikuje to w oczywisty sposób dobór materiału badawczego. Dostęp do wiarygodnych informacji dotyczących współczesnych działań wywiadowczych we wszystkich krajach na świecie jest niewątpliwie mocno utrudniony, zaś w Chiń-

[11] J. Chin, *China Says Prepared to Lead Global Economy if Necessary*, źródło: http://www.wsj.com (dostęp: 10.01.2018); *Diplomat says China would assume world leadership if needed*, źródło: http://www.reuters.com (dostęp: 10.01.2018).

[12] Hegemonia w *Leksykonie międzynarodowych stosunków politycznych* jest definiowana jako „(…) panowanie lub kierownictwo; oznacza sprawowanie przywódczej roli, posiadanie przewagi w stosunku do grupy społecznej lub w skali państwa. Może też być stosowana wobec regionu międzynarodowego": *Leksykon międzynarodowych stosunków politycznych*, red. Cz. Mojsiewicz, Wrocław 2004, s. 144.

[13] Zob. D. C. Gompert, A. Stuth Cevallos, C. L. Garafola, *War with China. Thinking Through the Unthinkable,* Santa Monica 2016, źródło: http://www.rand.org (dostęp: 10.01.2018).

[14] J. Dereń, A. Rabiak, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2014, s. 202.

[15] P. Borkowski, *Koncepcja cyberbezpieczeństwa w ujęciu Chińskiej Republiki Ludowej - wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, t. 7, nr 13, s. 52.

[16] Zob. M. Adamczyk, K. Baraniuk, *Służby wywiadowcze Chińskiej Republiki Ludowej – zarys struktur i metod działalności*, „Studia Orientalne" 2017, nr 2 (12), [przyjęte do druku].

skiej Republice Ludowej (która jest wciąż krajem o ustroju będącym na pograniczu totalitaryzmu i autorytaryzmu[17]) jest to wciąż prawdziwy temat tabu. Badacz pragnący podjąć się głębszej jego analizy skazany jest głównie na nieliczne publikacje zagraniczne[18] i pojedyncze opracowania polskie. Stosunkowo dużo informacji na temat ujawnionych aktów cyberszpiegostwa dostępnych jest na portalach internetowych zagranicznych *think tanków* oraz wiodących mediów krajowych i zagranicznych. Źródła elektroniczne, które są wciąż mało popularne wśród badaczy, odpowiednio opracowane stanowią wartościowe źródło najbardziej aktualnych informacji. Jednocześnie tematyka i ograniczona liczba opracowań naukowych wymuszają na autorze ich szerokie wykorzystanie. Autor zamierza przedstawić najbardziej znane chińskie operacje szpiegowskie w cyberprzestrzeni, które były wymierzone w USA. Ponadto pokrótce opisana zostanie działalność amerykańskich służb specjalnych na tym polu oraz prawdopodobny rozwój stosunków chińsko-amerykańskich w kontekście rywalizacji w cyberprzestrzenii.

## Akwizycja technologii

Wydaje się, iż niezbędnym elementem rozbudowy potencjału gospodarczego i militarnego Chińskiej Republiki Ludowej jest próba zniwelowania przewagi technologicznej krajów wysokorozwiniętych. Chiny przez wiele lat określane były mianem „fabryki świata" i kojarzone głównie z masową produkcją tanich oraz niezaawansowanych produktów. Jednakże przemiany w chińskiej gospodarce stają się co raz bardziej wyraźne, a kraj staje się źródłem innowacji na światowym poziomie[19] – warto zwrócić uwagę, iż rozwiązania *made in China* są już powielane przez koncerny zagraniczne[20]. Nim do tego doszło Pekin zmuszony był podjąć

[17] Więcej na temat dylematu klasyfikacji ustroju panującego w ChRL: M. Adamczyk, *Media we współczesnym państwie totalitarnym na przykładzie Chińskiej Republiki Ludowej*, [w:] *Media XXI wieku. Studia interdyscyplinarne*, red. A. Momot, A. Drabina, Wrocław 2016, s. 11-24.

[18] Zob. m. in.: R. Faligot, R. Kauffer, *Tajne służby Chin (1927-1987)*, Warszawa 1994, *passim*; R. Faligot, *Tajne służby chińskie: od Mao do igrzysk olimpijskich*, Katowice 2009, *passim*.

[19] Zob. W. Hübner, *Innowacje w Chinach: od starożytności do wyzwań dnia dzisiejszego*, „Kwartalnik Naukowy Uczelni Vistula" 2013, tom 36, nr 2, s. 16-39; M. Rybicka, W. Wieszczycka, *Chiny – rosnące mocarstwo innowacyjności*, źródło: http://www.pte.pl (dostęp: 10.01.2018). J. Furmanek, *Innowacje po chińsku. Jak rozwój technologii Made in China zmieni współczesny świat*, źródło: http://peoplessquare.pl (dostęp: 10.01.2018); J. Stojek, *Chiński zwrot ku innowacyjności*, źródło: http://www.psz.pl (dostęp: 10.01.2018).

[20] Zob m. in.. Ł. Kotkowski, *Nowy smartfon ZTE pokazuje, że ramki w smartfonach są całkowicie zbędne*, źródło: http://www.spidersweb.pl (dostęp: 10.01.2018); D. Kosiński, *Już rok temu Huawei zmienił oblicze mobilnej fotografii. Zauważyło to nawet Apple*, źródło: https://www.pcformat.pl (dostęp: 10.01.2018).

szereg działań mających na celu zmniejszenie technologicznego dystansu, jaki dzielił kraj od Stanów Zjednoczonych i państw Unii Europejskiej, ale także najlepiej rozwiniętych państw spośród grona „Azjatyckich Tygrysów" czy nawet Rosji. W efekcie inwestycje badawczo-rozwojowe zaczęły rosnąć w szybkim tempie[21], a wiele instytucji państwa skupiało się na pozyskaniu nowoczesnych technologii o przeznaczeniu cywilnym i militarnym. W tym celu ChRL z jednej strony dokonywało zakupu licencji, z drugiej zaś pozyskiwało np. niewielkie partie sprzętu i uzbrojenia, które poddawano procesowi odwróconej inżynierii. Wszystko po to, aby następnie produkować je masowo w chińskich zakładach (często bez licencji). Wprowadzono go następnie na uzbrojenie własnych sił zbrojnych, ale także podejmowano próby sprzedaży do krajów trzecich, już jako wytworu własnej myśli technicznej[22]. W przypadku technologii o przeznaczeniu cywilnym Państwo Środka przy okazji inwestycji kapitału zagranicznej proweniencji stosowało zasadę wymuszonego transferu. Firmy zagraniczne mogły inwestować w Chinach głównie w oparciu o spółki typu *joint venture*, w których większościowym kapitałem z zasady dysponowała strona chińska. Jak wskazuje Brunet i Guichard niezbędne *know-how* było przekazywane do zakładów przemysłowych „za Wielkim Murem", a ewentualne konflikty między partnerami zwyczajowo rozstrzygane na korzyść strony chińskiej[23]. Wraz z postępem technologicznym i bogaceniem się kraju, spółki z mieszanym kapitałem w roli narzędzia do pozyskiwania owoców zagranicznej myśli technicznej zostały zastąpione przez bezpośrednie transfery technologii. Były one niejako warunkiem otrzymania lukratywnych kontraktów na terenie ChRL. Autorzy przypominają tu m. in. słynną sprawę sprzedaży do tego kraju odrzutowców pasażerskich, który to kontrakt otrzymał koncern Airbus oferujący montaż swoich maszyn na miejscu w Chinach. Jak podkreślają, niedługo po uruchomieniu produkcji Pekin zaprezentował nowy samolot pasażerski dalekiego za-

[21] Zob. B. Góralczyk, *Chiny wyzywają Zachód na pojedynek technologiczny*, źródło: https://www.obserwatorfinansowy.pl (dostęp: 10.01.2018). *China überholt Europa bei Forschung und Entwicklung*, źródło: https://deutsche-wirtschafts-nachrichten.de (dostęp: 10.01.2018).

[22] Zob. M. Adamczyk, *Współpraca wojskowa kluczowym elementem relacji między Federacją Rosyjską a Chińską Republiką Ludową,* [w:] *Oblicza współczesnego terroryzmu,* red. G. Libor, s. l. 2016, s. 182-191.

[23] A. Brunet, J. P. Guichard, *op. cit.*, s. 157-158.

sięgu, bliźniaczo podobny do flagowego produktu europejskiego koncernu – Airbusa A380[24]. Kwestia ochrony własności intelektualnej jest zresztą jednym z kluczowych problemów w relacjach Chin z krajami Zachodu[25].

Mimo, iż znalezienie niepodważalnych dowodów na zaangażowanie służb wywiadowczych jest praktycznie niemożliwe, to jednak pozyskiwanie informacji istotnych dla rozwoju gospodarczego i bezpieczeństwa militarnego państwa jest niewątpliwie podstawowym celem wszystkich agencji wywiadowczych na świecie[26]. Ponadto, zdaniem wielu ekspertów, współcześnie chińskie służby specjalne koncentrują się głównie na szpiegostwie przemysłowym[27]. Z pewnością tylko część chińskich kopii powstało na podstawie wykradzionych planów[28], pozostałe zaś w ramach powielania sprzętu dostarczonego do Chin czy poprzez łamanie zasad licencji[29]. Choć nie jest to przedmiotem niniejszego opracowania, to warto wyjaśnić dlaczego inne kraje godziły się i godzą nadal na dość swobodne traktowanie przez Pekin praw własności intelektualnej. Stany Zjednoczone i niektóre państwa Zachodu starają się wymóc na Państwie Środka ich respektowanie[30], inne stają przed dylematem czy zgoda na kopiowanie własnych rozwiązań, nie tylko na

[24] *Ibidem*, s. 158-159.

[25] Zob. T. Kamiński, *Problemy gospodarcze w relacjach Unii Europejskiej z Chinami*, [w:] *Powrót smoka. Marsz ku pozycji globalnego mocarstwa*, red. J. Marszałek-Kawa, Toruń 2012, s. 52-53; M. Adamczyk, *W kierunku podważenia statusu państwa hegemonicznego: przegląd głównych aspektów współczesnych chińsko – amerykańskich stosunków gospodarczych i wojskowych*, [w:] *Wybrane determinanty polityki bezpieczeństwa XX wieku. Terroryzm i cyberbezpieczeństwo*, red. M. Górka, Poznań 2017 [w druku].

[26] Zob. m. in. M. Górka, *Mossad. Porażki i sukcesy tajnych służb izraelskich*, Warszawa 2015, s. 26-35; L. Korzeniowski, A. Pepłoński, *Wywiad gospodarczy. Historia i współczesność*, Kraków 2005, *passim*; M. Wojciszko, *Prawnoustrojowa pozycja wybranych organów państwa (ze szczególnym uwzględnieniem naczelnych organów) w kontekście realizacji przez nie zadań w obszarze bezpieczeństwa i obronności*, [w:] *Służba więzienna w systemie obronnym państwa*, red. Z. Piątek, S. Olearczyk, Warszawa 2011, s. 64-67.

[27] A. Książczak, *Chińskie służby specjalne XXI wieku – organizacja, metody i formy działania*, „Forum" 2015, nr 2, s. 32; S. Rodzik, *Chiński wywiad – w służbie ambicjom mocarstwowym Chińskiej Republiki Ludowej*, źródło http://www.polska-azja.pl, (dostęp: 10.01.2018).

[28] Zob. m. in. R. Farley, *5 Lethal Chinese Weapons of War (Stolen or Copied from Russia and America)*, źródło: http://nationalinterest.org (dostęp: 10.01.2018); D. Axe, *Go Ahead, China—Copy Our Crappiest Warplane*, źródło: http://www.thedailybeast.com (dostęp: 10.01.2018); I. Luo, *7 Military Weapons China Copied From the United States*: źródło: http://www.theepochtimes.com (dostęp: 10.01.2018); M. Weisgerber, *China's Copycat Jet Raises Questions About F-35*, źródło: http://www.defenseone.com (dostęp: 10.01.2018); https://news.usni.org (dostęp: 10.01.2018).

[29] T. Szulc, *Chiński śmigłowiec Z-9*, „Nowa Technika Wojskowa" 2010, nr 2, s. 70-79; T. Wójtowicz, *Od doktryny wojny ludowej do doktryny wojny informacyjnej: rola nowych technologii w transformacji Chińskiej Armii Ludowo-Wyzwoleńczej*, „Kultura i Polityka: zeszyty naukowe Wyższej Szkoły Europejskiej im. ks. Józefa Tischnera w Krakowie" 2014, nr 16, s. 129.

[30] M. Adamczyk, *W kierunku podważenia*...

potrzeby Chińskiej Armii Ludowo – Wyzwoleńczej (ChALW), lecz również w celu ich późniejszego eksportu, warta jest podpisania kontraktu np. na dostawę kilkudziesięciu egzemplarzy zaawansowanej techniki wojskowej. W takową swoistą „pułapkę uzależnienia" od eksportu sprzętu wojskowegoi uzbrojenia do Chin wpadła swego czasu Moskwa[31].

## Wiodące chińskie operacje cyberszpiegowskie wymierzone w USA

W swojej pracy dotyczącej roli nowoczesnych technologii w procesie modernizacji i transformacji chińskich sił zbrojnych, Tomasz Wójtowicz wskazał najważniejsze zidentyfikowane operacje szpiegowskie tego kraju w cyberprzestrzeni. Wskazał m. in. na mające miejsce na przełomie pierwszej i drugiej dekady XXI wieku w postaci operacji „Nocny Smok", „Aurora" oraz „Nitro"[32]. Inne głośne przypadki cyberataków wyprowadzonych najprawdopodobniej z Chin to m. in. działania grupy „Titan Rain"[33] czy wielokrotne kradzieże danych z programu myśliwca V generacji F-35 Lightning II[34]. Działalność „Titan Rain" (nazwa nadana grupie przez FBI) rozpoczęła się w 2003 roku, a największe natężenie osiągnęła w latach 2006-2008. Zaatakowane zostały głównie amerykańskie agencje rządowe (jak np. NASA) i firmy zbrojeniowe[35].

Operacja „Nocny Smok", która trwała prawdopodobnie 5 lat (2006-2011), miała na celu kradzież informacji z kilkudziesięciu amerykańskich firm komunikacyjnych, energetycznych, finansowych czy działających w sektorze bezpieczeństwa oraz 21 agencji rządowych[36]. Odpowiedzialnością za atak została obarczona niesławna jednostka ChALW z Szanghaju, o numerze 61398[37]. Jednocześnie Departament Sprawiedliwości zdecydował się na bezprecedensowy krok w postaci

[31] M. Adamczyk, *Współpraca wojskowa*..., s. 182-191.
[32] T. Wójtowicz, *op. cit.*, s. 137.
[33] J. Rogin, *The top 10 Chinese cyber attacks (that we know of)*, źródło: http://foreignpolicy.com (dostęp: 10.01.2018); N. Thornburgh, *The Invasion of the Chinese Cyberspies*, źródło: http://content.time.com (dostęp: 10.01.2018).
[34] J. Rogin, *op. cit.*; S. Gorman, A. Cole, Y. Dreazen, *Computer Spies Breach Fighter-Jet Project*, źródło: https://www.wsj.com (dostęp: 10.01.2018); D. Alexander, *Theft of F-35 design data is helping U.S. adversaries – Pentagon*, źródło: http://www.reuters.com (dostęp: 10.01.2018); M. Weisgerber, *op. cit.*
[35] J. Rogin, *op. cit.*; R.S. Spalding, A. Lowther, *Internet of Things: The Missing Link in an Off-Set Strategy*, źródło: http://thediplomat.com (dostęp: 10.01.2018); N. Thornburgh, *op. cit.*
[36] T. Wójtowicz, *op. cit.* s. 138.
[37] Pekin zaprzecza oficjalnie jej istnieniu, choć zebrane przez amerykańskich dziennikarzy śledczych dowody na jej istnienie i wrogą wobec USA działalność są dość przekonywujące: zob. D.E. Sanger, D. Barboza, N. Perlroth, *China's Army Is Seen as Tied to Hacking Against U.S,* źródło: http://www.nytimes.com (dostęp: 10.01.2018).

wniesienia aktu oskarżenia wobec pięciu oficerów chińskiej armii, których udało się zidentyfikować i powiązać z serią włamań do sieci komputerowych amerykańskich firm z sektora energetycznego i metalurgicznego[38].

W 2009 roku chińscy hakerzy w ramach operacji „Nitro" uderzyli w oddziały zagranicznych firm na terenie ChRL, Stanów Zjednoczonych, Wielkiej Brytanii czy Bangladeszu. Ofiarami ataków padło tym razem ponad 100 przedsiębiorstw z sektora chemicznego, motoryzacyjnego i zbrojeniowego[39]. Zaś rozpoczęta w tym samym roku „Aurora" wymierzona była w głównej mierze w wiodące amerykańskie koncerny technologiczne jak Google, Adobe, McAfee, Symantec, Yahoo, Rackspace czy Juniper, ale także w bank inwestycyjny Morgan Stanley oraz jedną z wiodących spółek zbrojeniowych na świecie - Northrop Grumman Corporation[40]. W związku z atakiem na koncerny Google i Microsoft w mediach pojawiły się informacje, jakoby wykradzione zostały również informacje o osobach inwigilowanych na zlecenie służb amerykańskich, za pośrednictwem oferowanych przez firmy usług (takich jak np. poczta Gmail). Dziennikarze zwracają uwagę, że mogło dotyczyć to również osób podejrzanych o szpiegostwo na rzecz Chin, dzięki czemu istniała możliwość, iż zostały one w porę ostrzeżone[41].

Wymienione powyżej chińskie operacje cyberszpiegowskie, to prawdopodobnie zaledwie wycinek działalności hakerów zza Wielkiego Muru. Joe McReynolds wyszczególnił trzy kategorie podmiotów prowadzących działania w cyberprzestrzeni na rzecz Pekinu: dedykowane jednostki wojskowe, cywilni pracownicy agencji rządowych (najczęściej wywiadu) oraz zewnętrzni „podwykonawcy"[42]. Jednocześnie raport zajmującej się cyberbezpieczeństwem amerykańskiej korporacji FireEye podkreśla, iż często powielanym mitem jest opinia,

[38] R. Cornwell, *US declares cyber war on China: Chinese military hackers charged with trying to steal secrets from companies including nuclear energy firm,* źródło: http://www.independent.co.uk (dostęp: 10.01.2018); S. Tiezzi, *US Indicts 5 PLA Officers For Hacking, Economic Espionage*, źródło: http://thediplomat.com, (dostęp: 10.01.2018).

[39] T. Wójtowicz, *op. cit.* s. 137-138.

[40] *Ibidem*, s. 138; L. Constantin, *Morgan Stanley Targeted in Operation Aurora*, źródło: http://news.softpedia.com (dostęp: 10.01.2018); M. Riley, *Morgan Stanley Attacked by China-Based Hackers Who Hit Goog*le, źródło: http://www.reuters.com (dostęp: 10.01.2018); L. Vaas, *Operation Aurora hack was counterespionage, not China picking on Tibetan activists,* źródło: https://nakedsecurity (dostęp: 10.01.2018).

[41] E. Nakashima, *Chinese hackers who breached Google gained access to sensitive data, U.S. officials say*, źródło: https://www.washingtonpost.com (dostęp: 10.01.2018); D. Goodin, *Chinese hackers who breached Google reportedly targeted classified data*, źródło: https://arstechnica.com (dostęp: 10.01.2018).

[42] M. Kumar, *China Finally Admits It Has Army of Hackers*, źródło: http://thehackernews.com, (dostęp: 10.01.2018).

że grupy hakerskie „zza Wielkiego Muru" tworzą swoisty monolit i realizują jedynie wytyczne płynące z najwyższych szczebli władzy w Pekinie. Zdaniem autorów raportu mamy do czynienia z mozaiką aktorów państwowych, wojskowych, prywatnych (działających z pobudek patriotycznych, ale również zwykłych „najemników") czy członków świata przestępczego. Ich sfery działania wzajemnie się przenikają, utrudniając identyfikację. Opracowanie wydane przez amerykańską korporację obejmuje okres od początku 2013 do czerwca 2016 roku. Wymieniono w nim 72 chińskie grupy, które były odpowiedzialne w tym okresie za 262 naruszenia sieciowe, z czego 182 ataków wymierzonych było w podmioty zlokalizowane na terenie USA, zaś pozostałe 80 wobec instytucji z 25 innych krajów (m. in. Wielkiej Brytanii, Japonii, Kanady, Włoch, Szwajcarii, Niemiec, ale i samych Chin)[43]. Warto podkreślić, iż to właśnie działalność „Titan Rain" czy jednostki 61398 rozpoczęła w USA debatę na temat ochrony amerykańskich tajemnic rządowych przed chińskimi atakami. Jak wskazuje cytowany już we wcześniejszych badaniach autora raport *Amerykańskiej Komisji ds. Handlu Międzynarodowego*, który ujrzał światło dzienne w 2011 roku, straty amerykańskich firm z tytułu piractwa *made in China* wyniosły w samym tylko 2009 roku 48 miliardów dolarów i kosztowały kraj utratę ponad 2 milionów nowych miejsc pracy w sektorze zaawansowanych technologii[44]. Ponadto wewnętrzny raport Agencji Bezpieczeństwa Narodowego (NSA) wskazał, iż od 2010 roku blisko 700 amerykańskich firm i instytucji padło ofiarą ataków cybernetycznych mających swoje źródło w Chinach, a których celem była kradzież nowoczesnych technologii[45]. Wcześniejsza analiza wykazała, iż w wielu wypadkach wykradzione dane mogą być wykorzystane zarówno w szeroko pojętym obszarze bezpieczeństwa państwa, jak i w gospodarce – dopiero weryfikacja rzeczywistego ich użycia pozwoliłaby na właściwe przyporządkowania aktów cyberszpiegostwa do odpowiedniej kategorii[46].

Chińscy oficjele regularnie i stanowczo przez ostatnie lata zaprzeczali jakoby rząd wspierał lub inspirował cyberataki wymierzone w Stany Zjednoczone czy jakikolwiek inny kraj na świecie[47]. Jednakże w ciągu ostatnich kilkunastu miesięcy

[43] *Redline Drawn: China Recalculates its use of Cyber Espionage*, źródło: https://www.fireeye.com (dostęp: 10.01.2018).
[44] M. Adamczyk, *W kierunku podważenia...*[w druku].
[45] R. Windrem, *Exclusive: Secret NSA map shows China cyber attacks on US target*, źródło: http://www.nbcnews.com (dostęp: 10.01.2018).
[46] M. Adamczyk, K. Baraniuk, *op. cit.*
[47] T. Stasiak, *Xi: Chiny nie wspierają cyber szpiegostwa*, źródło: https://www.pb.pl (dostęp: 10.01.2018); *Cyberatak na media w USA. Chiny: to nie my,* źródło: https://www.wprost.pl (dostęp:

nie tylko ujawnili fakt posiadania w swoim arsenale wyspecjalizowanych formacji wojskowych do działania w cyberprzestrzeni[48], ale także pod naciskiem Stanów Zjednoczonych zawarły porozumienie o wzajemnym ograniczeniu tego typu ataków[49]. Obie strony zobowiązały się powstrzymać od prowadzenia inspirowanego państwowo szpiegostwa przemysłowego w cyberprzestrzeni oraz od wspierania innych podmiotów w tego rodzaju działaniach. Ponadto powołano mechanizm konsultacyjny mający na celu pomóc w rozwiązywaniu najbardziej drażliwych kwestii w tym obszarze[50].

## Amerykańskie ataki w cyberprzestrzeni

Pomimo, iż autor w niniejszym opracowaniu głównie skoncentrował się na cyberszpiegostwie o chińskiej proweniencji, to należy pamiętać, iż Stany Zjednoczone niewątpliwie również prowadzą szeroko zakrojone działania w cyberprzestrzeni (w tym wobec Chin). Co ciekawe o amerykańskich cyberatakach wiadomo zdecydowanie mniej, niż o analogicznych działaniach hakerów zza Wielkiego Muru. Chińskie Ministerstwo Obrony w 2013 roku wydało komunikat w którym obarczyło USA odpowiedzialnością za ponad 60% ze 140 tysięcy ataków, których ofiarą co miesiąc padają podmioty w Chinach. Szczegóły oficjalnie nie są dostępne, gdyż jak twierdzi strona chińska „ich ujawnienie nie sprzyjałoby rozwiązaniu problemu”[51]. Przedstawiona przez ministerstwo liczba ataków wydaje się mało prawdopodobna, chyba, że przy ich zliczaniu zastosowano specyficzną metodologię, gdzie np. każdą wiadomość elektroniczną, rozsyłaną w ramach masowej próby *phishingu,* klasyfikowano jako osobny incydent. Zdaniem autora rząd chiński unika zbyt częstego informowania o tego typu incydentach z powodów wizerunkowych, a w samych Stanach z oczywistych względów wiadomości na ten

10.01.2018);*Chiny oburzone oskarżeniami nt. cyber-szpiegostwa*: źródło, https://www.wprost.pl (dostęp: 10.01.2018).

[48] M. Kumar, *op. cit*.

[49] *Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference*, źródło: https://obamawhitehouse.archives.gov (dostęp: 10.01.2018); *FACT SHEET: President Xi Jinping's State Visit to the United States*, źródło: https://obamawhitehouse.archives.gov (dostęp: 10.01.2018).

[50] *Ibidem.*

[51] M. Grzelak, *Wpływ szpiegostwa internetowego na stosunki między USA a Chinami*, „Bezpieczeństwo Narodowe” 2013, nr 26, s. 119; J. Cytryńska, *Cyberbezpieczeństwo – szansa na chińsko-amerykańską współpracę*, źródło: http://blog.centruminicjatyw.org (dostęp: 10.01.2018).

temat również nie są szeroko publikowane[52]. Ucieczka Edwarda Snowdena i związany z nią wyciek informacji na temat działalności NSA pozwolił zidentyfikować przynajmniej dwie antychińskie operacje amerykańskiego wywiadu w cyberprzestrzeni: podsłuch pracowników Uniwersytetu Tsinghua (jednego z wiodących pekińskich uniwersytetów technologicznych)[53] oraz uzyskanie dostępu do sieci firmy Huawei - co umożliwiło inwigilację użytkowników sprzętu tej firmy, w tym wielu członków chińskiej administracji rządowej i personelu wojskowego[54]. Wśród dokumentów ujawnionych przez Snowdena[55] znalazły się także te wydobywające na światło dzienne administrowany przez NSA niesławny program PRISM, w ramach którego amerykańskie służby miały dostęp do informacji (poczty elektronicznej, zapisów czatówi rozmów, nagrań audio i video itd.) przechowywanych na serwerach m. in. firm Microsoft, Yahoo, Apple, Google, Facebook czy AOL[56]. Kwestią wtórną pozostaje w tym momencie pytanie czy Snowden działał z wewnętrznych pobudek moralnych jako tzw. „whistleblower" (pol. sygnalista) czy też, jak sugerują niektórzy, miał on jednak związki np. z wywiadem ChRL[57].

## Zamiast zakończenia

Poprzednie badania pokazały, iż wspomniane powyżej chińsko-amerykańskie porozumienie zostało ogłoszone przez administrację Białego Domu jako znaczący sukces prezydenta Obamy[58]. Jednakże raport korporacji FireEye wskazuje, iż miało ono niewielki wpływ na natężenie aktywności szpiegowskiej Chin w cyberprzestrzeni. Dający się zauważyć spadek ilości ataków na podmioty ulokowane

[52] Zob. więcej: M. Grzelak, *Międzynarodowa strategia USA dla cyberprzestrzeni*, „Bezpieczeństwo Narodowe" 2011, nr 18, s. 139-147.

[53] K. Rapoza, *U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press*, źródło: https://www.forbes.com (dostęp: 10.01.2018).

[54] D.E. Sanger, N. Perlroth, *N.S.A. Breached Chinese Servers Seen as Security Threat*: źródło: https://www.nytimes.com (dostęp: 10.01.2018); M. Kan, *China's Huawei turns the table on security after Snowden NSA leaks*, źródło: https://www.pcworld.com (dostęp: 10.01.2018).

[55] Zob. więcej: *Snowden Digital Surveillance Archive*, źródło: https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi (dostęp: 10.01.2018).

[56] M. Grzelak, *op. cit.*, s. 119.

[57] G.G. Chang, *Snowden Lied About China Contacts?*, źródło: https://www.thedailybeast.com (dostęp: 10.01.2018); Nie ulega przy tym wątpliwości, iż w ciągu dwóch lat od jego ucieczki do wykradzionych dokumentów pełen dostęp uzyskali nie tylko Chińczycy, ale również Rosjanie: *Snowden's Gift to Russia and China*, źródło: https://www.wsj.com (dostęp: 10.01. 2018); E. Mac-Askill, *Snowden files 'read by Russia and China': five questions for UK government*, źródło: https://www.theguardian.com (dostęp: 10.01.2018).

[58] M. Adamczyk, K. Baraniuk, *op. cit.*

w Stanach Zjednoczonych[59] (oraz 25 innych krajach) miał miejsce na rok przed zawarciem rzeczonego porozumienia. Co ciekawe, odbyło się to już po słynnym przypadku skazania pięciu chińskich hakerów przez amerykański sąd tj. jeszcze w 2014 roku[60]. FireEye wskazuje, że liczba ataków spadła z ponad sześćdziesięciu miesięcznie w 2013 roku, do poziomu poniżej 10 ataków na koniec roku 2015[61]. Eksperci przyczyn upatrują jednakże głównie w polityce wewnętrznej Chin. Xi Jinping rozpoczął wdrażanie reformy ChALW, która ma m. in. doprowadzić do scentralizowania działań w cyberprzestrzeni, przy jednoczesnym zwiększeniu ich efektywności. Ponadto w ramach głośnej kampanii antykorupcyjnej przewodniczący ChRL zmierza do ukrócenia praktyk polegających na wykorzystywaniu państwowych zasobów w celu akwizycji technologii dla sektora prywatnego[62]. Warto podkreślić, że zarówno eksperci, jak i decydenci w samych Stanach są dość sceptyczni wobec efektów porozumienia. Cytowany przez Blaise Misztala senator Ben Cardin (członek senackiej Komisji Spraw Zagranicznych) twierdzi, iż nie może być mowy o spadku aktywności chińskich hakerów[63]. Misztal interpretując słowa senatora podkreśla, iż nie jest to pierwszy raz, gdy informacje wywiadowcze dystrybuowane wśród oficjeli są niespójne z tym, co w swoich raportach zamieszczają niezależne podmioty. Wskazuje on na dość oczywisty fakt, iż FireEye skupiając się na analizie działań 72 grup hakerskich, mogło źle zinterpretować ich znaczenie w chińskim systemie cyberszpiegostwa, a nawet źle określić przynależność państwową tychże grup. Z drugiej strony zarówno Blaise Misztal, jak i autorzy raportu zgadzają się co do tego, że ataki rodem z ChRL stają się mniej intensywne, lecz jednocześnie co raz bardziej wyrafinowane, skoncentrowane na celu i co za tym idzie stanowią równie istotne zagrożenie, co dotychczasowe zmasowane działania[64]. Misztal krytykuje amerykańską strategię odstraszania w cyberprzestrzeni, wskazując, że jest nieskuteczna – groźby odwetu były niewiarygodne, a działania wobec pojedynczych hakerów z Chin niewystarczające. Posuwa się on nawet do sugestii, że dążenie USA do zawarcia kompromisu w tej sprawie, mogło zostać

[59] Zob. więcej na temat ujawnionych cyberataków na amerykańskie przedsiębiorstwa w 2014 roku: R. Walters, *Cyber Attacks on U.S. Companies in 2014*, źródło: http://www.heritage.org (dostęp: 10.01.2018).

[60] F.S. Gady, *Are Chinese Cyberattacks Against US Targets in Decline?,* źródło: http://thediplomat.com (dostęp: 10.01.2018); B. Misztal, *Amerykańska strategia odstraszania chińskich hakerów nie działa*, źródło: http://www.cyberdefence24.pl, (dostęp: 10.01.2018); *Redline Drawn…*, *passim*.

[61] *Redline Drawn…*, s. 11.

[62] *Ibidem,* s. 5-6; F.S. Gady, *op. cit*.

[63] B. Misztal, *op. cit.*

[64] *Ibidem*; *Redline Drawn*..., s. 15.

odczytane w Chinach jako oznaka słabości[65]. Niedawne wydarzenie w postaci ataku cybernetycznego na jeden z amerykańskich lotniskowców klasy *Nimitz* (USS Ronald Reagan), jest w tym kontekście dość wymowne[66]. Jednocześnie inny ekspert, Franz Stefan Gady, zajął w tej kwestii mniej stanowcze stanowisko – jego zdaniem groźba sankcji wywarła wpływ na politykę Xi Jingpinga. Kwestia tego, czy był to efekt obaw przed skutkami ich wprowadzenia przez Stany Zjednoczone, czy też przewodniczący wykorzystał je jako pretekst do wzmocnienia swojej władzy na sektorem wojskowym i wywiadowczym, jest wtórna[67]. Natomiast Jacek Raubo podkreśla, iż ChRL w swojej działalności wywiadowczej kładzie nacisk na działania w cyberprzestrzeni oraz formułuje tezę, sygnalizowaną już przez autora niniejszego opracowania, iż „(...) dla Chińczyków kluczowym pozostaje wywiad naukowo-techniczny. Jak się wydaje, dynamicznie rozwijające się państwo i jego przemysł „zgłaszają zapotrzebowanie" na każdą formę urobku służb jeżeli chodzi o najnowsze technologie[68]. Należy się również zgodzić z Raubo, iż niewątpliwie następuje renesans klasycznego szpiegostwa, zaś wyścig zbrojeń w sferze wywiadowczej (i nie tylko) trwa w najlepsze. Cyberszpiegostwo w relacjach chińsko-amerykańskich ma więc przed sobą świetlaną przyszłość, przynajmniej do czasu, gdy Chinom uda się wyprzedzić Stany Zjednoczone w wyścigu technologicznym.

## Bibliografia

Adamczyk M., Baraniuk K., *Służby wywiadowcze Chińskiej Republiki Ludowej – zarys struktur i metod działalności*, „Studia Orientalne" 2017, nr 2 (12), [przyjęte do druku].

Adamczyk M., *Media we współczesnym państwie totalitarnym na przykładzie Chińskiej Republiki Ludowej*, [w:] *Media XXI wieku. Studia interdyscyplinarne*, red. A. Momot, A. Drabina, Wrocław 2016.

Adamczyk M., *Porównanie zmiany potencjału militarnego Chin na tle Rosji, Indii, Stanów Zjednoczonych oraz Japonii w okresie od 1989 do 2013 roku*, [w:] *Aspekty*

[65] B. Misztal, *op. cit.*
[66] *USS Ronald Reagan zaatakowany przez Chińczyków*, źródło: http://www.cyberdefence24.pl (dostęp: 10.01.2018).
[67] F.S. Gady, *op. cit.*
[68] J. Raubo, *Renesans klasycznego szpiegostwa. Mocarstwa wracają do wojny wywiadów*, źródło: http://www.defence24.pl (dostęp: 10.01.2018).

*bezpieczeństwa w życiu publicznym*, red. D. Magierek, M. Pogonowski, Koszalin 2015.

Adamczyk M., *W kierunku podważenia statusu państwa hegemonicznego: przegląd głównych aspektów współczesnych chińsko – amerykańskich stosunków gospodarczych i wojskowych*, [w:] *Wybrane determinanty polityki bezpieczeństwa XX wieku. Terroryzm i cyberbezpieczeństwo*, red. M. Górka, Poznań 2017 [w druku].

Adamczyk M., *Współpraca wojskowa kluczowym elementem relacji między Federacją Rosyjską a Chińską Republiką Ludową,* [w:] *Oblicza współczesnego terroryzmu,* red. G. Libor, s. l. 2016.

Alexander D., *Theft of F-35 design data is helping U.S. adversaries – Pentagon*, źródło: http://www.reuters.com (dostęp: 10.01.2018).

Andrijauskas K., *China's Economic Penetration into Post-Soviet Central Asia and Eastern Europe*, „Lithuanian Foreign Policy Review" 2013, nr 30.

Axe D., *Go Ahead, China—Copy Our Crappiest Warplane*, źródło: http://www.thedailybeast.com (dostęp: 10.01.2018).

Bernstein R., Munro R. H., *The coming conflict with China*, Nowy Jork 1998.

Białowąs T., *Inwestycje a wzrost gospodarczy Chin w latach 1980-2012*, „Annales Universitatis Mariae Curie-Skłodowska. Sectio H, Oeconomia" 2014, t. 48, nr 2.

Borkowski P., *Koncepcja cyberbezpieczeństwa w ujęciu Chińskiej Republiki Ludowej - wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, t. 7, nr 13.

Brunet A., Guichard J. P., *Chiny światowym hegemonem?*, Warszawa 2011.

Campbell H., *China in Africa: challenging US global hegemony*, „Third World Quarterly" 2008, nr 29, t. 1.

Chang G. G., *Snowden Lied About China Contacts?*, źródło: https://www.thedailybeast.com (dostęp: 10.01.2018)

Chin J., *China Says Prepared to Lead Global Economy if Necessary*, źródło: http://www.wsj.com (dostęp: 10.01.2018).

*China überholt Europa bei Forschung und Entwicklung*, źródło: https://deutsche-wirtschafts-nachrichten.de (dostęp: 10.01.2018).

*Chiny mogą zaszkodzić surowcom, ale wesprzeć konsumpcję*, źródło: http://www.bankier.pl (dostęp: 10.01.2018).

*Chiny oburzone oskarżeniami nt. cyber-szpiegostwa*, źródło: https://www.wprost.pl (dostęp: 10.01.2018).

Ciszak P., *Gospodarka Chin zwalnia. Niższe tempo wzrostu gospodarczego wpłynie na Europę,* źródło: https://www.money.pl (dostęp: 10.01.2018).

Constantin L., *Morgan Stanley Targeted in Operation Aurora*, źródło: http://news.softpedia.com (dostęp: 10.01.2018).

Cornwell R., *US declares cyber war on China: Chinese military hackers charged with trying to steal secrets from companies including nuclear energy firm,* źródło: http://www.independent.co.uk (dostęp: 10.01.2018)

*Cyberatak na media w USA. Chiny: to nie my,* źródło: https://www.wprost.pl (dostęp: 10.01.2018).

Cytryńska J., *Cyberbezpieczeństwo – szansa na chińsko-amerykańską współpracę*, źródło: http://blog.centruminicjatyw.org (dostęp: 10.01.2018).

Dereń J., Rabiak A., *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2014.

*Diplomat says China would assume world leadership if needed*, źródło: http://www.reuters.com (dostęp: 10.01.2018).

*FACT SHEET: President Xi Jinping's State Visit to the United States*, źródło: https://obamawhitehouse.archives.gov (dostęp: 10.01.2018).

Faligot R., Kauffer R., *Tajne służby Chin (1927-1987)*, Warszawa 1994.

Faligot R., *Tajne służby chińskie: od Mao do igrzysk olimpijskich*, Katowice 2009.

Farley R., *5 Lethal Chinese Weapons of War (Stolen or Copied from Russia and America)*, źródło: http://nationalinterest.org (dostęp: 10.01.2018).

Furmanek J.*, Innowacje po chińsku. Jak rozwój technologii Made in China zmieni współczesny świat*, źródło: http://peoplessquare.pl (dostęp: 10.01.2018)

Gady F. S., *Are Chinese Cyberattacks Against US Targets in Decline?,* źródło: http://thediplomat.com (dostęp: 10.01.2018)

Gompert D. C., Stuth Cevallos A., Garafola C. L., *War with China. Thinking Through the Unthinkable,* Santa Monica 2016, źródło: http://www.rand.org (dostęp: 10.01.2018).

Goodin D., *Chinese hackers who breached Google reportedly targeted classified data*, źródło: https://arstechnica.com (dostęp: 10.01.2018).

Góralczyk B., *Chiny wyzywają Zachód na pojedynek technologiczny*, źródło: https://www.obserwatorfinansowy.pl (dostęp: 10.01.2018).

Górka M., *Mossad. Porażki i sukcesy tajnych służb izraelskich*, Warszawa 2015.

Gorman S., Cole A., Dreazen Y., *Computer Spies Breach Fighter-Jet Project*, źródło: https://www.wsj.com (dostęp: 10.01.2018).

Grzelak M., *Międzynarodowa strategia USA dla cyberprzestrzeni*, „Bezpieczeństwo Narodowe" 2011, nr 18.

Grzelak M., *Wpływ szpiegostwa internetowego na stosunki między USA a Chinami*, „Bezpieczeństwo Narodowe" 2013, nr 26.

https://news.usni.org (dostęp: 10.01.2018).

Hübner W., *Innowacje w Chinach: od starożytności do wyzwań dnia dzisiejszego*, „Kwartalnik Naukowy Uczelni Vistula*"* 2013, tom 36, nr 2.

Kagan R., *Powrót historii i koniec marzeń,* Poznań 2009.

Kaliński A., *W Chinach wyhamowała konsumpcja*, źródło: https://www.obserwatorfinansowy.pl (dostęp: 10.01.2018).

Kamiński T., *Problemy gospodarcze w relacjach Unii Europejskiej z Chinami*, [w:] *Powrót smoka. Marsz ku pozycji globalnego mocarstwa*, pod red. J. Marszałek-Kawa, Toruń 2012.

Kamiński T., *Sypiając ze smokiem. Polityka Unii Europejskiej wobec Chin*, Łódź 2015.

Kan M., *China's Huawei turns the table on security after Snowden NSA leaks*: źródło: https://www.pcworld.com (dostęp: 10.01.2018).

*Kolejny znak spowolnienia chińskiej gospodarki. Eksport w styczniu spadł o 11,2 proc. rdr*, źródło: http://www.polskieradio.pl (dostęp: 10.01.2018).

Kolka M. A., *Czynniki wzrostu PKB i perspektywy rozwoju gospodarczego Chin do 2015 roku*, „Międzynarodowe stosunki gospodarcze - wybrane podmioty i procesy gospodarki światowej" 2012, nr 122.

Kopiński D., *Ekspansja gospodarcza Chin w Afryce – szansa na rozwój czy początek neokolonizacji?*, [w:] *Afryka na progu XXI wieku Polityka. Kwestie społeczne i gospodarcze*, red. D. Kopiński, A. Żukowskiego, Warszawa 2009.

Korzeniowski L., Pepłoński A., *Wywiad gospodarczy. Historia i współczesność*, Kraków 2005.

Kosiński D., *Już rok temu Huawei zmienił oblicze mobilnej fotografii. Zauważyło to nawet Apple*, źródło: https://www.pcformat.pl (dostęp: 10.01.2018).

Kotkowski Ł., *Nowy smartfon ZTE pokazuje, że ramki w smartfonach są całkowicie zbędne*, źródło: http://www.spidersweb.pl (dostęp: 10.01.2018)

Książczak A., *Chińskie służby specjalne XXI wieku – organizacja, metody i formy działania*, „Forum" 2015, nr 2.

Kumar M., *China Finally Admits It Has Army of Hackers*, źródło: http://thehackernews.com, (dostęp: 10.01.2018).

*Leksykon międzynarodowych stosunków politycznych*, red. Cz. Mojsiewicz, Wrocław 2004.

Liberska B., *System powiązań Ameryki Łacińskiej z Indiami i Chinami we współczesnej gospodarce światowej*, „International Journal of Management and Economics" 2008, nr 23.

Luo I., *7 Military Weapons China Copied From the United States*, źródło: http://www.theepochtimes.com (dostęp: 10.01.2018).

M. Weisgerber, *China's Copycat Jet Raises Questions About F-35*, źródło: http://www.defenseone.com (dostęp: 10.01.2018).

MacAskill E., S*nowden files 'read by Russia and China': five questions for UK government*, źródło: https://www.theguardian.com (dostęp: 10.01.2018).

Mencel M., *Strategia Chin wobec państw Ameryki Łacińskiej*, „Studia Gdańskie. Wizje i rzeczywistość" 2013, nr 10.

Misztal B., *Amerykańska strategia odstraszania chińskich hakerów nie działa*, źródło: http://www.cyberdefence24.pl, (dostęp: 10.01.2018).

Mosher S. W., *Hegemon: China's plan to dominate Asia and the world*, San Francisco 2002.

Nakashima E., *Chinese hackers who breached Google gained access to sensitive data, U.S. officials say*, źródło: https://www.washingtonpost.com (dostęp: 10.01.2018).

Rapoza K., *U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press*, źródło: https://www.forbes.com (dostęp: 10.01.2018).

Raubo J., *Renesans klasycznego szpiegostwa. Mocarstwa wracają do wojny wywiadów*, źródło: http://www.defence24.pl (dostęp: 10.01.2018).

*Redline Drawn: China Recalculates its use of Cyber Espionage*, źródło: https://www.fireeye.com (dostęp: 10.01.2018).

*Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference*, źródło: https://obamawhitehouse.archives.gov (dostęp: 10.01.2018).

Riley M., *Morgan Stanley Attacked by China-Based Hackers Who Hit Goog*le, źródło: http://www.reuters.com (dostęp: 10.01.2018).

Rodzik S., *Chiński wywiad – w służbie ambicjom mocarstwowym Chińskiej Republiki Ludowej*, źródło http://www.polska-azja.pl (dostęp: 10.01.2018).

Rogin J., *The top 10 Chinese cyber attacks (that we know of)*, źródło: http://foreignpolicy.com (dostęp: 10.01.2018).

Rousseau R., *China's Growing Economic Presence in Ukraine and Belarus*, „Strategic Analysis" 2012, nr 1 (36).

Roy D., *Hegemon on the Horizon? China's Threat to East Asian Security*, „International Security" 1994, Nr 19, t. 1.

Rybicka M., Wieszczycka W., *Chiny – rosnące mocarstwo innowacyjności*, źródło: http://www.pte.pl (dostęp: 10.01.2018).

Sanger D. E., Barboza D., Perlroth N., *China's Army Is Seen as Tied to Hacking Against U.S,* źródło: http://www.nytimes.com (dostęp: 10.01.2018).

Sanger D. E., Perlroth N., *N.S.A. Breached Chinese Servers Seen as Security Threat*, źródło: https://www.nytimes.com (dostęp: 10.01.2018).

*Snowden Digital Surveillance Archive*, źródło: https://snowdenarchive.cjfe.org (dostęp: 10.01.2018).

*Snowden's Gift to Russia and China*, źródło: https://www.wsj.com (dostęp: 10.01.2018)

Spalding R. S., Lowther A., *Internet of Things: The Missing Link in an Off-Set Strategy*, źródło: http://thediplomat.com (dostęp: 10.01.2018).

Stasiak T., *Xi: Chiny nie wspierają cyber szpiegostwa*, źródło: https://www.pb.pl (dostęp: 10.01.2018).

Stodolak S., *Na spowolnienie w Chinach nie ma sprawdzonych recept*, źródło: https://www.obserwatorfinansowy.pl (dostęp: 10.01.2018).

Stojek J., *Chiński zwrot ku innowacyjności*, źródło: http://www.psz.pl (dostęp: 10.01.2018).

Szulc T., *Chiński śmigłowiec Z-9*, „Nowa Technika Wojskowa" 2010, nr 2.

Thornburgh N., *The Invasion of the Chinese Cyberspies*, źródło: http://content.time.com (dostęp: 10.01.2018).

Tiezzi S., *US Indicts 5 PLA Officers For Hacking, Economic Espionage*, źródło: http://thediplomat.com, (dostęp: 10.01.2018).

*USS Ronald Reagan zaatakowany przez Chińczyków*, źródło: http://www.cyberdefence24.pl (dostęp: 10.01.2018).

Vaas L., *Operation Aurora hack was counterespionage, not China picking on Tibetan activists,* źródło: https://nakedsecurity (dostęp: 10.01.2018).

Walters R., *Cyber Attacks on U.S. Companies in 2014*, źródło: http://www.heritage.org (dostęp: 10.01.2018).

Windrem R., *Exclusive: Secret NSA map shows China cyber attacks on US target*, źródło: http://www.nbcnews.com (dostęp: 10.01.2018).

Wojciszko M., *Prawnoustrojowa pozycja wybranych organów państwa (ze szczególnym uwzględnieniem naczelnych organów) w kontekście realizacji przez nie zadań w obszarze bezpieczeństwa i obronności*, [w:] *Służba więzienna w systemie obronnym państwa*, red. Z. Piątek, S. Olearczyk, Warszawa 2011.

Wójtowicz T., *Od doktryny wojny ludowej do doktryny wojny informacyjnej: rola nowych technologii w transformacji Chińskiej Armii Ludowo-Wyzwoleńczej*, „Kultura i Polityka: zeszyty naukowe Wyższej Szkoły Europejskiej im. ks. Józefa Tischnera w Krakowie" 2014, nr 16.

*World Development Indicators*, źródło: http://data.worldbank.org (dostęp: 10.01.2018).

*World Economic Outlook Database April 2017*, źródło: https://www.imf.org (dostęp: 10.01.2018).

Żodź – Kuźnia K., Wiśniewski J., *Dynamika wzajemnych relacji między Unią Europejską a Chińską Republiką Ludową na początku XXI wieku,* „Przegląd Politologiczny" 2012, nr 2.

**Kamil Baraniuk**

Uniwersytet Wrocławski

# Zarys przemian instytucjonalnych rosyjskiego wywiadu radioelektronicznego w świetle literatury polsko- i angielskojęzycznej

Słowa kluczowe: wywiad radioelektroniczny, SIGINT, FAPSI, rosyjskie służby specjalne

## SIGINT jako źródło informacji wywiadowczej

Informacje pozyskiwane przez służby wywiadowcze mogą pochodzić ze źródeł różnego rodzaju. W nomenklaturze anglosaskiej wyróżnia się następujące dziedziny wywiadowcze[1]:

- HUMINT (Human Intelligence) – wywiad agenturalny, w przypadku którego źródłem informacji są osoby mające dostęp do ważnych informacji i zgodziły się (z różnych względów) je udzielać obcemu wywiadowi.
- OSINT (Open Source Intelligence) – wywiad jawnoźródłowy, opierający się na informacjach publicznie dostępnych informacji, jak i tych, które mają ograniczony dostęp rozpowszechniania, ale są jawne.
- IMINT (Imagery Intelligance) – wywiad obrazowy, który opiera się wykorzystywaniu w gromadzeniu informacji urządzeń, które służą do zapisu obrazu: kamer, aparatów fotograficznych, samolotów, dronów, satelitów itd.

[1] Szerzej na temat charakterystyki źródeł informacji wywiadowczej zob. M. Mikinia, *Sztuka wywiadu we współczesnym państwie*, Warszawa 2014, s. 178-193.

- SIGINT (Signal Intellgence) - wywiad radioelektroniczny, który polega na przechwytywaniu informacji pochodzących z łączności, radarów oraz urządzeń pomiarowych, który dzieli się na podział na:
    - wywiad radiowy, a więc COMINT (Communication Intelligence), który zajmuje się gromadzeniem informacji pochodzących
      z obcych systemów teleinformatycznych oraz urządzeń emitujących fale radiowe służących do komunikowania
    - wywiad elektroniczny, a więc ELINT (Electronics Signal Intellgence) – który opiera się na pozyskiwaniu informacji od systemów nie służących do komunikowania między ludźmi, ale urządzeń wytwarzających promieniowanie elektromagnetyczne (np. radary przeciwnika, systemy obrony powietrznej, systemy naprowadzania na cel).

Według *Słownika terminów i definicji NATO,* SIGINT określa rozpoznanie radiowe oraz elektroniczne, czyli wywiad radiowy i elektroniczny[2]. Wywiad radiowy traktuje się jako „pozyskiwanie danych wywiadowczych (rozpoznawczych) za pomocą środków i systemów łączności radiowej przez osoby nie będące właściwymi odbiorcami lub użytkownikami"[3] Rozpoznanie (wywiad) elektroniczny jest natomiast rozumiany jako „rozpoznawczy proces pozyskiwania danych i informacji rozpoznawczych z systemów niekomunikacyjnych przechwyconych przez innych odbiorców niż tych, do których są one adresowane"[4]. Zadania realizowane przez jednostki i instytucje zajmujące się wywiadem radioelektronicznym mogą być różne w zależności od rodzaju oraz poziomu działalności. W przypadku sił zbrojnych działania wywiadowcze na poziomie strategicznym będą dotyczyć przechwytywania i monitorowania szerokiego zakresu wyposażenia i systemów wojsk przeciwnika, co ma na celu dostarczenie informacji odnośnie wykorzystywanych przez niego technologii, taktyki czy procedur wewnętrznych. Wojskowy wywiad radioelektroniczny na poziomie taktycznym z kolei zajmuje się przechwytywaniem łączności i danych niekomunikacyjnych wojsk na poziomie lokalnym[5]. Omawiana

[2] Hasło: *SIGINT*, [w:] *Słownik terminów i definicji NATO. Zawierający wojskowe terminy i ich definicje stosowane w NATO,* źródło: wcnjk.wp.mil.pl (dostęp: 11.08.2016), s. 360.
[3] Hasło: *COMINT*, [w:] *Słownik…,* s. 102.
[4] Hasło: *ELINT*, [w:] *Słownik…,* s. 152.
[5] H. Zsolt, *Converegence between signals intelligence and electronic warfare suport measures,* „Technical Scienses" 2014, nr 3 (75), s. 328.

dziedzina wywiadowcza zajmuje się między innymi analizą techniczną przekazów radiowych, ustalaniem pracujących w sieci radiowej abonamentów, przechwytywaniem i deszyfracją danych wywiadowczych pochodzących z systemów łączności przeciwnika. Istotnym zadaniem wywiadu radioelektronicznego jest także monitorowanie oraz lokalizowanie za pomocą naziemnych radarów ważnych obiektów na terytorium przeciwnika oraz namierzanie urządzeń emitujących fale elektromagnetycznych[6].

W związku z rozwojem oraz możliwościami technologicznymi stale wzrasta znaczenie tego rodzaju wywiadu na świecie. Szczególnym impulsem dla rozwoju tej dziedziny wywiadowczej było wynalezienie radia na przełomie XIX i XX wieku[7]. Od tamtego czasu rozwój technologiczny znacznie zwiększył i spopularyzował możliwości komunikowania. Obecnie do głównych zalet wywiadu radioelektronicznego zalicza się szerokie możliwości oraz szybkość działania, przy zachowaniu względnej skrytości i tym samym ominięcia problemów prawnych i politycznych. Istnieją jednak również wady. Wiążą się one głównie z koniecznością wysokich nakładów finansowych oraz ogromną ilością pozyskiwanych danych, co wiąże się z utrudnieniami pracy analitycznej. Pamiętać również należy, że wywiad radioelektroniczny ma ograniczone możliwości w zakresie pozyskiwania informacji o nieutrwalonych planach przeciwnika, które często mają kluczowe znaczenie, a ich pozyskanie jest możliwe głównie dzięki HUMINT[8].

## SIGINT w radzieckich służbach specjalnych

Przedsięwzięcia z zakresu radiowywiadu były podejmowane od wczesnych lat istnienia ZSRR. Jako przykład można podać dekryptaż komunikacji obcych placówek dyplomatycznych realizowany przez Czeka[9]. Następnie tę dziedzinę funkcjonowania radzieckich służb specjalnych silnie rozwinął Gleb Bokij – założyciel i sprawujący przez szesnaście lat stanowisko szefa Oddziału Specjalnego GPU/OGPU zajmującego się kryptografą, radiowywiadem, radiokontrwywiadem oraz zabezpieczeniem tajemnicy w instytucjach państwowych. Bokij i inni wysocy

[6] Hasło: *Wywiad z kanałów łączności*, [w:] J. Larecki, *Wielki leksykon służb specjalnych świata. Organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny,* Warszawa 2007, s. 749.

[7] Szerzej na temat rozwoju wywiadu radiowego zob.: A. Nogaj, *Techniczne źródła pozyskiwania informacji wywiadowczych,* „Zeszyty Naukowe WSOWL" 2011, nr 4 (162), s. 111.

[8] M. Mikinia, *op. cit*., s. 189.

[9] Ch. Andrew, O. Gordijewski, *KGB*, Warszawa 1999, s. 35.

rangą funkcjonariusze tej jednostki posiadający wieloletnie doświadczenie w działalności kryptograficznej stali się jednak ofiarami „Wielkiej Czystki" i w większości zostali rozstrzelani. W latach 1938-1939 Oddział Specjalny został przekształcony w 7. Oddział GUGB, a na jego czele stanął kapitan Aleksandr Dimitrijewicz Bałamutow. Był to oficer OGPU, który nie posiadał jednak doświadczenia w zakresie radiowywiadu, co odbiło się na obniżeniu skuteczności funkcjonowania całej komórki. Sytuacja poprawiła się po utworzeniu w 1941 roku 5. Oddziału Specjalnego NKWD, na którego czele stanął Iwan Grigorijewicz Szewelew. Co prawda ten oficer również nie miał doświadczenia w kryptografii (wcześniej zajmował się walką z „ruchami kontrrewolucyjnymi"), ale odznaczał się rozwiniętymi zdolnościami organizatorskimi, co pozwoliło na zwiększenie skuteczności jednostki, której szefował i tym samym podniesienie jej rangi w ówczesnym systemie radzieckich służb specjalnych. Szewelew przez 13 lat stał na jej czele i kolejnych instytucji, które przejmowały jej zadania – 5. Wydziału Specjalnego NKGB oraz 6. Zarządu MGB. W 1949 roku przestał piastować stanowisko zwierzchnika cywilnego radzieckiego radiowywiadu i kontrwywiadu. Warto zauważyć, w pierwszych latach po II wojnie światowej tak wyspecjalizowana komórka w naturalny sposób cierpiała na niedobór kadrowy, a dodatkowo przegrywała rywalizację o środki budżetowe z większymi i silniejszymi jednostkami organizacyjnymi MGB zajmującymi się bezpieczeństwem wewnętrznym oraz wywiadem zagranicznym głównie w oparciu o osobowe źródła informacji. Sprawiło to, że początkowym etapie zimnej wojny radziecki wywiad radioelektroniczny posiadał ograniczone możliwości w zakresie kryptografii czy analizy informacji pozyskanych w ramach SIGINT[10].

Podejmując jednak temat radzieckiego wywiadu radioelektronicznego od momentu powstania KGB w 1953 roku należy wspomnieć o 8. Głównym Zarządzie KGB oraz 16. Zarządzie KGB. Do zadań funkcjonariuszy pierwszej z tych jednostek organizacyjnych należało przechwytywanie, monitorowanie oraz analizowanie sygnałów komunikacyjnych innych państw. Dodatkowo pracownicy tej struktury odpowiadali za system kryptograficzny wykorzystywany przez pozostałe jednostki organizacyjne KGB, a także za zagraniczne stacje nasłuchowe oraz rozwijanie zabezpieczeń łączności tej służby. Część z zadań skupiała się również na działalności kryptograficznej i w tym zakresie działalność 8. Zarządu Głównego często nakładała się na obszary zainteresowania 16. Zarządu. Skupiały się one bowiem głównie

[10] M. M. Aid, *Esdroppers of the Kremlin: KGB during the cold war*, [w:] *The History Information Security: A Comperehensive Handbook,* red. K. de Leeuw, J. Bergstra, Amsterdam 2007, s. 498-505.

na telefonicznych i radiowych systemach wykorzystywanych przez większość ważnych instytucji państwa radzieckiego[11]. Wspomnieć jednak należy, że radziecki SIGINT w czasie zimnej wojny miał charakter w większym stopniu zdecentralizowany, niż to miało miejsce na Zachodzie gdzie istniały dedykowane służby wywiadu i kontrwywiadu radioelektronicznego takie jak np. NSA czy GCHQ[12].

W kontekście jednostek organizacyjnych cywilnych radzieckich służb specjalnych warto również wspomnieć, że były one realizowane przez niektóre komórki funkcjonalne 1. Zarządu Głównego, który odpowiadał głównie za prowadzenie działalności wywiadowczej poza granicami ZSRR w oparciu o wywiad agenturalny. Jako przykład można podać pion łączności radiowej oraz pion szyfrów, które ściśle współdziałały z funkcjonariuszami wyżej wspomnianego 8. Zarządu Głównego KGB (pion szyfrów po 1975 został wchłonięty przez tą strukturę)[13].

Za wojskowy wywiad radioelektroniczny był odpowiedzialny 6. Zarząd GRU[14]. Podkreślić jednak należy, że wywiadem elektronicznym i komunikacyjnym zajmowały się również poszczególne rodzaje sił zbrojnych ZSRR. GRU usiłowała je sobie podporządkować, ale nie radziła sobie z pełną kontrolą działalności wojskowego wywiadu radioelektronicznego. W konsekwencji więc na przykład marynarka wojenna prowadziła własne działania w tym zakresie, podobnie jak lotnictwo strategiczne, które pozostawało niezależne od GRU[15].

Ograniczony dostęp do źródeł oraz niewielka liczba opracowań dotyczących radzieckiego wywiadu radioelektronicznego w czasie zimnej wojny utrudnia postawienie diagnozy co do efektywności KGB i GRU w tym omawianym zakresie. W wypowiedziach byłych radzieckich i zachodnich oficerów wywiadu jawi się ona jako jedna z najbardziej sprawnych w całej społeczności rosyjskiego wywiadu, a nawet działająca w tym okresie na większą skalę oraz z większymi sukcesami niż jej amerykańskie czy brytyjskie odpowiedniki. Jako podparcie tej tezy zwraca się uwagę na dwie podstawowe cechy, które dawały przewagę strukturom SIGINTu

[11] *Functions and Internal Organization,* źródło: http://www.globalsecurity.org (dostęp: 04.08.2016); W. T. Smith, *Encyclopedia of Central Intelligence Agency,* Nowy Jork 2003, s. 156; *Global National Security and Intelligence Agencies Handbook. Vol 1 strategic information and contact,* Waszyngton 2015, s. 204-205

[12] M. M. Aid, *op.cit.*, s. 498.

[13] L. Pawlikowicz, *Aparat centralny 1. Zarządu Głównego KGB jako instrument realizacji globalnej strategii Kremla 1954-1991*, Warszawa 2013, s. 299.

[14] *Signals Intelligence Programs and Activities*, źródło: http://www.globalsecurity.org (dostęp: 11.08.2016).

[15] M. M. Aid, *op.cit.*, s. 519.

KGB oraz GRU w stosunku do odpowiedników zachodnich. Po pierwsze służby radzieckie zatrudniały lub miały bezpośredni dostęp do wielu najlepszych matematyków i inżynierów telekomunikacji w całym ZSRR (na Zachodzie często byli oni zagospodarowani przez rynek prywatny). Po drugie KGB oraz GRU były ściśle zintegrowane z wywiadem agenturalnym, co w efekcie doprowadzało np. do wykorzystywania wywiadu agenturalnego do zdobywania kodów kryptograficznych[16]. Zadania polegające na zdobywaniu informacji o szyfrach, kodach czy urządzeniach szyfrujących realizował 16. Wydział 1. Zarządu Głównego. Funkcjonariusze tego pionu współdziałali z pozostałymi jednostkami wywiadu i kontrwywiadu radioelektronicznego KGB i zlecali pionom politycznym rezydentur operacje werbunkowe wobec szyfrantów obcych państw[17].

Główną barierą rozwoju radzieckiego wywiadu sygnałowego było zacofanie technologiczne w stosunku do służb zachodnich – według CIA w 1985 roku radzieckie komputery były wolniejsze o kilkadziesiąt razy od amerykańskich czy japońskich, które przewyższały je technologicznie o 10-15 lat. Zwraca się również uwagę na fakt, że Rosjanie stosunkowo późno zaczęli rozwijać swoje struktury do walki elektronicznej. Pierwszy lot z zamiarem przeprowadzenia wywiadu elektronicznego został przeprowadzony w 1953 roku, podczas gdy służby amerykańskie i angielskie przeprowadzały je już podczas drugiej wojny światowej. Do kolejnych mankamentów zalicza się ich silne upolitycznienie utrudniające przeprowadzenie obiektywnej analizy oraz przerośniętą biurokrację[18].

## SIGINT w strukturze współczesnych służb specjalnych Federacji Rosyjskich

Po likwidacji KGB w 1991, na jej bazie powstało kilka niezależnych instytucji, w tym odrębne służby dedykowane do: wywiadu strategicznego (SWR – Służba Wywiadu Zagranicznego), kontrwywiadu (FSK – Federalna Służba Kontrwywiadu, następnie przekształcona w FSB – Federalną Służbę Bezpieczeństwa), ochrony urzędników i instytucji państwowych (FSO – Federalna Służba Ochrony)

[16] *Ibidem*, s.518.

[17] L. Pawlikowicz, *op. cit.*, s. 256; Trudno jednak zakładać, że takie operacje były prowadzone jedynie przez służby wywiadowcze ZSRR. Według relacji jednego z byłych oficerów Departamentu I Służby Bezpieczeństwa PRL, w 1980 roku z rezydentury Nowego Jorku przeszedł na stronę Amerykanów szyfrant Waldemar Mazurkiewicz – zob. P. Reszka, M. Majewski, *Zawód: szpieg. Rozmowy z Aleksandrem Makowskim,* Warszawa 2014, s. 132-133.

[18] M. M. *op.cit.*, s. 519-520.

oraz inne, w tym odrębna służba specjalna do działań z zakresu SIGINT i zabezpieczenia komunikacyjnego Federacji Rosyjskiej – Federalna Agencja ds. Komunikacji i Informacji Rządowej (FAPSI). Po jej rozwiązaniu zadania przejęły: SWR, FSB i FSO, a także GRU, które nie uległo zmianom strukturalnym po rozpadzie ZSRR.

Powstanie FAPSI w 1991 roku należy uznać jako istotne wydarzenie w historii rosyjskiego wywiadu i kontrwywiadu radioelektronicznego. Jej pierwszym szefem został Aleksandr Starowojtow, który uprzednio pełnił funkcję zastępcy szefa wyżej wspominanego 8. Zarządu Głównego KGB[19]. Posadę szefa nowopowstałej służby otrzymał zastępca, a nie dyrektor 8. Zarządu Głównego (Anatolij Grigorijewicz Beda), ponieważ ten był odpowiedzialny za przerwanie linii komunikacyjnych pomiędzy Michaiłem Gorbaczowem jego daczy w Foros podczas puczu Janajewa w 1991 roku[20]. Starowojtow był specjalistą z zakresu kryptografii, systemów komunikacyjnych i wieloletnim współpracownikiem naukowo-technicznym produkującym specjalne systemy łączności dla radzieckich służb specjalnych. Do KGB wstąpił w 1984 roku. Pełnił również szereg innych funkcji o charakterze urzędniczym i akademickim – był m. in szefem Międzywydziałowej Komisji ds. Bezpieczeństwa Informacji Rady Bezpieczeństwa Federacji Rosyjskiej oraz pełnił funkcje w ciałach odpowiedzialnych za systemy kryptograficzne w Rosji i pozostałych członkach Wspólnoty Niepodległych Państw oraz był rektorem Rosyjskiej Akademii Kryptografii. Swój urząd na stanowisku szefa FAPSI sprawował do 1998 roku i był wówczas najdłużej urzędującym szefem tego typu służby na świecie[21]. Jego następcą został Petrowicz Szerstjuk, który poprzednio pełnił w tej służbie funkcję dyrektora jednostki organizacyjnej odpowiedzialnej za wywiad radioelektroniczny. W późniejszym czasie sprawował – podobnie jak poprzedni szef FAPSI - również funkcje Międzywydziałowej Komisji ds. Bezpieczeństwa Informacji Rady Bezpieczeństwa Federacji Rosyjskiej (od 24 grudnia 1998 roku) i członka Rady Bezpieczeństwa FR (od 1999 roku). Na stanowisku szefa FAPSI utrzymał się jedynie rok – w 1999 roku został zastąpiony przez Grigorijewicza Matjukchina, byłego funkcjonariusza 8. Głównego Zarządu KGB i dyrektora centrum naukowo-badawczego Głównego Zarządu Bezpieczeństwa i Komunikacji FAPSI[22].

[19] A. Knight, *Spies without Cloaks: The KGB's Succesors,* Princeton 2001, s. 36.
[20] G. Bennet, *The Federal Agency of Government Communications & Information,* „Conflict Studies Research Centre" 2000, nr 105, s. 3.
[21] *Ibidem*.
[22] *Ibdem*, s. 4.

Warto zwrócić uwagę, że cywilny wywiad i kontrwywiad radioelektroniczny były drugimi (po grupie jednostek specjalnych KGB „ALFA") rozwiązanymi i restrukturyzowanymi jednostkami organizacyjnymi KGB, co wynikało z ich bezpośredniego wpływu na bezpieczeństwo wówczas urzędującego Michaiła Gorbaczowa (szczególnie po nieudanym puczu)[23]. W rezultacie, na krótko przed powstaniem FAPSI została powołana w sierpniu 1991 roku nowa struktura o nazwie Komitetu Komunikacji Rządowej (KPS), która powstała na bazie trzech jednostek organizacyjnych KGB – wcześniej wspominanych 8. Zarządu Głównego i 16. Zarządu, a także Wydziału 12., który był odpowiedzialny za działalność podsłuchową wobec rządu i członków partii. Struktura ta miała charakter przejściowy i 24 grudnia 1991 roku została przekształcona w FAPSI. Wówczas w skład tej instytucji wchodziły[24]:

- jednostki organizacyjne KPS, a więc:
    - Zarząd Główny ds. Łączności Rządowej,
    - Zarząd Główny ds. Bezpieczeństwa Komunikacji (w tym centrum-naukowo techniczne),
    - Zarząd Główny ds. Wywiadu Radioelektronicznego,
    - Zarząd Informacyjno-Analityczny,
    - Zarząd ds. Łączności Rządowej Rosyjskiej Socjalistycznej Republiki Radziecki (odrębna jednostka organizacyjna utworzona po konsultacjach z Borysem Jelcynem),
    - Zarząd Kadr,
    - Zarząd Administracyjny,
    - Zarząd Obiektów Wojskowych,
    - Zarząd Finansów i Planowania,
    - Sekretariat,
    - Wydział Gospodarczy,
    - Wydział Organizacyjny i Mobilizacyjny,
    - Wydział Prawny,
    - Służba Wewnętrzna,
    - Rada Naukowo-Techniczna,
    - Archiwum,
    - Centrum Prasowe,

[23] *Ibidem*, s. 4.
[24] *Ibidem*, s. 5

    - Akademia Kryptograficzna,
    - Rządowe Wojska Komunikacyjne.
- Państwowa Komputerowa Baza Danych,
- Moskiewski Instytut Elektroniki Przedsiębiorstwa Naukowo-Produkcyjnego „Awtomatika".

W późniejszym okresie organizacja FAPSI była zbliżona do tej, którą odziedziczono po KPS. Składały się na nią m. in. struktury odpowiedzialne za linie łączności prezydenta FR oraz łączność służb specjalnych oraz prowadzenie wywiadu sygnałowego. W ramach struktury wyróżniono również centra naukowo-techniczne, które wspierały naukowo i produkcyjnie służbę (np. w zakresie kryptografii, produkcji sprzętu, zarządzania dokumentami, informacjami i archiwami), a także placówki naukowo-dydaktyczne kształcące kadry funkcjonariuszy oraz specjalistów w tej dziedzinie[25].

Jak widać zakres zadań FAPSI był szeroki, a do jego najważniejszych kierunków można zaliczyć[26]:

- Zabezpieczenie państwowych linii komunikacyjnych, w tym innych służb specjalnych.
- Przechwytywanie oraz deszyfracja otwartej i kodowanej obcej łączności;
- Modernizacja istniejących rozwiązań technicznych wykorzystywanych w komunikacji.
- Utrzymywanie bliskich kontaktów z państwami-byłymi republikami radzieckimi (głównie była to ochrona infrastuktury wywiadowczej, np. w Estonii baza SIGINT w Juri działała do 1993 roku).
- Kontrola i obsługa komercyjnych sieci komunikacyjnych, urządzeń kryptograficznych i oprogramowania komputerowego.
- Zadania analityczne ze źródeł otwartych dla urzędu prezydenta FR – w latach 90. m. in. zagadnienia związane z eksportem metali szlachetnych oraz surowców energetycznych.

FAPSI decyzją prezydenta Władimira Putina została rozwiązana w 2003 roku. Jako przyczyny tego posunięcia podaje się szereg czynników, a między innymi: wy-

[25] *FAPSI Organization,* źródło: http://fas.org (dostęp: 11.08.2016).
[26] G. Bennet, *The Federal Agency* …, s. 8.

żej wspomniany zbyt szeroki zakres zadaniowy oraz postępującą fluktuację kadrową, infrastukturalną, a także budżetową do FSB i jednostek Ministerstwa Obrony Narodowej FR.

Po rozwiązaniu FAPSI jej zadania przejęły głównie FSB, FSO, SWR, a także jednostki Ministerstwa Obrony Narodowej FR. W przypadku FSB należy wymienić 16. Zarząd (FSB TSRRSS), który jest odpowiedzialny za przechwytywanie, łamanie oraz przetwarzanie komunikacji elektronicznej oraz 18. Zarząd (FSB ISC) zajmujący się m.in. monitoringiem sieci oraz operacjami kontrwywiadowczymi w tym środowisku. Obie struktury funkcjonują również jako jednostki wojskowe: - Vch 71330 w przypadku FSB TSRRS oraz Vch 64829 w przypadku FSB ISC[27]. W FSB znajdują się również jednostki organizacyjne odpowiedzialne za udzielanie licencji i certyfikatów podmiotom wchodzącym na obszary rynku objęte bezpieczeństwem informacyjnym, a także kwestiami związanymi z importem oraz eksportem technologii kryptograficznych oraz urządzeń służących do obserwacji. Wspomnieć również należy o 8. Zarządzie FSB (Centrum Bezpieczeństwa Komunikacyjnego – CBS FSB), który prowadzi działalność kontrolną w zakresie spełniania standardów bezpieczeństwa przez urządzenia używane do łączności w rządowych sieciach komunikacyjnych[28]. FSB jest również odpowiedzialne za program SORM I i II, które uważa się za odpowiedniki amerykańskiego programu PRISM i również są one ukierunkowane na masową inwigilację sieci internetowej i telefonicznej[29].

FSO jest natomiast służbą odpowiedzialna za ochronę rosyjskich urzędników państwowych i infrastrukturę państwową. Liczy ona ok. 20 tys. funkcjonariuszy, i przejęła po FAPSI część zadań odpowiedzialnych za zabezpieczenie rządowych sieci informatycznych i komunikacyjnych, a także monitoruje podsłuchy telefoniczne, również prowadzi inwigilację Internetu, łączności bezprzewodowej oraz ma dostęp do zasobów satelitarnych[30].

Możliwości prowadzenia strategicznego wywiadu sygnałowego ma SWR. Posiada ona dostęp do zarządzania wojskowymi i komercyjnymi systemami satelitarnymi oraz monitorowania urządzeń komunikacji bezprzewodowej. Wspólnie

[27] *Russia Federal Security Service (FSB) Internet Operations Against Ukraine*, źródło: https://www.ecirtam.net (dostęp: 07.08.2016).
[28] J. Carr, *Inside Cyber Warfar: Mapping the Cyber Underworld*, Sebastopol 2011, s. 230.
[29] P. Paganini, *The Russian Prime Minister Dmitry Medvedev has signed a decree that will extend the use of SORM-2 to social network surveillance*, źródło: http://securityaffairs.co (dostep: 07.08.2016).
[30] R. Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations,* FOI, Sztokholm 2010, s. 28.

z GRU (poprzednio także z FAPSI) obsługuje również stacje radioelektroniczne w Louders na Kubie oraz Rahm Bay w Wietnamie i prawdopodobnie również na wyspie Socotra należącej do Jemenu i położonej na terytorium Oceanu Indyjskiego w bliskiej odległości Zatoki Adeńskiej[31]. Zdaniem emerytowanego generała i przewodniczącego komitetu obrony rosyjskiej Dumy, Andrieja Nikolayewa, baza na Kubie pomogła Rosjanom w zdobyciu niemal 40 % wszystkich informacji o Stanach Zjednoczonych i regonie[32]. Warto zaznaczyć, że baza od 2001 roku pozostawała nieczynna, jednak według doniesień medialnych jej działalność miała zostać wznowiona w 2016 roku[33].

Istotnym elementem rosyjskiego wywiadu komunikacyjnego i elektronicznego pozostaje GRU, które posiada w tym zakresie również dostęp do zasobów satelitarnych, a także samolotów i okrętów rozpoznania i walki elektronicznej[34]. Z dostępnych materiałów trudno szczegółowo poznać strukturę tej służby. W połowie lat 80 były oficer, który przeszedł na stronę amerykańską, Wiktor Suworow (wł. Władimir Rezun) podawał, że za wywiad radioelektroniczny i sygnałowy był odpowiedzialny 6. Zarząd, przy czym oraz przekonywał, że dysponuje również Zarządem Wywiadu Kosmicznego. W kontekście wojskowego wywiadu sygnałowego i jednostek walki elektronicznej należy również wspomnieć o wywiadzie Marynarki Wojennej FR[35]. Należy przy tym zaznaczyć, że wojska walki elektronicznej (Voyska radioelektronnoy bor'by) stanowią dedykowany element rosyjskich Sił Zbrojnych do tego rodzaju działalności, a o ich funkcjonowaniu pisze się często w kontekście konfliktu w Gruzji w 2008 roku. Obecnie działanie w tym wymiarze może być rozpatrywane zarówno na szczeblu taktycznym, jak i strategicznym[36]. Jednostki walki elektronicznej stanowią istotne dopełnienie rosyjskiej koncepcji walki informacyjnej, która opiera się na założeniu podejmowania przedsięwzięć o charakterze holistycznym – od nacisku politycznego, manipulacji

[31] *Ibidem*, s. 31.
[32] A. Szczerbakow, *Aleksey Shcherbakov's view of the Security & Intelligence scene from Moscow*, źródło: http://fas.org (dostęp: 11.08.2016).
[33] J. Raubo, *Rosja reaktywuje dawną stację SIGINT na Kubie?*, źródło: http://www.cyberdefence24.pl (dostęp: 11.08.2016).
[34] *Intelligence threat handbook,* źródło: http://fas.org (dostep: 11.08.2016).
[35] *GRU,* źróło: http://fas.org (dostęp: 11.08.2016).
[36] K. Giles, *„Information Troops" a Russian Cyber Command*, [w:] *3rd International Conference on Cyber Conflict*, red. C. Czosseck, E. Tyuegu, T. Wingfield, Tallin 2011, s. 51-52.

społeczeństwa, aktywności hakerów, po działania jednostek sił specjalnych oraz elementy walki elektronicznej (np. zagłuszanie sygnału telekomunikacyjnego, urządzeń wojskowych itd.)[37].

## Bibliografia

Aid M. M., *Esdroppers of the Kremlin: KGB during the cold war*, [w:] *The History Information Security: A Comperehensive Handbook,* red. K. de Leeuw, J. Bergstra, Amsterdam 2007.

Andrew Ch., Gordijewski O., *KGB*, Warszawa 1999.

Bennet G., *The Federal Agency of Government Communications & Information,* „Conflict Studies Research Centre" 2000, nr 105.

Carr J., *Inside Cyber Warfar: Mapping the Cyber Underworld*, Sebastopol 2011.

*FAPSI Organization,* źródło: http://fas.org (dostęp: 11.08.2016).

Franke U., *War by non-military means. Understanding Russian information warfare,* Sztokholm 2015.

*Functions and Internal Organization,* źródło: http://www.globalsecurity.org (dostęp: 04. 08.2016).

Giles K., *„Information Troops" a Russian Cyber Command*, [w:] *3rd International Conference on Cyber Conflict*, red. C. Czosseck, E. Tyuegu, T. Wingfield, Tallin 2011.

*Global National Security and Intelligence Agencies Handbook. Vol 1 strategic information and contact,* Waszyngton 2015.

*GRU,* źródło: http://fas.org (dostęp: 11.08.2016).

Heickero R., *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations,* FOI, Sztokholm 2010, s. 28.

[37] U. Franke, *War by non-military means. Understanding Russian information warfare,* Sztokholm 2015, s. 32.

*Intelligence threat handbook,* źródło: http://fas.org (dostep: 11.08.2016).

Knight A., *Spies without Cloaks: The KGB's Succesors,* Princeton 2001.

Larecki J., *Wielki leksykon służb specjalnych świata. Orga-nizacje wywiadu, kontr-wywiadu i policji politycznych świata, terminologia profesjonalna i żargon opera-cyjny,* Warszawa 2007.

Mikinia M., *Sztuka wywiadu we współczesnym państwie*, Warszawa 2014.

Nogaj A., *Techniczne źródła pozyskiwania informacji wywiadowczych,* „Zeszyty Naukowe WSOWL" 2011, nr 4 (162).

Paganini P., *The Russian Prime Minister Dmitry Medvedev has signed a decree that will extend the use of SORM-2 to social network surveillance*, źródło: http://security affairs.co (dostep: 07.08.2016).

Pawlikowicz L., *Aparat centralny 1. Zarządu Głównego KGB jako instrument reali-zacji globalnej strategii Kremla 1954-1991*, Warszawa 2013.

Raubo J., *Rosja reaktywuje dawną stację SIGINT na Kubie?*, źródło: http://www. cyberdefence24.pl (dostęp: 11.08.2016).

Reszka P., Majewski M., *Zawód: szpieg. Rozmowy z Aleksandrem Makowskim,* Warszawa 2014.

*Russia Federal Security Service (FSB) Internet Operations Against Ukraine,* źródło: https://www.ecirtam.net (dostęp: 07.08.2016).

*Signals Intelligence Programs and Activities*, źródło: http://www.globalsecurity.org (dostęp: 11.08.2016).

*Słownik terminów i definicji NATO. Zawierający wojskowe terminy i ich definicje stosowane w NATO,* źródło: wcnjk.wp.mil.pl (dostęp: 11.08.2016).

Smith W. T., *Encyclopedia of Central Intelligence Agency,* Nowy Jork 2003.

Szczerbakow A., *Aleksey Shcherbakov's view of the Security & Intelligence scene from Moscow*, źródło: http://fas.org (dostęp: 11.08.2016).

Zsolt H., *Converegence between signals intelligence and electronic warfare suport measures,* „Technical Scienses" 2014, nr 3 (75).

Tetiana W. Nagachevskaya
Lyudmila Frliksowa

Kijowski Uniwersytet Narodowy im. Tarasa Szewczenki

# Напрямки формування міжнародної конкурентоспроможності ІТ-сектору України

Słowa kluczowe: sektor IT, konkurencyjność, Networked Readiness Index, Ukraina

*Актуальність та постановка проблеми.* В умовах глобалізації та посилення інтеграційних процесів актуальним є здійснення пошуку нових напрямків підвищення конкурентоспроможності окремих галузей та секторів економіки України. Адже при посиленні конкуренції на світових ринках успіх одного чи декількох підприємств не може забезпечити зростання конкурентоспроможності галузі в цілому. Одним із найперспективніших для України є ІТ-сектор. Так, за оцінками Міністерства економічного розвитку та торгівлі України, частка ІТ-сектору у ВВП країни в 2015 р. перевищила 3%. Галузь вийшла на третє місце за обсягом експорту показавши в 2015 році 10% зростання на фоні падаючої економіки країни. ІТ-сектор стає двигуном зростання економіки України. Проте, загострення конкуренції актуалізує питання пошуку шляхів та інструментів зростання конку-рентоспроможності вітчизняного ІТ-сектору на міжнародних ринках.

Теоретичні та практичні аспекти проблематики стратегічного управління міжнародною конкурентоспроможністю присвячені праці українських та зарубіжних вчених. Проблематиці міжнародної конкурентоспроможності на галузевому рівні присвячені праці таких зарубіжних вчених як М. Портер, Р. Каулі, Д. Хосперз,Р. Манселл, П. Готшальк, О. Шай, Д. Тапскотт та інших. Теоретикомето

дологічні засади аналізу міжнародної конкурентоспроможності галузі, методи її оцінки та впливу на конкурентоспроможність національних економік розкриті в працях вітчизняних науковців: Беззубченко О.А., Геєць В.М., Бажал Ю.В., Каніщенко О.Л., Ковалець Б.М., Пащук Л.В., Побережець Н.Б., Старостіна А.О., Шевченко М.М. та ін. В пра-цях вітчизняних вчених розкрито стан, особливості та тенденції розвитку ІТ-ринку України. Разом з тим, недостатньо дослідженими аспектами проблеми є визначення сильних та слабких сторін конкурентоспроможності ІТ-сектору України на міжнародних ринках, виявлення моделей його розвитку на сучасному етапі, та обґрунтування на цій основі напрямів зростання конкурентних позицій вітчизняних ІТ-компаній на міжнародних ринках, що визначає мету та завдання даного дослідження.

Розглянемо ключові показники розвитку вітчизняного ІТ-сектору. Вартісний обсяг ІТ-сектору України оцінюється експертами в більш ніж 5 млрд. дол[1]. Структура ІТ-ринку України характеризується низькою сукупною часткою програмного забезпечення (ПЗ) і послуг, а саме: 15-16% і 10%, що в 4 рази менше аніж в розвинутих країнах. Так, в 2014 р.

в Україні 75% ринку ІТ припадало на АЗ (апаратне забезпечення), 13,4% - на ПЗ, 11,6% - на ІТ-послуги, в той час як в Німеччині: 38% - на устаткування, 23% - на ПО, 39% - на ІТ-послуги[2]. В Україні в 2015 р. діяло близько 8500 ІТ-компаній, серед яких більше 500 – аутсорсингові, близько 100 глобальних R&D центрів, 127 компаній в галузі електронної торгівлі, запущено близько 2000 ІТ-стартапів. Наразі в Україні функціонує 7 ІТ-кластерів, найпотужнішим з яких є Львівський (більше 6500 ІТ-спеціалістів, 35 ІТ-компаній. 2 універ-ситети), Київський (65 ІТ-компаній малого та середнього розмірів, більше 900 розробників), Харківський (20 ІТ-компаній, 5 місцевих університетів), а також Одеський, Дніпро-петровський, Букови-нський, Луцький, Черкаський, Сумський ІТ-кластер (створюється)[3].

[1] *Zwit pro Robotunacionalnoji komisiji, szczo zdijsniuje derżawne rehuluwannia usferizwjazku ta informatyza*, Kyjiw 2015, s. 35.

[2] *CompTIA's IT Industry Outlook 2015,* źródło: https://www.comptia.org (dostęp: 15.03.2016).

[3] *Zwit pro Robotunacionalnoji komisiji…*, s.42.

Відповідно до даних Всесвітнього економічного форуму в 2014 р. Україна зайняла 81 позицію серед 148 країн за Індексом мережевої готовності (Network Readiness Index), що вимірює схильність країн використовувати можливості, які породжуються інформаційними та комунікаційними технологіями (ІКТ). В 2015 р. Україна піднялася на 10 позицій, зайнявши 71 місце[4]. Покращення зумовлено зростанням частки ІТ-сектору в ВВП України та експорті, посиленням конкурентних переваг на світовому ринку ІТ-аутсорсингу, впровадженням стратегії дерегуляції, спрощенням процедури співпраці українських фрілансерів з іноземними замовниками, зростанням державного замовлення на випускників ІТ-факу, підтримкою ІТ-розробників, які беруть участь в державних тендерах інших країн завдяки приєднанню України до угоди GPA.

Найвищі позиції за ІМГ Україна займає за субіндексом готовності (Табл.1). Даний субіндекс включає в себе складову ІТ-інфраструктури (високі показники по обсягу покриття мобільним зв'язком та якості Інтернет-зв'язку), ІТ-спроможності (високий показник за тарифами на широкосмуговий Інтернет) та складову людського капіталу (високі показники грамотності дорослого населення та якості матема-тичної освіти).

Таблиця 1. Міжнародна конкурентоспроможність ІТ-сектору України за Індексом мережевої готовності (ІМГ) в 2015р.

| Субіндекс ІМК | Складові субіндексу | Місце в рейтингу | Значення (max.6) |
|---|---|---|---|
| **Субіндекс середовища** | | **104** | **3,6** |
| | Політичне та регулятивне | 122 | 3 |
| | Бізнес та інновації | 77 | 4,2 |
| **Субіндекс готовності ІТ** | | **28** | **5,6** |
| | ІТ-інфраструктура | 46 | 4,7 |

[4] *The World Economic Forum The Global Information Technology Report 2015*, źródło: http://www3.weforum.org (dostęp: 15.03.2016).

| Субіндекс ІМК | Складові субіндексу | Місце в рейтингу | Значення (max.6) |
|---|---|---|---|
| | ІТ-спроможність | 10 | 6,6 |
| | Наявність людського капіталу | 36 | 5,6 |
| **Субіндекс використання ІТ** | | **94** | **3,4** |
| | Попит з боку д/г на ІТ | 78 | 3,7 |
| | Попит з боку бізнесу на ІТ | 78 | 3,5 |
| | Попит з боку держави на ІТ | 124 | 2,9 |
| **Субіндекс впливу ІТ** | | **82** | **3,5** |
| | Економічний вплив ІТ | 67 | 3,3 |
| | Соціальний вплив ІТ | 89 | 3,7 |

*Джерело:* складено авторами за даними: *The World Economic Forum The Global Information Technology Report 2015*…

Найнижчі позиції в рейтингу Україна має за субіндексом середовища: за складовою політичного та регулятивного середовища найнижчі показники український ІТ-сектор займає за рівнем незалежності судової влади та ефективністю роботи правотворчих органів, а за складовою «бізнес та інновації» – за наявністю передових технологій в урядових службах закупівель,а також їх використанню в бізнесі. Тим не менш, вищі бали в рейтингу за субіндексом середовища в 2015 р. Україна отримала за станом

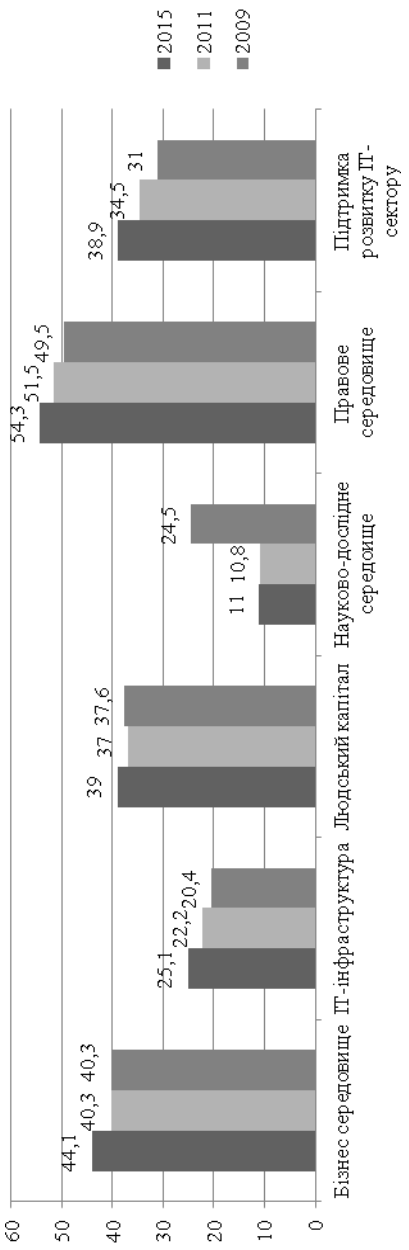



Рис. 1. Динаміка складових індексу міжнародної конкурентосп-роможності ІТ-сектору України, 2009-2015 рр.

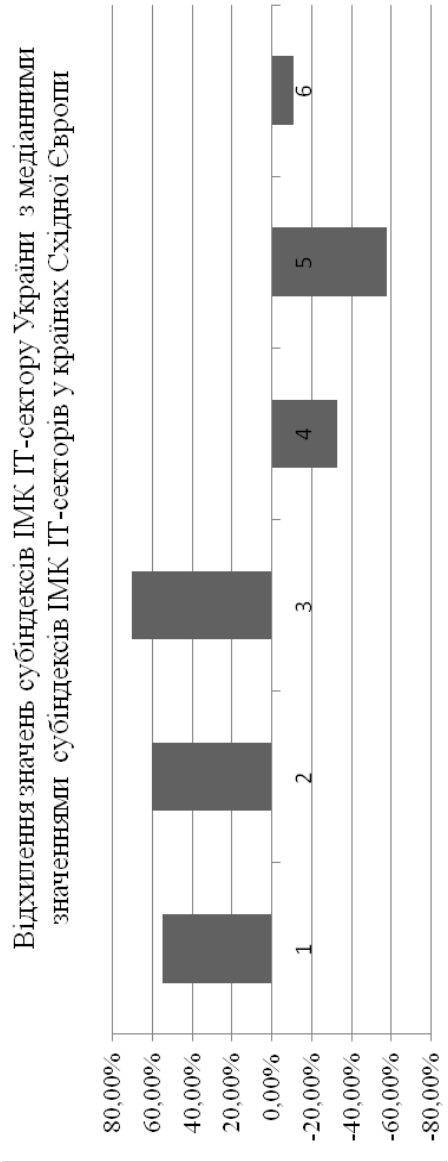
*Джерело:* складено авторами за даними: *Global Information Technology Report 2014*, źródło: http://www3.weforum.org (dostęp: 15.03.2016); *The World Economic Forum The Global Information Technology Report 2015…*, *World Economic Forum, The Global Information Technology Report, 2011-2012 …*

правового середовища, наявним людським капіталом та станом бізнес-середовища[5].

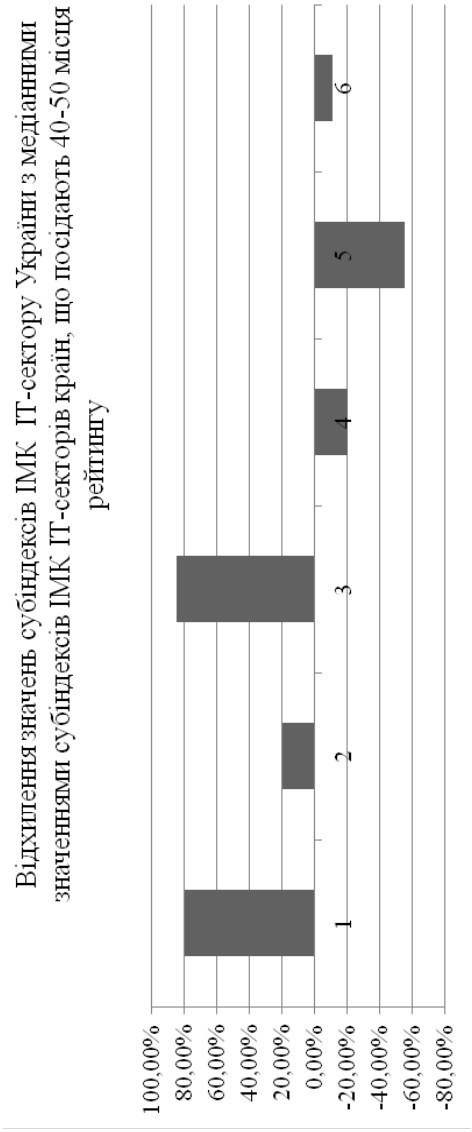
За останні 6 років спостерігається тенденція до покращення науково-дослідного середовища, погіршення правового середовища, погіршення стану ІТ-інфраструктури, зменшення підтримки розвитку ІТ-сектору (рис. 1), що ставить відповідні завдання перед державними органами України.

Порівняємо відхилення показників конкурентоспроможності ІТ-сектору України від медіанних значень у країнах Східної та Західної Європи, а також тих, що посідають 40-50 місця (див. рис. 2). Серед країн Східної Європи (11 країн) Україна найбільше відстає у частині забезпечення правового середовища та рівня зацікав-леності держави та бізнесу в продукції ІТ-сектору. Положення ІТ-сектору України у групі країн, що посідають 40-50 місця рейтингу визначається, з одного боку, високим значенням показника стану середовища досліджень і розробок, що оцінювалося на основі визначення: кількості вітчизняних патентів; надходжень від роялті і ліцензій; валових державних та приватних витрат на дослідження й розробки, а також показником наявності людського капіталу. З іншого боку, негативний вплив переважно здійснювали відносно низькі оцінки правового та економічного середовища галузі. Основними конкурентами України в Східній Європі є Польща, Росія та Білорусь. Високий рівень міжнародної конкурентоспроможності ІТ-сектору Польщі обумовлений наявністю високої якості послуг, низькими витратами на оплату праці, доступом до дешевого капіталу. Основними міжнародними конкурентними перевагами ІТ-сектору Росії є значний обсяг внутрішнього попиту на ІТ-продукти, конкурентоспроможна система інженерно-технічної освіти. Проте недостатній досвід реалізації масштабних ІТ-проектів, нестабільний бізнес-клімат, санкції, недовіра зарубіжних партнерів ставлять під загрозу конкурентні можливості ІТ-сектору Росії в майбутньому,

[5] *CompTIA's IT Industry Outlook 2015*, źródło: https://www.comptia.org (dostęp: 15.03.2016); *World Economic Forum, The Global Information Technology Report, 2011-2012*, źródło: http://www3.weforum.org (dostęp: 15.03.2016).


Відхилення значень субіндексів ІМК ІТ-сектору України з медіанними значеннями субіндексів ІМК ІТ-секторів у країнах Східної Європи
80,00%
60,00%
40,00%
20,00%
0,00%
-20,00%
-40,00%
-60,00%
-80,00%
1
2
3
4
5
6

Відхилення значень субіндексів ІМК ІТ-сектору України з медіанними значеннями субіндексів ІМК ІТ-секторів країн, що посідають 40-50 місця рейтингу



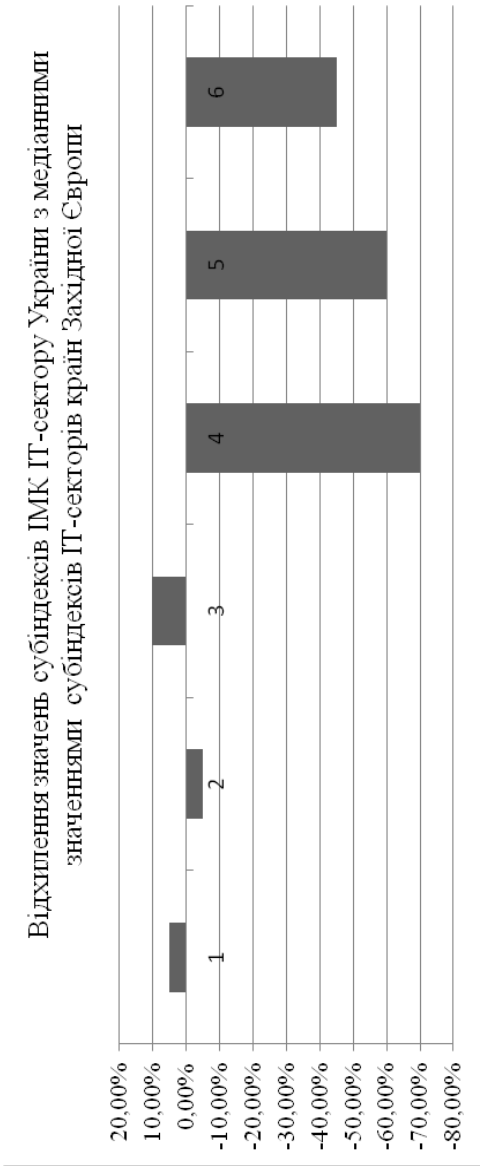



Рис. 2. Порівняння відхилень значень субіндексів ІМК ІТ-сектору України з медіанними значеннями груп країн, 2015 р.

1 - середовище наукових досліджень і розробок, 2 – інфраструктура ІТ-сектору, 3 – людський капітал, 4 - державне, бізнес та індивідуальне використання продукції ІТ-сектору, 5 – правове середовище, 6 – економічне середовище ІТ-сектору.

*Джерело:* складено авторами за даними: *CompTIA's IT Industry Outlook 2015*…; *The World Economic Forum The Global Information Technology Report 2015*…

що дає шанс Україні та іншим конкурентам відвоювати частину замовлень на ІТ-послуги та відповідно частку ринку[6].

Проведемо аналіз міжнародної конкурентоспроможності ІТ-сектору України за моделлю Портера (за параметрами наявних факторів та попиту). В результаті даного аналізу виявлено, що за фактором праця та капітал міжнародними конкурентними перевагами ІТ-сектору України є наступні: наявний трудовий потенціал; високий рівень володіння англійською мовою більшої частини вітчизняних ІТ-спеціалістів; наявність значної кількості фрілансерів в ІТ-секторі (близько 100 тис. чол.), які користуються значним попитом на світовому ІТ-ринку; дешева оренда офісних приміщень усіх класів (у порівнянні з США, Англією, Росією, Францією, Швейцарією, Норвегією, Німеччиною та ін..); один з найдешевших в світі швидкісний доступ до мережі Інтернет (див. табл.2).

За фактором умов попиту міжнародними конкурентними перевагами ІТ-сектору України є наступні: спеціалізація українських ІТ-компаній на наданні широкого спектру ІТ-послуг; однин із найнижчих в світі рівень собівартості ІТ- послуг; низька вартість праці ІТ-спеціаліста (на 25% менша ніж в Росії; на 40% - ніж в Східній Європі; на 400 % - ніж в Західній Європі та США); наявність досвіду спільного виконання окремих частин великого замовлення, які отримують компанії Ізраїлю або Росії; висока якість ІТ-послуг.

Разом з тим виявивлено наступні міжнародні конкурентні недоліки ІТ-сектору України: відсутність внутрішнього виробництва експортноорієнтованого АЗ (hardware); повна асиметрія в бік переважання надання ІТ-послуг над виробництвом ІТ-товарів; низький рівень внут-рішнього попиту на вітчизняні ІТ-товари; неспроможність вітчизняних виробників конкурувати на внутрішньому ринку АЗ з глобальними виробниками; розвинуте піратство як фактор стримування розвитку розробки ПЗ; поступове зростання дефіциту ІТ-кадрів через зростання кількості фахівців, що виїжджають за кордон.

[6] M. Jarowaja, *Kryzys w Ukrayne otkatył ukraynskyj rynok IT na piat' łet nazad — yssledowanye IDC*, źródło: https://ain.ua (dostęp: 15.03.2016); W. Nekrasow, *Hod proszeł ne zria. 10 samych hławnych prorywow w ukraynskom IT-sektore*, źródło: http://www.epravda.com.ua (dostęp: 15.03.2016).

Україна експортує ІТ-послуги за різними напрямками, не виробляючи експортноорієнтованого АЗ, як це роблять розвинуті країни світу. Тому наразі експортноорієнтованою продукцією ІТ-сектору України, яка користується попитом на світовому ринку та визнається експертами як конкурентоздатна (див. рис. 3) є ІТ-послуги, які надаються замовникам за офшорними чи аутсорс-инговими схемами. Починає визнаватися як конкуренто-здатна на міжнародному ринку продукція ПЗ.

Таблиця 2. Міжнародні конкурентні переваги та недоліки ІТ-сектору України за параметрами наявних факторів та попиту

**Конкурентні переваги** ІТ-сектору України за **параметрами факторів (праця та капітал):**

- Наявний трудовий потенціал: 4 місце в світі за кількістю сертифікованих ІТ-спеціалістів (після США, Індії та Росії).
- 75% ІТ-спеціалістів мають спеціалізовану вищу освіту, 6% - докторський ступінь.
- Високий рівень володіння англійською мовою: 40,2% - вільне володіння; 38,6% - середній рівень; 21,2% - елементарний.
- Наявність значної кількості фрілансерів в ІТ-секторі (близько 100 тис.чол), які користуються значним попитом на світовому ІТ-ринку.
- Щорічне поповнення кількості ІТ-спеціалістів випускниками ВУЗів (на 16 тис.).
- Дешева оренда офісних приміщень усіх класів (у порівнянні з США, Англією, Росією, Францією, Швейцарією, Норвегією, Німеччиною).
- Максимальний в Європі показник використання «хмар» - 86% (найвищий ступінь заміни серверів зберіганням баз даних в «хмарах»).
- Дешевий швидкісний доступ до мережі Інтернет (один з найдешевших в світі).

**Конкурентні недоліки** ІТ-сектору України за **параметрами факторів:**

- Поступове зростання дефіциту ІТ-кадрів ( 100 тис. в 2015 р.), але не в таких масштабах, як він наявний в США та більшості країн ЄС.

**Конкурентні переваги** ІТ-сектору України за **параметрами попиту:**

- Спеціалізація українських ІТ-компаній на наданні широкого спектру ІТ-послуг (в сфері управління ІТ-інфраструктури (web-хостинг), розробці корпоративного ПЗ, додатків, а також їх техпідтримка, спеціалізовані та високоякісні ІТ-послуги, електронний бізнес та мережеве управління).
- Одна з найнижчих в світі собівартість ІТ- послуг (низька вартість праці, низька орендна плата за приміщення та підключення до мережі Інтернет).
- Низька вартість праці ІТ-спеціаліста (середньомісячна заробітна плата ІТ-спеціаліста в Україні на 25% менша, аніж в Росії; на 40% - аніж в Східній Європі; в 4-5 разів менша ніж в Західній Європі та США).
- Зростання замовлень з боку країн ЄС (Ірландія, Великобританія, Німеччина, Австрія та Нідерланди) та США.
- Наявність досвіду спільного виконання окремих частин великого замовлення, які отримують компанії з Ізраїлю або Росії.

**Конкурентні недоліки** ІТ-сектору України **за параметрами попиту:**

- Відсутність внутрішнього виробництва експортноорієнтованого апаратного забезпечення (hardware), повна асиметрія в бік переважання надання ІТ-послуг над виробництвом ІТ-товарів.
- Відсутність внутрішнього попиту на вітчизняні ІТ- товари (ПК, планшети, ноутбуки і т.д).

- Неспроможність вітчизняних виробників конкурувати на внутрішньому ринку апаратного забезпечення з глобальними виробниками.
- Розвинуте піратство як фактор стримування розвитку розробки ПЗ.

*Джерело:* складено авторами на основі: *CompTIA's IT Industry Outlook 2015*…; *Global Information Technology Report 2014*…; *The World Economic Forum The Global Information Technology Report 2015*…, W. Nekrasow, *Hod proszeł ne zria*…; zob. M. Poter, *Konkurencija*, Williams Publishing House, 2006.

Рис. 3. Експертна оцінка наявності міжнародних конкурентних переваг українських ІТ-компаній, 2015 р.
*Джерело:* складено авторами.


Значна частина ІТ-послуг українських компаній надається клієнтам з США. Частка ЄС у загальному експорті ІТ-послуг України займає тільки 35%[7]. Проте, протягом останніх 2-3 років європейські замовники стали активнішими, що в першу чергу пояснюється географічною і культурною близькістю України. Лідерами серед

[7] *Oficijnyj sajt Derżawnoji służby statystyky Ukrajiny*, źródło: http://www.ukrstat.gov.ua (dostęp: 15.03.2016).

європейських замовників є Ірландія, Великобританія, Німеччина, Австрія та Нідерланди. Для великих замовлень не завжди вистачає авторитету бренду, який би визначав Україну як країну, де ІТ-спеціалісти виконують якісні та складні ІТ-замовлення для іноземних компаній. Експерти ринку вважають, що угода про асоціацію з ЄС дозволить збільшити кількість ІТ-замовлень для українських компаній.

Для підвищення міжнародної конкурентоспроможності ІТ-сектору рекомендується: вдосконалити законодавчу базу в сфері захисту прав інтелектуальної власності; покращити бізнес-клімат в галузі завдяки створенню економічних стимулів для розвитку НДДКР та інновацій (що відповідає орієнтації на вищий рівень конкурентоспроможності); розвивати інноваційну інфраструктуру, сприяти розвитку ІТ-кластерів та технопарків; збільшувати державне замовлення на ІТ-спеціалістів; здійснювати фінансування розбудови ІТ-інфраструктури; стимулювати зростання попиту на ІТ-товари та послуги зі сторони вітчизняних домогосподарств, бізнесу та держави; вдосконалити систему державної підтримки венчурного інвестування в ІТ-сектор; розгорнути кампанію просування українських ІТ-компаній на ринках державних закупівель в рамках Угоди про Державні закупівлі; залучати українську діаспору для іміджевого просування українських ІТ-компаній.

Такі заходи визначатимуть орієнтацію на вищий рівень конкурентоспроможності (high road to competitiveness) - шлях до економічного зростання та міжнародної конкурентоспроможності на основі прискореного освоєння найсучасніших світових технологій і знань в сукупності з проведенням власних НДДКР і розвитком власного інноваційного виробництва. Дана перспективна стратегія протиставляється орієнтації на нижчий рівень конкурентоспроможності (low road to competitiveness) - найбільш поширеній моделі виходу країн, що розвиваються на міжнародні ринки шляхом залучення іноземних інвестицій в обмін на надання якомога більш дешевих природних і трудових ресурсів (див. табл. 3). Орієнтуючись на наведені в таблиці фактори та здійсненій оцінці міжнародної конкурентоспроможності ІТ-сектору України можна стверджувати,

що сьогодні його розвиток відбувається саме таким шляхом і потребує переорієнтації на «high road to competitiveness».

Таблиця 3. Порівняльна характеристика моделей підвищення міжнародної конкурентоспроможності ІТ-сектору України

*Джерело:* складено авторами на основі: *Uprawlinnia miżnarodnoju konkurentospromożnistiu w umowach hłobalizaciji ekonomicznoho rozwytk*u, pod red. D. H. Łukjanenko, A. M. Porucznyk, Kyjiw 2006, s. 529.

| **Орієнтація на «Вищий рівень конкурентоспроможності»** | **Орієнтація на «Нижчий рівень конкурентоспроможності»** |
|---|---|
| Розробка новітніх ІТ-технологій | Освоєння і впровадження застарілих технологій |
| Підвищення конкурентоспроможності за рахунок створення нових ринків і властивостей ІТ-продуктів | Конкурентоспроможність за рахунок низьких витрат та їх зниження |
| Організація глобальних виробничих ланцюжків | Участь в найменш вигідних ланках транснаціональних ланцюжків (ІТ-аутсорсинг) |
| Захищеність від цінової конкуренції | Висока цінова конкуренція |
| Підвищення оплати праці веде до накопичення людського капіталу | Підвищення оплати праці веде до підриву міжнародної конкурентоспроможності |
| «Приплив мізків» і приплив капіталу | «Витік мізків» і «втеча капіталу» |
| Стійке зростання за рахунок технологічних переваг | Загроза призупинення економічного зростання |

Для підвищення міжнародної конкурентоспроможності ІТ-сектору України вітчизняним ІТ-компаніям рекомендується: розвивати спільну підприємницьку діяльність з іноземними фірмами; залучати іноземні кредити та інвестиції, в т.ч. венчурне фінансу-

вання, кошти фондів прямих інвестицій; залучати іноземних ІТ-спеціалістів на посади керівників українських ІТ-компаній; здійснювати ефективне управління інноваціями та технологіями виходячи із світових тенденцій розвитку; здійснювати ефективне управління людськими ресурсами розширюючи співпрацю з університетами; розвивати ІТ-кластери; вступати в партне-рство із іноземними компаніями в боротьбі за тендерні замовлення; впроваджувати новітні технології ведення бізнесу.

*Висновки.* Отже, вітчизняний ІТ-сектор демонструє позитивну динаміку і має значні перспективи зростання. Міжнародна конкуренто-спроможність ІТ-сектору України має ряд ключових переваг та недоліків. У формуванні державної політики сприяння розвитку ІТ-сектора слід обрати модель орієнтації на вищий рівень конкурентоспроможності (high road to competitiveness). Для підвищення міжнародної конкуренто-спроможності ІТ-сектору України рекомендується запровадити ряд заходів на рівні державних органів та на рівні ІТ-компаній. Реалізація запропонованих заходів дозволить збільшити частку вітчизняного ІТ-сектору на міжнародних ринках.

*Перспективи подальших досліджень.* Сформовані напрямки підвищення міжнародної конкурентоспроможності ІТ-сектору України, а також виявлені ключові його міжнародні конкурентні переваги та недоліки, дають підстави для подальших досліджень конкурен-тоспроможності сектору в контексті розвитку процесів інтеграції України з країнами ЄС, а також в дослідженні конкурентних переваг окремих областей ІТ-сектору.

## БІБЛІОГРАФІЯ

*Zwit pro Robotunacionalnoji komisiji, szczo zdijsniuje derżawne rehuluwannia usferizwjazku ta informatyza*, Kyjiw 2015.

*CompTIA's IT Industry Outlook 2015,* źródło: https://www.comptia.org (dostęp: 15.03.2016).

*The World Economic Forum The Global Information Technology Report 2015*, źródło: http://www3.weforum.org (dostęp: 15.03.2016).

*CompTIA's IT Industry Outlook 2015*, źródło: https://www.comptia.org (dostęp: 15.03.
2016).

*World Economic Forum, The Global Information Technology Report, 2011-2012*, źródło: http://www3.weforum.org (dostęp: 15.03.2016).

Jarowaja M, *Kryzys w Ukrayne otkatył ukraynskyj rynok IT na piat' łet nazad – yssłedo-wanye IDC*, źródło: https://ain.ua (dostęp: 15.03.2016).

Nekrasow W., *Hod proszeł ne zria. 10 samych hławnych prorywow w ukraynskom IT-sektore*, źródło: http://www.epravda.com.ua (dostęp: 15.03.2016).

*Oficijnyj sajt Derżawnoji służby statystyky Ukrajiny*, źródło: http://www.ukrstat.
gov.ua (dostęp: 15.03.2016).

**Wojciech Gajewski**

Uniwersytet Gdański

# Religijne i parareligijne grupy destrukcyjne: wyzwania w cyberprzestrzeni

Słowa kluczowe: internet, sekta, grupa destrukcyjna

Współczesny człowiek, spędzający coraz częściej większość wolnego czasu przed monitorem komputera, narażony jest na propagandę ze strony grup destrukcyjnych o podłożu religijnym czy pseudoreligijnym. Cyberprzestrzeń jest wykorzystywana przez tego typu grupy w celu promocji swoich idei i pozyskiwania wyznawców. Sprzyja temu nade wszystko popularność i atrakcyjność Internetu[1]. Tu każdy może być ekspertem od spraw religijnych i udzielać porad duchowych. Dwie trzecie Polaków (64,9%) posiada komputer w domu, a wśród najczęstszych powodów jego zakupu wymienia się korzystanie z Internetu (66,4%). Ponad dwie trzecie użytkowników (70,4%) łączy się z siecią codziennie. Szczególnie dominują osoby z grupy wiekowej 15-29 lat (ponad 80%)[2]. Wirtualna rzeczywistość przepełniona jest różnego rodzaju treściami, w tym satanistycznymi, magicznymi i okultystycznymi. Poziom zagrożenia obecnie wyraźnie wzrasta, o czym może świadczyć bogata literatura przedmiotu[3].

[1] A. Zwoliński podaje, że liczba witryn internetowych szacowana w październiku 2007 r. wynosiła około 150 mln., *idem*, *Sekty w Internecie*, Kraków 2008, s. 95.

[2] Dane za: Ł. Tomczyk, *Społeczeństwo informacyjne a działalność grup religijnych oraz sekt w Internecie*, [w:] *Sekty i nowe ruchy religijne – wolność czy zniewolenie. Zagadnienia interdyscyplinarne,* red. P. Chrzczonowicz, I. Kamiński, Toruń 2012, s. 123-124.

[3] Z bogatej literatury przedmiotu, poza przywołanymi powyżej, odwołam się do kilku: M. Szostak, *Sekty destrukcyjne. Studium metodologiczno-kryminalistyczne*, Zakamycze 2001; P. Siuda, *Religia a internet. O przenoszeniu religijnych granic do cyberprzestrzeni*, Warszawa 2010 (szczególnie rozdział czwarty: „Nowe religie a internet", s. 142-194); M. Romańczuk-Grącka, *Przeszkody kryminalizacyjne dotyczące zachowań związanych ze zjawiskiem psychomanipulacji w sektach destrukcyjnych*, [w:] *Sekty i nowe ruchy religijne – wolność czy zniewolenie. Zagadnienia interdyscyplinarne,* red.

## Sekty a grupy destrukcyjne: problem metodologiczny

Na problem zdefiniowania sekty zwraca się uwagę w wielu opracowaniach, w tym w oficjalnym raporcie Ministerstwa Spraw Wewnętrznych i Administracji (2000 r.)[4], gdzie między innymi czytamy: „W Polsce na gruncie prawa pozytywnego pojęcie sekty nie istnieje. W prawodawstwie nie stosuje się terminu „sekta". Ustawodawca polski w żadnym z obowiązujących aktów prawnych nie podał znaczenia tego terminu, nie dokonał wykładni autentycznej"[5]. Na innym miejscu stwierdza: „Zdefiniowanie pojęć i terminologii dotyczącej fenomenu tzw. sekt stwarza olbrzymie trudności. Wynika to z faktu, iż z jednej strony zagadnienie to stanowi zróżnicowaną, niejednoznaczną, skomplikowaną rzeczywistość, z drugiej natomiast brak jest ścisłej i spójnej terminologii w tym zakresie w obrębie socjologii, religioznawstwa, psychologii społecznej oraz innych dziedzin nauk"[6]. Autorzy opracowania dodają: „Bez zdefiniowania zjawiska niemożliwe jest jednak ścisłe określenie przedmiotu badań"[7]. W zgodzie z Konstytucją RP (z 1997 r.) każdemu gwarantuje się wolność religijną i światopoglądową[8]. Działalność grup religijnych nie może być jednak sprzeczna z przepisami chroniącymi porządek publiczny i bezpieczeństwo, podstawowe prawa wolności innych osób czy publiczną moralność.

Na gruncie oryginału Nowego Testamentu oraz jego tłumaczenia na łacinę (*Vulgata*) dostrzec można zbieżność terminologiczną terminów gr. *hairesis* i łac.

P. Chrzczonowicz, I. Kamiński, Toruń 2012, s. 273-289; P. Chrzczonowicz, *Sekty destrukcyjne: wybrane zagadnienia prawne, kryminologiczne i społeczne*, Toruń 2013, a także I. Kamiński, *Sekty i nowe ruchy religijne w 365 pytaniach i odpowiedziach*, Warszawa 2013. Przegląd literatury na temat sekt (w tym destrukcyjnych) zob. P.T. Nowakowski, *Polska bibliografia artykułów na temat sekt i nowych ruchów religijnych od 1990 do 2003 roku*, s. 175-248 (bibliografia przywołuje 1.420 pozycji), [w] *ABC o sektach,* red. M. Gajewski, Tychy 2004; I. Kamiński, *Polska bibliografia na temat sekt i Nowych Ruchów Religijnych od 1800 do 2005*, [w] *Słownik sekt, nowych ruchów religijnych i okultyzmu,* red. G.A. Mather, L.A. Nichols, s. 629-784 (przywołuje 6.700 pozycji).

[4] *Raport o niektórych zjawiskach związanych z działalnością sekt w Polsce*, Warszawa 2000.

[5] *Ibidem*, s. 4.

[6] *Ibidem,* s. 11.

[7] *Ibidem*.

[8] Konstytucja RP, art. 12: „Rzeczpospolita Polska zapewnia wolność tworzenia i działania związków zawodowych […] innych dobrowolnych zrzeszeń oraz fundacji. Art. 25.1-2 Kościoły i inne związki wyznaniowe są równouprawnione. Władze publiczne w Rzeczypospolitej Polskiej zachowują bezstronność w sprawach przekonań religijnych, światopoglądowych i filozoficznych, zapewniając swobodę ich wyrażania w życiu publicznym. Art. 53, 1-2 Każdemu zapewnia się wolność sumienia i religii. Wolność religii obejmuje wolność wyznawania lub przyjmowania religii według własnego wyboru oraz uzewnętrzniania indywidualnie lub z innymi, publicznie lub prywatnie, swojej religii przez uprawianie kultu, modlitwę, uczestniczenie w obrzędach, praktykowanie i nauczanie".

*secta*. Ostatecznie historia nadała obu rzeczownikom znaczenie pejoratywne, którego pierwotnie oba terminy nie posiadały. Pierwszy (*hairesis* – pol. herezja) oznaczało w grece *wybór, stronnictwo, odłam, drogę* (w znaczeniu *szkoły filozoficznej czy religijnej*). Posługiwano się nim między innymi na określenie oficjalnych stronnictw w judaizmie Drugiej Świątyni (faryzeuszy czy saduceuszy)[9], a także chrześcijan[10]. Hieronim, tłumacząc Nowy Testament na łacinę, użył słowa *secta*, pochodzące od *secare – odcinać, oddzielać*, lub raczej *sequor – iść, podążać za czymś/kimś*[11]. Oba słowa weszły na stałe do języka religijnej inwektywy stając się synonimami i tak każdy heretyk był sekciarzem, a każdy sekciarz – heretykiem. W ten sposób słowo „sekta" zmieniło swoje znaczenie i w odbiorze powszechnym nabrało cech jednoznacznie negatywnych, stając się pojęciem z obszaru patologii społecznej.

Posługiwanie się terminem „sekta" może zawierać krzywdzący sąd, płynący z ignorancji bądź lęku, niekoniecznie natomiast ze złej woli[12]. Dla pewnej części naszego społeczeństwa każdy Kościół lub inna wspólnota religijna, poza wyznaniem rzymskokatolickim, podpada pod definicję sekty, na co wskazują badania opinii publicznej[13], a czego przykłady możemy znaleźć także w publikacjach naukowych i popularnych[14].

Istnieje niebezpieczeństwo uznawania wszystkich nowych ruchów religijnych za niebezpieczne dla porządku publicznego, stosujące przemoc wobec swoich współwyznawców, zmuszające do narkomanii, prostytucji, czy samobójstw, stosujące techniki psychomanipulacji, tzw. „pranie mózgu"[15]. Takie uogólnienie jest nie

[9] Dzieje Apostolskie 5:17.

[10] Dzieje Apostolskie 24:5.

[11] Por. W. Gajewski, *Kościół wobec herezji w I wieku*, „Gdański Rocznik Ewangelicki" 2009, nr 3, s. 126-127, także nota 10.

[12] M. Szostak, *op.cit.*, s. 238; por. J. K. Frankowiak, *Mity i uproszczenia dotyczące działalności sekt, a także środowisk zajmujących się problematyką funkcjonowania tego typu grup,* [w:] *Człowiek w sieci zniewolonych dróg,* red. M. Jędrzejko, W. Bożejewicz, Pułtusk 2007, s. 53-59.

[13] Na podstawie badań OBOP można stwierdzić, że część naszego społeczeństwa uważa za sekty m.in. Kościół Ewangelicko-Augsburski (luteran), a także Żydów czy Kościół Prawosławny, por. P. Chrzczonowicz, *Sekty destrukcyjne*, s. 183.

[14] Por. P. Siuda, *Religia a internet,* (na s. 146 autor dzieli nowe ruchy religijne na sekty i kulty; na s. 148 przedstawia jeden z oficjalnie istniejących Kościołów w RP, posiadających regulację prawną na mocy ustawy Państwo – Kościół, zaliczając do tego grona). B. Ferdek, definiując sekty i nowe ruchy religijne, podkreśla pewne ich cechy – wyróżniki, do których zalicza m.in.: odrzucenie dialogu ekumenicznego, uzupełnianie Biblii o różne dodatkowe objawienia, redukowanie możliwości zbawienia wyłącznie do członków własnej sekty, odrzucenie wiary w Trójcę Świętą i Jezusa Chrystusa jako Zbawiciela, aby następnie … zaliczyć do tego grona Kościoły, których te zarzuty nie dotyczą (*idem*, *Sekty i nowe ruchy religijne*, Wrocław 1998, s. 27, 31, 56-59).

[15] Por. E. Barker, *Nowe ruchy religijne*, tł. T. Kunz, Kraków 1997, s 87-90.

tylko krzywdzące, ale także prowadzić może do ograniczenia swobód obywatelskich poprzez wywieranie nacisku na społeczeństwo na przykład ze strony środków masowego przekazu, które posługują się stereotypami i uogólnieniami w komunikacji.

Z powodu zaszłości historycznych oraz nieostrości pojęcia „sekta", część badaczy posługuje się innymi terminami, z których najpopularniejszym jest obecnie nazwa „nowe ruchy religijne" (NRR, ang. New Religious Movements, NRM). Badacze wciąż jednak próbują wypracować najbardziej adekwatne[16].

Wśród nowych ruchów religijnych istnieją grupy religijne i parareligijne posługujące się destrukcją lub do niej dążące (łac. *destructio – zniszczenie, naruszenie całości, zrujnowanie*). Przez „religijną grupę destrukcyjną" rozumie się zazwyczaj środowisko o podłożu religijnym[17], które wywiera niszczący wpływ na jednostkę i społeczeństwo. Podobnie jak sekta, religijna grupa destrukcyjna nie jest pojęciem ścisłym, nie przynależy do języka prawnego, żaden dokument normatywny nie posługuje się tym pojęciem[18]. M. Libiszowska-Żółtkowska proponuje następującą definicję grupy destrukcyjnej: „godząca w porządek prawny i społeczny przez całkowite podporządkowanie (uzależnienie, ubezwłasnowolnienie) sobie członków przez przywódców na drodze ich psychicznej destabilizacji i zerwania dotychczasowych więzi społecznych"[19]. M. Szostak natomiast konstatuje: „Pojęcie destrukcyjności zatem dotyczy wskazania na atrybuty takich zachowań w sektach religijnych, które wywierają negatywny wpływ na jednostkę, a w konsekwencji grupy społeczne. Sekta destrukcyjna zatem musi posiadać swoiste atrybuty odróżniające ją od innych grup o proweniencji religijnej"[20]. Aby doprecyzować pojęcie destrukcyjności autor posłużył się charakterystyką wypracowaną przez oddział Chrześcijańskiego Instytutu Badawczego w Toronto (Christian Research Institute). Wymienia ono dziesięć cech, po których można rozpoznać grupę destrukcyjną[21].

[16] P. Chrzczonowicz wymienia 35 takich terminów, *idem*, *Sekty destrukcyjne*, s. 188-189, a I. Kamiński aż 67, *idem*, *Sekty i nowe ruchy religijne*, s. 27.

[17] Mogą to być grupy wyrosłe na gruncie religii istniejących (chrześcijaństwa, islamu, judaizmu, hinduizmu czy buddyzmu, ale też promujące powrót do dawnych kultów etnicznych, czyli rodzimowiercy) lub formacje nowe.

[18] P. Chrzczonowicz, *Sekty destrukcyjne*, s. 255, nota 341.

[19] M. Libiszowska-Żółtkowska, *Nowe ruchy religijne w zwierciadle socjologii*, Lublin 2001, s. 47.

[20] M. Szostak, *op.cit.*, s. 69.

[21] Istnieje wiele innych opisowych definicji (religijnej) sekty destrukcyjnej, por.: Dominikańskie Centrum Informacji o Nowych Ruchach Religijnych i Sektach: totalny charakter. (1) liderzy grupy przypisują sobie absolutny autorytet i prawo ingerowania we wszystkie dziedziny życia swoich członków, nawet te najbardziej intymne; (2) nowych członków pozyskują uciekając się do najróżniejszych podstępów i kłamstw, zatajając istotne informacje o działaniu grupy, jej celach i doktrynie; (3) uzależniają

Obecność już jednej z nich powinna wzmóc czujność: (1) kontrola umysłu; próba przejęcia kontroli nad obiegiem informacji krytycznych na temat grupy; (2) zmiany w diecie, niedożywienie; celem jest stępienie myślenia niezależnego – największego wroga grupy; (3) bezwzględne i absolutne posłuszeństwo liderowi (guru) lub przywódcom grupy; (4) namawianie do nieuczciwych odpowiedzi i/lub ukrywania prawdy przed osobami z zewnątrz; (5) utrzymywanie, że osiągnięcie zamierzonych celów (zbawienie, władza, wzrost duchowy, spełnienie siebie) możliwe jest wyłącznie poprzez przynależność do grupy; (6) oddzielenie od członków rodziny, przyjaciół, społeczności; negowanie potrzeby zdobywania wykształcenia, by ograniczyć lub uniemożliwić myślenie niezależne; (7) przemęczenie wynikające z zagospodarowania czasu na pracę na rzecz grupy lub dużą ilość spotkań, by w miarę możliwości ograniczyć aktywność poza grupą; (8) pozbawianie prywatności; (9) głęboka indoktrynacja skutkująca poczuciem winy i strach przed wykluczeniem z grupy; (10) totalitarny światopogląd dzielący rzeczywistość na „my" i „oni"; dobro grupy najwyższym dobrem jednostki[22].

Składowym elementem prowadzenia działalności grup destrukcyjnych jest psychomanipulacja totalna[23]. Jej metody mają charakter zaplanowany, świadomy i celowy. Pierwszym celem jest dezorientacja jednostki wywołująca zmianę zachowań, poglądów, postaw i przekonań manipulowanego zgodnych jedynie z wolą i celami osoby manipulującej. Obliczone to bywa na osiągnięcie konkretnych korzyści, poprzez wzbudzenie zaufania i lojalności, wyzyskanie niewiedzy, zdobycie (w niezauważalny sposób) pełnej kontroli nad jednostką, aż po pozbycie się przez jednostkę autonomicznego światopoglądu.

uczestników psychicznie i ekonomicznie za pomocą technik (psycho)manipulacji – wywierają niekorzystny wpływ na rozwój psychiczny adepta i jego relacje społeczne (np.: zerwanie więzi z najbliższymi, porzucenie pracy lub studiów); (4) posiadają charakter kultowy w szerokim rozumieniu, niekoniecznie religijnym. Może to być kult osoby, energii, zdrowia, pieniędzy, sukcesu itp.; (5) wytwarzają ostry podział rzeczywistości na to co „dobre", czyli związane z grupą i „zagrażające", odnoszące się do świata zewnętrznego (biało-czarna wizja rzeczywistości); (6) wpajają swoim członkom przekonanie o elitarności ruchu i niechęć do dialogu światopoglądowego (*Jak rozpoznać sektę (grupę destrukcyjną)*, źródło: http://sekty.dominikanie.pl <<dostęp: 15.12.2016>>).

[22] M. Szostak, *op.cit.*, s. 71.

[23] M. Jankowska, *Psychomanipulacja jako technika werbunku wykorzystywana przez sekty oraz ich fasadowe organizacje*, „Warmińsko Mazurski Kwartalnik Naukowy. Nauki Społeczne" 2012, nr 4/4, s. 161

## Obecność religijnych grup destrukcyjnych w Internecie

Zagrożenie ze strony religijnych sekt destrukcyjnych jest powszechne, o czym świadczą z jednej strony przypadki zbrodni popełnionych przez tego typu organizacje[24], z drugiej terrorystyczna aktywność fundamentalistycznych sekt islamskich, zbliżonych w swojej strukturze do klasycznych religijnych grup destrukcyjnych (e-dżihad). W drugim przypadku można przywołać autora propagandowych filmów internetowych, francuskiego ideologa tzw. Państwa Islamskiego, Omara Diaby, który swoją aktywnością w sieci skłonił setki młodych Europejczyków do porzucenia domów rodzinnych i wyruszenia na wojnę w Syrii[25]. E. Pępiak przywołuje kilka innych dowodów na wykorzystywanie Internetu przez islamskie sekty, jak w przypadku saudyjskiego członka tzw. Państwa Islamskiego, który stwierdził: „Arabskie media i strony internetowe dżihadystów przekonały mnie, by przyjechać [do Iraku – przyp. E.P.]"[26].

Internet, jako doskonałe medium komunikacyjne w społeczeństwie, oferuje kontakt ze światem, który w realu nie jest możliwy w takim stopniu i w tym zakresie. I. Kamiński na pytanie o to, gdzie *sekty najczęściej werbują?* plasuje Internet na jedenastym miejscu (na dwanaście)[27]. Nie wydaje się to uzasadnione. Propaganda środowisk, o których mowa, w Internecie jest zdecydowanie bardziej aktywna, na co wskazują badania A. Zwolińskiego[28]. Anonimowość, którą cechuje się sieć, pozwala stworzyć nawet małej grupie wrażenie dobrze prosperującej instytucji religijnej. Do tego celu nie potrzeba zaangażowania poważnych środków finansowych. Udzielający porad jest nieznany, ale jeśli uda mu się utrafić w oczekiwanie i potrzebę, szybko może stać się guru.

Więzi społeczne można podzielić na silne i słabe. Według P. Siudy zdecydowana większość relacji cechujących cyberprzestrzeń ma charakter więzi słabych, ponieważ występowanie silnej odmiany nie jest koniecznością[29]. Społeczność sieciowa promuje właśnie więzi słabe, które łączą ludzi w oparciu o wspólne zainteresowania, poglądy i wartości[30]. Nie zmienia to faktu, że sieć ma nieskończoną możliwość propagowania dowolnej idei. W ten sposób stanowi wymarzoną przestrzeń dla

[24] I. Kamiński, *Sekty i nowe ruchy religijne*, s. 17-22.
[25] E. Pępiak, O *sposobach zarażania Państwem Islamskim. Memetyka a hegemoniczne dyskursy państwowości*, „Teksty z ulicy" 2015, nr 16, s. 79.
[26] *Ibidem*, s. 85.
[27] I. Kamiński, *Sekty i nowe ruchy religijne*, s. 117.
[28] A. Zwoliński, *op.cit.*, s. 95-104.
[29] P. Siuda, *op.cit.,* s.145-146.
[30] *Ibidem*, s. 146.

działalności grup religijnych i parareligijnych o charakterze destrukcyjnym. Autor, opierając się na badaniach L.L. Dawson i J. Hennebry[31] stwierdza: „samo zaistnienie ruchu w Internecie nie wystarczy. Według badaczek proces konwersji opiera się na tworzeniu silnych więzi z potencjalnymi wyznawcami. Internet nie jest w stanie automatycznie zapewnić konwersji, za dostarczeniem informacji o ruchu musi iść bowiem osobisty kontakt, musi być nawiązanie relacji z członkiem. Oczywiście, bardzo często sieć elektroniczna umożliwi to w sposób pośredni. Ktoś, kto znalazł serwis danego ruchu, może za jego pomocą nawiązać kontakt „na żywo". Sam internet jednak nie jest w stanie zapewnić nawrócenia"[32].

Przytoczona wyżej opinia, odnosząca się ogólnie do nowych ruchów religijnych, wydaje się szczególnie trafna w stosunku do religijnej grupy destrukcyjnej. O ile przynęta może być zarzucona w sieci, o tyle zdobycz musi być wyciągnięta w realu. Dopiero tu bowiem, można w pełni kontrolować umysł wyznawcy i poziom jego życia. Nie zmienia to jednak faktu, że cyberprzestrzeń doskonale nadaje się do pierwszego kontaktu, ale także wstępnego przygotowania adepta poprzez nakreślenia wizji świata i przedstawienia pewnych założeń. Grupy tego typu nie zdradzają w sieci szczegółów swoich działań, nie podają również prawdziwych intencji, które im przyświecają.

Przykładem takiej właśnie aktywności w sieci może być Kościół Scjentologiczny[33]. Założony przez Rona L. Hubbarda w 1951 r. stał się jednym z najbardziej rozpoznawalnych „znaków towarowych" rodem z USA i najbardziej dochodowym ruchem religijnym[34]. Założyciel, wcześniej autor drugorzędnych powieści science fiction, sformułował główne tezy ruchu w książce *Dianetyka, czyli nowoczesna wiedza o zdrowiu psychicznym* (1950)[35]. Scjentologia (łac. *scio nauka* i gr. *logos – wiedza*) łączy cechy sprawnie zorganizowanego przedsiębiorstwa, a raczej szeregu organizacji ekonomicznych, z koncepcjami parareligijnymi[36]. W niektórych państwach zarejestrowany został jako organizacja religijna (USA, Australia, Kanada

[31] L.L. Dawson, J. Hennebry, *New Religions and he Internet: Recruting in a New Public Space*, [w:] *Religion On-line. Finding Faith in the Internet,* red. L.L. Dawson, D.E. Cowan, New York 2004, s. 151-171.

[32] P. Siuda, *op.cit.*, s. 149.

[33] H. Karp, *Maski sekt. Sekty w obliczu komercjalizacji rynku religijnego (Kościół Scjentologiczny)*, [w:] *Sekty i nowe ruchy religijne – wolność czy zniewolenie. Zagadnienia interdyscyplinarne,* red. P. Chrzczonowicz, I. Kamiński, Toruń 2012, s. 329-337.

[34] *Ibidem*, s. 331

[35] Dianetyka pochodzi z dwóch słów greckich *dia – przez* i *nous – umysł*. Termin oznacza ogół idei i metod psychoterapii stanowiących podstawę scjentologii.

[36] E.M. Guzik-Makaruk, *Sekty religijne w Polsce,* Warszawa 2004, s. 112.

i we Włoszech). H. Karp stwierdziła: „Scjentologia ma różne szyldy i nazwy. Przedstawiana bywa jako „technologiczny buddyzm" czy „technologiczny gnostycyzm", jednak bez względu na szyldy, jej składowe to magiczne praktyki i filozofia Wschodu, struktura organizacyjna Zachodu oraz działanie i język technologiczny połowy lat XX wieku"[37]. We Francji organizacja ta została uznana za religijną grupę destrukcyjną i uznana za organizację przestępczą[38]. W Niemczech traktuje się ją nie jako sektę religijną, ale nowy typ ekstremizmu politycznego[39]. Do Polski pierwsi scjentolodzy przybyli w 1991 r. Próby zarejestrowania Kościoła Scjentologicznego nie powiodły się (1995), ale rejestrację uzyskało stowarzyszenie Centrum Dianetyki we Wrocławiu[40]. W kwietniu 2007 r. prasa poinformowała, że scjentolodzy mają swoją placówkę w Warszawie i prowadzą działalność werbunkową[41]. Ruch przyjmuje postać różnych stowarzyszeń, organizacji i spółek, zajmujących się odnową psychiczną, kursami komunikacji czy psychoterapią. Ważnym medium, poza publikacjami książkowymi, są strony internetowe[42]. Pełnią one rolę zarzucania przynęty, poszukiwania kandydatów na adeptów.

## Zakończenie

Cechą charakterystyczną sieci jest stosunkowa łatwość zamieszczania informacji i trudność związana z usuwaniem elementów szkodliwych, mogących potencjalnie wpływać na statystycznego użytkowania[43]. Specjaliści od prawa i kryminalistyki postulują rozwiązania systemowe. Od strony środowiska badawczego wymagane byłoby precyzyjniejsze zdefiniowanie pojęć związanych z ochroną obywateli przed niebezpiecznymi sektami[44]. A. Zwoliński postuluje wprowadzenie w instytucjach związanych z edukacją i wychowaniem dzieci i młodzieży (czyli osób najbardziej narażonych na działalność omawianych grup) zajęć informujących o zagrożeniach

[37] H. Karp, *op.cit.*, s. 334, zob. nota 1007.
[38] M. Szostak, *op.cit.*, s. 149.
[39] E.M. Guzik-Makaruk, *op.cit.,* s. 116.
[40] *Ibidem*, s. 112.
[41] J.R. Sielezin, *Destrukcyjna rola sekt i związków wyznaniowych w XX i XXI wieku – problem cywilizacyjny i polityczny,* ,,Wrocławskie Studia Politologiczne" 2012, nr 13, s. 193.
[42] H. Karp, *op.cit.*, s. 331.
[43] Ł. Tomczyk, *op.cit.*, s. 130.
[44] Na niedomagania w tym zakresie zwrócił uwagę. J.R. Sielezin: „Brak przejrzystych definicji dotyczących sekty i ruchu religijnego lub związku światopoglądowego, narzędzi badawczych, zacieranie kontekstów i podtekstów oraz skryte oblicze sekt i dynamika ich rozwoju stanowią poważne utrudnienie procesu badawczego" (J.R. Sielezin, *op.cit.*, s. 196).

płynących ze strony sekt destrukcyjnych[45]. Należy do tego dołączyć uwagi dotyczące środowisk akademickich. Wśród nich zaś w pierwszej kolejności podkreślanie w pracy z młodzieżą wagi myślenia krytycznego, ważnego i niezbędnego elementu chroniącego przed manipulacją i demagogią. Konieczny jest bowiem zwyczajny zdrowy rozsądek i ostrożność w kontakcie z tymi, którzy pod różnymi religijnymi szyldami prowadzą działalność destrukcyjną.

## Bibliografia

Chrzczonowicz P., *Sekty destrukcyjne: wybrane zagadnienia prawne, kryminologiczne i społeczne*, Toruń 2013,

Dawson L. L., Hennebry J., *New Religions and he Internet: Recruting in a New Public Space*, [w:] red. L.L. Dawson, D.E. Cowan, *Religion On-line. Finding Faith in the Internet*, New York 2004.

Frankowiak J. K., *Mity i uproszczenia dotyczące działalności sekt, a także środowisk zajmujących się problematyką funkcjonowania tego typu grup,* [w:] *Człowiek w sieci zniewolonych dróg,* red. M. Jędrzejko, W. Bożejewicz, Pułtusk 2007.

Gajewski W., *Kościół wobec herezji w I wieku*, „Gdański Rocznik Ewangelicki" 2009, nr 3.

Guzik-Makaruk E. M., *Sekty religijne w Polsce,* Warszawa 2004.

*Jak rozpoznać sektę (grupę destrukcyjną)*, źródło: http://sekty.dominikanie.pl (dostęp: 15.12.2016).

Jankowska M., *Psychomanipulacja jako technika werbunku wykorzystywana przez sekty oraz ich fasadowe organizacje*, „Warmińsko Mazurski Kwartalnik Naukowy. Nauki Społeczne" 2012, nr 4/4.

Kamiński I., *Polska bibliografia na temat sekt i Nowych Ruchów Religijnych od 1800 do 2005*, [w:] *Słownik sekt, nowych ruchów religijnych i okultyzmu,* red. G.A. Mather, L.A. Nichols.

Kamiński I., *Sektyi nowe ruchy religijne w 365 pytaniach i odpowiedziach*, Warszawa 2013.

[45] A. Zwoliński, *op.cit.*, s. 144.

Karp H., *Maski sekt. Sekty w obliczu komercjalizacji rynku religijnego (Kościół Scjentologiczny)*, [w:] *Sekty i nowe ruchy religijne – wolność czy zniewolenie. Zagadnienia interdyscyplinarne,* red. P. Chrzczonowicz, I. Kamiński, Toruń 2012.

Libiszowska-Żółtkowska M., *Nowe ruchy religijne w zwierciadle socjologii*, Lublin 2001.

Nowakowski P. T., *Polska bibliografia artykułów na temat sekt i nowych ruchów religijnych od 1990 do 2003 roku*, [w:] *ABC o sektach* red. M. Gajewski, Tychy 2004.

Pępiak E., O *sposobach zarażania Państwem Islamskim. Memetyka a hegemoniczne dyskursy państwowości*, „Teksty z ulicy" 2015, nr 16.

*Raport o niektórych zjawiskach związanych z działalnością sekt w Polsce*, Warszawa 2000.

Romańczuk-Grącka M., *Przeszkody kryminalizacyjne dotyczące zachowań związanych ze zjawiskiem psychomanipulacji w sektach destrukcyjnych*, [w:] *Sekty i nowe ruchy religijne – wolność czy zniewolenie. Zagadnienia interdyscyplinarne*, red. P. Chrzczonowicz, I. Kamiński, Toruń 2012.

Sielezin J. R., *Destrukcyjna rola sekt i związków wyznaniowych w XX i XXI wieku – problem cywilizacyjny i polityczny,* „Wrocławskie Studia Politologiczne" 2012, nr 13.

Siuda P., *Religia a internet. O przenoszeniu religijnych granic do cyberprzestrzeni*, Warszawa 2010.

Szostak M., *Sekty destrukcyjne. Studium metodologiczno-kryminalistyczne*, Zakamycze 2001.

Tomczyk Ł, *Społeczeństwo informacyjne a działalność grup religijnych oraz sekt w Internecie*, [w:] *Sekty i nowe ruchy religijne – wolność czy zniewolenie. Zagadnienia interdyscyplinarne*, red. P. Chrzczonowicz, I. Kamiński, Toruń 2012.

Zwoliński A., *Sekty w Internecie*, Kraków 2008.

**Lucjan Klimsza**

Uniwersytet Ostrawski

# Filozoficzne aspekty działania Internetu w kontekście zadań misyjnych Kościoła

Słowa kluczowe: Kosciół, cyberpstrzeń, edukacja, teologia

## Wstęp

Istnienie *cyberprzestrzeni* jest z punktu widzenia filozofii ściśle związane z *τεχνη*[1]. Pierwsze prace na temat *τεχνη* znajdujemy już w filozofii antycznej, a dokładnie w dorobku Platona. Według tego filozofa, problem techniki jest związany z rozwojem nauki i poznania świata, dokonanym przez pokolenia wczesnych filozofów jońskich. Podkreślmy, że jońską szkołę filozoficzną tradycja filozofii niemieckiej określa mianem „Naturphliosophie", czyli szkoła filozofii przyrody, która związana była z poszukiwaniem *αρχη*. Farringhton w swej pracy *Nauka w Starej Grecji* wskazuje na związek przyczynowo-skutkowy pomiędzy techniką, a filozofią. Ta więź, a dokładniej związek *znajomości procesów produkcji* i *filozofii* odegrał znaczącą rolę w rozwoju poznania i interpretacji świata[2]. W platońskiej myśli filozoficznej znajdujemy jednakże krytykę tej relacji. Znajomość procesów produkcji Platon nazywa *τεχνη*. Termin ten można w ujęciu filozofa przetłumaczyć na kilka sposobów. Pierwszą z możliwości jest po prostu *technika*, lecz można również *τεχνη* za Patočką ująć jako *sztukę*. Nadmieńmy, że Platon przez termin *sztuka* rozumie jednak *poznanie* czy *wiedzę*, która prowadzi człowieka do konkretnego celu. Dla wytłumaczenia znaczenia słowa *τεχνη* przyjrzyjmy się dialogowi Ion[3].

[1] W tłumaczeniu technika, praca, dzieło czy też sztuka.

[2] B. Farrington, *Věda ve starém Řecku*, Brno, 1950, s. 43.

[3] Platon, *Ion*, źródło: http://www.perseus.tufts.edu (dostęp: 16.04.2017).

Platon przedstawia w nim *τεχνη* jako wiedzę, która pomaga człowiekowi w poznaniu świata, w celu jego zdominowania. *Τεχνη* jest więc wiedzą, która prowadzi do pewnego celu. Sama nie jest celem, ale środkiem, który prowadzi do pewnego celu. W dialogu Ion jednak filozof wykazuje, iż sama *τεχνη* jako środek prowadzący do określonego celu jest niewystarczająca. *Τεχνη* pokazuje, jak można coś osiągnąć, lecz nie przedstawia tego, czy dany środek jest dobry lub zły. Nie rozstrzyga też, czy dany cel jest dobry albo zły.

Sofistyczny pogląd na problematykę *τεχνη* reprezentuje w dialogu *Ion.* Mówi, iż *τεχνη* jest środkiem do pewnego celu, jak również jest dobrem czy cnotą. Dlatego cel może uświęcać środki, kiedy *τεχνη* stanie się równocześnie *αρετη*. Platon odróżnia *τεχνη* i *αρετη*. Gdyby *τεχνη* było tym samym co *αρετη,* człowiek byłby Bogiem, twierdzi filozof. Człowiek posiadając wyłącznie wiedzę techniczną nie posiada wiedzy etycznej, bowiem nie można z wiedzy technicznej wyprowadzić wiedzy etycznej i na odwrót. Cnoty nie posiada obiekt, lecz cnota jest jakością subjektu. Człowiek z wiedzy technicznej potrafi uczynić dobro lub zło, indywidualne albo społeczne.

Uczeń Platona, Arystoteles rozszerzył w swej pracy *Poetyka* zakres działania człowieka. Na pytanie, czym jest sztuka człowieka, odpowiada następująco: „działalność człowieka dzieli się na badanie, działanie i twórczość”[4]. Władysław Tatarkiewicz na podstawie *Poetyki* Arystotelesa dochodzi do wniosku, iż każdy człowiek, który bada to, co chce uczynić, zastanawia się nad sposobem wykonania dzieła oraz doprowadza do istnienia owo dzieło, staje się artystą[5]. Powodem jest sztuka, która stała się całością, a którą nabył człowiek ucząc się wiedzy o świecie, metafizyki oraz rzemiosła. Również taki człowiek jest artystą w określonej dziedzinie, ponieważ posiada pewną *τεχνη*.

Martin Heidegger napisał niewielką książeczkę**,** która nosi tytuł *Nauka, technika oraz kontemplacja*[6]. W pracy tej pochyla się nad fenomenem wiedzy technicznej i samym istnieniem techniki. Porusza niezmiernie ważny temat stosunku *bytu technicznego* do samej *techniki*. Pierwszym i zasadniczym twierdzeniem jest zdanie: „podstawa istnienia techniki nie jest niczym technicznym”[7]. Heidegger sugeruje nam, iż na podstawie używania techniki nigdy nie określimy, czym technika dla

[4] Arystoteles, *Ποιετικη*, źródło: http://www.perseus.tufts.edu (dostęp: 16.04.2017).
[5] W. Tatarkiewicz, *Historia estetyki*, t.1, Wrocław 1962, s. 167-168.
[6] Cytujemy tutaj z czeskiego tłumaczenia M. Heideggera *Věda, technika a zamýšlení* (2004).
[7] M. Heideggera *Věda, technika a zamýšlení,* Praha 2004, s. 7.

nas jest. Należy przy tym zaznaczyć, iż Heidegger odróżnia *podstawę istnienia techniki* (Wesen technik) od *istnienia techniki* (Dasein technik). Istnienie techniki rozumie tutaj jako używanie techniki, a zatem co innego niż fenomen istnienia podstawy techniki.

Pytając o to, czym jest technika, docieka pierwszoplanowo nie o to, jak używamy techniki, lecz jakie są podstawy bytu techniki. Szukając podstaw techniki, pyta o Wesen Technik czyli o to, *czym to coś jest*[8]. Heidegger na to pytanie najpierw odpowiada dwoma sposobami. Po pierwsze, odnosząc się do sprawy istnienie techniki powtarza za Platonem „Technika jest środkiem do osiągnięcia pewnych celów". Po drugie, powtarza myślą Arystotelesa, że „Technika jest działalnością człowieka"[9]. Heidegger jednakowoż, jak pokazaliśmy wyżej, nie do końca cytuje Arystotelesa. Pokazuje, iż τεχνη jest działalnością człowieka, a zarazem, że definicja nie jest w stanie określić podstawy bytu techniki.

Proponuje więc inne rozwiązanie, którym jest połączenie myśli Platona i Arystotelesa: „Oba te określenia techniki przynależą do siebie. Albowiem ustanawiać cele, angażować w nie środki i używać ich, jest działalnością człowieka"[10]. Tak więc, za Heideggerem możemy zaproponować definicję podstawy bytu techniki:

- ustanawianie celów,
- wytwarzanie środków do ich realizacji,
- używanie ich,
- działalność człowieka.

W oparciu o to ujęcie można stwierdzić, iż w filozofii Heideggera nie ma techniki bez człowieka. Nie można powiedzieć również, by technika miała sama swoją własną podstawę, skoro jest ona związana z *byciem-tu-oto* człowieka. Z tego powodu Heidegger dochodzi do wniosku, że technika nie jest czymś neutralnym, albowiem jest ludzkim dziełem. Heidegger dodaje, iż *podstawie bytu techniki* jest przynależne wytwarzanie i używanie instrumentów, maszyn. Do *podstawy bytu techniki* należy zarówno to, co jest wytworzone i używane, jak i potrzeby oraz cele, którym te środki służą[11].

Podstawę bytu techniki możemy więc rozdzielić na:

– wytwory techniki,

[8] *Ibidem*.
[9] *Ibidem,* s. 7.
[10] *Ibidem*, s. 7.
[11] *Ibidem*, s. 8.

– potrzeby, które są zaspokajane poprzez te maszyny.

Pytając więc o cyberprzestrzeń, dociekamy jakie potrzeby prowadziły czy wciąż prowadzą do sprzęgnięcia *hardwaru* i *softwaru* oraz podłączania telefonów, komputerów a także innych urządzeń do globalnej. W ten sposób możemy zrozumieć zasadniczą tezę, której autorem jest CEO Apple Tim Cook: „Kupując iPhone zyskujemy lepsze życie”[12]. Stosunek *bycia-tu-oto* do podstawy bycia techniki jest więc stosunkiem potrzeb człowieka do wytworów techniki.

## Technika a Kościół

Liczba teologów, którzy interesowali się techniką i jej związkiem z Kościołem jest bardzo mała. Chociaż internet ma swego patrona, na którego Kościół katolicki wybrał św. Izydora z Sewilii[13], to jednak brakuje teologów chrześcijańskich, którzy podejmują tę problematykę. Jednym z nielicznych, a jednak bardzo znaczącym jest Paul Johannes Tillich, autor tekstu *Techniczne miasto jako symbol*. W rozprawie tej wskazuje, że ludzkie działania mają dwa wymiary. Tym pierwszym jest rzecz sama w sobie, a drugim rzecz, która jest równocześnie symbolem. W takim razie możemy stwierdzić, że wytwór człowieka jest:

– rzeczą, która służy do pewnego celu i poprzez sam cel jest określona,
– symbolem, który deklaruje bycie i jest przez nie określone[14].

W związku z powyższym Tillich twierdzi, że każda rzecz, w tym i technika, ma dwie płaszczyzny. Pierwszą jest *płaszczyzna horyzontalna* każdej rzeczy, która wskazuje na użyteczność danego wyrobu. Drugą płaszczyzną danego wyrobu jest *płaszczyzna wertykalna*. *Płaszczyzna horyzontalna* pozwala człowiekowi przetrwać w świecie. Natomiast druga, umożliwia określenie tożsamość człowieka wobec świata, innych ludzi, samego siebie i Boga oraz odpowiada na pytanie: „kim ja jestem poprzez dzieło swoich rąk?”. W tym właśnie miejscu zaistniała korelacja pomiędzy kulturą człowieka, a religią, ponieważ każde pytanie o sens w ostatecznym rozrachunku prowadzi do religii. Dociekając sensu istnienia, rozpoczniemy

[12] T. Cook, *Apple keynote (2013)*, źródło: http://www.apple.com (dostęp: 16.04.2017).

[13] „Św. Izydor żył na przełomie VI i VII w., a mimo to został patronem Internetu, który jest znakiem czasów nam współczesnych. Hiszpańscy informatycy ze Służby Obserwacyjnej Internetu w Barcelonie, inspirowani wskazówkami Papieskiej Rady Środków Społecznego Przekazu zgłosili kandydaturę św. Izydora na patrona globalnej sieci. Wybór świętego został potwierdzony w głosowaniu przeprowadzonym na włoskiej stronie www.santibeati.it. Mówi się, że stworzony przez św. Izydora 20-tomowy zbiór wiadomości z różnych dziedzin wiedzy „Etymologiarum libri XX seu Origines” to prototyp baz danych stosowanych obecnie w informatyce” (A. Kwaśnicka, *Parafiane w cyberprzestrzeni*, http://kosciol.wiara.pl <<dostęp: 16.04.2017>>).

[14] P.J. Tillich, *Die Technische Stadt als Symbol*, Stuttgart 1962, s. 220.

od pytań odnoszących się do banalnych problemów. W ostateczności przychodzi nam odpowiedzieć na najważniejsze pytanie, które dotyczy sensu istnienia. To pytanie możemy wyrazić właśnie poprzez dzieło naszych rąk.

Tillich na początku analizowanego tekstu mówi o domu – miejscu, które człowiek wybudował dla zabezpieczenia samego siebie przed nieprzyjaznym, niezdefiniowanym, niezmierzonym światem, którego nie potrafił określić. Wraz z domem powstało *miejsce* w tym świecie, które człowiek potrafił określić, a tym samym poczuł się bezpiecznie[15]. Miasto jest kwantyfikacją domu. W mieście człowiek wybudował w nieokreślonym świecie określone miejsce swego istnienia. Dom i miasto na płaszczyźnie horyzontalnej służą do mieszkania, a na płaszczyźnie wertykalnej do przezwyciężenia obcości w nieokreślonym świecie[16].

W tym miejscu trzeba jeszcze powiedzieć parę słów o przymiotniku *techniczny*. Oświecenie stechnicyzowało świat, rozumiejąc go jako maszynę, a człowieka jako doskonałą maszynę. Techniczny dom, to symbol stechnicyzowanego świata, który został *zdominowany* przez naukę i technikę. Wrogość i nieokreśloność świata zostały przezwyciężone przez technicyzację środowiska naturalnego. Możemy więc powiedzieć, iż dzięki technice świat stał się technicznym domem czy też technicznym miastem. Podkreślmy jednak, że człowiek spokoju nie znajduje ani w przyrodzie, ani w mieście, a już na pewno nie w technicznym świecie. Ostatecznie ponownie pojawia się pytanie o sens istnienia i to w stosunku do dzieła, które człowiek wzniósł po to, by w ostateczny sposób odpowiedzieć na pytanie o sens istnienia człowieka. To właśnie pytanie w końcowym rozrachunku dotyczy trudu, który podjął względem swej własnej śmiertelności. Techniczne miasto stało się zatem w swym wertykalnym rozmiarze niczym innym jak pytaniem o sens. Tillich w końcu konstatuje, iż techniczny dom i techniczne miasto stały się człowiekowi obce[17]. Ta obcość to brak stosunku żywego człowieka do żywej natury, to brak interpersonalnego stosunku człowieka do człowieka. To również brak stosunku żywego człowieka do żywego Boga.

[15] Tillich pisze: *Das Haus ist die Zelle der Stadt, udn wie das Haus, so ist auch die Stadt Symbol jener urmenschlichen Flucht von dem Unheimlichen* (*Ibidem*, s. 222).
[16] Tillich pisze: *Wie haus und Stadt das Mittel der Einfügung ins menschliche Dasein, so ist alle Technik eine Unheimlichen in den Dingen* (*Ibidem*, s. 222).
[17] *Ibidem.*

## Ontologia cyberprzestrzeni

Pytanie o to czym jest cyberprzestrzeń nie należy do łatwych. Pod względem ontologicznym nakładają się bowiem na problem cyberprzestrzeni kwestie związane z urządzeniami (komputer, modem, router) oraz oprogramowaniem (system operacyjny itd.). David Koepsell nazywa ów problem obiektem utylitarnym[18], czyli użytecznym obiektem, który zaspokaja potrzeby człowieka. Lecz czym cyberprzestrzeń tak naprawdę jest? Koepsell dodaje, iż z punktu widzenia filozofii nie wiemy tak naprawdę, czym jest cyberprzestrzeń oraz, jak ją mamy poznawać.

## Ontologia cyberprzestrzeni według ontologii Arystotelesa

Arystoteles definiuje bycie przez dziesięć kategorii, które pokazują nie tyle istotę bytu, co jakość bytu. Arystoteles uważał pierwsze cztery kategorie za najważniejsze, a wśród nich jako najbardziej istotną kategorię ουσια czyli substancję. Na pytanie czym jest substancja, odpowiada Arystoteles w swej Metafizyce, że to byt samoistny, określony przez ilość, jakość i stosunek. Tak naprawdę, to z tych czterech kategorii właśnie substancja określa byt. Tatarkiewicz pisze: „W prawdzie byt można rozważać w różny sposób: jako zespół rzeczy, ale także jako zespół jakości, kwantów lub stosunków różnego rodzaju"[19], ilość, jakość i stosunki to przypadłości bytu.

Tak więc można zadać pytanie czy cyberspace nie jest bytem samoistnym? Na nie, wnioskując z arystotelesowskich kategorii, możemy odpowiedzieć jednak przecząco. Dalej odwołując się do ujęcia bytu przez Arystotelesa zauważamy, że:

- Ilość – nie jest odpowiedzią: cyberprzestrzeni nie można objąć. Cyberprzestrzeń jest przechstrzenią generowaną przez możliwości komputera, czyli jest dana za sprawą hardwaru i softwaru danego urządzenia. Można powiedzieć, iż komputer ma 2GB pamięci, ale taka konstatacja nie jest odpowiedzią na pytanie filozofii. Nie ma odpowiedzi na pytanie ILE.
- Jakość – jaka cyberprzestrzeń jest? Można powiedzieć, iż cyberprzestrzeń jest zapisana w binarnym kodzie, ale nie można odpowiedzieć na pytanie, jaka ona jest. Można by było odpowiedzieć na pytanie, jakie są jakości pewnej aplikacji, systemu operacyjnego lub komputera, nie cyberprzestrzeni.

[18] D.R. Koepsell, *The Ontology of Cyberspace,* New York 2000., s. 3.
[19] W. Tatarkiewicz, *Historia filozofii*, t. I, Warszawa 2002. s. 111.

– Relacja – można powiedzieć coś na temat stosunku maszyny do człowieka, oprogramowania do człowieka, ale nie cyberprzestrzeni do człowieka.

| KATEGORIE | Arystoteles | Cyberprzestrzeń |
|---|---|---|
| | **Substancja** | NIE |
| | **Ilość** | NIE |
| | **Właściwość** | NIE |
| | **Stosunek** | NIE |
| | **Miejsce** | NIE |
| | **Czas** | NIE |
| | **Położenie** | NIE |
| | **Posiadanie** | NIE |
| Wytwarzaniem hardware i software | **Wytwarzanie** | TAK |
| Pracując z komputerem w OS. | **Doświadczenie** | TAK |

Cyberprzestrzeń jest więc potencją stworzoną przez człowieka, która jest definiowana przez możliwości hardwarowe, które się co roku multiplikują według pewnego współczynnika oraz przez możliwości systemu i języka, a więc systemu operacyjnego oraz języka programowania. To jednak nadal nie umożliwia nam zrozumienia, czym jest cyberprzestrzeń.

## Fenomenologiczna ontologia cyberprzestrzeni

Na podstawie epoché, czyli fenomenologicznej redukcji, możemy powiedzieć, iż chodzi o bycie w – czyli aspekt intencjonalny, w którym człowiek określa coś na podstawie terminologicznego uchwycenia fenomenu, w naszym przypadku cyberprzestrzeni. Chodzi więc o *bycie-tu-oto* cyberprzestrzeni w przestrzeni. Cyberprzestrzeń nie może istnieć bez przestrzeni i bez czasu. Ona jest w przestrzeni i w czasie. Nie może być ponad czasem i przestrzenią, ponieważ zawsze jest tutaj człowiek, który tą przestrzenią manipuluje i nadaje jej pewien kształt.

W jaki sposób jest nam dana cyberprzestrzeń? Przede wszystkim poprzez zmysły. Sama w sobie nie miałaby sensu. Bez ludzkich zmysłów cyberprzestrzeń jest niczym. Ona się nam daje poznać poprzez zmysły, a tym samym bez nich, by dla nas nie istniała. Cyberprzestrzeń istnieje o tyle, o ile programista używa konkretnego języka programowania i tworzy program. Dalej, cyberprzestrzeń istnieje wówczas, gdy użytkownik komputera aktywuje aplikację i używa jej. Nie jest to zatem

wejście w przestrzeń, lecz wytwarzanie jej. Tak więc to człowiek stanowi o cyberprzestrzeni.

## Cyberprzestrzeń jako symbol

Czym jest zatem *bycie-tu-oto* cyberprzestrzeni? I czym jest cyberprzestrzeń na obu płaszczyznach? Przede wszystkim cyberprzestrzeń definiujemy jako produkt, który jest wytworem człowieka i służy mu do zaspokojenia jego potrzeb. Jako taki, jest określony przez swoją funkcję. Na płaszczyźnie horyzontalnej wskazuje to na jego ontologię. Lecz cyberprzestrzeń jest także symbolem. Symbolem, który pokazuje, w jaki sposób człowiek pragnie przezwyciężyć niedostępność i odległość w komunikacji (komunikacja), dzielić się informacjami (uczenie się), wytwarzać produkty (praca) i spędzać wolny czas (zabawa). Cyberprzestrzeń jest więc symbolem, który także wskazuje na pytanie o sens istnienia człowieka w przestrzeni i czasie, o sens istnienia myśli, o sens istnienia pracy oraz zabawy. Jest symbolem, który równocześnie pyta o *communio*[20] między człowiekiem a człowiekiem. Obecnie – podkreślmy – liczba aplikacji wytworzonych do komunikacji między ludźmi jest olbrzymia.

## Cyberprzestrzeń jako służba

Zadajmy więc pytanie o to, jak technologia cyberprzestrzeni służy człowiekowi do zaspokajania jego potrzeb? Pokazaliśmy już, iż technologia internetu jest pomocna w pracy, komunikacji, ułatwia życie, służy do kształcenia i równocześnie do zabawy. Na samym początku, kiedy tworzono pierwsze komputery osobiste, a więc w latach sześćdziesiątych i siedemdziesiątych dwudziestego wieku, Bush, Licklider i Engelbart przepowiadali, iż staną się one instrumentami wspierającymi twórczość osobistą człowieka i współpracę międzyludzką, wzmacniając w ten sposób inteligencję ludzi[21].

Cyberprzestrzeń zrodziła się z myślą o tym, by służyć ludziom na przykład poprzez tworzenie wspólnot. Pierwszą taką wspólnotą był portal TheWELL[22]. Jednym z haseł jego duchowego ojca – Stewarta Branda – było zdanie: „Jesteście panami własnych słów"[23]. Każdy użytkownik musiał się zalogować swym własnym

[20] Tłumaczymy jako pospolitość czy wspólnota.
[21] W. Isaacson, *Inovátoři. Jak skupinka vynálezců, hackarů, géniu a nadšenců stvořila digitální revoluci*, Praha 2015, s. 470.
[22] http://www.well.com – portal funkcjonuje stale.
[23] W. Isaacson, *op. cit.*, s. 476.

imieniem i nazwiskiem. Anonimowość była niedopuszczalna i, jak dodaje Walter Isaacson, każdy był odpowiedzialny za swe własne słowa[24]. Dzisiejszy internet różni się od swych początków przede wszystkim anonimowością, a co za tym idzie brakiem odpowiedzialności.

A jednak owo pierwotne posłannictwo komputera, internetu oraz oprogramowania przetrwało w pewnej formie, którą znajdujemy w firmie Apple. Hardware i software są tworzone z myślą o użytkowniku, który dzięki urządzeniom takim jak iPhone, iPad, iMac i iWatch potrafi lepiej organizować swój czas, pracę, naukę i odpoczynek. Idea, z którą przychodzi dzisiaj Apple przez swój Applestore, otwiera drzwi również dla Kościoła.

## Kościół a cyberprzestrzeń

Luterańska tradycja rozumie Kościół jako miejsce, gdzie zwiastuje się ewangelię i we właściwy sposób udziela sakramentów. Kościół jest więc określony przez miejsce, w którym dzieje się zwiastowanie ewangelii oraz udzielanie sakramentów. Nie może nie istnieć takie miejsce, ponieważ bez określonego „tutaj" nie ma podstawowej posługi Kościoła, czyli zwiastowania. Przez posługę zwiastowania ewangelii Chrystusowej Kościół nabywa swej jakości. Odpowiada więc na pytanie, jak istnieje Kościół? Nieprawdziwe byłoby stwierdzenie, iż Kościół nie potrzebuje swych świątyń, kościołów. Pojęcie estetyczne takiego miejsca, to osobna kwestia. Nie jest to jednak przedmiotem niniejszego artykułu.

Kościół oprócz swego „tu" musi mieć równocześnie swe „teraz". Jest to czas, w którym głosi się ewangelię oraz udziela sakramentów. Bez czasu nie można by mówić o Kościele, skoro Kościół to zgromadzenie świętych, czyli tych, którzy za sprawą ewangelii przyjęli sakrament Chrztu Świętego.

Kościół jest więc miejscem i czasem interpersonalnego spotkania człowieka z samym sobą, spotkania człowieka z bliźnim, a przede wszystkim spotkania człowieka z Bogiem. Osobistego spotkania nie zastąpi telefon, wideokonferencja czy efektywna aplikacja, na przykład do spowiedzi.

Przed Kościołem otwierają się jednak w cyberprzestrzeni pewne możliwości, takie jak:

- aplikacje wspierające modlitwę, czytanie Pisma Świętego oraz medytację,
- aplikacje umozliwiające tworzenie prezentacji,
- aplikacje wspierające edukację ,

[24] *Ibidem*, s. 476.

– aplikacje umożliwiające przekazywanie wiadomości z życia Kościoła i poszczególnych parafii.

Przykładem aplikacji, które kształcą, wspierają i ubogacają życie modlitewne jest oprogramowanie dostępne w Appstore. Trzeba jeszcze dodać, że przywołane aplikacje zostały wytworzone w odpowiedzi na zapotrzebowanie szkół podstawowych i średnich w Republice Czeskiej, a ich analizy dokonano w ramach projektu badawczego Chytráci[25].

## Zakończenie

Cyberprzestrzeń jest produktem człowieka, przeznaczonym do zaspokajania jego potrzeb. Jednak owo zaspokajanie służy nie tylko potrzebom definiowanym przez samą cyberprzestrzeń. Równocześnie jest to próba zaspokojenia potrzeb, które nazywamy religijnymi, jak na przykład przezwyciężenie obcości świata oraz przezwyciężenie jego rozległości i wielkości.

Na pytanie cyberprzestrzeni o istnienie świata i człowieka nie można odpowiedzieć za pomocą samej cyberprzestrzeni. Takiej odpowiedzi powinna udzielić teologia Kościoła. Kościół odpowiada na pytania o ostateczny sens istnienia świata i ludzi. Kościół nie może jednak stać się wirtualnym, by takiej odpowiedzi udzielić. Musi mieć swe tu i teraz, by wykonywać swoją posługę głoszenia ewangelii jako odpowiedzi na ostateczne pytania człowieka o sens bycia.

Kościół był zawsze multimedialny. Takim ma pozostać i wykorzystać możliwości cyberprzestrzeni. Może je wykorzystać w przeróżny sposób, duszpasterski, edukacyjny czy wykorzystać sieci socjalne w celu przekazywania poselstwa ewangelii.

## Bibliografia

Arystoteles, *Ποιετικη*, źródło: http://www.perseus.tufts.edu (dostęp: 16.04. 2017).

Cook T., *Apple keynote (2013)*, źródło: http://www.apple.com (dostęp: 16.04. 2017).

[25] Chytří pomocníci do škol – aplikacja dostępna w Appstore: *The History of Western Philosophy, The History of Western Ethics oraz The History of Western Theology*.

Farrington B., *Věda ve starém Řecku*, Brno, 1950.

Heideggera M. *Věda, technika a zamýšlení,* Praha 2004.

http://www.well.com

Isaacson W., *Inovátoři. Jak skupinka vynálezců, hackarů, géniu a nadšenců stvořila digitální revoluci*, Praha 2015.

Koepsell D. R., *The Ontology of Cyberspace,* New York 2000.

Kwaśnicka A., *Parafianew cyberprzestrzeni*, źródło: http://kosciol.wiara.pl (dostęp: 16.04.2017).

Platon, *Ion*, źródło: http://www.perseus.tufts.edu (dostęp: 16.04.2017).

Tatarkiewicz W., *Historia estetyki*, t.1, Wrocław 1962.

Tatarkiewicz W., *Historia filozofii*, t. I, Warszawa 2002.

Tillich P. J., *Die Technische Stadt als Symbol*, Stuttgart 1962.

**Przemysław Mikiewicz**

Uniwersytet Wrocławski

# Cyberbezpieczeństwo jako konstrukt w polskiej przestrzeni publicznej

Słowa kluczowe: bezpieczeństwo, cyberbezpieczeństwo, zagrożenie, strategia, polityka

Zasadniczym celem autora niniejszego tekstu jest refleksja nad obecnością kategorii cyberbezpieczeństwa w polskiej przestrzeni publicznej. Przestrzeń publiczna, w której odbywa się „obieg" idei, koncepcji i politycznych została na potrzeby tekstu ograniczona do opiniotwórczego oddziaływania centralnych instytucji państwowych oraz partii politycznych. W refleksjach poniższych pominięto idee cyberbezpieczeństwa zawartych w szeroko rozumianym dyskursie medialnym, ponieważ jest to zagadnienie odrębne, wymagające głębszych studiów. Takie założenia umożliwiły autorowi skoncentrowanie swych dociekań na instytucjach odpowiedzialnych za bezpośrednie konceptualne i rzeczowe kreowanie polityki państwa.

Z racji czasu, w zwłaszcza szczególnego charakteru momentu, w którym następuje zmiana polityczna w Polsce (2014-2015 r.) autor zdecydował się skoncentrować się na bieżącym stanie dyskursu, ze szczególnym uwzględnieniem wyborów 2015 r.

Odnosząc się do powyższego autor próbuje odpowiedzieć na następujące pytania:

1. W jakiej mierze w polskiej przestrzeni publicznej obecny jest termin cyberbezpieczeństwo"?
2. W jaki sposób polskie instytucje pojmują cyberbezpieczeństwo?
3. Jak pojęcie to sytuowane jest się w szerszym kontekście?
4. Jaki obraz świata wyłania się z dyskursu o cyberbezpieczeństwie?

Kilkuletnia obecność pojęcia cyberbezpieczeństwa w polskiej przestrzeni publicznej jest argumentem na rzecz wagi i znaczenia, jakie jest przypisywane temu pojęciu oraz potencjalnie bogatej treści, które ze sobą niesie. Z jednej strony jest to więc pojęcie względnie nowe, którego pojawienie się w dyskursie publicznym było odpowiedzią nie tylko na popularne w dyskursie publicznym nowe „wyzwania" ery informacyjnej, lecz zostało także wymuszone przez dokumenty instytucji międzynarodowych, które wprowadziły do dyskursu szeregu pojęć związanych z bezpieczeństwem w sieci. Z drugiej jednak strony w polskim myśleniu o cyberbezpieczeństwie trudno dostrzec jakiekolwiek elementy nowatorstwa czy oryginalności. Fakt ten przyznają sami twórcy dokumentów oficjalnych, w których kategoria ta zajmuje istotne miejsce. Doktryna Cyberbezpieczeństwa RP przyznaje, że punktem jej wyjścia była Strategia Bezpieczeństwa Cybernetycznego UE[1]. Tym samym umiejscowienie cyberbezpieczeństwa nie ma wyłącznie endogenicznego charakteru, lecz jest wywołane presją instytucjonalną otoczenia międzynarodowego.

O ile w przestrzeni instytucjonalnej państwa polskiego pojęcie cyberbezpieczeństwa jest obecne wprost lub w sposób opisowy, o tyle w dyskursie politycznym obecność ta ma charakter „szczątkowy", co w interesujący sposób kontrastuje z występowaniem tego terminu w oficjalnych dokumentach rangi państwowej. Spośród sześciu komitetów wyborczych, które zdołały wprowadzić swych kandydatów do Sejmu oraz jednego komitetu o znaczącym poparciu (lewica) w wyborach w dniu 25 października 2015 r., zaledwie w dokumentach trzech zauważona została problematyka cyberbezpieczeństwa. Fakt ten zdaje się potwierdzać, że obecność cyberbezpieczeństwa jest w znacznej mierze uwarunkowana instytucjonalną presją otoczenia międzynarodowego. Impulsy wewnętrzne zdają się nie wzbudzać tak istotnych potrzeb debaty politycznej w tej kwestii, jak zewnętrzne uwarunkowania.

## Obecność cyberbezpieczeństwa

Odwołanie do oficjalnych dokumentów strategicznych ukazuje obecność cyberbezpieczeństwa w myśleniu strategicznym. W tejże sferze najwyżej w hierarchii dokumentów strategicznych są usytuowane zwykle strategie bezpieczeństwa. W polskim przypadku aktualnie obowiązującym dokumentem jest Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, przyjęta w roku 2014 i zaakceptowana przez ówczesnego prezydenta Bronisława Komorowskiego. Dokument

[1] *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, źródło: http://en.bbn.gov.pl (dostęp: 09.08.2016), s. 7.

ten zastąpił poprzednią *Strategię*, pochodzącą z 2007 r. Jako jeden z celów strategicznych wymienionych w dokumencie wskazane zostało „zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni”[2]. Tym samym cyberbezpieczeństwo zostało umieszczone jako jeden z celów strategicznych, albo inaczej - jako jedno z zadań podstawowych w obszarze bezpieczeństwa państwa, ale bez użycia samego pojęcia.

Dokumentem o niższej randze, ale skoncentrowanym za to na zagadnieniach bezpieczeństwa w sieciach teleinformatycznych, jest *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*. Dokument ten powstał we współpracy Ministerstwa Administracji i Cyfryzacji z Agencją Bezpieczeństwa Wewnętrznego, a przyjęty został w 2013 także jako dokument o charakterze strategicznym. Opracowanie dokumentu nastąpiło w oparciu o *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia*, a także okresowe raporty o stanie bezpieczeństwa, publikowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL oraz decyzję Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji z dnia 24 stycznia 2012 r., dotyczącą powołania Zespołu zadaniowego do spraw ochrony portali rządowych[3].

*Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* jest dokumentem, w którym określone zostało umiejscowienie własne tekstu pośród dokumentów o charakterze strategicznym, „doprecyzowujacych kierunki działań wskazanych w strategiach, programach rozwoju i innych dokumentach programowych (...)”[4]. W tekście sformułowany został cel strategiczny, którym ma być „osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa”[5]. Podobnie zatem jak w Strategii Bezpieczeństwa Narodowego RP w omawianym dokumencie opisywane jest dążenie do celu, jakim ma być pożądany stan bezpieczeństwa w sieciach teleinformatycznych, lecz w tym celu nie posłużono się pojęciem „cyberbezpieczeństwa”.

Kolejnym dokumentem wnoszącym wkład do publicznych rozważań o bezpieczeństwie w sieciach jest *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, opublikowana w 2015 roku, a powstała w wyniku prac ekspertów w Biurze Bez-

[2] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej,* Warszawa 2014, źródło: https:// www.bbn.gov.pl (dostęp: 09.08.2016), s. 12.
[3] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, 2013, źródło: www.cert.gov.pl (dostęp: 09.08.2016), s.3.
[4] *Ibidem*, s. 4.
[5] *Ibidem*, s.6.

pieczeństwa Narodowego. Prace te odbywały się z udziałem przedstawicieli administracji publicznej, środowiska akademickiego, organizacji pozarządowych oraz sektora prywatnego. Według BBN Doktrynę należy traktować jako dokument, którego treścią jest „podstawa koncepcyjna, zapewniająca spójne i kompleksowe podejście do zagadnień cyberochrony i cyberobrony"[6]. Z uwagi na treść, skoncentrowaną na konkretnych zagadnieniach bezpieczeństwa teleinformatycznego, tekst tego dokumentu stanowi nowość w polskim systemie dokumentów strategicznych.

Tekst poprzedzony jest Wstępem napisanym przez ówczesnego prezydenta, Bronisława Komorowskiego. Prezydent stwierdza w nim wprost, że cyberprzestrzeń stała się nowym obszarem aktywności państwa; dlatego jednym z priorytetów polskiej strategii jest „bezpieczeństwo tego nowego środowiska"[7]. Jako strategiczny cel w obszarze cyberbezpieczeństwa stawia się - jak stwierdza dokument - „zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni"[8].

Osobną kategorię stanowią dokumenty powstałe w polskim życiu politycznym jako swoiste przejawy „polskiej myśli politycznej"[9]. Niewątpliwie partie polityczne stanowią istotną kategorię instytucji publicznych, zarówno ze względu na zdolność do kształtowania systemu prawnego, jak i możliwość podejmowania decyzji lub wpływu na decyzje. Z punktu widzenia partii politycznych rola idei w polityce jest oczywista: w programach i kampaniach wyborczych, politycy formułują przekaz mający na celu mobilizację polityczną i uzyskanie poparcia. Przekaz ten musi zatem zawierać kwestie, na które jest społeczne zapotrzebowanie. Czy jest zatem zapotrzebowanie na cyberbezpieczeństwo? Na potrzeby niniejszego tekstu przeanalizowano dokumenty partii stojących na czele swych komitetów wyborczych oraz koalicyjnych komitetów wyborczych, biorących udział w wyborach 2015 r.

Jedynie dwie partie i jedna koalicja wyborcza dostrzegły problemy cyberprzestrzeni w swoich programach przygotowanych do wyborów parlamentarnych w 2015 r. Ze względu na czysto hasłowy wymiar zawartych tam stwierdzeń, treść

[6] B. Komorowski, *Słowo wstępne Prezydenta Rzeczypospolitej Polskiej*, [w:] *Doktryna Cyberbezpieczeństwa...*, s. 5.
[7] *Ibidem*, s. 4.
[8] *Doktryna Cyberbezpieczeństwa...*, s. 9.
[9] Oczywiście mówienie lub pisanie o „polskiej myśli politycznej" w dziedzinie cyberbezpieczeństwa może mieć charakter jedynie ironiczny.

tych wypowiedzi zostanie zanalizowana niżej w powiązaniu z kontekstami cyberbezpieczeństwa.

## Konteksty cyberbezpieczeństwa

Wyżej wskazane zostały dokumenty, w których pojawia się kategoria cyberbezpieczeństwa lub w których kategoria ta ma swoje nienazwane odpowiedniki. Obecnie przedstawione zostaną konteksty, w których w polskim dyskursie publicznym występuje ta kategoria.

Jak zaznaczono już wyżej, w 2014 r. ówczesny prezydent Bronisław Komorowski zaakceptował Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Odnosząc się do strategii obronnych w tekście wskazano potrzebę rozwijania zdolności do działań zarówno defensywnych, jak i ofensywnych. W *Strategii* uznano za działania istotne dla bezpieczeństwa współpracę i koordynację działań z sektorem prywatnym, a także działania prewencyjne i profilaktyczne w odniesieniu do cyberprzestrzeni. Uznano za ważne rozpoznawanie i zapobieganie przestępstwom dokonywanym w cyberprzestrzeni, a także ściganie sprawców tychże przestępstw oraz prowadzenie walki informacyjnej, łącznie z sojuszniczą współpracą, skonkretyzowaną w formie wymiany doświadczeń i dobrych praktyk[10]. Dążenie do cyberbezpieczeństwa nabrało zatem w literze dokumentu charakteru swoistej strategii „wielowymiarowej" - od działań na rzecz walki z przestępczością aż po kooperację w ramach układów sojuszniczych.

Międzynarodowy aspekt cyberbezpieczeństwa wspomniany jest w *Strategii* w tych fragmentach dokumentu, w których jest mowa o środowisku bezpieczeństwa Polski. To środowisko nabiera - według tekstu - również globalnego charakteru, przede wszystkim dzięki postępowi technologicznemu. Istotne znaczenie posiada fakt zachodzenia zmian, zarówno w technologiach informatycznych, jak i w samych sieciach teleinformatycznych. W tym kontekście w dokumencie stwierdza się, że w technologiach informatycznych i w samej sieci Internet ujawniają się nowe zagrożenia, pośród których wymienia się: „cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych i cyberwojna"[11], rozumiana, jako konfrontacja w cyberprzestrzeni między państwami. Strategia jednoznacznie stwierdza, że współczesne trendy wskazują na wzrost znaczenia bezpieczeństwa sfery cyfrowej na ogólny poziom bezpieczeństwa

[10] *Strategia Bezpieczeństwa...,* s. 12.
[11] *Ibidem*, s. 19.

państwa. Rosnące uzależnienie od technologii teleinformatycznych sprawia, że konflikty w cyberprzestrzeni mogą „poważnie zakłócić funkcjonowanie społeczeństw i państw”[12].

Uzależnienie od technologii cyfrowej nakłada na państwa - według Strategii - rosnącą odpowiedzialność zapewnienie bezpieczeństwa w cyberprzestrzeni. Dokument wskazuje na politykę organizacji międzynarodowych oraz struktur współpracy, w ramach których działa również Polska. Wspomina się w dokumencie także o współpracy bilateralnej z niektórymi państwami, a szczególnie - członkami Unii Europejskiej i Paktu Północnoatlantyckiego[13].

Dla twórców *Strategii* kwestią oczywistą jest to, iż bezpieczne funkcjonowanie systemu teleinformatycznego staje się warunkiem sprawnego działania państwa. W tym kluczowe wydaje się zapewnienie „dostępności, integralności i poufności danych”, które są przetwarzane przez systemy teleinformatyczne działające w administracji publicznej. Wedle autorów Strategii istotne znaczenie z punktu widzenia bezpieczeństwa ma niewystarczającą wiedza użytkowników o zagrożeniach występujących w cyberprzestrzeni. Zauważa się także istnienie „dylematu” ujawniającego się pomiędzy wolnością osobistą, ochroną praw jednostki a środkami stosowanymi w celu ochrony bezpieczeństwa państwa[14]. Uznano również rolę podsystemów ochronnych, które jako dostosowane do strategii „operacyjnej”, mają za cel rozwój „organizacyjny”, „techniczny”, „szkoleniowy” służb, straży, instytucji odpowiedzialnych za ochronę ludności, porządek publiczny i zarządzanie kryzysowe, a także odpowiadających za swobodę korzystania z praw i wolności obywatelskich[15].

*Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* jest dokumentem z 2013 r. Już we wprowadzającym rozdziale dokumentu pojawia się ukierunkowująca światopoglądowo treść. Bezpieczeństwo w cyberprzestrzeni powiązano z procesami globalizacji i stwierdzono, że dzięki niej bezpieczeństwo cyberprzestrzeni uznać należy, wedle autorów tekstu, za jeden z podstawowych celów w polityce bezpieczeństwa każdego państwa. Zwrócono też uwagę na kwestię swobody przepływu informacji. Stwierdzono, że państwa demokratyczne muszą posiadać odpowiednie mechanizmy umożliwiające zwalczanie zagrożeń w cyberprzestrzeni[16].

[12] *Ibidem*, s. 19.
[13] *Ibidem*, s. 23.
[14] *Ibidem*, s. 25.
[15] *Ibidem*, s. 48.
[16] Polityka Ochrony..., s. 4.

W dokumencie wskazano na zgodność treści z celami zawartymi różnych dokumentach: *Europejskiej Agendzie Cyfrowej Rady Europejskiej* [*KOM(2010)245*], *Strategii Rozwoju Społeczeństwa Informacyjnego*, *Strategii Bezpieczeństwa Narodowego, Średniookresowej Strategii Rozwoju Kraju, Strategii „Europa 2020"* i *Strategii Sprawne Państwo*[17]. Następnie poprzez wyliczenie wskazano „cele szczegółowe": „zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej Państwa", „zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni" i „zmniejszenie skutków incydentów godzących w bezpieczeństwo teleinformatyczne*"* itd.[18]

*Politykę Ochrony Cyberprzestrzeni RP* postanowiono zaadresować do użytkowników cyberprzestrzeni w obrębie Polski i poza terytorium kraju tam, gdzie znajdują się przedstawicielstwa i kontyngenty wojskowe. W tekście dokumentu pada stwierdzenie, że Polityka obowiązuje administrację rządową i jest rekomendowana dla administracji samorządowej oraz innych urzędów. Dla innych użytkowników cyberprzestrzeni, nie wymienionych w tekście Polityki, dokument ma stanowić wskazówkę do dalszych działań[19].

Z dokumencie stwierdza się, że rząd dostrzega konieczność zapewnienia bezpieczeństwa infrastruktury teleinformatycznej Państwa. Enigmatycznie głosi się w tekście wyznaczenie „minimalnego standardu bezpieczeństwa wewnętrznego", którego utrzymanie miałoby zapewnić realizację zadań państwa[20]. W dalszym wywodzie poświęca się uwagę bezpieczeństwu portali administracji rządowej jako środka wymiany informacji między instytucjami a obywatelem w „e-społeczeństwie". Ogłoszono, że strony administracji rządowej powinny spełniać wymagania bezpieczeństwa, a zwłaszcza wyszczególnione jako: „dostępność, integralność i poufność danych"[21]. Z wymogu zapewnienia bezpieczeństwa wynika, że jednostki organizacyjne administracji powinny prowadzić szacunki ryzyka dla swoich witryn, na podstawie których będzie można zastosować odpowiednie rozwiązania „organizacyjno-technologiczne. Za tworzenie rozwiązań właściwą instytucją ma być odpowiedzialny Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL[22].

Szczególną konsekwencją publikacji *Polityki Ochrony Cyberprzestrzeni* było pojawienie się ograniczonej debaty publicznej, wynikającej z kontrowersji, jakie ze

[17] *Ibidem*, s. 6.
[18] *Ibidem*, s. 4.
[19] *Ibidem*, s.7.
[20] *Ibidem*, s.9.
[21] *Ibidem*, s. 11.
[22] *Ibidem*, s. 10-11.

sobą niosły treści w niej zawarte. Dokument poddany został bowiem krytyce ze strony Najwyższej Izby Kontroli, która w raporcie zatytułowanym *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP* stwierdziła, że dokument cechuje się nierzetelnością i brakiem odpowiedniego przygotowania[23]. Krytyka jednak na tym się nie wyczerpała: krytyczne stanowisko wobec *Polityki Ochrony Cyberprzrestrzeni* zajęły instytucje społeczeństwa obywatelskiego. Stowarzyszenie Euro-Atlantyckie, Fundacja Bezpieczna-Cyberprzestrzeń i Instytut Mikromakro opublikowały wspólne stanowisko, które zawarte zostało w dokumencie zatytułowanym *Komentarz do projektu „Polityka Ochrony Cyberprzestrzeni RP".* Zdaniem autorów wspólnego stanowiska *Polityka Ochrony Cyberprzestrzeni* niewłaściwe jest ograniczenie zakresu obowiązywania dokumentu do administracji rządowej i sfery publicznej, a w dokumencie widoczne jest „zamieszanie terminologiczne" i błędy merytoryczne[24].

Kolejnym dokumentem dotyczącym problematyki cyberbezpieczeństwa jest *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, która została opublikowana w 2015 roku. We Wprowadzeniu do tekst *Doktryny* pojawiają się rozważania ogólnej natury przemian w dziedzinie bezpieczeństwa. W dokumencie stwierdza się mianowicie, że bezpieczeństwo zyskało „dodatkowy wymiar", co ma oznaczać, że cyberprzestrzeń istnieje obok „lądu, wody, powietrza i przestrzeni kosmicznej" jako ten dodatkowy „wymiar". W różnych sferach, militarnych czy pozamilitarnych, wewnętrznych czy zewnętrznych, przejawia się współczesne bezpieczeństwo. Dostrzega się także w dokumencie wagę kwestii politycznych, albowiem działania w cyberprzestrzeni muszą uwzględniać prawa człowieka i obywatela, poszanowanie prywatności i wolności słowa, a środki służące urzeczywistnieniu bezpieczeństwa musza wykazywać się proporcjonalnością w stosunku do zagrożeń i być oparte na odpowiednio przeprowadzonej analizie ryzyka[25].

Z punktu widzenia kontekstów, w których osadzone jest cyberbezpieczeństo, istotną treść zawiera rozdział drugi, w którym opisana jest kwestia środowiska cyberbezpieczeństwa. Opis zagrożeń zaczyna się od środowiska wewnętrznego państwa. W jego ramach wymieniono takie zjawiska jak: „cyberprzemoc, cyberprzestępczość, cyberprotesty czy cyberdemonstracje o charakterze destrukcyjnym"[26].

[23] *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP,* Warszawa 2015, źródło: https://www.nik.gov.pl (dostęp: 09.08.2016), s. 35-37.
[24] *Komentarz do projektu* „Polityka Ochrony Cyberprzestrzeni RP", Warszawa 2012, źródło: https://www.cybsecurity.org (dostęp: 09.08.2016) s. 2, 4, 6.
[25] *Doktryna Cyberbezpieczeństwa*..., s. 5.
[26] *Ibidem*, s. 10.

W omawianym dokumencie uznaje się za szczególnie istotne zagrożenia w cyberprzestrzeni odnoszące się do zależnej od systemów teleinformatycznych infrastruktury krytycznej państwa. W tym obszarze postrzega się celowe ataki na systemy komunikacji jako „nadzwyczaj niebezpieczne dla państwa"[27].

Osobno dokument traktuje zagrożenia zewnętrzne, wśród których *Doktryna* wymienia „cyberkryzysy i „cyberkonflikty", „cyberwojny", jako potencjalne elementy wojen hybrydowych, zarówno z udziałem podmiotów państwowych jak i niepaństwowych. Osobno traktuje się „cyberszpiegostwo", zagrożenia ze strony ekstremizmów i terroryzmu w sieciach teleinformatycznych[28]. Dostrzega się też zagrożenia na poziomie międzynarodowym, co wymaga uczestnictwa w międzynarodowym reagowaniu na cyberzagrożenia w ramach instytucji międzynarodowych (wykorzystanie potencjału wynikającego z członkostwa Polski w NATO i UE). Podkreśla się znaczenie wymiany doświadczeń i dobrych praktyk na arenie międzynarodowej oraz działań w sferze transnarodowej (struktury sektora prywatnego). Wymienia się też rolę sektora obywatelskiego i prywatnego, zwłaszcza w dziedzinie międzynarodowej wymiany informacji o podatnościach, zagrożeniach, i incydentach[29].

## Partie polityczne i komitety wyborcze wobec cyberbezpieczeństwa

Osobną kategorię tworzą partie polityczne i komitety wyborcze, powołane do realizacji zadań wyborczych. W wyborach 2015 r. wśród znaczących partii i komitetów wyborczych jedynie dwie partie i jedna koalicja wyborcza dostrzegły problemy cyberprzestrzeni w swoich programach przygotowanych do wyborów parlamentarnych. Na potrzeby analizy autor zastosował parlamentarne (z jednym wyjątkiem), biorąc pod uwagę jedynie sześć komitetów wyborczych, które wprowadziły swych reprezentantów do Sejmu w wyniku wyborów 2015 r. W analizie autor uwzględnił także Koalicyjny Komitet Wyborczy Zjednoczona Lewica (SLD+TR+PPS+UP+Zieloni) ze względu na skalę poparcia (7,55% oddanych głosów) oraz historyczne znaczenie partii wchodzących w jego skład, chociaż komitet ten nie uzyskał wymaganego poparcia (8%), by wprowadzić swych reprezentantów do Sejmu RP[30]. Wyniki te pozwalają na dość jasne konkluzje.

[27] *Ibidem*, s.10.
[28] *Ibidem*, s. 13.
[29] *Ibidem*, 13-15.
[30] *Wyniki wyborów do Sejmu RP*, źródło: http://parlament2015.pkw.gov.pl (dostęp: 09.08.2016).

Program partii Prawo i Sprawiedliwość pod nazwą *Program Prawa i Sprawiedliwości 2014* został ogłoszony w 2014 roku. Problematyka powiązana z cyberbezpieczeństwem została uwzględniona w *Programie* w niewielkim stopniu, lecz w klarownym kontekście obrony i zagadnień bezpieczeństwa międzynarodowego. W programie zakłada się, że Polska winna dążyć do tego, aby Sojusz Północnoatlantycki po zakończeniu misji w Afganistanie skoncentrował się na problemach wewnętrznych państw członkowskich. Za szczególnie istotne uznano działania zmierzające do umocnienia „integralności terytorialnej państw członkowskich we wszystkich współczesnych aspektach zagrożeń dla niej, także w wymiarze cyberbezpieczeństwa"[31]. Cyberbezpieczeństwo przewija się także w materiałach z konferencji programowej PiS, która odbyła się w lipcu 2015 r., które wspomniane jest tam w kontekście informatyzacji i cyfryzacji kraju[32].

Nie mniej zdawkowo potraktowany został problem u konkurentów politycznych. Program polityczny Platformy Obywatelskiej zatytułowany *Polska Przyszłości* został opublikowany w 2015 r. W programie tym uwzględniono bezpieczeństwo cybernetyczne, ale znalazło się ono wśród strategicznych priorytetów bezpieczeństwa wewnętrznego. Platforma wyraziła tym samym potrzebę zagwarantowania przez państwo funkcjonowania krytycznych - z punktu widzenia państwa i obywateli - systemów, wystawionych na „poważne zagrożenia cybernetyczne"[33].

Trzeci przypadek obecności w polskich programach poltycznych treści dotyczących cyberbezpieczeństwa znaleźć można w dokumencie lewicy, nieobecnej od 2015 r. w Sejmie. Program wyborczy Zjednoczonej Lewicy opracowany z myślą o wyborach parlamentarnych 2015 r. pod nazwą *Program wyborczy - Zjednoczona Lewica*. Jeden z rozdziałów 23-stronicowego Programu został zatytułowany *Bezpieczeństwo państwa i obywatela*. W dość standardowy sposób wskazano w nim wiele problemów z zakresu współczesnego bezpieczeństwa. Wśród różnych kwestii (Policja, sądownictwo, służby specjalne, siły zbrojne, sojusze) wskazany został postulat „przygotowania państwa do ochrony przed cyberatakami"[34]. W dokumencie wymienia się kilka państw (Stany Zjednoczone, Japonia, Niemcy, Wielka Brytania, Izrael, Arabia Saudyjska), które utworzyły specjalne struktury wojskowe, skoncentrowane na ochronie państwa przed cyberatakami.

[31] *Program Prawa i Sprawiedliwości 2014,* źródło: http://pis.org.pl (dostęp: 09.08.2016), s.167.
[32] *Myśląc Polska,* 2015, źródło: http:// pis.org.pl (dostęp: 09.08.2016), s. 23.
[33] *Polska Przyszłości* 2015, źródło: http://wybory.platforma.org (dostęp: 09.08.2016), s. 76.
[34] *Program wyborczy - Zjednoczona Lewica 2015,* źródło: http://lewicarazem.org (dostęp: 09.08.2016), s.46.

## Wnioski

Cyberbezpieczeństwo obecne jest w polskiej przestrzeni publicznej dwojako: szeroko wspominane w ogólnikowy sposób w dokumentach rządowych o znaczeniu strategicznym i obecne w szczątkowej postaci w dokumentach partii politycznych i komitetów wyborczych. W obu jednak przypadkach cyberbezpieczeństwo jest sytuowane w szerszym kontekście zagrożeń współczesnego świata, nierzadko w „sąsiedztwie" problematyki zagrożeń militarnych. Wspomina się bowiem o cyberbezpieczeństwie jako swoistej „części" składowej ogólnie pojmowanego bezpieczeństwa, kojarzonego z obroną przed zagrożeniami zewnętrznymi, co z kolei nasuwa skojarzenia o charakterze przede wszystkim militarnym. Wspomniany już program program Zjednoczonej Lewicy twierdzi, że wiele państw „stworzyło specjalne wojskowe struktury do obrony państwa przed cyberatakami"[35].

Program PiS sytuuje z kolei zagrożenia w cyberprzestrzeni w kontekście zadań NATO, które winno skupić się na obronie integralności terytorialnej - w tym kontekście pisze się o współczesnych aspektach zagrożeń - także w obszarze cyberbezpieczeństwa[36] (Program PiS, s. 162). Inaczej jest w Programie wyborczym PO, który sytuuje cyberbezpieczeństwo w kontekście standardowych problemów bezpieczeństwa wewnętrznego państwa.

Analiza obecności i kontekstów polskiej debaty nad cyberbezpieczeństwem pozwala na sformułowanie czterech końcowych wniosków:

1. W polskiej przestrzeni publicznej dokumenty strategiczne szeroko, chociaż powierzchownie omawiają zagadnienia z zakresu cyberbezpieczeństwa, ale partie polityczne traktują zagadnienie jako niewarte uwagi lub marginalne.
2. Cyberbezpieczeństwo jest umiejscawiane w kontekście zagrożeń tradycyjnych, kojarzonych z instytucjami siłowymi - wojskiem lub policją.
3. Cyberbezpieczeństwo jako kategoria jest konceptem zapożyczonym z zewnątrz (lub rozwijanym pod presją instytucji międzynarodowych), o którym należy pisać i mówić, bo jest to wymóg instytucjonalny, ale które nie daje podstaw do trwałego wytwarzania kapitału politycznego, zdolnego do mobilizacji wyborczej.

[35] *Ibidem*.
[36] *Program Prawa i Sprawiedliwości*..., 162.

4. Cyberbezpieczeństwo jest rodzajem konstruktu, a przy tym swoistego obrazu świata współczesnego, wypełnionego nienamacalnymi oraz nieuchwytnymi zagrożeniami, których zwalczanie - zgodnie z logiką zawartą w urzędowych strategiach - wymaga publikowania dokumentów pod postacią kolejnych doktryn i strategii walki z zagrożeniami w cyberprzrestrzeni.

## Bibliografia

*Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, źródło: http://en.bbn.gov.pl (dostęp: 09.08.2016).

*Komentarz do projektu „Polityka Ochrony Cyberprzestrzeni RP"*, Warszawa 2012, źródło: https://www.cybsecurity.org (dostęp: 09.08.2016).

Komorowski B., *Słowo wstępne Prezydenta Rzeczypospolitej Polskiej*, [w:] *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, źródło: http:// en.bbn.gov.pl (dostęp: 09.08.2016).

*Myśląc Polska,* 2015, źródło: http:// pis.org.pl (dostęp: 09.08.2016).

*Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, 2013, źródło: www. cert.gov.pl (dostęp: 09.08.2016).

*Polska Przyszłości* 2015, źródło: http://wybory.platforma.org (dostęp: 09.08. 2016).

*Program Prawa i Sprawiedliwości 2014,* źródło: http://pis.org.pl (dostęp: 09.08. 2016).

*Program wyborczy - Zjednoczona Lewica 2015,* źródło: http://lewicarazem.org (dostęp: 09.08.2016).

*Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP,* Warszawa 2015, źródło: https://www.nik.gov.pl (dostęp: 09.08.2016).

*Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej,* Warszawa 2014, źródło: https://www.bbn.gov.pl (dostęp: 09.08.2016).

*Wyniki wyborów do Sejmu RP*, źródło: http://parlament2015.pkw.gov.pl (dostęp: 09.08.2016).

Grzegorz Tokarz

Uniwersytet Wrocławski

# Internet jako instrument nawoływania do przemocy – przykład organizacji „Krew i Honor" Polska

Słowa kluczowe: internet, przemoc, rasizm, narodowy socjalizm.

Organizacja „Krew i Honor" powstała w 1987 r., założył ją Anglik, Ian Stuart Donaldson, muzyk związany z nurtem White Power. Była to klasyczna struktura odwołująca się do idei narodowego socjalizmu, jej celem było po pierwsze: zjednoczenie białej młodzieży, po drugie: propagowanie tzw. białej siły[1].

Wspomnieć należy o brytyjskiej organizacji COMBAT 18, która została powołana do życia przez członków „Krwi i Honoru", była to konsekwencja porozumienia między nimi a Brytyjską Partią Narodową oraz kibicami klubu piłkarskiego Chelsea. Miało to być swoistego rodzaju zbrojne ramię zwolenników ruchu narodowo-socjalistycznego. Cyfra 18 odwołuje się do urodzin Adolfa Hitlera, pierwsza litera alfabetu A i ósma H[2].

Podkreślić należy, że na głównej stronie internetowej polskiej wersji „Krwi i Honoru", obydwa słowa dzieli znak graficzny Combat 18[3].

[1] Cyt. za J. Tomasiewicz, *Combat 18-terroryści czy chuligani ?*, źródło: http://www.terroryzm.com (dostęp: 10.08.2016).

[2] *Ibidem*, por. *Combat 18 - co to za organizacja*, źródło: http://lublin.com.pl (dostęp: 13.08.2016).

[3] *Strona główna*, źródło: http://www.bhpoland.orgia (dostęp: 10.08. 2016).

Organizacja „Krew i Honor" znalazła się w centrum zainteresowania polskich sił bezpieczeństwa. W 2014 policja wkroczyła do kilkudziesięciu lokali (w sumie 55 adresów). Jednak w wyniku tej akcji nikt nie został zatrzymany, skonfiskowano natomiast narodowo-socjalistyczne materiały propagandowe. W następnym roku funkcjonariusze Centralnego Biura Śledczego zatrzymali 13 osób, podejrzewano, że działali w ramach grupy przestępczej, oskarżono ich między innymi o wytwarzanie i posiadanie ładunków wybuchowych[4].

Wspomnieć należy, że w 2006 r. w Polsce zatrzymano mężczyznę, który administrował polską stroną internetową organizacji „Krew i Honor". Wśród zarzutów, jakie mu postawiono było uczestnictwo w grupie przestępczej oraz nawoływanie do nienawiści o charakterze rasowym. Co ciekawe, wiekowo nie należał do osób, które można określić jako podatne na indoktrynację, liczył sobie 31 lat. Do jego obowiązków należało między innymi wprowadzanie nowych danych na stronę Redwatch Polska. Inny administrator, również w tym samym roku zatrzymany miał 36 lat [5].

Funkcjonariusze polskich sił porządkowych próbowali doprowadzić do zamknięcia strony internetowej „Krew i Honor". Problemem było to, że witryna była umieszczona na amerykańskim serwerze. W 2006 r. strona polska zwróciła się do tamtejszych władz o jej zamknięcie, na co one zresztą przystały[6].

Jednak powyższa próba niewiele dała, strona nadal funkcjonuje, co więcej, pojawiają się na niej liczne aktualizacje.

Na swojej stronie umieszczają również artykuły z wydawanego, również w języku polskim, pisma „Stormer"[7].

Polscy narodowi socjaliści w sposób jednoznaczny identyfikują zagrożenie, jest nim tzw. Zionist Occupation Government, co można przetłumaczyć jako Syjonistyczny Rząd Okupacyjny. Zdaniem członków „Krew i Honor" biała rasa jest rządzona przez zdrajców i osoby, które podporządkowane są nacjonalistom żydowskim. W tym kontekście wspomnieć należy o tym, iż rządzący wywodzą się z międzynarodowej finansjery. Głównym celem okupantów jest po pierwsze: prowadzenie tyrańskiej polityki wobec narodów, likwidacja współzawodnictwa pomiędzy

[4] *Propagowali rasizm, totalitaryzm. Krzyczeli krew i honor. Policja rozbiła gang*, źródło: http://www.newsweek.pl (dostęp: 11.08. 2016).

[5] *Strona „Krew i Honor" zamknięta*, źródło: http://www. policja.pl (dostęp: 13.08.2016), por. *Krew i Honor*, źródło: http://www.hacking.pl (dostęp: 10.08.2016); D. Kulbaka, *Strona „Krew i Honor" została zamknięta*, źródło: http://webinside.pl (dostęp: 18.08.2016).

[6] *Strona „Krew i …*

[7] *Stormer*, źródło: http://www.bhpoland.org (dostęp:18.08.2016).

poszczególnymi nacjami, homogenizacja kulturowa, stworzenie społeczeństwa, które „nie myśli". Wszystko to doprowadzi do osłabienia białych, a tym samym ułatwi rządzenie nimi. Jako przykład rządu, podporządkowanego ZOG wymieniano np. gabinet brytyjskiego premiera Tony Blaira. Niestety, biali ludzie w większości już nie dostrzegają nie tylko zagrożenia, ale sami prowadzą destrukcyjne dla siebie działania. Zdaniem zwolenników ruchu „Krew i Honor" współczesne warunki, wymagają podjęcia innych działań, niż miało to miejsce w latach trzydziestych XX wieku w Europie. Nie zdołano wtedy ochronić białej rasy, przegrano jeden z etapów konfliktu. Teraz należy podjąć inne kroki, po pierwsze: należy się przegrupować, po drugie: znaleźć się w podziemiu, po trzecie: przygotować się do kontrofensywy[8].

Zwolennicy „Krwi i Honoru" uzasadniają swoje twierdzenie, że ludy aryjskie ukazały swoją wyższość nad innymi rasami. Przejawem tego był podbój nie tylko kontynentu europejskiego, ale również stworzenie cywilizacji, które trwały tysiące lat. Można w tym kontekście mówić o wynalazkach czy sztuce, żadne inne rasy nie mogą się z tymi osiągnięciami równać. O tym, czy biali ludzie przetrwają zdecyduje siła – impet. Sytuacja białej rasy jest obecnie dramatyczna, jedynym ratunkiem jest ogólnorasowy zryw. Należy za pomocą broni odzyskać honor, ziemię i możliwość ewolucji. Stwierdzają, że słabe przestanie istnieć, rządzić zaś będą silni[9].

Osoby związane z polską sekcją „Krew i Honor" w sposób szczegółowy opisują, jaki charakter powinna mieć ich aktywność. Pierwszy podział, który wprowadzają to działalność jawna i niejawna. Ta pierwsza, zakładająca działanie w ramach obowiązującego systemu – prawa, jest akceptowalna, ale jednocześnie najmniej ceniona. Wynika to z kilku przyczyn, przede wszystkim aktywność ta nie jest wystarczająco skuteczna, polega głównie na działalności propagandowej, takiej jak między innymi wydawanie czy rozpowszechnianie ulotek. Negatywnym aspektem jest to, że służby, broniące zastanego systemu, będą mogły rozpracować jego przeciwników, zrobić im zdjęcia itp. Z tego też względu najefektywniejszym działaniem jest aktywność niejawna. Można ją prowadzić na płaszczyźnie bezpośredniej, politycznej i społecznej. Najbardziej cenione są te pierwsze, których celem jest zakłócenie i eliminacja tego, co jest niezgodne z interesem białego człowieka i znajduje w opozycji do idei narodowego socjalizmu. Jednak wymaga to szczególnego typu działań, w tym kontekście pisze się o metodzie „samotnego wilka". Przede wszyst-

[8] *Czym jest ZOG?*, źródło: http://www.bhpoland.org (dostęp:17.08.2016).
[9] *NS-Uniwersalny System Ludzkości*, źródło: http://www.bhpoland.org (dostęp: 10.08.2016).

kim łatwo uniknąć wykrycia przez służby, gdyż nie utrzymuje się kontaktu z innymi wrogami systemu, tym samym wiedza o działaniach i poglądach jednostki pozostanie ukryta. Jednocześnie taki działacz nie jest zależny od pomocy innych, a liczyć może, co jest kolejnym pozytywem, tylko na siebie i bezpieczeństwo zależy od niego samego. Akcje prowadzone w sposób bezpośredni są określane jako najbardziej odważne i bohaterskie. Podkreślić jednak należy, że zwolennicy „Krwi i Honoru" dopuszczają również działanie w ramach niewielkiej komórki, składającej się z kilku osób. Kwestią podstawową jest zaufanie, poszczególni członkowie powinni ufać innym tak samo, jak samym sobie. Kolejna płaszczyzna ma charakter polityczny. Należy zdobywać zwolenników dla idei narodowego socjalizmu, można to robić wchodząc w skład różnych organizacji narodowych. Jednak należy utrzymać swoje poglądy narodowosocjalistyczne w dyskrecji i w sposób konfidencjonalny przekonywać poszczególnych członków obozu narodowego do własnych idei. Szczególnie ważną działalnością, wymagającą jednak odpowiednich umiejętności, jest wchodzenie w struktury lewicowe, czy inne, wrogie koncepcjom narodowego socjalizmu. Należy oczywiście ukryć prawdziwe swoje poglądy i jednocześnie zdobywać informacje na temat wroga i sposobów jego działania. Powinno się także w odpowiedni sposób destabilizować od wewnątrz te organizacje. Ostatnia płaszczyzną działania jest aktywność społeczna. W tym kontekście wymienić można pracę nauczyciela, zwolennik narodowego socjalizmu, pracując w jednostce edukacyjnej, powinien ukrywać swoje poglądy, jednak w czasie lekcji w sposób „ukryty", „zawoalowany", zręczny" promować swoje idee. Przecież gdyby nauczyciel nie krył idei w których partycypuje, wtedy utraciłby pracę. Ponadto, należy pełnić ważne role w systemie, można pomagać w sposób tajny ruchowi narodowo-socjalistycznemu, zarówno służąc swoją pozycją, finansami i umiejętnościami. Trzeba także długofalowo infiltrować struktury społeczne, które konstytuują wrogi system, atakować go porozumiewając się z „samotnymi wilkami" czy komórkami, które prowadzą akcję bezpośrednią. Nie należy także zapominać o potrzebie kreowania małych błędów w systemie, które nawarstwiając się, będą przynosić wymierne szkody dla obozu wroga[10].

Na stronie internetowej „Krwi i Honoru" znaleźć można tzw. Prawa Samotnego Wilka. Jest to kolejny już zbiór zasad, jakich powinni przestrzegać członkowie ruchu narodowo-socjalistycznego, podejmującego walkę z systemem. Przede wszystkim wskazuje się, że każdy człowiek może zostać samotnym wilkiem, opór powinien być sposobem na życie bojownika. Nie należy nikomu, nawet osobom

[10] *Działalność niejawna*, źródło: http://www.bhpoland.org (dostęp: 13.08.2016).

z organizacji o podobnej proweniencji wspominać o swojej działalności. Szczególnie ważną radą jest to, aby bojownik miał zaoszczędzone fundusze, które mogą mu się przydać, kiedy zagrozi mu np. dekonspiracja. Należy również zorganizować sobie, w przypadku tzw. wpadki nowy dowód tożsamości. Apeluje się o nie nawiązywanie żadnej współpracy z agentami lub reprezentantami ZOG. Konsekwencją jest wykluczenie z Ruchu. Co ciekawe, jeśli „samotny wilk" posiadał kontakty z konfidentem, może spotkać go surowsza, niż wydalenie, kara, przy czym nie określa się, co nią może być[11].

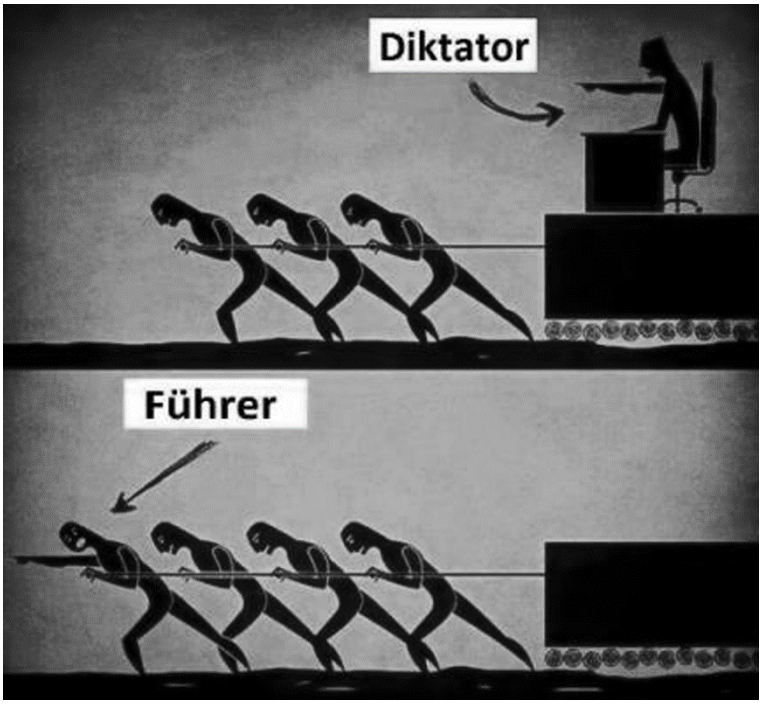
Interesujące wydają się rady, jakie można znaleźć dla zwolenników „Krwi i Honoru" na ich polskiej stronie internetowej, odnoszące się do sytuacji, kiedy brakuje dowódcy. Określa się je jako „Opór Bez Przywódcy". Znaleźć tam można takie stwierdzenie, iż działacz odwołujący się do idei narodowego socjalizmu jest „politycznym żołnierzem", przy czym jego walka będzie trwać, biorąc pod uwagę siłę wrogiego systemu, bardzo długo. Owszem, walczy się z wieloma rasami, jednak pamiętać należy, że większość wrogów ma białą skórę. Należy stosować podstępy, udając że można osiągnąć sukces bez przemocy, ale także że tę ostatnią należy wykorzystywać. Jednocześnie wyraźnie się podkreśla, że obrona nie jest najlepszym rozwiązaniem, aby wygrać wojnę, nigdy zresztą nie było takiego przypadku w historii, należy atakować. Wśród innych wskazań znaleźć możemy „koniec robi usprawiedliwienia, ale tylko wtedy, gdy wygasły wszystkie zagrożenia, nie ufaj kompletnie nikomu, miej uszy i oczy otwarte na wszystkich jak to tylko możliwe, zebranie grupy dla samotnych wilków jest jak samotny pływak w rzece piranii, rób akcje warte ceny, jeśli ktoś kiedyś zawiedzie nie spełniając tych reguł, nigdy nie dawaj mu drugiej szansy. Jeśli zdradzą Twoje zaufanie raz, zrobią to z pewnością po raz kolejny"[12].

Podkreślają znaczenie wodzostwa w swojej ideologii. Najlepszym wzorcem, do którego się na swoich stronach odwołują jest Adolf Hitler. Starają się go ukazać jako najwybitniejszego osobnika reprezentującego rasę aryjską (piszą, że był umysłem wszechczasów). Wymieniają wiele argumentów, które mają o tym świadczyć. Pogrupować je można następująco – A. Hitler jako polityk: wymieni się w tym kontekście walkę z komunizmem, oddanie (zdaniem zwolenników „Krwi i Honoru") władzy narodowi niemieckiemu, prawo do głosowania dla kobiet w czasie trwania II wojny światowej - Führer jako reformator gospodarczy: czyli promowanie rozwoju innych źródeł energii, dbanie o ochronę środowiska, finansowanie

[11] T. Metzger, *Prawa Samotnego Wilka*, źródło: http://www.bhpoland.org (dostęp:10.08.2016).
[12] *Opór Bez Przywódcy*, źródło: http://www.bhpoland.org (dostęp: 13.08.2016).

technologii rakietowych, rozbudowa przemysłu samochodowego i infrastruktury drogowej – wódz III Rzeszy jako aktywista społeczny: urlopy macierzyńskie dla kobiet, płatne wakacje fundowane robotnikom, święto 1 maja – Szef NSDAP jako humanista: kochający sztukę artysta, przeciwnik eksperymentów prowadzonych na zwierzętach[13].

Przy czym nie należy władzy, jaką sprawował A. Hitler, czy inny przywódca odwołujący się do idei narodowo-socjalistycznej utożsamiać np. z dyktaturą czy tyranią. W tym przypadku posługują się atrakcyjnymi (ich zdaniem) rysunkami. Poniżej przedstawiony jest jeden z nich:




Źródło: http://www.bhpoland.org (dostęp: 13.08.2016).

Jedną z ważniejszych akcji, jaką podjęło środowisko związane z „Krwią i Honorem" była Inicjatywa Redwatch. Nie narodziła się w Polsce, wcześniej zainicjowana została przez narodowych socjalistów w Wielkiej Brytanii i Niemczech. Polscy aktywiści, wprowadzając ją do III Rzeczpospolitej dwojako argumentują, mającą uzasadnić ich działania. Po pierwsze, chce się pokazać wszystkim Polakom, że środowiska związane z narodowym socjalizmem działają na ziemi polskiej, po

[13] *Adolf Hitler*, źródło: http://www.bhpoland.org (dostęp:13.08.2016).

drugie: ma to być swoistego rodzaju odpowiedź na aktywność różnego rodzaju struktur antyfaszystowskich, które zbierają informacje o zagrożeniach rasizmem i ksenofobią w Polsce. Narodowi socjaliści, w ramach Inicjatywy Redwatch apelują do swoich sympatyków, aby zbierali dane dotyczący działaczy organizacji lewicowych, antyrasistowskich, mniejszości narodowych, członków różnych kościołów (uznanych przez rasistów za destrukcyjne). Mają to być takie dane jak: imiona i nazwiska, miejsce zamieszkania, numery telefonów czy nawet tablic rejestracyjnych samochodów. Na stronie, gdzie umieszczono powyższy apel znaleźć możemy wyeksponowane słowa Iana Stuarta Donaldsona - „pamiętaj miejsca, twarze zdrajców rasy, oni wszyscy zapłacą za swoje zbrodnie”[14].

Na swoich stronach internetowych zwolennicy „Krwi i Honoru” publikują wizerunki osób, uznanych przez nich za zdrajców rasy. Można tam znaleźć (zdobyte w niewiadomy sposób przez aktywistów Redwatch Polska), także zdjęcia i adresy świątyń religii destrukcyjnych. Wprowadzono podział na województwa, upublicznia się dane wrogów z mazowieckiego, pomorskiego, podkarpackiego, łódzkiego, lubuskiego, kujawsko-pomorskiego, zachodniopomorskiego, śląskiego, małopolskiego, dolnośląskiego, warmińsko-mazurskiego, wielkopolskiego. Co ciekawe, zdjęcia tych osób ukazują się nie tylko na różnego rodzaju manifestacjach, ale także na prywatnych uroczystościach[15].

Jeden z kandydatów do Sejmu z Ruchu Palikota, startujący z okręgu gdyńsko-słupskiego (został zresztą posłem), działacz mniejszości seksualnych, został „rozpracowany” przez Redwatch Polska. Na stronie internetowej ukazało się jego zdjęcie, krótki życiorys zawodowy, miejsce zamieszkania, adres firmy, którą prowadzi, adres internetowy. Co ciekawe, podano liczbę osób, które na niego głosowały, podając szczegółowe dane odnośnie miasta Gdynia i Słupsk oraz ich powiatów. Napisano, że głosowało na niego 16 919 zboczeńców[16].

Publikuje się między innymi zdjęcia kobiet w towarzystwie Żyda czy Palestyńczyka, i podaje informacje, że imię i nazwisko należy ustalić, inna fotografia przedstawia parę Polkę i czarnego, przy czym kobietę podpisuje się jako zdrajczynię rasy, czy zdjęcie Roma, z podpisem iż jest „brudasem” do tego zarażonym wirusem HIV[17].

[14] *Redwatch Polska*, źródło: http://www.redwatch.info (dostęp: 17.08.2016).
[15] *Aktualności*, źródło: http://www.redwatch.info (dostęp: 17.08.2016).
[16] Pomorskie, źródło: http://www.redwatch.info (dostęp: 18.08.2016).
[17] *Warszawa*, źródło: http://www.redwatch.info (dostęp: 17.08.2016); *Śląsk i Zagłębie*, źródło: http://www.redwatch.info (dostęp: 13.08.2016).

Zauważyć należy, że swój przekaz, nawołujący do zbierania danych o wrogach narodowego socjalizmu wzmacniają wizualną oprawą, mającą na celu po pierwsze: przekonać swoich sympatyków do działania, po drugie: wykazać czystość idei, po trzecie: uatrakcyjnić poglądy. Obrazować to może poniższy obraz, w którym małe, może dwuletnie dziecko w białym cylindrze, na którym znajduje się znak Combat 18, owinięte jest białą wstęgą z czerwonym napisem Redwatch.info. Siedzi przed klawiaturą komputera, co sugeruje, że wprowadza „właściwe" dane. Poniższy obrazek pojawił się, aby uczcić dwa lata istnienia Akcji Redwatch Polska.


Źródło: *Obchodzimy drugie urodziny Akcji Redwatch Polska*, http://www.redwatch.info (dostęp: 13.08.2016).

Narodowi socjaliści z organizacji „Krew i Honor" w sposób radykalny chcą odmienić wewnętrzną, polityczną sytuację Polski. Jednym z ważnych żądań, które formułują, jest pozbawienie wpływów osób, które w przeszłości należały do Polskiej Zjednoczonej Partii Robotniczej. W tym kontekście należy przytoczyć jedną z opinii na ten temat, którą można znaleźć na stronie internetowej polskich narodowych socjalistów „czas najwyższy ustawą odsunąć od życia publicznego byłych członków PZPR. Na wojnie musi się słać trup wroga, bo w przeciwnym razie w piach idzie polska krew. Nie da się tej wojny wygrać bez wystrzału, nie da się jej

wygrać z braniem jeńców. Bez wymiany elit, bez odstrzelania marginesu, Polska nie będzie Polską! Żadnej litości, żadnych sentymentów, wycinać jak leci"[18].

W tym kontekście należy podać jeszcze jeden cytat, który świadczy o charakterze osób, które tworzą tę strukturę (pisownia oryginału) „zeszły tydzień przyniósł dwie dobre wiadomości: zdechła sendlerowa, Lechia Gdańsk nareszcie powróciła na swoje miejsce w extra klasie"[19].

Podkreślić należy, że w sposób krytyczny, a co najważniejsze, wrogi ustosunkowują się do większości środowisk narodowych działających w Polsce, również odwołujących się do działań radykalnych. Kością niezgody jest religia, otóż ruch odwołujący się do narodowych i socjalistycznych idei negatywnie odnosi się do chrześcijaństwa, uznając, że religia ta zniewala białego człowieka. Tymczasem nacjonaliści III Rzeczpospolitej podkreślają właśnie fundamentalne znaczenie Jahwe i jego syna Jezusa Chrystusa. W rzeczywistości obóz narodowo-radykalny to zdrajcy Polski i białej rasy. Pozbyć się ich tylko można w jeden sposób jak piszą zwolennicy „Krwi i Honoru „zdrajców nie powinno się pytać dlaczego zdradzili, do zdrajców powinno się strzelać"[20].

Wspomniano już, że aktywiści „Krwi i Honoru" starają się posługiwać atrakcyjnymi grafikami na łamach swojej strony internetowej. Warto jednak również zacytować słowa jednego z utworów wykonywanych przez zespół muzyczny, który dla działaczy tego ugrupowania wydaje się ważny, zresztą jest cytowany na ich stronie internetowej, „za każdą kroplę krwi, każdego z moich braci, za kłamstwa i oszczerstwa wymierzone w rasę, komunistyczny łagr i lata zniewolenia, syjonistyczny chłam i czasy upodlenia. A gdy pewnego dnia usłyszysz w dali strzały: to idzie przeznaczenie – to my do was strzelamy! Zapłonął wielki stos i nigdy już nie zgaśnie, zbrojne ramię rewolucji – Combat 18!"[21].

W Polsce działa wiele radykalnych ugrupowań, zarówno na prawej, jak i lewej stronie politycznej. Na łamach pism, stronach internetowych możemy znaleźć szereg haseł, które muszą wzbudzać niepokój, biorąc pod uwagę polski system prawny czy polityczny. Jednak Autor powyższego opracowania uważa, że nie ma bardziej

[18] *Aktualności, 20.03.2016*, źródło: http://www.bhpoland.org (dostęp:13 sierpień 2016).

[19] Irena Sendlerowa w trakcie II wojny światowej przyczyniła się do uratowania około 2,5 tysięcy dzieci żydowskich, aresztowana przez Gestapo była torturowana, więźniarka Pawiaka, skazana na karę śmierci, udało się jej przeżyć, w Powstaniu Warszawskim była sanitariuszką, po 1945 r. represjonowana przez Urząd Bezpieczeństwa, w: *Biografia Ireny Sendlerowej*, źródło: http://www.tak.opole.pl (dostęp: 13.08.2016); *Aktualności, 18.05.2008*, źródło: http://www.bhpoland.org (13.08.2016).

[20] *Aktualności, 06.04.2015*, źródło: http://www.bhpoland.org (dostęp: 18.08.2016).

[21] *Potop - Combat 18*, źródło: http://www.tekstowo.pl (dostęp: 18.08.2016), por. *Potop 318*, źródło: http://www.bhpoland.org (dostęp: 18.08.2016).

niebezpiecznej struktury, działającej zresztą niszowo, niż środowiska związane z „Krwią i Honorem". Wolność, między innymi słowa, jest jedną z najważniejszych wartości konstytuujących współczesną cywilizację europejską. Jednak należy zastanowić się, w którym momencie, odwołując się do niej, narodowi socjaliści wykorzystują ją do szerzenia przemocy w imię własnych ideałów. Wydaje się, że „Krew i Honor" uderza w zasadnicze wartości kultury, którą tworzyli Grecy, Rzymianie i chrześcijaństwo. We współczesnej Polsce środowisko to jest po pierwsze niewielkie, po drugie działa w konspiracji. Nie oznacza to jednak, że nie stanowi zagrożenia dla cywilizacji europejskiej, szczególnie dzisiaj, kiedy w społeczeństwach europejskich radykalizują się nastroje społeczne.

## BIBLIOGRAFIA

*Adolf Hitler*, źródło: http://www.bhpoland.org (dostęp:13.08.2016).

*Aktualności, 06.04.2015*, źródło: http://www.bhpoland.org (dostęp: 18.08.2016).

*Aktualności, 18.05.2008*, źródło: http://www.bhpoland.org (13.08.2016).

*Aktualności, 20.03.2016*, źródło: http://www.bhpoland.org (dostęp:13 sierpień 2016).

*Aktualności*, źródło: http://www.redwatch.info (dostęp: 17.08.2016).

*Biografia Ireny Sendlerowej*, źródło: http://www.tak.opole.pl (dostęp: 13.08. 2016).

*Combat 18 - co to za organizacja*, źródło: http://lublin.com.pl (dostęp: 13.08. 2016).

*Czym jest ZOG?*, źródło: http://www.bhpoland.org (dostęp:17.08.2016).

*Działalność niejawna*, źródło: źródło: http://www.bhpoland.org (dostęp: 13.08. 2016).

http://www.bhpoland.orgia (dostęp: 10.08. 2016).

*Krew i Honor*, źródło: http://www.hacking.pl (dostęp: 10.08.2016)

Kulbaka D., *Strona „Krew i Honor" została zamknięta*, źródło: http://webinside.pl (dostęp: 18.08.2016).

Metzger T., *Prawa Samotnego Wilka*, źródło: http://www.bhpoland.org (dostęp:10.08.2016).

*NS-Uniwersalny System Ludzkości*, źródło: http://www.bhpoland.org (dostęp: 10. 08.2016).

*Opór Bez Przywódcy*, źródło: http://www.bhpoland.org (dostęp: 13.08.2016).

Pomorskie, źródło: http://www.redwatch.info (dostęp: 18.08.2016).

*Potop - Combat 18*, źródło: http://www.tekstowo.pl (dostęp: 18.08.2016).

*Potop 318*, źródło: http://www.bhpoland.org (dostęp: 18.08.2016).

*Propagowali rasizm, totalitaryzm. Krzyczeli krew i honor. Policja rozbiła gang*, źródło: http://www.newsweek.pl (dostęp: 11.08. 2016).

*Redwatch Polska*, źródło: http://www.redwatch.info (dostęp: 17.08.2016).

*Stormer*, źródło: http://www.bhpoland.org (dostęp:18.08.2016).

*Strona „Krew i Honor" zamknięta*, źródło: http://www. policja.pl (dostęp: 13.08. 2016).

*Śląsk i Zagłębie*, źródło: http://www.redwatch.info (dostęp: 13.08.2016).

Tomasiewicz J., *Combat 18-terroryści czy chuligani ?*, źródło: http://www.terro ryzm.com (dostęp: 10.08.2016).

*Warszawa*, źródło: http://www.redwatch.info (dostęp: 17.08.2016).

Mariusz Kozerski

Uniwersytet Wrocławski

# Dawne afery polityczne ze współczesnej perspektywy: przykład sprawy Barschela/Pfeifera

Słowa kluczowe: afera polityczna, media, czarna kampania.

Nie będzie odkrywczym stwierdzenie, że aferami politycznymi w szczególności interesuje się świat mediów. To na łamach gazet, w programach telewizyjnych, w serwisach informacyjnych w radiu czy w Internecie afery są upubliczniane i rozpowszechniane, nabierają tempa i dramaturgii. W tych samych mediach giną po nasyceniu się opinii publicznej skandalizującymi informacjami i pod natłokiem nowych wiadomości, a niekiedy – wskutek oskarżenia winnych naruszenia norm oraz po wyjaśnieniu sprawy. W aferach, będących swego rodzaju przedstawieniami teatralnymi, swe dramatyczne role odgrywają reprezentanci świata polityki, osoby do niego aspirujące bądź jednostki i podmioty zamierzające wywierać wpływ na politykę. Świat ten może nie tylko kreować nielegalne zdarzenia i czyny, ale również bezwzględnie rozliczać i wykorzystywać sprawę w politycznej rozgrywce, usuwając ze swojego otoczenia zdeprawowane, niewiarygodne lub „niewygodne" w kontekście osiągania celów politycznych jednostki czy grupy osób. Epilog afery (nie tylko politycznej) – co warto obiektywnie stwierdzić – może stanowić również oczyszczenie z zarzutów dotyczących domniemanego naruszenia obowiązujących norm.

Z co najmniej dwóch względów do rehabilitacji dochodzi jednak rzadko. Po pierwsze – oburzona haniebnym czynem opinia publiczna domaga się wymierzenia kary i zastosowania konsekwencji w odniesieniu do oskarżonych osób. Wywołane aferą i nierozliczeniem jej poczucie niesmaku wśród obywateli łatwo i szybko może przeistoczyć się w postawy negacji i odwrócenia się od partii podczas kolejnych wyborów. Po drugie – ugrupowania polityczne i formacje rządzące chcą uchodzić

za niezdreprawowane i czyste, a system polityczny – za sprawny i funkcjonalny. W imię tych wartości aferzyści powinni więc zostać nie tylko wskazani, ale również osądzeni i wykluczeni – nawet jeśli wina „sprawców" nie jest przesądzona, a cała sprawa wielowątkowa, złożona i niejednoznaczna w obiektywnej ocenie.

Na wstępie rozważań warto wreszcie zaznaczyć, że współcześnie afery polityczne jako swego rodzaju inscenizacje teatralne zmieniają swoje oblicze. Ta sama pozostaje ich istota oraz motywy podejmowania nielegalnych działań. W czasach, gdy życie polityczne toczy się także w cyberprzestrzeni, zmienia się jednak dynamika fabuły, zwiększa się scena, przeistacza sceneria, stosowane są nowe środki „artystycznego" wyrazu, zaś aktorzy posługują się szerszą paletą rekwizytów. W tyle nie pozostaje uczestnicząca w przedstawieniu publiczność, która jest liczniejsza, bardziej dociekliwa i krytyczna.

## Afera polityczna w świetle teorii

Afery polityczne stały się również przedmiotem zainteresowania badaczy i naukowców, dla których nie stanowią one sensacji, lecz materiał empiryczny, przedmiot obserwacji, prowadzących do wysuwania hipotez, formułowania wniosków, tworzenia klasyfikacji czy wskazywania na ich powtarzalne cechy. Rozważania i wyniki badań naukowców nie muszą być osadzone jedynie w wymiarze teoretycznym, lecz w sensie normatywnym powinny stanowić cenne wskazówki dla przedstawicieli świata polityki i podmiotów systemu politycznego. Rezultaty dociekań badawczych są zatem jednocześnie podpowiedzią, jak afer unikać, jakie konsekwencje wiążą się z podjęciem nielegalnych działań oraz jak bez szkody dla siebie, swojej partii i całego systemu politycznego należy poruszać się w sferze publicznej. Szerzej ujmując – wyniki badań i przedstawiane wnioski mogą stanowić wymowną przestrogę przed uwikłaniem się w niezwykle skomplikowany, dynamiczny i niekiedy nieprzewidywalny proces i rozwój wypadków.

Różnorodności w przebiegu afer i skandali politycznych z pewnością nie można zaprzeczyć. Badacze wychodzą jednak z założenia, że w ciągu wydarzeń wynikających z naruszenia norm można dopatrywać się pewnej powtarzalności. Obserwacja ta uprawnia m.in. do podejmowania prób zdefiniowania podstawowych pojęć i scharakteryzowania procesów zachodzących w sytuacji ujawnienia opinii publicznej nielegalnych działań.

Zgodnie z podejściem naukowym tego typu afery uznaje się zatem za osiąganie korzyści politycznych w wyniku podjęcia nielegalnych i sprzecznych z obowiązującym prawem działań. Aby zdarzenie mogło zostać określone mianem

skandalu politycznego (pokrewnego aferze), zdaniem Karla Otto Hondricha powinny zostać spełnione trzy warunki: musi nastąpić faktyczne bądź przypuszczalne naruszenie norm przez osobę, grupę ludzi lub instytucję, jego upublicznienie oraz wywołane nim oburzenie opinii publicznej[1].

Wyróżnić można ponadto trzy grupy podmiotów, zaznaczających w swój udział w aferach i skandalach politycznych. Uwikłaną w nie „triadę aktorów" tworzą: ujawniający naruszenie norm dziennikarze i informatorzy, posądzani o naruszenie norm oraz publiczność rozumiana jako odbiorcy informacji pochodzących z mediów[2].

Szukając prawidłowości i powtarzalności w rozwoju zagadnień poddawanych ocenie opinii publicznej Niklas Luhmann wyodrębnił kilka ich faz rozwojowych: utajoną, przełomową, popularności, punktu kulminacyjnego oraz zmęczenia[3]. Teorię niemieckiego socjologa można odnieść również do afer i skandali politycznych. Założyć zatem można, że pierwszej fazie dochodzi do podjęcia nielegalnego i sprzecznego z przyjętymi normami życia politycznego. Przełom oznaczać będzie upublicznienie budzącej podejrzenia sprawy w mediach oraz przedstawienie pierwszych oskarżeń. W kolejnej fazie (popularności) oskarżeni i oskarżający wchodzą w otwarty spór. Formułowane są kolejne zarzuty, a wokół sprawy tworzy się nierzadko klimat powszechnego oburzenia. W fazie kulminacyjnej zwiększa się nacisk opinii publicznej, domagającej się wyjaśnienia sprawy, a nierzadko złożenia dymisji przez obwinionych. Tymczasem strony konfliktu z jeszcze większą mocą bronią swoich racji i formułują dalsze oskarżenia. Zamykająca aferę faza zmęczenia oznacza z jednej strony znużenie opinii publicznej trwającym od dłuższego czasu ciągiem zdarzeń. Malejące zainteresowanie mobilizuje do podjęcia ostatecznych decyzji i zamknięcia sprawy. Dla poddanych krytyce osób oznacza to nierzadko pozbawienie zajmowanych stanowisk lub rezygnację z pełnionych funkcji, a w obrębie systemu politycznego – niekiedy powołanie do życia parlamentarnej komisji śledczej mającej zbadać i wyjaśnić okoliczności sprawy oraz wskazać winnych naruszenia prawa[4].

[1] K. O. Hondrich, *Enthüllung und Entrüstung: eine Phänomenologie des politischen Skandals*, Frankfurt am Main 2002, s. 40.
[2] D. Greveldinger, *Anatomie eines Proteststurmes. Blick ins Innere des Shitstorms*, Trier 2014, s. 15.
[3] Zob. N. Luhmann, *Politische Planung: Aufsätze zur Soziologie von Politik und Verwaltung*, Opladen 1971, s. 18-19.
[4] Por. B. Dücker, *Der Fragmentenstreit als Produktionsform neuen Wissens*, [w:] *Lessings Skandale*, hrsg. v. J. Stenzel und R. Lach, Tübingen 2005, s. 32-33.

Do teorii N. Luhmanna (posługującego się kategorią „zagadnień poddawanych ocenie opinii publicznej") nawiązują w swoich pracach m.in. wspomniany Karl Otto Hondrich oraz Steffen Burkhardt. Odnosząc się bezpośrednio do skandali politycznych wyodrębniają cztery ich fazy rozwojowe. Pierwszy z badaczy nazywa je: dopuszczeniem się uchybienia, ujawnieniem uchybienia, oburzenia i przywracania równowagi. Burkhardt wyróżnia z kolei fazy stanowiące odniesienia do cykli życia: uśpienia, ożywienia, stabilizacji i punktu kulminacyjnego oraz zwrotu, nie wykluczając piątej – rehabilitacji[5]. Uwzględniając powyższe rozważania i klasyfikacje można utwierdzić się w przekonaniu, iż w aferach i skandalach politycznych – pomimo ich każdorazowo odmiennego przebiegu i różnej dynamiki – można dopatrywać się pewnych prawidłowości i wspólnych cech.

W każdej z przedstawionych koncepcji niezwykle istotną rolę odgrywają media, reprezentujący je dziennikarze i ich informatorzy. To ich aktywność sprawia, iż nieznane dotychczas opinii publicznej nielegalne działania podejmowane w obszarze polityki mogą doczekać się ujawnienia i nagłośnienia.

Należy zauważyć, że współczesne media mogą zdecydowanie skuteczniej niż 20 czy 30 lat temu wypełniać rolę demaskatora naruszeń obowiązujących norm politycznych. Wynika to z ich (ciągle zwiększającego się) zaawansowania technologicznego, możliwości dotarcia do coraz szerszej grupy odbiorców, zwiększenia kanałów przepływu informacji oraz niewiarygodnie szybkiego w dzisiejszych czasach rozprzestrzeniania się wiadomości w przestrzeni publicznej, zwłaszcza w internetowych serwisach informacyjnych, forach i sieciach społecznościowych.

Powyższe zmiany zdecydowanie zmieniły „układ sił" i relacje pomiędzy podmiotami zaangażowanymi w rozwój afer politycznych. We wspomnianej „triadzie aktorów" swą przewodnią rolę coraz wyraźniej zaznaczają działające w przestrzeni internetowej media, które z coraz większą skutecznością mogą tropić afery, ujawniać je i domagać się rozliczenia winnych. Należy jednak podkreślić, że skuteczność mediów w tym zakresie nadal zależy od decydentów politycznych. Mogą oni bowiem ograniczać wolność słowa, stosować cenzurę czy ograniczać dostęp do Internetu w celu niedopuszczania informacji o aferach politycznych i innych dysfunkcjach systemu. Nie powinna więc dziwić ścisła zależność między liczbą ujawnianych afer a typem reżimu politycznego. W krajach o wyraźnie demokratycznym

[5] *Skandale: Strukturen und Strategien öffentlicher Aufmerksamkeitserzeugung*, hrsg. v. K. Bulkow, Ch. Petersen, Wiesbaden 2011, s. 179-180.

profilu upublicznianych jest zdecydowanie więcej informacji o nielegalnych działaniach politycznych niż w państwach nieuznających lub ograniczających wolność słowa.

Biorąc pod uwagę przedstawione wyżej zależności, w tym zwłaszcza zwiększającą się rolę mediów w nagłaśnianiu i poddawaniu krytyce czynów związanych z naruszeniem norm, należy założyć, iż dawne afery w dzisiejszych realiach – w warunkach i na płaszczyźnie politycznej cyberprzestrzeni – mogłyby przebiegać inaczej. Na przykładzie niemieckiej afery Pffeifera/Spiegla chciałbym poniżej ukazać, w jaki sposób i przy użyciu jakich (dodatkowych) środków mógłby rozwijać się współcześnie scenariusz jednej z najgłośniejszych afer w historii RFN.

## Przebieg afery Barschela/Pffeifera

Nazwana została „aferą Barschela" lub „aferą Barschela/Pffeifera; znana jest jednak również jako „afera Pffeifera/Spiegla (Pfeiffer/Spiegel-Affäre), „afera kilońska" lub „Waterkantgate-Affäre". To ostatnie określenie nawiązuje po pierwsze do słowa „Waterkant", które w dialekcie dolnoniemieckim oznacza „wybrzeże", a w języku potocznym jest synonimem wybrzeża północnych Niemiec. Po wtóre – stanowi ono jako gra słowna nawiązanie do amerykańskiej „afery Watergate" z lat 70. XX wieku. To określenie o podwójnym znaczeniu sugeruje, że jako ciąg zdarzeń związanych z nielegalnymi działaniami w polityce rozegrała się północnoniemieckim landzie Szlezwik-Holsztyn, a ściślej ujmując w jego stolicy – Kilonii.

„Triadę aktorów" w rozwoju afery stanowili oskarżeni o naruszenie norm: premier landu – Uwe Barschel oraz jego asystent ds. mediów – Reiner Pffeifer; stroną ujawniającą nielegalne działania był tygodnik „Der Spiegel", zaś publicznością – czytelnicy magazynu, a szerzej – opinia publiczna w Szlezwiku-Holsztynie i w całych Niemczech Zachodnich.

Główną postacią afery był znany polityk Unii Chrześcijańsko-Demokratycznej (CDU), szef rządu krajowego w Kilonii – Uwe Barschel. Urodzony w 1944 r. w miejscowości Glienicke (Brandenburgia) Barschel pełnił w przeszłości wiele znaczących funkcji partyjnych i państwowych: w latach 1967-1971 był przewodniczącym młodzieżówki CDU *Junge Union* w Szlezwiku-Holsztynie, w roku 1971 r. został deputowanym do krajowego Landtagu, by niespełna dwa lata później przejąć funkcję przewodniczącego frakcji CDUw tymże parlamencie. Zajmował również

stanowisko ministra finansów oraz ministra spraw wewnętrznych w kilońskim rządzie[6]. Ostatnią, a zarazem najpoważniejszą funkcję polityczną – premiera kraju związkowego Szlezwik-Holsztyn – pełnił w latach 1982-1987. Uwe Barschel był ponadto doktorem nauk prawnych, autorem wielu publikacji z zakresu prawa publicznego i nauk politycznych. W 1987 r. gotowa niemal już była jego praca habilitacyjna. W przeszłości wykonywał także zawód adwokata i notariusza, był prezesem *Fundacji Herzogtum Lauenburg* oraz członkiem zarządu *Fundacji Hermanna Ehlersa*. Prywatnie był mężem arystokratki, Frei Barschel (z domu von Bismarck), oraz ojcem czwórki dzieci.

Drugi bohater afery – dziennikarz Reiner Pfeiffer – od lat 70. dał poznać się jako kontrowersyjny, cechujący się krytycznym stosunkiem do partii socjaldemokratycznej, redaktor naczelny bremeńskiego pisma „Weser Report". Stosowane przez niego metody pracy były oględnie mówiąc dyskusyjne. Zarzucano mu m.in. manipulowanie publikowanymi na łamach gazety zdjęciami, formułowanie bezpodstawnych oskarżeń wobec polityków oraz stosowanie prowokacji dziennikarskiej w celu potwierdzenia stawianych przez niego kontrowersyjnych tez. Jednym ze sprzecznych z etyką zawodową działań Pffeifera było celowe wprowadzenie w błąd urzędu paszportowego w Bremie. Podając fałszywe dane osobowe i uzyskując na ich podstawie paszport oraz ujawniając sprawę w „Weser Report" chciał udowodnić, że „oszuści paszportowi" w mieście mają ułatwione zadanie. Po odejściu z redakcji lokalnego pisma na krótko podjął współpracę w Wydawnictwem Springera. Następnym etapem pracy zawodowej – jak okazało się zdecydowanie przełomowym – była praca w Kancelarii Państwowej (Staatskanzlei) premiera kraju związkowego Szlezwik-Holsztyn. W ten sposób pod koniec 1986 r. skrzyżowały się zawodowe drogi Barschela i Pffeifera[7].

Strona oskarżająca w aferze – tygodnik „Der Spiegel" – uznawany jest za symbol niemieckiego dziennikarstwa śledczego oraz medium w znaczący sposób wpływające na kształt i przebieg debaty publicznej w Niemczech[8]. Uważnym obserwatorem zachodnioniemieckiej sceny politycznej, a jednocześnie pismem uciążliwym

[6] Zob. A. Wirsching, *Barschel-Pffeifer-Affäre*, [w:] *Skandale in Deutschland nach 1945*, hrsg. v. Stiftung Haus der Geschichte der Bundesrepublik Deutschland, Bonn 2007, s. 137-138

[7] T. Ramge, *Die großen Polit-Skandale. Eine andere Geschichte der Bundesrepublik*, Frankfurt am Main 2003, s. 200-201.

[8] O pozycji magazynu „Der Spiegel" na niemieckim rynku medialnym bliżej A. Hess, A. Szymańska, *Pomost medialny: rola mediów w międzynarodowej komunikacji politycznej na przykładzie relacji polsko-niemieckich*, Kraków 2009, s. 95.

i irytującym wielu polityków, magazyn był również w czasie politycznego i medialnego zamieszania wokół osoby Uwe Barschela, a więc w roku 1987.

Faza uśpienia afery Barschela/Pffeifera rozpoczęła się wraz z podjęciem przez nich decyzji o podjęciu niezwykle ryzykownej gry, której stawką było utrzymanie wpływów politycznych i realnej władzy w landzie. To nielegalne działanie zakończy się ostatecznie fiaskiem w sensie politycznym oraz tragedią w wymiarze ludzkim. Jak wynika z późniejszych ustaleń dziennikarzy „Der Spiegla" i dochodzenia parlamentarnej komisji śledczej premier wraz ze swoim asystentem rozpoczęli przed jesiennymi wyborami do Landtagu Szlezwiku-Holsztynu „czarną kampanię" wymierzoną w partię SPD i ubiegającego się o fotel premiera – socjaldemokratę Björna Engholma. Działania te miały jednocześnie na celu „przywrócenie dawnego blasku wizerunkowi premiera"[9]. Kampania polegająca na skutecznej autopromocji, a jednocześnie dyskredytowaniu przeciwnika politycznego, miała odwrócić negatywny trend, jaki wyznaczyły wyniki wyborów komunalnych z 1986 r. (w Szlezwiku-Holsztynie), w których CDU zanotowała znaczny spadek poparcia. Utrzymanie tego trendu mogło oznaczać dla Barschela utratę stanowiska szefa rządu w Kilonii po wyborach krajowych zaplanowanych na 1987 r.

Realizacji „czarnej kampanii" podjął się osobiście Reiner Pffeifer, jednak, jak przekonywał z późniejszych zeznaniach, działał na wyraźnie polecenie premiera Szlezwiku-Holsztynu i był przez niego inspirowany. Nielegalne i sprzeczne z jakimikolwiek standardami politycznymi działania asystenta ds. mediów były zakrojone na szeroką skalę. Björna Engholma współpracownik Barschela próbował zdyskredytować i oczernić w oczach opinii publicznej na wiele sposobów.

Jednym z nich było wysłanie do ministra finansów Szlezwiku-Holsztynu anonimowego doniesienia, w którym zawiadomiono o rzekomych nieścisłościach w zeznaniu podatkowym socjaldemokratycznego kandydata na stanowisko premiera. W rzeczywistości, pomimo usilnych starań i dokonanej przez Pffeifera dogłębnej analizy dokumentów, zeznanie to nie zawierało nieprawidłowości. Co ciekawe podobna denuncjacja trafiła również na biurko Uwe Barschela, a więc osoby, która zgodnie z późniejszą relacją referenta ds. mediów sama podyktowała mu treść anonimu[10].

Innym nielegalnym działaniem było zlecenie śledzenia prywatnego życia Engolma przez agencję detektywistyczną. Trwające dwa tygodnie „śledztwo" było

[9] A. Wirsching, *op.cit.*, s. 138.
[10] T. Ramge, *op.cit.*, s. 203.

prowadzone zwłaszcza pod kątem wykazania niemoralnego prowadzenia się polityka SPD. I tym razem nie zebrano przeciwko socjaldemokracie żadnych kompromitujących dowodów. Nieuczciwością wykazali się za to zleceniodawcy, ponieważ rachunek za usługi detektywów pokrył Karl Josef Ballhaus – bliski znajomy Uwe Barschela, a jednocześnie szef koncernu kosmetycznego *Schwarzkopf*[11].

Kolejnym „chwytem poniżej pasa" była próba psychicznego złamania Engolma w kluczowym okresie kampanii wyborczej. Reiner Pffeifer – jak okazało się bezskutecznie – próbował wmówić rywalowi Barschela (podając się w rozmowie telefonicznej za lekarza), że został zarażony wirusem HIV. Działaniem obliczonym na zdyskredytowanie całej formacji socjaldemokratycznej w oczach opinii publicznej było zainstalowanie na prośbę Barschela podsłuchu w jego własnym telefonie, następnie „przypadkowe" odkrycie pluskwy i przekazanie tej informacji mediom. W ten sposób premier dał do zrozumienia, że jest ofiarą niecnych praktyk konkurencji politycznej[12].

W dniu 31 V 1987 r., zaledwie 3,5 miesiąca przed wyborami do landtagu, doszło do niezwykle tragicznego wydarzenia, które nie sposób uznać za zaplanowany punkt kampanii wyborczej. Na lotnisku w Lubece-Blankensee (niedaleko granicy z NRD) rozbił się niewielki samolot, którym Uwe Barschel wracał z Bonn, ze spotkania chadeckich premierów landów z kanclerzem Helmutem Kohlem. W katastrofie spowodowanej uderzeniem maszyny w maszt nadawczy w złych warunkach pogodowych, zginęli obaj piloci oraz ochroniarz premiera. Sam Barschel wyszedł z wypadku niemal bez szwanku[13].

Po powrocie ze szpitala Barschel sprawiał wrażenie odmienionej, niejako nawróconej na empatię i refleksyjne podejście do życia osoby. W tej części kampanii wyborczej nie ujawniał się już jako bezwzględny i ogarnięty manią władzy polityk. Zdaniem jego kolegi z CDU, Trutza Grafa Kerssenbrocka, wewnętrzna przemiana premiera była przejawem umiejętnie wyreżyserowanej gry politycznej, w której Barschel był niezrównanym mistrzem[14].

Afera kilońska weszła w fazę przełomu w dniu 7 IX 1987 r., a więc sześć dni przed wyborami krajowymi w Szlezwiku-Holsztynie. To wówczas tygodnik „Der Spiegel" opublikował na swoich łamach artykuł, w którym poinformowano o pro-

[11] *Ibidem*, s. 202.
[12] A. Wirsching, *op.cit.*, s. 139.
[13] *Tod im Kornfeld*, „Der Spiegel" 1987, nr 24, s. 201.
[14] *31. Mai 1987 - Uwe Barschel überlebt einen Flugzeugabsturz*, http://www1.wdr.de (dostęp: 05.01. 2017).

wadzeniu przez CDU „czarnej kampanii" wymierzonej w socjaldemokratów i personalnie w Björna Engholma. Dziennikarze nie wskazali na osoby stojące za nielegalnymi działaniami i intrygami, mającymi przybliżyć chadeków do wyborczego zwycięstwa.

W kolejnym artykule, datowanym na 14 IX 1987 r. (który ukazał się zatem dzień po wyborach), nie pozostawiono już wątpliwości, że niechlubnych czynów w okresie kampanii dopuścił się Uwe Barschel. Okazało się jednocześnie, że ujawnione przez dziennikarzy informacje, m.in. o śledzeniu Engholma, pochodziły bezpośrednio od niedawnego współpracownika premiera – Reinera Pffeifera. Wyjawienie kompromitujących faktów o przedwyborczych działaniach Barschela informator „Der Spiegla" umotywował „względami sumienia" oraz „zwykłą ludzką przyzwoitością"[15].

Wynik wyborczy CDU (42,6 % - najgorszy od 1958 r., niegwarantujący przedłużenia koalicji rządowej z liberalną FDP[16]) oraz spowodowane najnowszymi doniesieniami oburzenie opinii publicznej, sprawiły, iż Barschel znalazł się ogniu krytyki o podwójnej sile rażenia. Wyjaśnień domagała się bowiem zarówno rodzima partia CDU, jak i zwykli obywatele. Odpowiadając na ataki zwołał 18 IX 1987 r. konferencję prasową, w której przekonywał o swojej niewinności i bezpodstawności stawianych wobec niego zarzutów. Zwrócił jednocześnie uwagę, że słowo premiera znaczy więcej niż zdanie niepoważnego i mało znaczącego referenta ds. mediów. Konferencja, podczas której Barschel przyjął postawę obronną, padające wówczas kontrargumenty ze strony Pffeifera, wysoka temperatura sporu oraz oburzenie opinii publicznej mogą utwierdzać w przekonaniu, że afera weszła w tym czasie w fazę popularności.

W dynamicznym rozwoju wydarzeń związanych ze sprawą premiera Szlezwiku-Holsztynu trudno jest jednocześnie wskazać na moment otwierający okres kulminacyjny w rozwoju afery kilońskiej. Za taki w moim przekonaniu można uznać dymisję złożoną przez U. Barschela w dniu 2 X 1987 r. W specjalnym oświadczeniu przyznał wówczas, że nielegalne działania podczas kampanii wyborczej miały miejsce i bierze za nie polityczną odpowiedzialność. Wyraźnie jednak zaznaczył, że czyny te odbyły się bez jego współudziału i wiedzy[17].

[15] A. Wirsching, *op.cit*.

[16] Wybory w Szlezwiku-Holsztynie wygrała wówczas SPD zdobywając 45,2 % głosów. FDP zanotowała wynik wyborczy na poziomie 5,2 %. Pełne wyniki wyborów z 1987 r. zob. http://www.wahlrecht.de (dostęp: 09.01.2017).

[17] T. Kortsch, *Professionelle Selbstdarsteller: Selbstdarstellung am Beispiel von Politikern*, Norderstedt 2008, s. 16.

Fazę kulminacyjną afery zamykają tragiczne wydarzenia, które rozegrały się 11 X 1987 r. w Genewie. Uwe Barschel trafił do jednego z tamtejszych hoteli w drodze powrotnej z rodzinnego urlopu spędzonego na Wyspach Kanaryjskich. Były premier musiał przerwać wypoczynek i pozostawić na miejscu rodzinę, ponieważ w trybie pilnym został wezwany przez utworzoną w międzyczasie parlamentarną komisję śledczą. Miał złożyć przed nią obszerne wyjaśnienia w sprawie afery. Nie mając bezpośredniego połączenia lotniczego z Las Palmas do Hamburga, Barschel musiał przesiąść się w Genewie i tam spędzić w oczekiwaniu na lot jeden dzień.

W hotelu 11 X polityk CDU miał udzielić wywiadu dziennikarzowi magazynu „Stern". Sebastian Knauer nie mogąc doczekać się na swojego rozmówcę w umówionym miejscu, postanowił zajrzeć do pokoju Barschela. Tam odkrył leżące w wannie zwłoki byłego premiera. Nie wezwał od razu policji; zrobił natomiast zdjęcia, które ukazały się w następnym wydaniu pisma. Ich zamieszczenie na okładce „Sterna" wywołało kolejny skandal oraz pytania o etykę i granicę przyzwoitości w pracy dziennikarskiej[18].

W toku prowadzonego śledztwa stwierdzono, że przyczyną zgonu Uwe Barschela było przedawkowanie leków uspokajających, które zażywał od dłuższego czasu. Okoliczności śmierci polityka CDU nie zostały jednak po dzień dzisiejszy wyjaśnione. Brak jednoznacznych ustaleń sprzyjał formułowaniu różnych teorii spiskowych, zgodnie z którymi w genewskim hotelu dokonano zabójstwa. Wśród państw i ich służb wywiadowczych, które miałyby targnąć się na życie byłego premiera Szlezwiku-Holsztynu, wymieniano m.in.: RPA, NRD, ZSRR, Iran, Izrael, Koreę Północną, a nawet samą RFN. Pozbawienie życia miało być związane z rzekomym pośredniczeniem Barschela w zakrojonym na skalę międzynarodową nielegalnym handlu bronią[19].

W obliczu tak tragicznych wydarzeń określenie „faza zmęczenia" w odniesieniu do afery Pffeifera/Spiegla byłoby zdecydowanie nie na miejscu. Abstrahując od kwestii nazewnictwa warto zauważyć, że afera kilońska zwieńczona została (niemal modelowo) podjęciem ostatecznych decyzji na poziomie politycznym i prawnym oraz zamknięciem sprawy. Parlamentarna (szlezwicko-holsztyńska) komisja śledcza, która zakończyła swą pracę 5 II 1988 r., uznała Uwe Barschela winnym i odpowiedzialnym za nielegalne działania w czasie niedawnej kampanii wyborczej.

[18] R. Pörtner, *Barschels ungeklärter Tod*, „Stuttgarter Zeitung" 2012, 10 XII.

[19] "*Was macht so einer hier?" Das seltsame Doppelleben und der merkwürdige Tod des Dr. Uwe Barschel (Teil II)*, „Der Spiegel" 2007, 15 X, s. 52 nn.

W tym samym roku umorzone zostało prowadzone przez prokuraturę w Lubece śledztwo w sprawie śmierci polityka CDU[20].

Po pięciu latach wyszły na jaw nowe okoliczności sprawy Barschela, które uznać można za zaskakujący (i ostateczny) finał tej głośnej afery. Wiosną 1993 r. na łamach magazynu „Stern" ukazał się artykuł, w którym rządzącym w Szlezwiku-Holsztynie socjaldemokratom zarzucono, iż po 1988 r. przekazali Reinerowi Pffeiferowi łącznie ok. 25 000 DM. Efektem publikacji było powołanie drugiej już parlamentarnej komisji śledczej, która ustaliła, że SPD wiedziała o skierowanych przeciw niej działaniach referenta ds. mediów, a informacje te wykorzystała do realizacji celu politycznego, jakim było zwycięstwo w wyborach w 1987 r. Ustalono ponadto, że Björn Engholm, następca Barschela na stanowisku premiera landu, w okresie kampanii wyborczej był informowany o machinacjach Reinera Pfeiffera. Ujawnienie tej sprawy doprowadziło do dymisji Engholma, która nastąpiła w maju 1993 r.

## Gdyby Afera Barschela/Pffeifera przebiegała dziś…

Powracam do pytania, które postawiłem na wstępie: w jaki sposób afera kilońska przebiegałaby w dzisiejszych realiach, w warunkach i na płaszczyźnie politycznej cyberprzestrzeni? Referent ds. mediów, zajmujący się brudną kampanią wyborczą, współczesny Pffeifer, jako aferzysta dysponowałby niewątpliwie znacznie szerszym instrumentarium i bardziej zaawansowanymi środkami oddziaływania na opinię publiczną niż 30 lat temu. Odpowiednich umiejętności i niezbędnych doświadczeń nabrałby z pewnością jako redaktor w lokalnym, nastawionym na tanią sensację piśmie czy portalu internetowym. Nieobce byłoby mu nie tylko manipulowanie publikowanymi zdjęciami, ale również pospieszne zamieszczanie niesprawdzonych, a niekiedy nieprawdziwych informacji o miejscowych politykach czy urzędnikach. Już wówczas dostrzegałby walory zawrotnego tempa, z jakim w wirtualnej przestrzeni rozprzestrzenia się wiadomość czy plotka.

Już jako doradca, asystent, czy referent pracujący w nieformalnym sztabie wyborczym współczesny Pffeifer mógłby zlecać organizowanie ataków hakerskich na witrynę internetową dzisiejszego kontrkandydata na stanowisko premiera landu. Wyobrażam sobie ponadto śledzenie jego aktywności nie tylko w „realnym" życiu prywatnym, ale również w Internecie, podsłuchiwanie na znacznie szerszą skalę

[20] Zob. J. Schmid, *Die „Kieler Affäre": Symptom eines deformierten Regierungssystems, Tat eines Einzelnen oder Kulminationspunkt einer schleswig-holsteinischen Sonderentwicklung?*, „Zeitschrift für Parlamentsfragen" 1988, nr 4, s. 500.

jego rozmów telefonicznych, monitorowanie jego konwersacji na wirtualnych komunikatorach, przechwytywanie maili i smsów oraz ich upublicznianie. Przeciwnicy współczesnego Engholma nie omieszkaliby zapewne również oczerniać go na forach internetowych, kraść jego tożsamość i podszywać się pod niego w sieciach społecznościowych, wykorzystywać jego zdjęcia w celu ośmieszenia go lub zdyskredytowania, ujawniać jego dane osobowe czy rozpowszechniać na jego temat w Internecie nieprawdziwe informacje. Kanałem, przez który następowałoby psychiczne wyprowadzanie z równowagi przeciwnika politycznego, byłaby nie tylko sieć telefoniczna, ale również wiadomości mailowe czy smsowe – oczywiście przy zachowaniu anonimowości dręczyciela.

Natomiast współczesna parlamentarna komisja śledcza powołana do celów wyjaśnienia sprawy mogłaby stać się wielkim przedstawieniem medialnym, trafiającym do szerokiej grupy odbiorców. Zakładam również, że aktywność członków komisji mogłaby stać się przepustką do dalszej kariery politycznej i gwarancją rozpoznawalności, jednym słowem – niepowtarzalną okazją do wypromowania swojego nazwiska i marki w świecie polityki. Podsumowując i puentując: zadanie postawione przez Pfeifferowi, a mianowicie: *przywrócenie dawnego blasku wizerunkowi premiera, a z drugiej strony skuteczne podważenie wiarygodności kontrkandydata z SPD* mogłoby być dzisiaj – w warunkach cyberprzestrzeni – realizowane pełniej, skuteczniej i przy wykorzystaniu znacznie szerszego wachlarza środków oddziaływania.

## Bibliografia

"*Was macht so einer hier?" Das seltsame Doppelleben und der merkwürdige Tod des Dr. Uwe Barschel (Teil II)*, „Der Spiegel" 2007, 15 X.

*31. Mai 1987 - Uwe Barschel überlebt einen Flugzeugabsturz*, http://www1.wdr.de (dostęp: 05.01. 2017).

Dücker B., *Der Fragmentenstreit als Produktionsform neuen Wissens*, [w:] *Lessings Skandale*, hrsg. v. J. Stenzel und R. Lach, Tübingen 2005.

Greveldinger D., *Anatomie eines Proteststurmes. Blick ins Innere des Shitstorms*, Trier 2014.

Hess A., Szymańska A., *Pomost medialny: rola mediów w międzynarodowej komunikacji politycznej na przykładzie relacji polsko-niemieckich*, Kraków 2009.

Hondrich K. O., *Enthüllung und Entrüstung: eine Phänomenologie des politischen Skandals*, Frankfurt am Main 2002.

http://www.wahlrecht.de (dostęp: 09.01.2017).

Kortsch T., *Professionelle Selbstdarsteller: Selbstdarstellung am Beispiel von Politikern*, Norderstedt 2008.

Luhmann N., *Politische Planung: Aufsätze zur Soziologie von Politik und Verwaltung*, Opladen 1971.

Pörtner R., *Barschels ungeklärter Tod*, „Stuttgarter Zeitung" 2012, 10 XII.

Ramge T., *Die großen Polit-Skandale. Eine andere Geschichte der Bundesrepublik*, Frankfurt am Main 2003.

Schmid J., *Die „Kieler Affäre": Symptom eines deformierten Regierungssystems, Tat eines Einzelnen oder Kulminationspunkt einer schleswig-holsteinischen Sonderentwicklung?*, „Zeitschrift für Parlamentsfragen" 1988, nr 4.*Skandale: Strukturen und Strategien öffentlicher Aufmerksamkeitserzeugung*, hrsg. v. K. Bulkow, Ch. Petersen, Wiesbaden 2011.

*Tod im Kornfeld*, „Der Spiegel" 1987, nr 24.

Wirsching A., *Barschel-Pfeifer-Affäre*, [w:] *Skandale in Deutschland nach 1945*, hrsg. v. Stiftung Haus der Geschichte der Bundesrepublik Deutschland, Bonn 2007.

# SUMMARY

„Cybersecurity as the challenge of the XXI century" is a collection of considerations dedicated to various aspects of security in cyberspace. Authors, who have been invited to this project, present different views on this subject.

An author of the first chapter, „The main actors of cyberspace and their activities", is Tomasz Hoffman. Writing from a legal and political perspective, including the achievements of security sciences, he tries to present potential actors of cyberspace, and their activities, including behaviors against the law. Cybersecurity, according to Hoffman, is a new element of national security and is related to challenges, such as cybercrime and cyberterrorism.

The second chapter, „Cybersecurity as a challenge for modern countries and societies", has been written by Marek Górka. The researcher has reviewed the current situation of the cybersecurity in the context of the spread of dangers in cyberspace, created by government and non-government organizations. Górka states that cyberspace has become a basic feature of the world and has created a new reality for almost all countries, what caused that the problems with cybercrime and cybersecurity became significant in both, the political and the economic aspect.

A text, which corresponds to the Górka's thoughts, is the text „Cyberterrorists in digital times - professionalization and digitalization of modern terrorist organizations" by Bogusław Węgliński. The author has analyzed the instruments used by terrorist groups. The instruments which have been evolving along with the development of technology. The most important of them is the Internet, which has opened new opportunities for terrorists, including digital communicating. The text also includes aspects of the usage of drones by terrorists.

The fourth chapter, „Cyber-physical attacks and the national security system", by Bogusław Olszewski, is also related to the previously mentioned issues. This part of the book deals with matters of the undesirable impact of cyber-physical systems on the safety of the international environment. According to Olszewski, their hybrid (digital-material) character causes that they affect not only the logical aspect of cyberspace but also the physical one. They enable destabilization of the internal structure of countries, what can lead to destructive changes

in the wider, international context. They are a multifaceted danger to the broadly understood system of the global security.

In the fifth chapter, Marcin Adamczyk has presented a text titled „Cyberspying in Chinese-American relations, in the context of the potential change of the world hegemon". The study is dedicated to the activities of the People's Republic of China in cyberspace, taken to acquire American military and civil technologies. The author claims that China is currently the only country that could challenge the global domination of the United States. However, to obtain the status of the hegemonic state, Beijing would need to build a solid coalition, supporting China on the international arena, but also reduce the economic distance between Beijing and Washington.

An author of the next chapter is Kamil Baraniuk, who has prepared a text titled „Outline of the institutional changes in the Russian radio-electronic intelligence". Baraniuk emphasizes that the high level of computerization of societies and the common use of information technologies makes the signal and electromagnetic data a very important source of information for specialized institutions dealing with information collection and processing. In this context the author outlines the genesis and the institutional transformation of the Russian radio-electronic intelligence, as well as the military and civil institutions dealing with this kind of activities over the last decades, analyzing their tasks and personnel changes in their management.

The seventh chapter has been written by two authors from Ukraine. Tetiana W. Nagachevskaya and Lyudmila Frliksowa prepared a text „Napryamky formuvannya mizhnarodnoyi konkurentospromozhnosti IT-sector Ukrayiny". This text contains an analysis of the current situation and peculiarities in the shaping of the international competitiveness of the IT sector in Ukraine. Nagachevskaya and Frliksowa have presented the position of the Ukrainian IT sector, considered in the context of the Networked Readiness Index, which measures the tendency of different countries to use the opportunities offered by informational and communicational technology. In addition, they have shown competitive advantages and disadvantages of Ukrainian IT companies on international markets, and directions of growth of the international competitiveness of the IT sector in Ukraine.

Next two chapters have been related to religious issues in cyberspace. „Religious and pseudoreligious destructive groups: the challenges of cyberspace" has been written by Wojciech Gajewski, who pays attention to the matter of penetrating of the virtual space by various destructive religious groups. In his opinion, they

become increasing dangers not only for individual users of the cyberspace but also for entire social groups. The religious scholar is a supporter of extensive research, educational and even legal activities, that suppose to reduce the negative consequences of the sectarian activity in cyberspace. Next author, Lucjan Klimsza, has presented a text „Philosophical aspects of the Internet in the context of missionary tasks of the Church". Klimsza, who is a Protestant pastor, pays attention to the possibilities that the access to the digital space opens to contemporary Christianity. He clearly states that the current Church must be a multimedia, but not a virtual community, distant from a man and his real existence. The author sees the Internet as a meta-medium enabling the transmission of religious content, which may be helpful in cognition and relationship between man and God, as well as between man and man.

Tenth chapter, „Cybersecurity as a construct in the Polish public space", has been written by Przemysław Mikiewicz from a political perspective. The text is a reflection of the presence of the cybersecurity in Polish public space, which has been specified by the author as the opinion-making influence of the central government institutions and political parties. The author indicates that the concept of the cybersecurity is present in the Polish public space in government documents and programs of political parties. According to Mikiewicz, there is a fundamental asymmetry between these two types: government documents pay a lot of attention to cybersecurity, programs of political parties, however, only mention about the issue. Finally, cybersecurity appears as a kind of a construct used to create an image of the modern world, full of immaterial dangers, which might be eliminated only by publication of new doctrines and strategies, created to combat dangers in cyberspace.

The political aspect of the cybersecurity issue is present also in the next two texts. An author of the first one is Grzegorz Tokarz, whose section has been titled „The Internet as an instrument to incite violence - an example of <Blood and Honor> Poland". The text introduces activities of the Polish section of this neo-Nazi organization, including the content of its website, which is an important tool, used to promote the ideas of this environment, as well as a source of information about people and institutions considered to be the traitors of the "white race".

The second text, which also ends this book, has been prepared by Mariusz Kozerski. In this chapter, titled „Former political scandals from a modern perspective: an example of the Barschel/Pffeifer case", the analyzed issue is the role played by media to publicize political scandals. The author has reviewed incidents that

took place in the 1980s, in the German land of Schleswig-Holstein. A significant role in those happenings was played by "Der Spiegel", an opinion-forming weekly magazine. Let's add that Kozerski also tries to answer the question of how that, so-called „Kiel scandal" could look like if it happened today, in the context of the contemporary informational/opinion-forming potential, which characterizes the global computer network.

*Tomasz R. Dębowski*

# Biogramy

(kolejność alfabetyczna)

**Adamczyk Marcin**
mgr, Wydział Nauk Społecznych, Uniwersytet Wrocławski.

**Baraniuk Kamil**
mgr, Wydział Nauk Społecznych, Uniwersytet Wrocławski.

**Dębowski Tomasz R.**
dr hab., Instytut Studiów Międzynarodowych, Uniwersytet Wrocławski.

**Frliksowa Lyudmila**
mgr, Kijowski Uniwersytet Narodowy imienia Tarasa Sewczenki.

**Gajewski Wojciech**
prof. dr hab., Wydział Historyczny, Uniwersytet Gdański.

**Górka Marek**
dr, Wydział Humanistyczny, Politechnika Koszalińska.

**Hoffman Tomasz**
prof. dr hab., Wydziała Humanistyczny, Politechnika Koszalińska.

**Klimsza Lucjan**
dr, Pedagogiczny Fakultet, Uniwersytet Ostrawski,

**Kozerski Mariusz**
dr, Instytut Studiów Międzynarodowych, Uniwersytet Wrocławski.

**Mikiewicz Przemysław**
dr hab., Instytut Studiów Międzynarodowych, Uniwersytet Wrocławski.

**Nagachevskaya Tetiana W.**
dr, Katedra Międzynarodowej Ekonomii i Marketingu, Kijowski Uniwersytet Narodowy imienia Tarasa Sewczenki.

**Olszewski Bogusław**
mgr, Wydział Nauk Społecznych, Uniwersytet Wrocławski

**Tokarz Grzegorz**
dr, Instytut Studiów Międzynarodowych, Uniwersytet Wrocławski.

**Węgliński Bogusław**
dr, Wydział Nauk Społecznych i Dziennikarstwa, Dolnośląska Szkoła Wyższa.

Wydawnictwo Naukowe Archaegraph
Diana Łukomiak
Łączna 57/70, 93-166 Łódź
NIP: 7292686082
REGON: 367964185
@: archgaegraph@gmail.com

ISBN: 978-83-66035-02-7
ISBN: 978-83-66035-03-4