

# e-terroryzm.pl

WYZWANIA

TERRORYZM

DONIESIENIA

ZAGROZENIA

BEZPIECZEŃSTWO

SPRAWOZDANIA

DYLEMATY

OCHRONA

ANALIZY

Zjawisko terroryzmu w Inguszetii

str. 10

str. 6

Terroryzm Al-Shabaab

Klasyfikacja ataków w cyberprzestrzeni

str. 13

str. 4

Instalacja atomowa w Świerku  
zagrożona atakiem terrorystycznym?

Metody szkolenia politycznego  
funkcjonariuszy SB i MO

str. 26

str. 40

Model działań bezpieczeństwa  
teleinformatycznego

	str.
<b>Terroryzm</b>	
- Instalacja atomowa w Świerku zagrożona atakiem terrorystycznym?.....	4
- Terroryzm Al-Shabaab .....	6
- Zjawisko terroryzmu w Inguszetii.....	10
- Klasyfikacja ataków w cyberprzestrzeni .....	13
<b>Bezpieczeństwo</b>	
- Z działalności ABW w 2012 roku.....	19
- Błąd w zabezpieczeniach kart SIM.....	21
<b>Kryminologia</b>	
- Okoliczności przesłuchania śledczego niepełnoletniej i małoletniej osoby w trakcie postępowania karnego.....	22
<b>Historia</b>	
- Metody szkolenia politycznego funkcjonariuszy SB i MO .....	26
- Cichociemni .....	31
- 31 października 1984 r. ....	36
<b>Ludzie wywiadu i kontrwywiadu</b>	
- Pułkownik Georgij Mordwinow.....	38
<b>Ochrona informacji niejawnych</b>	
- Model działań bezpieczeństwa teleinformatycznego .....	40
<b>Warto poznać</b>	
- Droga ku jakości i odpowiedzialności policji.....	46
- Bezpieczeństwo międzynarodowe - współczesne koncepcje .....	50
- Elita szpiegów - Guido Knopp .....	53
<b>Felieton</b>	
- Dębica (nie) spokojna .....	55
<b>Kartki z kalendarza</b> .....	57

## Redakcja

### Biuletyn redagują:

Przemysław Bacik  
 Agnieszka Bylica  
 Hanna Ismahilova  
 Jacek Kowalski  
 dr Kazimierz Kraj  
 Tobiasz Małyśa  
 Natalia Noga  
 Piotr Podlasek  
 Anna Rejman  
 dr Jan Swół  
 Bernadetta Stachura-Terlecka  
 Tomasz Tylak  
 Ewa Wolska  
 Anna Wójcik

**Skład techniczny:** Tobiasz Małyśa  
**Administrator www:** Bernadetta Stachura-Terlecka

INSTYTUT STUDIÓW  
 NAD TERRORYZMEM

WYŻSZA SZKOŁA  
 INFORMATYKI I ZARZĄDZANIA  
 z siedzibą w Rzeszowie



Publikacja jest bezpłatna, a zespół redakcyjny oraz Autorzy nie odnoszą z niej korzyści materialnych. Publikowane teksty stanowią własność Autorów, a prezentowane poglądy nie są oficjalnymi stanowiskami Instytutu Studiów nad Terroryzmem oraz Wyższej Szkoły Informatyki i Zarządzania.

Artykuły poruszane w czasopiśmie służą celom edukacyjnym oraz badawczym. Redakcja nie ponosi odpowiedzialności za inne ich wykorzystanie.

Zespół redakcyjny tworzą pracownicy Katedry Bezpieczeństwa Wewnętrznego i Instytutu Studiów nad Terroryzmem Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie oraz skupieni wokół tych jednostek znawcy i entuzjaści problematyki.

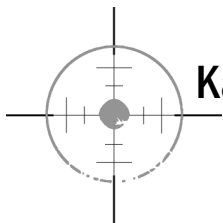
### Adresy i kontakt:

- Poczta redakcji biuletynu:  
[redakcja@e-terroryzm.pl](mailto:redakcja@e-terroryzm.pl)
- Strona internetowa biuletynu:  
[www.e-terroryzm.pl](http://www.e-terroryzm.pl)
- Instytut Studiów nad Terroryzmem:  
[www.terroryzm.rzeszow.pl](http://www.terroryzm.rzeszow.pl)
- Wyższa Szkoła Informatyki i Zarządzania:  
[www.wsiz.rzeszow.pl](http://www.wsiz.rzeszow.pl)

**Fotografia na okładce:** Żołnierze z 1st Brigade of U.S. Army Europe's 1st Armored Division rozmieszczają się po desancie ze śmigłowca UH-60 Black Hawk podczas misji na pustyni Al Jazeera Desert (Irak).

Fot. Staff Sgt. Aaron Allmon, U.S. Army, [http://commons.wikimedia.org/wiki/File:1st\\_Armored\\_Division\\_dismount\\_a\\_UH-60\\_Blackhawk.jpg](http://commons.wikimedia.org/wiki/File:1st_Armored_Division_dismount_a_UH-60_Blackhawk.jpg)

Wyższa Szkoła Informatyki i Zarządzania w Rzeszowie,  
 ul. Sucharskiego 2, 32-225 Rzeszów



## Kalendarium

- 2013.08.29. Afganistan:** Piętnastu policjantów zginęło w zasadzce zorganizowanej przez talibów, a dziesięciu zostało rannych. Do ataku doszło na górskiej przełęczy, podczas patrolowania drogi.
- 2013.08.28. Afganistan:** W wyniku odparcia ataku talibów na bazę Ghazni rannych zostało dziesięciu polskich żołnierzy. Wszyscy napastnicy zginęli.
- 2013.08.28. Irak:** Co najmniej 30 osób zginęło, a 130 zostało rannych w zamachach w Bagdadzie i jego okolicach. Ekspłodowało około dziesięciu VBIED. Do ataków doszło w regionach zamieszkałych przez większość szyicką.
- 2013.08.27. Inguszetia:** Nieznani sprawcy dokonali udanego zamachu na sekretarza Rady Bezpieczeństwa Republiki Inguszetii. Samochód, którym podróżował został ostrzelany. W ataku zginął także kierowca sekretarza. Napastników nie schwytano.
- 2013.08.25. Jemen:** Przynajmniej sześć osób zginęło, a 26 zostało rannych. To bilans ataku bombowego na autobus jemeńskich sił powietrznych. Do ataku nikt się nie przyznał.
- 2013.08.25. Kolumbia:** W ataku FARC zginęło 13 żołnierzy kolumbijskiej armii. Do starcia doszło podczas patrolu na granicy z Wenezuelą.
- 2013.08.24. Afganistan:** Podczas likwidacji składowiska broni oraz materiałów wybuchowych, w wyniku zadziałania miny pułapki, zginął polski komandos chor. Mirosław Łucki.
- 2013.08.23. Irak:** Co najmniej 26 osób zginęło, a 50 zostało rannych w wyniku samobójczego ataku, do którego doszło w popularnym parku w Bagdadzie.
- 2013.08.16. Liban:** W najkrwawszym od ok. 30 lat zamachu w tym państwie zginęło co najmniej 18 osób, a 280 zostało rannych. Ekspłodował samochód-pułapka.
- 2013.08.15. Irak:** W pięciu atakach, w Bagdadzie, śmierć poniosły co najmniej 23 osoby. Jedna z bomb wybuchła na dworcu autobusowym.
- 2013.08.08. Pakistan:** Na pogrzebie policjanta zastrzelonego zginęło 28 osób, głównie policjantów. Ładunek został zdetonowany przed meczetem. Do zamachu nikt się nie przyznał.
- 2013.08.07. Irak:** Seria zamachów bombowych na bazarach i ulicach handlowych Bagdadu spowodowała śmierć co najmniej 51 osób, a ponad 100 zostało rannych.

### Szanowni Czytelnicy!

Mimo pięknej pogody i trwających wakacji, do rąk Czytelników dostarczamy kolejny numer miesięcznika. W nim nasi nowi autorzy (Agata Kita i Kamil Pietrasik) piszą o terroryzmie AI – Shabaab oraz zjawisku terroryzmu w Inguszetii. Kontynuujemy problematykę cyberterroryzmu. Bernadetta Terlecka zapoznaje nas z zagrożeniami związanymi z zabezpieczeniami kart SIM, który to problem dotyczy użytkowników telefonów komórkowych. Zainteresowani przestępczością nieletnich poznają zasady ich przesłuchiwanie na Ukrainie (Hanna Ismahilova). Nawiązując do historii, zdobywamy wiedzę na temat metod szkolenia politycznego funkcjonariuszy, MO i SB (Jan Swół) oraz przypominamy chlubne tradycje cichociemnych, elity polskich żołnierzy, protoplastów naszych współczesnych komandosów. W obszernym artykule, autorstwa Tobiasza Małysy, zaznajamiamy się z działaniami na rzecz bezpieczeństwa teleinformatycznego, w oparciu o ustawę o ochronie informacji niejawnych. Ponadto kalendarium, kartki z kalendarza, recenzje, felieton i kolejna notka biograficzna niezwykłego i mało znanego człowieka wywiadu.

Studenckie wakacje dobiegają końca, niektórzy, którym powinęła się noga podczas egzaminów, we wrześniu będą zaliczać poprawki. Trzymamy za nich kciuki. Inni będą nadal wypoczywać, czasem pracować i przygotowywać się do inauguracji nowego roku akademickiego. Do nowych wyzwań.

Zapraszam do lektury.

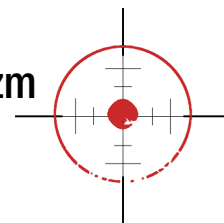
**Za zespół  
Kazimierz Kraj**

**2013.08.07. Pakistan:** W eksplozji bomby w Karaczi zginęło co najmniej 11 osób, a 28 zostało rannych. Ładunek wybuchowy ukryty był w motocyklu.

**2013.08.06. Pakistan:** Do ataku, na konwój pięciu autobusów, doszło w południowo – zachodniej części kraju. Napastnicy wprowadzili i zabili 13 pasażerów.

**2013.08.03. Afganistan:** W ataku samobójczym na konsulat Indii w Dżalalabadzie, śmierć poniosło 6 osób, a 22 zostały ranne. Zamachowiec wysadził się w samochodzie wypełnionym materiałami wybuchowymi.





Załogę parolotni stanowiło dwóch dziennikarzy z województwa świętokrzyskiego, którzy tłumaczyli się ze swojej eskapady, że przygotowują materiał o instalacjach jądrowych. Film z lotu ptaka miał być ważnym elementem projektu. Należy nadmienić, że załoga parolotni nie miała stosownych zezwoleń, a w myśl art. 212 prawa lotniczego, który zakazuje lotów w przestrzeni zamkniętej ze względów wojskowych lub bezpieczeństwa publicznego grozi do pięciu lat więzienia.

Nad całym tym wydarzeniem i przykładem głupoty oraz nieodpowiedzialności można by przejść do porządku dziennego – w końcu są ważniejsze problemy w Polsce – gdyby ten fakt nie świadczył o:

- braku zrozumienia i wyczulenia społeczeństwa dla zagrożenia atakiem terrorystycznym w aspekcie „tu i teraz”, a w szczególności niektórych elementów służb, w których działaniach jest odpowiedzialność za bezpieczeństwo państwa;
- nieznamomości zasad zachowania się w przypadku zagrożenia atakiem terrorystycznym i postępowanie z ujawnionymi oznakami (potencjalnego lub przypadkowego) zagrożenia. Mam na myśli działania „Panów ochroniarzy” z NCBJ w Świerku;
- małej wyobraźni ludzi będących na najniższych szczeblach ochrony infrastruktury krytycznej, spełniających swoją pracę formalnie, na zasadach „bramkarza” sprawdzającego przepustkę.

Nie będę podejmował problematyki oraz tematu uruchomienia procedury „Renegade” i co by się za tym kryło z przyczyn obiektywnych. W każdym bądź razie ta procedura mogła sprowadzić szereg nieszczęść na amatorów filmów z lotu ptaka.


Wszystkich czytelników chcę w związku z powyższym wydarzeniem sprowokować do udzielenia odpowiedzi na dwa proste pytania:



Mapa 2. Narodowe Centrum Badań Jądrowych

Źródło: Otwock, Józefów, Karczew, Plan Miasta, Agencja Regraf 2007.

- co by było gdyby to był prawdziwy atak terrorystyczny?
- czy inne obiekty np. przemysłowe, komunalne i użyteczności publicznej nie mogą znaleźć się podobnej sytuacji, ale jako cel potencjalnego ataku.

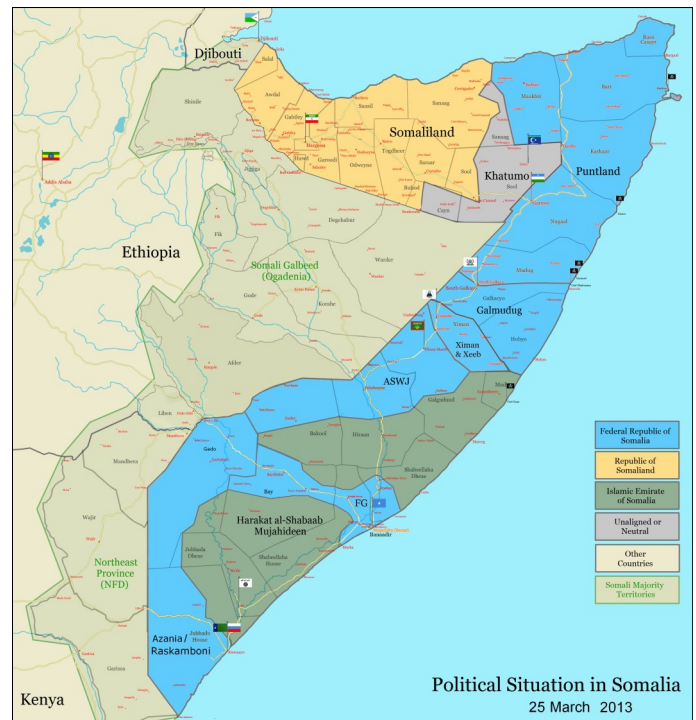
W kontekście wydarzenia w przestrzeni powietrznej Narodowego Centrum Badań Jądrowych w Świerku jest jednak pozytywny wydźwięk – reakcja dyżurnego kontroli lotów lotniska z Okęcia oraz Policji w Otwocku. I dobrze, że jeszcze ktoś ma odrobinę wyobraźni. 

**dr Czesław Marcinkowski**  
Wszechnica Polska  
Szkoła Wyższa w Warszawie

## Terroryzm Al-Shabaab

Upadek państwowości w Somalii na przestrzeni ostatnich 20-stu lat stworzył sprzyjające warunki do rozwoju wszelkiego rodzaju przestępczości, w tym, tej o zasięgu międzynarodowym. Nieвозмоść państwa wyrażona brakiem nadzoru i regulacji procesów społecznych i politycznych na własnym terytorium, jak zauważył Marek Madej, oznacza dla podmiotów pozapaństwowych szersze perspektywy rozbudowy struktur transnarodowych oraz nowe obszary, formy i rodzaje aktywności. Przykładowo istnieje szansa wzrostu nielegalnej działalności, jak handel narkotykami czy bronią, zasilającej źródło utrzymania grup eksterminacyjnych<sup>1</sup>. Somalia idealnie pasuje do powyższego opisu. Piractwo, zagrażające bezpiecznej żegludze na wodach Zatoki Adeńskiej i Oceanu Indyjskiego oraz skrajne islamskie organizacje o charakterze militarnym, szerzące terror w regionie, to dzisiaj bolączka całej społeczności międzynarodowej.

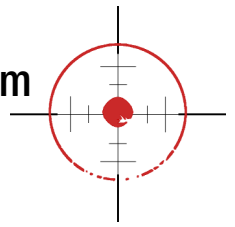
W doniesieniach prasowych Somalia często określana jest jako przystań światowego terroryzmu, podobnie jak Afganistan czy Pakistan. Czy rzeczywiście kraj ten jest bezpieczną oazą dla terrorystów? Próbę odpowiedzi na tak postawione pytanie podjęła Julie Cohn w artykule „*Terrorism havens: Somalia*”<sup>2</sup>. Z jednej strony, Somalia jest biednym, pogrążonym w chaosie, muzułmańskim krajem, bez centralnego rządu, ale z długą, niestrzeżoną linią brzegową. Daje to każdemu możliwość przedostania się na terytorium kraju bez konieczności posiadania wizy, a w samym interiorze, nie ma żadnych przeszkód prawnych do prowadzenia określonej działalności. Te czynniki z całą pewnością czynią Somalię atrakcyjnym miejscem dla transnarodowego terroryzmu, co już wcześniej próbowała wykorzystać al-Kaida.



Obecny „podział wpływów” w Somalii. Kolory: Niebieski - Federalna Republika Somalii. Żółty - Republika Somalilandu. Zielony - Islamski Emirat Somalii. Szary - Niesprzymierzeni bądź neutralni. Zakres zielony - Obszar z większością ludności Somalijskiej poza granicami (~97% ludności w kraju).  
Fot. commons.wikimedia.org

Z drugiej strony, topografia Somalii w żaden sposób nie może równać się z afgańską, która oferuje mnóstwo naturalnych kryjówek, koniecznych do prowadzenia terrorystycznej działalności. Kolejną przeszkodą, zdaniem autorki wspomnianego już artykułu, to struktura klanowa somalijskiego społeczeństwa, które bardzo wrogo nastawione jest do wszelkich obcych ideologii, w tym, ideologii eksterminacyjnych. Co więcej, Somalijczycy od początku byli wyznawcami islamu sufickiego, czyli tego bardziej umiarkowanego. Fundamentalizm islamski jest dla nich czymś absolutnie nowym.

W latach 90-tych ubiegłego stulecia al-Kaida, wycofała się z Somalii, bo jak stwierdził były amba-



## Terroryzm Al-Shabaab

sador USA w Etiopii, David Shinn, jej liderzy przece-  
nili stopień zaangażowania samych Somalijczyków  
w ogłoszony przez nich *dżihad*<sup>3</sup>. Zdaniem autorki,  
może to być dobra prognoza w obliczu ciągle wzmo-  
żonej aktywności fundamentalistów z Al-Shabaab  
na południu kraju. To właśnie ta grupa obecnie  
uważana jest za największe terrorystyczne zagroże-  
nie nie tylko dla Somalii ale i dla całego Rogu Afry-  
ki. Szczególnie po tym jak w lutym 2012 roku przy-  
wódca al-Kaidy, Alman al-Zawahiri, oficjalnie poin-  
formował o współpracy między dwoma organizacja-  
mi<sup>4</sup>. Kim zatem są bojownicy Al-Shabaab?

Organizacja Al-Shabaab, której pełna nazwa  
brzmi Ruch Młodych Bojowników Świętej Wojny (w  
skrótce: „Młodzi”), to radykalna, somalijska, islami-  
styczna organizacja militarna, obecnie licząca ok.  
15 tysięcy bojowników<sup>5</sup>. Potocznie jej członkowie  
nazywani są *szababami*. Pierwotnie organizacja ta  
była skrzydłem zbrojnym Unii Trybunałów Islam-  
skich, która w 2006 roku przejęła kontrolę nad po-  
łową Somalii. W 2007 roku, w skutek interwencji  
etiopskiej w Somalii, wspieranej przez rząd amery-  
kański, grupa ta wzięła udział w bitwie o Mogadi-  
szu. Po zajęciu stolicy przez wojska etiopskie, *sza-  
babowie* skupili się na umacnianiu swojej pozycji  
na południu kraju. To czas kiedy zaczyna się dzia-  
łalność terrorystyczna organizacji. W 2008 roku  
zorganizowali, przy użyciu granatów, atak na etiop-  
skich emigrantów w Bosaso, miejscowości na pół-  
nocy Somalii. Zginęło wówczas, jak pisze Jakub  
Kłószewski, 25 osób a blisko 90 zostało rannych<sup>6</sup>.  
To wtedy amerykański rząd wpisał ugrupowanie na  
listę organizacji terrorystycznych.

W 2009 roku, kiedy wojska Etiopii opuściły  
Mogadysz i władzę w stolicy przejęła Unia Trybuna-  
łów Islamskich, *szababowie* wypowiedzieli wojnę  
nowemu rządowi, oskarżając przywódcę Unii i jed-  
nocześnie nowego prezydenta Sharifa Sheikha  
Ahmeda, o kolaborację z władzami Etiopii. Nie prze-  
konało ich nawet wprowadzenie *szariatu*, co zresz-



Al-Shabaab, flaga wojenna.

tą wcześniej postulowali. Zdaniem autorki to poka-  
zuje, że religia jest dla tych grup tylko pretekstem  
do podejmowania działalności przestępczej, środ-  
kiem, który pozwala na realizację chorych politycz-  
nych ambicji kilku liderów, żadnych władzy i zysków  
jakie mogą z niej czerpać.

Dobitnie obrazuje to sytuacja ludności za-  
mieszkującej na terytorium kontrolowanym przez  
*szababów*. Jako zwolennicy wahabickiej wersji isla-  
mu występującej w Arabii Saudyjskiej, wprowadzają  
własną interpretację *szariatu*, zamieniając życie  
lokalnych mieszkańców w horror. Zakazano wszel-  
kich nie-islamskich rozrywek typu słuchanie muzy-  
ki, taniec, palenie, sprzedaż i żucie *khatu* – narko-  
tycznej rośliny. Cudzołóstwo karane jest kamienio-  
waniem a kradzież obcięciem kończyny<sup>7</sup>. Jak poda-  
je *Human Rights Watch* w raporcie dotyczącym sy-  
tuacji w Somalii, szczególnego dramatu doświad-  
czają kobiety. Ponad to, publiczna chłosta, masowe  
egzekucje domniemanych zdrajców poprzez ścięcie  
głowy – to codzienność. Wszystko to w oparciu  
o doraźne wyroki. Na terenach zajętych przez bo-  
jowników obserwowane jest zjawisko uprowadza-  
nia młodych chłopców i siłowego wcielania do ar-  
mii. Bardzo często atakują oni szkoły i tam dokonu-  
ją rekrutacji. Wspomniano też o aktach przemocy  
wobec wyznawców innych religii, głównie chrześci-

jan. Szczególnie narażeni są pracownicy akcji humanitarnych i organizacji międzynarodowych, pracujących w Somalii<sup>8</sup>.

Prawdziwe oblicze *szababów* świat, a także sami Somalijczycy, poznali w 2011 roku, kiedy w Somalii z powodu głodu umierały tysiące osób, a bojownicy skutecznie blokowali wszelkie próby niesienia pomocy głodującym. Nie zgadzając się z oficjalną decyzją ONZ o ogłoszeniu klęski głodu w rejonie, którą uznali za przesadzoną, uniemożliwiali pomoc potrzebującym. Z powodu skrajnej niechęci do organizacji zagranicznych, dokonywali i nadal dokonują zuchwałych ataków na transporty z żywnością, oskarżając pracowników tych organizacji o szpiegostwo i szerzenie chrześcijaństwa.

Dopóki nie ujawniono powiązań somalijskich islamistów z al-Kaidą, ich działalność przez ekspertów była postrzegana jako zagrożenie dla Somalii, jednak nie dla świata. Dzisiaj zachodni analitycy nie mają złudzeń, że Al-Shabaab stanowi zagrożenie dla pokoju, stabilności i bezpieczeństwa w znacznie szerszym, międzynarodowym znaczeniu. Grupa aktywnie umacnia powiązania z innymi ekstremistycznymi organizacjami takimi jak *Muslim Youth Centre (Al-Hijra)* w Kenii czy *Ansar Muslim Youth Centre* in Tanzania. Obie organizacje zajmują się gromadzeniem funduszy na działalność Al-Shabaab, oraz rekrutacją i wysyłką nowych bojowników do Somalii<sup>9</sup>. Obawy mają też sami Amerykanie, ponieważ Al-Shabaab skutecznie rekrutuje swoich bojowników wśród somalijskiej diaspory w Minnesocie. FBI uważa to za czołowe wewnętrzne zagrożenie terrorystyczne<sup>10</sup>. Ochotnicy pochodzą też z innych zachodnich państw. Zamachowiec – samobójca, który wysadził się w punkcie kontrolnym w mieście Baidoa na południu Somalii w 2007 roku, zabijając 20 żołnierzy, był 21 latkiem dorastającym w londyńskiej dzielnicy Ealing, który porzucił studia w Oxfordzie i przyłączył się do terrorystów w Somalii<sup>11</sup>. Jego rodzina ciągle mieszka w Anglii i

## Terroryzm Al-Shabaab



Widok zniszczonej ulicy w centrum Mogadishu, po trwających kilka dni walkach z ugrupowaniem Al-Shabaab. 5 sierpnia 2011 r.

Fot. Africa Renewal,

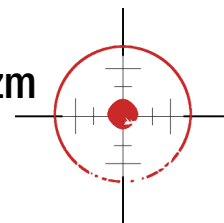
<http://www.flickr.com/photos/africa-renewal/6036306900/>

nie zezwoliła na ujawnianie imienia i nazwiska zamachowca. Wśród przybyłych do Anglii emigrantów z Somalii byli Yasin Omar i Ramzi Mohammed, skazani za podłożenie bomb w londyńskim metrze 21 lipca 2005 roku<sup>12</sup>.

Lista przestępstw i zamachów zorganizowanych przez członków Al-Shabaab jest bardzo długa. Oprócz notorycznych zamachów bombowych w Mogadishu i innych somalijskich miastach, wymierzonych przeciwko pracownikom rządowym i żołnierzom AMISOM, organizacja przyznała się do zamachu w Kampali – stolicy Ugandy w czerwcu 2010 roku. Zginęło w nim 76 osób oglądających finałowy mecz mistrzostw świata. W ten sposób *szababowie* ukarali Ugandę za wysłanie swoich żołnierzy do Somalii, jednocześnie kierując ostrzeżenie do innych państw, angażujących się w próbę rozwiązania konfliktu somalijskiego.

Somalijskich bojowników oskarża się także o uprowadzanie zagranicznych turystów z Kenii. We wrześniu 2011 roku zamordowano brytyjskiego obywatela, a jego żonę uprowadzono. Miesiąc później porwano niepełnosprawną turystkę z Francji. Zarówno Brytyjczycy jak i Francuzka wypoczywali na






kenijskim wybrzeżu, skąd siłą zabrała ich grupa uzbrojonych mężczyzn. Według świadków łodziami przetransportowano ich w kierunku Somalii. W październiku z Kenii uprowadzono także dwie hiszpańskie obywatelki, pracujące dla organizacji Lekarze Bez Granic<sup>13</sup>. Incydenty te przyspieszyły decyzję rządu kenijskiego o wysłaniu do Somalii wojsk, mających wesprzeć AMISOM.

W styczniu 2013 roku głośno było w światowych mediach o nieudanej próbie odbicia francuskiego zakładnika, Denisa Allexa z rąk radykalnych somalijskich islamistów. Przetrzymywany od lipca 2009 roku Francuz był agentem tajnych służb DGSE. Został zatrzymany w Mogadiszu, razem z innym agentem, któremu udało się uciec z rąk porwaczy. Obaj panowie pracowali jako doradcy rządu tymczasowego, którego jurysdykcji nie uznawało Al-Shabaab. W akcji, jak oficjalnie podał rząd francuski, zginęło dwóch komandosów oraz siedemnastu bojowników islamskich. Zginął też zakładnik, jednak nie wiadomo czy zabito go w czasie akcji, czy kilka dni później, ponieważ stanowiska stron są sprzeczne<sup>14</sup>.

„Somalia nigdy nie stanie się drugim Pakistanem, ale to nie znaczy, że nie jest zagrożeniem” – taką opinię wyraził dr Peter Neumann z Centrum Studiów nad Terroryzmem w King’s College w Londynie<sup>15</sup>. Pozornie wydaje się, że Al-Shabaab jest tylko lokalną organizacją, która nie ma takiej siły i środków, aby móc zorganizować zamach terrorystyczny. W połączeniu z Al-Kaidą, jest to już wysoce prawdopodobne. Ponad to, zdaniem autorki, zagrożenie płynie z faktu rekrutacji swoich „żołnierzy” wśród Somalijszczyków mieszkających w krajach Zachodu. Wyszukani w obozach szkoleniowych w Somalii, a co do faktu ich istnienia nie ma wątpliwości, z łatwością mogą przenosić pewne treści na terytorium Europy czy Stanów Zjednoczonych i tam je urzeczywistniać.

W opinii autorki, istnieje jeszcze jeden powód dla którego sytuacja w Somalii powinna być monitorowana. Kraje Rogu Afryki to ważny kanał przemytu broni i narkotyków z azjatyckiego Środkowego Wschodu do Europy. Somalia w tej kwestii to przypadek szczególnie – jak podaje Artur Gruszczak, na jej terytorium „działają liczne grupy przestępcze trudniące się kontrabandą, przemytem broni i narkotyków, fałszowaniem środków płatniczych i podrabianiem dokumentów”<sup>16</sup>. To wystarczające powody, aby nie pozostawiać Somalii samej sobie. 

### Przypisy

- 1 Zob. szerzej: M. Madej, Zagrożenia asymetryczne. Bezpieczeństwo państw obszaru transatlantyckiego, Warszawa 2007, s. 54-61
- 2 Zob. szerzej: Julie Cohn, Terrorism havens: Somalia, June 2010, Council on Foreign Relations, [www.cfr.org](http://www.cfr.org).
- 3 Tamże.
- 4 Zob. szerzej: National Counterterrorism Center/Groups/ Al-Shabaab, [www.nctc.gov](http://www.nctc.gov).
- 5 T. Strójwąg, Rozwój sytuacji w Jemenie i Somalii jako przykład szans i zagrożeń dla pokoju i bezpieczeństwa na półwyspie Arabskim i Rogu Afryki. Tekst zamieszczony w monografii stanowiącej podsumowanie II Międzynarodowej Konferencji Naukowe „Czarny Łąd i Świat Arabski”, Gdynia 2012, s.207, [www.struna.edu.pl](http://www.struna.edu.pl).
- 6 J. Kłoszewski, Somalia: Szababowie, czyli kto?, 27 stycznia 2013, Polityka Globalna, [www.politykaglobalna.pl](http://www.politykaglobalna.pl).
- 7 Zob. szerzej: Jonathan Masters, Al-Shabaab, 5 February 2013, Council on Foreign Relations, [www.cfr.org](http://www.cfr.org).
- 8 Human Rights Watch, World Report 2012; Somalia, s. 3-4, [www.hrw.org](http://www.hrw.org).
- 9 Raport ONZ dotyczący Somalii i Erytrei z 27 czerwca 2012, s.. 92, [www.somaliareport.com](http://www.somaliareport.com).
- 10 Zob. szerzej: Jonathan Masters, Al-Shabaab, 5 February 2013, Council on Foreign Relations, [www.cfr.org](http://www.cfr.org).
- 11 Zob. szerzej: Euroislam, Somalijscy fundamentaliści przynoszą terror do Anglii, 27 lutego 2009, [www.euroislam.pl](http://www.euroislam.pl).
- 12 Tamże.
- 13 Zob. szerzej: Jeffrey Gettleman, Gunmen seize 2 aid workers near Kenya-Somalia border, 13 October 2011, [www.nytimes.com](http://www.nytimes.com).
- 14 J. Kłoszewski, Somalia: Szababowie, wyd. cyt..
- 15 Zob. szerzej: Euroislam, Somalijscy fundamentaliści przynoszą terror do Anglii, 27 luty 2009, [www.euroislam.pl](http://www.euroislam.pl).
- 16 A. Gruszczak, Państwa upadłe jako zagrożenie bezpieczeństwa wewnętrznego UE, [w:] Problem upadku państw w stosunkach międzynarodowych, red. R. Kłosowicz, A. Mania, Kraków 2012, s. 183.

## Zjawisko terroryzmu w Inguszetii

Inguszetię zawsze dotykały różne problemy natury etnicznej ze strony władz ZSRR. Od 1934 do 1936 r. Inguszetia była połączona z Czechenią i tworzyła Czecheńsko-Inguski Obwód Autonomiczny, jednak wraz z powstaniem nowej konstytucji stalinowskiej pod koniec 1936 r. Inguszetia wraz z Czechenią tworzyły już Czecheńsko-Inguską ASRR. Nastąpił rok 1944 r. a konkretnie 23 lutego tego roku. Józef Stalin rozkazał wywieźć niepokorne ludy kaukaskie do niezaludnione tereny Turkestanu, a głównie Kazachstanu, ale również Kirgistanu czy Uzbekistanu oraz Południowej Syberii. Od roku 1956 r. Inguszowie i Czecheni dekretem Nikity Chruszczowa mogli wrócić do swoich ojczyzn ziem po wielkiej stalinowskiej deportacji z lutego 1944 r. W 1957 r. przywrócono ponownie do życia Czecheńsko-Inguską ASRR.

Czecheńsko-Inguska ASRR przestała istnieć 4 czerwca 1992 r., ze względu na różnice zdań dot. słynnego wyborczego Borysa Jelcyna "Bierzcie tyle wolności, ile jesteście w stanie unieść". Czechenia za wszelką cenę nie chciała podpisać układu federacyjnego z 31 marca 1992 r. Inguszetia podpisała, gdyż Borys Jelcyn obiecywał, że od momentu podpisania owego układu skończą się problemy Inguszetii z Osetią Północną<sup>1</sup>.

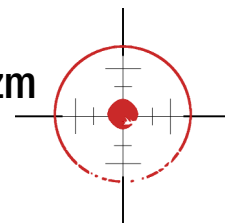
Sytuacja zmieniła się po usunięciu przez Moskwę prezydenta Inguszetii generała Rusłana Auszewa i wyznaczeniu na jego stanowisko niezdecydowanego, pozbawionego charyzmy i poparcia społecznego, lecz całkowicie lojalnego wobec Kremla Murata Ziazikowa (oficera Federalnej Służby Bezpieczeństwa w maju 2001 r.). Inguszetia została wówczas faktycznie, choć nie formalnie objęta operacją antyterrorystyczną, co oznaczało m.in. skierowanie do republiki dodatkowych oddziałów armii, MSW i FSB<sup>2</sup>. Ofiarami stosowanych przez nie repre-



Mapa polityczna Kaukazu. Inguszetia w centrum, obok Czechenii oraz Osetii Północnej. Fot. Jeroencommons commons.wikimedia.org

sji byli początkowo przebywający w Inguszetii uchodźcy czecheńscy, prześladowania objęły jednak wkrótce również społeczeństwo inguskie. Próby pokojowych protestów i apeli do Moskwy, organizowane m.in. przez opozycję skupioną wokół Magomieda Jewłojewa (założyciela cieszącej się ogromną popularnością niezależnej od władz strony internetowej *ingushetiya.ru*) i Makszaripa Auszewa nie przyniosły żadnych rezultatów. Obaj przywódcy zostali zamordowani<sup>3</sup>.

W Inguszetii nie było terroryzmu przez wiele lat oraz za kadencji prezydenta Rusłana Auszewa. Generał, był popularny wśród ludności inguskiej oraz utrzymywał pokój i stabilność w swojej republice. Wpuszczał czecheńskich uchodźców w trakcie pierwszej wojny czecheńskiej do swojej republiki mimo wydanej decyzji B. Jelcyna, aby zamknąć granice i ich nie wpuszczać. Kraj Stawropolski oraz Dagestan zastoso-

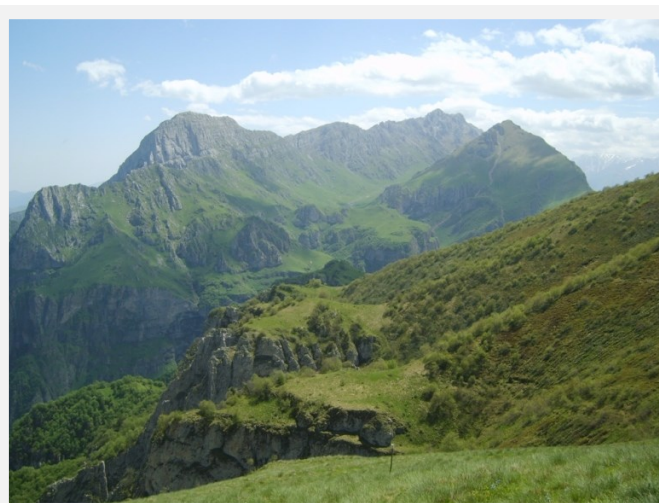


## Zjawisko terroryzmu w Inguszetii

wały się do decyzji ówczesnego prezydenta Rosji i uszczelniły swoje granice z Czeczenią. Auszew to także negocjator, który brał udział w rozmowach z terrorystami, którzy zajęli szkołę podstawową nr 1 w Biesłanie w republice Osetii Południowej, w dniach od 1 do 3 września 2004 r. Jako jedyny ze znanych ludzi na Kaukazie Północnym rozmawiał z terrorystami. Ówczesny prezydent Inguszetii, Murat Ziazikow Osetii oraz Władimir Putin, nie pofatygowali się na miejsce dramatu.

Obecny prezydent republiki Inguskiej, generał Junus-bek Jewkurow, nie cieszy się dobrą opinią wśród obywateli, jakby nie było jest to prokremlowski człowiek w Inguszetii. Popadł także w konflikt z innym prokremlowskim prezydentem Czeczenii Ramzanem Kadyrowem<sup>4</sup>. Chodzi o ustalenie granic pomiędzy Czeczenią i Inguszetią<sup>5</sup>.

Za Iwoną Kaliszewską: „Wciąż dochodzi tam do zamachów na organy władzy. Są to głównie wybuchy bomb oraz strzelaniny, zdarzały się też pojedyncze ataki terrorystyczne dokonywane przez terrorystów-



Krajobraz górski Inguszetii. Fot. Timur Ziev, commons.wikimedia.org.

samobójców. Warto jednak zwrócić uwagę na fakt, że w sąsiedniej Inguszetii, a nawet w Dagestanie (o których w mediach polskich lub zachodnich słyszymy niezwykle rzadko), tego typu zamachy to codzienność, do której mieszkańcy już dawno się przyzwyczaili. Akcje są *stricto* wymierzone przeciwko organom władzy –

	Region	Liczba wybuchów	Ataki Terrorystyczne	Wszyscy zabici i ranni (w nawiasach liczba rannych)	Zabici cywile (w nawiasach liczba rannych)	Zabici i ranni w zamachach samobójczych (w nawiasach liczba rannych)	Wybuchy w 2009 r.	Ataki samobójcze w 2009 r.
1	Dagestan	112	6	68 (195)	37 (65)	31 (132)	69	1
22	Czeczenia	39	4	41(88)	4(17)	23(54)	62	9
33	Północna Osetia-Ałanija	3	2	22(163)	20(163)	20(163)	-	-
34	Inguszetia	40	2	8(78)	4(39)	5(2)	86	4
45	Kabardo-Bałkaria	41	1	4(53)	1(37)	1	12	-
56	Stawropol	3	-	8(79)	8(79)	-	-	-
	<b>Razem:</b>	238	15	151(656)	74(400)	80(351)	229	14

Tab. 1. Ataki terrorystyczne i zamachy bombowe na Północnym Kaukazie w 2009 - 2010 r.

Źródło: <http://www.kavkaz-uzel.ru/articles/182170/>


policji, OMON-owi, urzędnikom MSW. Stosunkowo rzadko giną w nich cywile<sup>6</sup>. W tabeli 1. zaprezentowano daną za lata 2009-2010. Dane dot. liczby i charakteru ataków terrorystycznych mających miejsce w północnokaukaskich republikach Rosji.

Jednym ze skutków działań podejmowanych przez prorosyjskie formacje czeczeńskie przeciwko bojownikom, było przeniesienie się części ich oddziałów (a co za tym idzie, również prowadzonych przez nich działań dywersyjnych) do Inguszetii i Dagestanu<sup>7</sup>.

Jednak, jak donosi *Ria Novosti*, według kaukaskiej policji, obecnie działa 40 nielegalnych formacji zbrojnych i jest w nich około 600 bojowników na całym Północnym Kaukazie. Według szacunków policji, w Czeczenii jest dziesięć formacji, w Inguszetii - trzy, w Kabardyno-Bałkarii – pięć, w Karaczajo-Czerkiesji – jedna, a w Dagestanie – aż szesnaście formacji zbrojnych<sup>8</sup>. Terrorysty pochodzą także z Inguszetii, wskazuje na to fakt, iż w styczniu 2011 r., pochodzący z Inguszetii zamachowiec-samobójca wysadził się na moskiewskim lotnisku Domodedowo, zabijając trzydzieści siedem osób (dwie zmarły w szpitalu)<sup>9</sup>. W ciągu następnych miesięcy doniesienia o różnego rodzaju zamachach, porwaniach, eksplozjach i zbrojnych starciach napływały regularnie z Dagestanu, Czeczenii i Inguszetii (według danych Memoriału, od stycznia do czerwca w Dagestanie zginęło minimum 177 osób)<sup>10</sup>.

Zbliżające się Igrzyska Olimpijskie w Soczi (Kraj Krasnodarski) 2014 roku, mogą spowodować, iż może być nie tylko niebezpiecznie w Kraju Krasnodarskim, ale także w republikach na całym Kaukazie Północnym, w tym również w Inguszetii. Terrorysty z obozów Doku Umarowa, mogą werbować w Inguszetii, głównie Inguszy<sup>11</sup> do swoich szeregów, aby ci byli aktywni militarnie w Soczi w 2014 r. Chętnych może nie brakować. Brak perspektyw życiowych wśród Inguszy może spowodować, iż będą zasilac grupy terrorystyczne działające głównie m.in. w Dagestanie i sąsiedniej Czeczenii. Duże bezrobocie sięgające 49 proc. w okresie od października 2011 do stycznia

2012 r.<sup>12</sup>, może również być tym czynnikiem, które będzie przemawiać, że jednak warto przejść na stronę terrorystów kaukaskich.

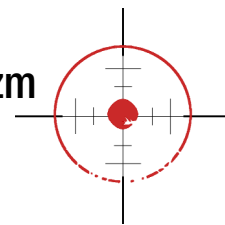
Reasumując należy podkreślić, iż, mimo, że Inguszetię nie zamieszkuje zbyt wielka liczba ludności to jednak republika jest podatna na wpływy terrorystów z obozów Doku Umarowa oraz innych lokalnych watazków. Wpływ może mieć także położenie geograficzne w Rosji, bliskość z obszarami, które słyną z walkami z terrorystami i terroryzmem powoduje, iż niebezpieczeństwo rozciąga się nie tylko od Dagestanu do Inguszetii, ale także aż po Kraj Krasnodarski po drodze zaczepiając o inne niespokojne republiki północnokaukaskie: Karaczajo-Czerkiesję oraz Kabardyno-Bałkarię i Osetię Północną. 

**Kamil Pietrasik**

(Wyższa Szkoła Studiów Międzynarodowych w Łodzi)

### Przypisy

- 1 Spory dot. głównie terenów, które należały do 1944 r. do republiki Inguskiej a pod wpływem zlikwidowania Cz-I ASRR, przeszły pod „skrzydła” Osetii Północnej. Głównie chodzi o obwód Prigorodny oraz o pierwszą inguską osadę – Władykaukaz, obecną stolicę Osetii Północnej.
- 2 M. Falkowski, M. Marszewski, Kaukaskie „terytoria plemienne”. Kaukaz Północny – cywilizacyjnie obca enklawa w granicach Rosji, „Prace OSW”, nr 34/2010, s. 20.
- 3 Tamże.
- 4 Najmłodszy prezydent Czeczenii, który funkcję pełni nieprzerwanie od 2007 r.
- 5 Do dziś nie ma ustalonej prawnie granicy między republikami.
- 6 I. Kaliszewska, Czeczenia Ramzana, „Nowa Europa Wschodnia” nr 5-6/2009, s. 121.
- 7 M. Falkowski, Czeczenia między kaukaskim dżihadem, a „ukrytym” separatyzmem, OSW, Warszawa 2007, s. 18.
- 8 <http://polit.ru/news/2013/01/25/boeviki>, dostęp: 2.08.2013.
- 9 W. Górecki, Dokąd zmierza Kaukaz Północny, „Nowa Europa Wschodnia”, nr 6/2011, s. 77.
- 10 Tamże.
- 11 W 2010 r. stanowili oni niemal 94.1 proc. społeczeństwa (ponad 385 tys. ludzi) zamieszkałego w tej republice, następni są Czeczeni: 4.6 proc. (ponad 18 tys.) oraz Rosjanie: 0.8 proc. (ponad 3 tys.) dane za: <http://www.perepis-2010.ru/news/detail.php?ID=6936>, dostęp: 3.08.2013.
- 12 Dane za: [http://ria.ru/research\\_rating/20120322/602723913.html](http://ria.ru/research_rating/20120322/602723913.html), dostęp: 3.08.2013.



NATALIA NOGA

## Cyberterroryzm - nowe oblicze terroryzmu, cz. V Internet jako cel ataków terrorystów - Klasyfikacja ataków w cyberprzestrzeni

**Obawy związane z aktywnością terrorystyczną w sieci w ostatnich latach przybierają na sile. W przypadku takich działań skutki destrukcyjne mogą mieć ogromny zasięg, tym bardziej, że uzależnienie społeczeństw od technologii informatycznych wciąż postępuje. Wielu specjalistów coraz częściej zdaje sobie sprawę z rosnącego zagrożenia zjawiskiem cyberterroryzmu.**

Dyrektor FBI - Louis Freeh twierdził, że FBI „uważa, że cyberterroryzm, czyli stosowanie cybernarzędzi do wyłączania, uszkodzania i powodowania zaniechania świadczenia usług przez infrastruktury krytyczne – takie jak energia, transport, łączność i służby rządowe – służy do wpływania siłą na działania rządu oraz do zastraszania władz i ludności. Jest to nowa groźba, która zmusza nas do stworzenia specjalnego systemu obrony, odstraszenia i odpowiadania na ataki”<sup>1</sup>. Wraz z rosnącym postępowaniem technologicznym i rosnącymi możliwościami jego niewłaściwego wykorzystania, należałoby sklasyfikować, z jakimi atakami ze strony organizacji terrorystycznych w sieci możemy mieć do czynienia. Zgodnie z definicją zjawiska „cyberterroryzmu” M. Pollita, wyróżnić można dwa rodzaje akcji cyberterrorystycznych, które mogą się wzajemnie uzupełniać i być samodzielną akcją lub częścią większej kampanii. Należą do nich: ataki mające miejsce w cyberprzestrzeni i ataki fizyczne na systemy informacyjne. Każdy z nich może zachwiać stabilność gospodarki.

W przypadku ataku fizycznego terrorystów w cyberprzestrzeni dokonują działań ułatwiających bądź pozorujących uderzenie w realnym świecie. Nie trzeba w tym przypadku znać się nawet na in-

formatyce, można użyć tradycyjnych środków (np. materiałów wybuchowych) i jedynie wiedzieć, gdzie uderzyć. Już w 1985 roku japońska grupa terrorystyczna Frakcja Środka uszkodziła kable telefoniczne i kable energetyczne systemu sterowania komputerowego ruchem pociągów, czym spowodowała chaos w komunikacji, w czasie największego ruchu. Atak miał być demonstracją solidarności ze strajkującymi kolejarzami, którzy protestowali przeciw prywatyzacji japońskich kolei. Wskutek działań około 6, 5 miliona osób nie dojechało do pracy<sup>2</sup>. Ataki mogą być zatem prowadzone starymi metodami, jednak zmienione zostały cele tych akcji – organizacje terrorystyczne zdają sobie bowiem doskonale sprawę z tego, że atak na infrastrukturę informacyjną może odnieść większe skutki niż atak konwencjonalny. Również w latach 70. organizacje terrorystyczne podejmowały próby niszczenia powstających sieci informatycznych. Firmy elektroniczne i komputerowe we Włoszech zostały 27 razy zaatakowane przez Czerwone Brygady, których członkowie głosili, że niszcząc systemy i instalacje komputerowe „atakują samo serce państwa”<sup>3</sup>. Fizyczne niszczenie elementów sieci komputerowych i infrastruktury informatycznej jest łatwe do przeprowadzenia, ale pozwala terrorystom jedynie na osiągnięcie efektu wyłącznie w skali lokalnej. Znaczenie tego ataku rośnie jednak, gdy stanowi element wspierający główną operację terrorystyczną.

Klasyczny atak mający miejsce w cyberprzestrzeni ma na celu ingerencję w sieci informatyczne, z zamiarem zniszczenia bądź uniemożliwienia ich funkcjonowania lub sprawowania nad nimi kontroli. Ataki te mogą obejmować oprogramowanie

przeciwnika (software) lub systemy informacyjne i sprzęt komputerowy (hardware). Ze względu na różnorodność form ataku oraz różnorodność kryteriów opisu tego zjawiska nie ma jednoznacznej klasyfikacji. W swojej książce „Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie” A. Bógdał – Brzezińska i M.F. Gawrycki przedstawiają w wyczerpujący sposób ten problem.

## Klasyfikacja ataków

Pierwszą, zaprezentowaną metodą klasyfikacji jest lista siedmiu kategorii działań w cyberprzestrzeni, opracowana przez S. Bellovina i W. Cheswicka:

1. Stealing passwords (tłum. z ang. kradzież haseł) – metoda polegająca na uzyskaniu haseł dostępu do sieci;
2. Social engineering (tłum. z ang. inżynieria społeczna) – wykorzystanie niekompetencji osób mających dostęp do systemu;
3. Bugs and backdoors (tłum. z ang. błędy i tylne drzwi) – używanie oprogramowania z nielegalnych źródeł lub korzystanie z systemu bez specjalnych zezwoleń;
4. Authentication failures (tłum. z ang. błędy uwierzytelniania) – zniszczenie lub uszkodzenie procedur mechanizmu autoryzacji;
5. Protocol failures (tłum. z ang. błędy protokołu) – wykorzystywanie luk w zbiorze reguł, które sterują wymianą informacji pomiędzy dwoma lub wieloma niezależnymi urządzeniami bądź procesami;
6. Information leakage (tłum. z ang. wyciek informacji) – uzyskanie informacji dostępnych tylko administratorowi, które niezbędne są do poprawnego funkcjonowania sieci;
7. Denial of services (tłum. z ang. odmowa usługi) – uniemożliwienie użytkownikom korzystania z systemu<sup>4</sup>.

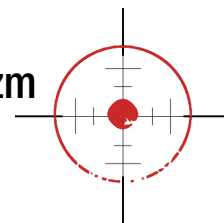
## Internet jako cel ataków terrorystów - klasyfikacja ataków w cyberprzestrzeni

Mając na uwadze powyższą listę kategorii, F. Cohen stworzył własną kategoryzację. Sformułowana jest ona na zasadzie opisu rezultatu ataku w cyberprzestrzeni:

1. Corruption (tłum. z ang. zepsucie, rozkład) – nieuprawniona zmiana informacji;
2. Leakage (tłum. z ang. wyciek) – informacja znalazła się w niewłaściwym miejscu;
3. Denial (tłum. z ang. odmowa) – kiedy sieć lub komputer nie nadają się do użytkowania<sup>5</sup>.

Atakujący dokonują uderzenia w niecodziennych sytuacjach. Wynika stąd, że działań w sferze cyberprzestrzeni nie da się zakwalifikować wyłącznie do jednej kategorii. Dłuższą listę, opartą na danych empirycznych, stworzyli zatem P. Neumann i D. Parker. Lista ta daje możliwość klasyfikacji różnego rodzaju ataków:

1. External Information Theft (tłum. z ang. zewnętrzna kradzież informacji) – kradzież lub przeglądanie informacji przez osobę spoza systemu;
2. External Abuse of Resources (tłum. z ang. zewnętrzne nadużywanie zasobów) – niszczenie twardego dysku;
3. Masquerading (tłum. z ang. podszycie, maskarada) – podawanie się za kogoś innego;
4. Pest Programs (tłum. z ang. szkodliwe programy) – instalacja złośliwego programu;
5. Bypassins Authentication or Authority (tłum. z ang. omijanie autentyczności lub autoryzacji) – łamanie haseł;
6. Authority Abuse (tłum. z ang. nadużywanie autoryzacji) – fałszowanie danych;
7. Abuse Through Inaction (tłum. z ang. nadużywanie bezczynności) – celowe prowadzenie złego zarządzania;
8. Indirect Abuse (tłum. z ang. pośrednie nadużycie) – używanie innych systemów do tworzenia złośliwych programów<sup>6</sup>.



Kategoryzacja ta wydaje się najpełniejsza spośród wcześniej omawianych. Innym rozwiązaniem, stworzonym przez C. Landwehra i A.R. Buli, są tzw. matryce pojęciowe. Opierają się one na następujących aspektach:

1. Genesis (tłum. z ang. geneza) – wykorzystaniu luk w zabezpieczeniach;
2. Time of Introduction (tłum. z ang. moment wprowadzania) – czasie „życia” oprogramowania i sprzętu komputerowego;
3. Location (tłum. z ang. lokalizacja) – lokalizacji „dziur” w oprogramowaniu i sprzęcie komputerowym<sup>7</sup>.

Matryca ta bardzo dokładnie opisuje różne rodzaje ataków w cyberprzestrzeni. Jednak przydaje się do klasyfikacji indywidualnych uderzeń (takich, które można przypisać do jednej kategorii). Nie jest to łatwe w przypadku ataków złożonych.

Inną, ostatnią już klasyfikacją opartą na działaniu jest zdefiniowanie czterech rodzajów ataków przez W. Stallingsa. Ma jednak ona ograniczoną możliwość zastosowania, gdyż dotyczy jedynie ataków traktowanych jako seria działań. Są to:

1. Interruption (tłum. z ang. przerwanie) – nie można zastosować zabezpieczenia systemu lub zostało ono zniszczone;
2. Interception (tłum. z ang. przechwytywanie) – dostęp do istniejących zabezpieczeń zdobyła nieuprawniona osoba;
3. Modification (tłum. z ang. modyfikacja) – nieuprawniona osoba zdobyła dostęp a także manipulowała zabezpieczeniem;
4. Fabrication (tłum. z ang. produkcja) – przez nieuprawnioną osobę do systemu wprowadzony został sfałszowany obiekt<sup>8</sup>.

Przedstawiona różnorodność klasyfikacji aktów cyberterrorystycznych jest dowodem na wieloaspektowość tego zagadnienia, jak również dynamikę zjawisk zachodzących w cyberprzestrzeni. Stwo-

wienie słownika pojęć związanych z cyberterroryzmem daje zatem możliwość scharakteryzowania różnego rodzaju ataków w cyberprzestrzeni.

### Metody ataków

Bardzo przydatne w ustaleniu potencjalnych metod, jakimi mogą posługiwać się cyberterrorysty, są informacje uzyskane od pana mgr. Waldemara Mielniczek – dostawcy Internetu w firmie Neconet. Osoba ta jest specjalistą w zakresie bezpieczeństwa sieci i wielokrotnie w swojej pracy miała do czynienia z przestępcami komputerowymi. Co prawda, nie można było ich zaliczyć do grona cyberterrorystów, ale nie należy zapominać, że cyberterrorysty mogą się również posługiwać tradycyjnymi i prostymi metodami, a cyberprzestępczość coraz częściej przyjmuje wymiar cyberterroryzmu. W rozmowie, mgr W. Mielniczek wspomina, że najczęstszą metodą działań osób niepożądanych w sieci jest zdobywanie informacji, które są niezbędne do poprawnego działania sieci dostępnych wyłącznie dla administratora, a ponadto uniemożliwienie użytkownikom korzystania z ich systemów. Twierdzi również, że jedną z bardziej popularnych metod cyberataku, może być uzyskanie dostępu do sieci za pomocą hasła poprzez wykorzystanie niekompetencji osób mających dostęp do systemu. Ponadto, cyberagresorzy, aby mieć dostęp do sieci, mogą zniszczyć mechanizm używany do autoryzacji, wykorzystać luki w zbiorze reguł sterujące wymianą informacji pomiędzy dwoma (lub wieloma) niezależnymi urządzeniami lub procesami a także korzystać z systemu bez specjalnych zezwoleń lub używać oprogramowania z nielegalnych źródeł. Rozmówca oprócz udzielenia informacji na temat potencjalnych metod ataku cyberterrorystów wyraził opinię nt. możliwości przeprowadzenia takiego cyberataku. Jest zdania, że w dobie społeczeństwa informacyjnego i niezwykle dynamicznego rozwoju systemów kom-

puterowych a także nieograniczonego dostępu do Internetu w oczywisty sposób jesteśmy narażeni na ataki, a przestępczość będzie coraz częściej przybierać taką formę. Twierdzi, że jest to łatwe do przeprowadzenia, a narzędzia do przeprowadzenia takiego ataku są dostępne nawet w Internecie.

Podobnie twierdzi Grzegorz Krasnodębski, który wymienia zagrożenia wynikające z ataków w cyberprzestrzeni. Widać, że jest ich bardzo wiele. Niektóre z nich wskazują na aktywność niszczącą, inne na zakłócającą. Ponadto, niektóre wskazują, że środkami do prowadzenia ataków mogą być zasoby komputerowe, inne, że systemy informacyjne są celami tych ataków. Zdaniem tego autora zauważyć można, iż wśród najczęstszych zagrożeń wynikających z ataków w cyberprzestrzeni są:

1. Uszkodzenie i nieuprawnione modyfikacje łącz telekomunikacyjnych;
2. Brak wiedzy oraz świadomości wśród personelu i kadry zarządzającej w zakresie bezpieczeństwa teleinformatycznego;
3. Niewłaściwa ochrona elementów sieci;
4. Niepożądane działania administratorów i użytkowników, a nawet celowe wprowadzanie szkodliwego oprogramowania do systemów lub jego uszkodzenie<sup>9</sup>.

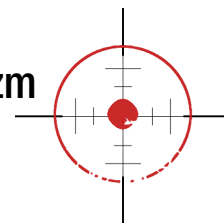
Nieco inny podział metod ataku opisuje w swoim artykule R. Kośla. Jego zdaniem, ogólne metody ataku cyberterrorystycznego to: metoda fizyczna, ataki elektroniczne i ataki sieciowe<sup>10</sup>. W metodzie fizycznej użyte są środki konwencjonalne, które skierowane zostają przeciw instalacjom komputerowym lub liniom transmisyjnym. Dominują tu działania związane z np. niszczeniem infrastruktury teleinformatycznej za pomocą materiałów wybuchowych lub przerywaniem linii przesyłowych. Ataki elektroniczne realizowane mogą być poprzez szereg sposobów wykorzystujących zjawiska fizyczne – począwszy od impulsu elektromagnetycznego

(wyzwalanego np. w czasie wybuchu jądrowego) poprzez stosowanie silnych pól magnetycznych, skończywszy na zastosowaniu urządzeń elektronicznych do generowania silnego pola elektromagnetycznego o określonej charakterystyce<sup>11</sup>. Niektórzy specjaliści twierdzą, że nawet oddziaływanie telefonu komórkowego ma negatywne skutki, gdyż za jego pomocą można otworzyć zatrask zamka elektronicznego lub uszkodzić płytę główną komputera PC. Mówiąc o atakach sieciowych, należy wziąć pod uwagę przede wszystkim nieupoważnione wejście do systemu czy manipulowanie informacją, jak również wszelkie ataki na usługi dostępne w sieci. Posługujący się tą metodą cyberterrorysty (jak niemal wszyscy przestępcy komputerowi) działają wg pewnego schematu. Zawiera on następujące kroki:

1. Rekonesans. W etapie tym cyberterrorysta poszukuje danych, które mogą być użyteczne w późniejszym nielegalnym dostępie do sieci – wirusy, metody socjotechniczne.
2. Skanowanie. Etap ten polega na sprawdzeniu przez atakującego, na ile wiarygodne i użyteczne są zdobyte informacje. Tworzone jest oprogramowanie wykorzystane później do ataku, jednak jeszcze nie odbywa się ingerencja w system.
3. Uzyskanie dostępu. Krok ten polega na przejęciu kontroli nad systemem – cyberterrorysta może np. nadać sobie uprawnienia administratora.
4. Zacieranie śladów. Ostatni etap obejmuje zniszczenie wszelkich śladów w systemie, które mogły zarejestrować działanie cyberterrorysty (pod warunkiem, że celem ataku było utrzymanie tego w tajemnicy, a nie działanie spektakularne)<sup>12</sup>.

Metody cyberataków identyfikuje w swym raporcie też M.A.Vatis<sup>13</sup>. Uwzględnia on podział na:





- a. Modyfikowanie stron WWW, szerzenie informacji i propagandę;
- b. Sabotaż komputerowy, którym jest naruszenie lub paraliżowanie systemów komputerowych za pomocą wirusów i robaków komputerowych lub poprzez przeprowadzenie ataków na DoS (Denial of Service Attacks);
- c. Zamachy mogące powodować zakłócenia w funkcjonowaniu infrastruktury krytycznej i zniszczenie danych dla niej kluczowych.

Strony WWW – jak powszechnie wiadomo – mogą być wykorzystywane na wiele sposobów, głównie przez firmy. Jednym z nich jest reklama, która pozwala ukazać najnowsze osiągnięcia, gadżety czy podać szczegółowe informacje o ważnych działaniach. Wszystkie te działania – mimo, że pozytywne dla przemysłu technologicznego, mogą stanowić zagrożenie bezpieczeństwa narodowego. Ponadto, internetowe strony WWW są znakomitym miejscem dla terrorystów poszukujących informacji o infrastrukturze krytycznej, która może być zarazem potencjalnym celem ataku. Gdy terrorysta zbierze potrzebne mu informacje z różnych stron i połączy je w całość, może otrzymać informację, która powinna być zakwalifikowana jako tajna. Najlepszym przykładem będzie znalezienie w jaskiniach Afganistanu laptopa należącego do jednego z członków AI - Kaidy. W komputerze tym znajdowały się ważne informacje na temat amerykańskiej infrastruktury.


Ataki na strony WWW prowadziła również pro-palestyńska grupa hackerska USG (Unix Security Guards). Miała ona na celu przeciwstawienie się amerykańskiej wojnie z terroryzmem i działaniom określanym jako agresja Indii przeciw muzułmanom w Kaszmirze. Grupa zniekształcała strony WWW, które wyglądały jak montaż multimedialne. Często złożone były z muzyki arabskiej i zdjęć zniszczeń. Grupę tą uznano za odpowiedzialną za zniszczenie

prawie 2 tysięcy stron WWW i umieszczenie na nich informacji antyizraelskich i antyamerykańskich. Kolejną powstała grupa pro-palestyńska było WFD, która identyfikuje się ideologicznie z organizacją terrorystyczną, jaką jest Hezbollah. Przeprowadzała ona dobrze zorganizowane operacje, których skutkiem było m.in. zablokowanie oficjalnej strony wyborczej izraelskiego premiera Ariela Sharony oraz spenetrowanie indyjskiego Ministerstwa Informacji i Technologii<sup>14</sup>. Działania te pokazały, że grupy hackerskie mogą spowodować bardzo poważne uszkodzenia i zniszczenia – a w przypadku tej grupy nawet kryzys w Izraelu. Wydawać się może, że uszkodzenie stron WWW nie są poważnym problemem, ale jednak mogą być one doskonale zorganizowane, a cele ataku są zwykle przemysłowe. Innym przykładem, w 2001 roku, grupa będąca muzułmańskim sojuszem AI - Kaidy zwana AIC (Anti-India Crew) przeprowadziła ataki na serwery należące do Generalnego Biura Rozrachunkowego GAO (odpowiednik polskiej Najwyższej Izby Kontroli). Do grupy tej należą osoby z profesjonalnym wykształceniem, a także posiadacze certyfikatów z różnych dziedzin wiedzy technicznej. Oprócz zniszczenia witryny GAO wyłączono internetowy system automatycznego rozsyłania raportu oraz zmodyfikowano stronę tak, by wyświetlała komunikat głoszący: „Będziemy atakować serwery rządowe (amerykańskie, indyjskie i izraelskie), aż wokół nas zapanuje pokój!”<sup>15</sup>.

Grupy terrorystyczne mogą również prowadzić akcje sabotażowe. Kampanię taką zauważono już w 1997r. Na przedmieściach Algierii muzułmańscy fundamentaliści fizycznie zaatakowali systemy telekomunikacyjne i sparaliżowali algierski system telefoniczny. Ataki przyczyniły się do uniemożliwienia korzystania z telefonów na przedmieściach Algieru oraz zakłócenia dostaw gazu i elektryczności w stolicy. Gospodarka krajowa w wyniku tych aktów straciła ponad 2 miliardy dolarów<sup>16</sup>.

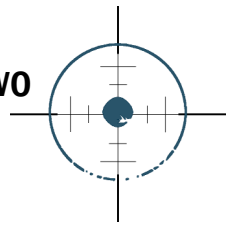
Jedną z metod, którą coraz częściej zaczynają stosować w atakach cyberterrorystów, jest wykorzystanie sieci bezprzewodowych. Obecnie coraz większa liczba firm z różnych sektorów gospodarki spieszy się z zastosowaniem sieci bezprzewodowych i technologii internetowych, nie zwracając uwagi na zagrożenia temu towarzyszące. Wraz z nadejściem ery technologii bezprzewodowej zmienia się nieodwracalnie koncepcja Internetu. Dostęp do danych finansowych za pomocą urządzeń bezprzewodowych jest coraz częściej uzyskiwany przez klientów, jednakże dostęp do nich w instytucjach finansowych, bankach i innych firmach świadczących usługi komunikacyjne i pośredniczące w dokonywaniu transakcji oznacza wzrost liczby punktów ułatwiających ataki. Jeden ze scenariuszy wykorzystania technologii bezprzewodowych przez terrorystów opisuje Dan Verton. Mówi on, że „zaszyfrowane dane docierają z sieci bezprzewodowej do bramki, przez którą są przekazywane do Internetu, a stamtąd do firmy świadczącej usługi finansowe. Jednakże sieci bezprzewodowe i kablowe używają do przesyłania zaszyfrowanych danych innych protokołów komunikacyjnych. W rezultacie w bramce dane są na kilka sekund odszyfrowywane i następnie szyfrowane ponownie. W ciągu tych kilku sekund mogą być przechwycone przez hakerów i już przyczyniło się to do utraty setek milionów dolarów”.

Oprócz omówionych metod ataku w cyberprzestrzeni należy szczególną uwagę zwrócić na tzw. „swarming attack” (jednoczesne wykonywanie wielu ataków konwencjonalnych oraz cyberataków wymierzonych w liczne infrastruktury). Jest to najgroźniejsza metoda, jaką mogą posługiwać się terrorystów, a polega ona na spiętrzeniu i nałożeniu na siebie ataków przeciwko infrastrukturze krytycznej państwa prowadzonych w cyberprzestrzeni oraz fizycznie, przeciwko jej materialnym nośnikom<sup>18</sup>. Jest to o tyle istotne, że w przypadku ataku w cyberprzestrzeni zakłóceniu ulec może działanie ma-

terialnych elementów infrastruktury krytycznej. Howard Schmidt – były przewodniczący Prezydenckiej Rady ds. Ochrony Infrastruktury Krytycznej mówi, że „cyberprzestrzeń, z Internetem jako ważnym elementem, stworzyła zależności, które teraz w nieprzewidywalny i groźny sposób zmieniają swą naturę (...). To właśnie swarming attack jest tym, czego powinniśmy się najbardziej obawiać przy każdym ataku fizycznym, a także przy każdej akcji kryminalnym i kataklizmie naturalnym. Takim zdarzeniu zwykle towarzyszy uszkodzenie lub degradacja linii i usług telekomunikacyjnych. To są właśnie te wzajemne zależności, których obawiamy się najbardziej”<sup>19</sup>. Należy wspomnieć, że infrastruktura teleinformatyczna i systemy telekomunikacyjne mają wiele słabych punktów. Umożliwiają one przeprowadzenie cyberataku, który w istotny sposób może obniżyć ich wartość i sprawność. 

### Przypisy

- 1 Oświadczenie byłego dyrektora FBI Louisa Freeh'a przed United States Senate Committees on Appropriations, Armed Services oraz przed Select Committee on Intelligence, 10 maja 2001.
- 2 D. Denning., *Wojna informacyjna...*, dz. cyt., s. 230.
- 3 M.F. Gawrycki, *Cyberterroryzm...* dz. cyt., s. 140.
- 4 Tamże, s. 142.
- 5 Tamże.
- 6 Tamże, s. 142-143.
- 7 Tamże, s. 143.
- 8 Tamże, s. 143-144.
- 9 G. Krasnodębski, *Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego*, [z:] [http://www.uwm.edu.pl/.../42\\_](http://www.uwm.edu.pl/.../42_), z dnia 15.06.2012, s. 5.
- 10 L. Wolaniuk, *Cyberterroryzm...* dz. cyt., s.161.
- 11 Tamże.
- 12 Tamże, s.162.
- 13 D. Opalach – Nusbaum, *Cyberterroryzm...* dz. cyt., s.304.
- 14 D. Verton, *Black ice...*, dz. cyt., s. 156 - 158.
- 15 Tamże, s. 160.
- 16 D. Denning, *Wojna informacyjna...*, dz. cyt., s. 229.
- 17 D. Verton, *Black ice...*, dz. cyt., s. 121.
- 18 K. Liedel, *Bezpieczeństwo informacyjne...*, dz. cyt., s. 41.
- 19 D. Verton, *Black ice...*, dz. cyt., s. 300.



## Z działalności ABW w 2012 roku

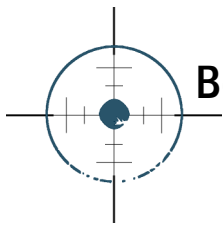
Jak każda, szanująca się instytucja państwowa, Agencja Bezpieczeństwa Wewnętrznego przedstawiła informację, ze swojej działalności. Raport ABW został zamieszczony na oficjalnej stronie służby. Łącznie liczy 34 strony, bogato ilustrowane zdjęciami, schematami i wykresami. Raport został podzielony na 5 części: ABW – ogólna charakterystyka, Bezpieczeństwo wewnętrzne, Popularyzacja problematyki bezpieczeństwa, Doskonalenie kwalifikacji, Komunikacja ze społeczeństwem. Oprócz ostatniej części, każda jest podzielona na kilka podrozdziałów.

W pierwszej części przedstawione zostały sprawy organizacyjne, modernizacja struktury, działania ABW, problematyka budżetu, nadzór i kontrola nad Agencją oraz współpraca międzynarodowa. Jak dowiadujemy się analizując zawartość tej części raportu, Agencja sporządziła, jak to napisano, 200 produktów analityczno – informacyjnych (rodzi się pytanie, o jakość tych produktów), poświęconych problematyce zagrożeń ze strony obcych służb specjalnych, ochrony kontrwywiadowczej kluczowych sektorów gospodarki narodowej, prognozowanych zagrożeń bezpieczeństwa RP czy zagrożeń cyberprzestępczością. Następnie omówione zostały działania operacyjno – rozpoznawcze, procesowe, kwestie wydawanych poświadczeń bezpieczeństwa, czy też przedstawione statystyki dotyczące decyzji o ich cofnięciu. Przedstawione zostały statystyki sprawdzeń w niedostępnych powszechnie ewidencjach, wydanych świadectw bezpieczeństwa przemysłowego (ich cofnięcia lub odmowie wydania). Opisano kwestie akredytacji urządzeń teleinformatycznych przetwarzających niejawne dane czy zagadnienia związane np. z legalizacją pobytu cudzoziemców w Polsce, wydawanych koncesji na obrót bronią i amunicją, wydanie Karty Polaka czy opinio-



wanie wniosków wizowych. Ostatnie podrozdziały zostały poświęcone budżetowi ABW i nadzorowi nad jej pracą.

Część druga, Bezpieczeństwo wewnętrzne, poświęcona została zagadnieniom przeciwdziałania terroryzmowi i ekstremizmowi, działalności Centrum Antyterrorystycznego ABW, statystykom raportów operacyjnych i sytuacyjnych, niestety bez szczegółów, ze zrozumiałych względów. Sporo miejsca poświęcono zagadnieniom zapewnienia bezpieczeństwa podczas EURO 2012 oraz sprawie Brunona K. W mojej ocenie, aby podnieść rangę sukcesu (dobry PR jest ważny), blok poświęcony adiunktowi z Krakowa zilustrowano dużą ilością obrazków. Innym sukcesem, którym pochwaliła się ABW, było zatrzymanie cudzoziemca (Czeczena) próbującego wwieźć na terytorium RP dwa karabiny snajperskie oraz 340 sztuk amunicji i 1000 zapalników elektrycznych. Powstaje pytanie, ile wwieziono karabinów nie znalezionych przez celników. Innymi omawianymi w tej części problemami są zagadnienia



ochrony i profilaktyki kontrwywiadowczej, ochrona bezpieczeństwa ekonomicznego, przestępstwa gospodarcze, nielegalny obrót paliwami czy zwalczanie korupcji zagrażającej ekonomicznym interesom państwa. W oryginale napisano „...korupcji zagrażającej...”. W tej części autorzy rozwodzą się także nad sprawą Amber Gold.

Pozostałe części informują nas o działaniach Agencji Bezpieczeństwa Wewnętrznego w zakresie popularyzacji problematyki bezpieczeństwa, odbytych w związku z tym konferencjach i warsztatach, szkoleniach urzędników i osób publicznych. Inną, moim zdaniem bardzo ciekawą inicjatywą jest konkurs szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa. Z raportu dowiadujemy się także o projektach realizowanych przez Agencję, że środków unijnych, projektach naukowo – badawczych oraz prowadzonych studiach podyplomowych z dziedziny bezpieczeństwa wewnętrznego na Uniwersytecie Warszawskim, prowadzonych już od kilku lat. Ostatnia część przedstawia sposoby komunikowania się agencji ze społeczeństwem: witryny internetowe ABW, periodyku Przegląd Bezpieczeństwa Wewnętrznego oraz rzecznika prasowego ABW.

Opracowanie zamykają dane teled adresowe delegatur ABW. Nie dowiadujemy się, czy szefowie delegatur i kierownictwo centrali ABW, przyjmuje jak dawniej szefowie Służby Bezpieczeństwa obywateli, w ramach skarg i wniosków.

Raport jest o tyle interesujący, że podaje dane statystyczne, które trudno byłoby pozyskać, ze środków masowego przekazu. Natomiast, co do

## ZOBACZ WIĘCEJ:

– Raport z działalności ABW w 2012 roku  
<http://www.abw.gov.pl/portal/pl/236/575/Raporty.html>

## Z działalności ABW w 2012 roku

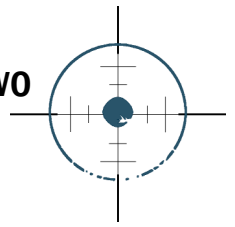


Gmach ABW przy ulicy Rakowieckiej.  
Fot. Lukasz2, commons.wikimedia.org

całej zawartości, zresztą zreczonnie podanej, to każdy, kto śledzi prasę, wiadomości internetowe (stronę ABW) i literaturę fachową, regulacje prawne z tego zakresu, posiada te same informacje, które w zostały przedstawione w raporcie. Np. kwestie zatrudnienia zostały przedstawione enigmatycznie, gdyż nic nie napisano o odejściu ze służby kilkuset (400 – stu?) funkcjonariuszy ABW, jak należy domniemywać z największym doświadczeniem zawodowym. A na ten temat było sporo w innych publikacjach.

Raport może być pomocny studentom piszącym projekty czy też eseje na temat funkcjonowania kontrwywiadu. Jest dobrym brykiem, dotyczącym funkcjonowania ABW i studenci np. nauk o bezpieczeństwie czy politologii powinni się z nim, oraz wcześniejszymi raportami zapoznać. Ciekawa byłaby analiza porównawcza tego raportu z raportami wcześniejszymi, np. w ramach pracy licencjackiej. Może też być wzorem, na przygotowanie własnej informacji, ekspertyzy, opinii czy też produktu analityczno – informacyjnego. 🚫

KPK



## Błąd w zabezpieczeniach kart SIM

Karsten Nohl odkrył luki w zabezpieczeniach kart SIM. Odkrycia dokładnie zaprezentował na Black Hat w Las Vegas. Według Nohla luki w kartach spowodowane są dwiema rzeczami, a mianowicie błędami w oprogramowaniu i wykorzystywaniu metody szyfrowania DES (symetryczny szyfr blokowy zaprojektowany w 1975 roku przez IBM).

Dzięki tym lukom hakerzy poprzez wysłanie binarnego smsa (takiego jakie wysyłane są przez operatorów telefonii komórkowej w celu konfiguracji np. sieci czy mmsów), mogą przejąć kontrolę nad kartą lub też ją sklonować. Taką kartę, można wykorzystać w celu dokonania przestępstw finansowych.

ITU sklasyfikowała to jako błąd wysokiego ryzyka. Hamadoun Touré z ITU poinformował, że wiadomość ta została przekazana do operatorów GSM w prawie 200 krajach oraz do agencji rządowych.

Nie wszystkie karty SIM są podatne na tego typu ataki. Nohl przez ponad 2 lata przeprowadzał testy i ustalił, że co czwarta karta posiada luki umożliwiające wykonanie tego typu ataków. Na dzień dzisiejszy szacuje się, że jest to 750 mln kart SIM.

Pierwszym poinformowanym przez odkrywcę był GSM Association zrzeszający operatorów telefonii komórkowej. Rzeczniczka prasowa GSMA poinformowała, że luki te staną się tematem badań ekspertów i do około 800 operatorów zrzeszonych w ramach GSMA zostaną podane zalecenia w tej sprawie. „Jesteśmy w stanie rozważyć konsekwencje oraz udzielać wskazówek operatorom, których ta podatność może dotyczyć” – rzecznik GSMA. Dodatkowo wysiłki GSMA w sprawie usunięcia luk wspiera największy producent kart SIM, którym jest Gemalto NV.



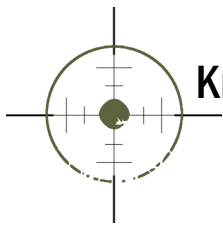
Fot. Bjoertvedt, commons.wikimedia.org

Dyrektor BlackBerry, zapowiedział przeprowadzenie analizy bezpieczeństwa i zagrożeń, oraz poinformował, że w ubiegłym roku BlackBerry proponował wprowadzenie innych standardów dla kart SIM. Ich wykorzystanie miałyby chronić przed atakami, jakie opisywał Nohl.

Nohl szacuje, że liczba kart podatnych na ataki może się zwiększać, wraz ze znalezieniem nowych sposobów na wykorzystanie tych luk. Dodatkowo stara się on uzmysłowić użytkownikom, jak niebezpieczne są opisywane luki. Są one jak Święty Graal dla hakerów umożliwiając im podszywanie się pod właściciela karty.

„Mając kartę SIM możemy zrobić wszystko, co mogą zrobić zwykli użytkownicy telefonu, jeżeli masz tam zapisany numer karty kredytowej czy dostęp do konta PayPal, my mamy go również.” Bardzo często spotykamy w Polsce uwierzytelnianie sms'em dla przelewów wychodzących. Pocięszające może być to, że podatne na tą lukę są tylko dane zapisane na karcie SIM. 🇵🇱

Bernadetta Terlecka



## Okoliczności przesłuchania śledczego niepełnoletniej i małoletniej osoby w trakcie postępowania karnego

Śledztwo w sprawie przestępstwa często wygląda, jak konflikt pomiędzy śledczym i podejrzanym - oskarżonym, a także świadkiem. Długi proces dialogów i monologów, kiedy potencjalny przestępca lub świadek stara się ukryć prawdę z różnych przyczyn: lęku, złości, uświadomienia tego, co zostało przez niego popełnione, lęk o swoje życie i życie bliskich - to uczucie może występować, tak u świadka, jak i przestępcy. W tych ważnych momentach śledztwa, zasadnicze jest to, żeby nie dopuścić się błędów w zastosowaniu taktycznych metod ze strony śledczego, które mogłyby oddziaływać na przebieg całego śledztwa.

Czynności w postępowaniu karnym często podejmowane jest wobec osób niepełnoletnich lub małoletnich. W razie przesłuchania osoby niepełnoletniej lub małoletniej przesłuchanie przyjmuje inną formę taktycznych metod, ponieważ psychika niepełnoletniego czy małoletniego ma inną charakterystykę w odróżnieniu od osoby dorosłej. Na przykład śledczy swoimi groźbami może spowodować nieodwołalne szkody psychiczne niepełnoletniego lub małoletniego. Co negatywnie wpłynie na późniejszy stan psychiczny tej osoby w życiu dorosłym.

Zgodnie do art.3 ust.1 pkt.11 Kodeksu postępowania karnego Ukrainy (dalej nazywanego Kodeksem), osoba **małoletnia** - dziecko do osiągnięcia czternastu lat, oprócz tego art.3 ust.1 pkt.12 Kodeksu daje **pojęcie osobie niepełnoletniej**, która na Ukrainie jest wskazana, jako osoba małoletnia, a także dziecko w wieku od czternastu do osiemnastu lat<sup>1</sup>.

Następne ważne pojęcie, zgodnie do art. 95 ust.1 Kodeksu, to jest zeznanie. Dlatego aby zrozumieć, takie działanie, jak przesłuchanie. **Zeznaniem** jest wiadomości, które przekazywane są w formie ust-



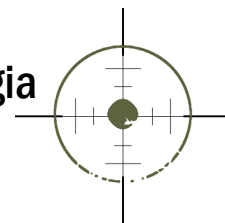
Fot. Адвокатский кабинет

<http://www.yristukconsult.ru/ugolovnyie-dela/ugolovnaya-otvetstvennost-nesovershennoletnih.html>

nej albo pisemnej podczas przesłuchania podejrzanego<sup>2</sup>, oskarżonego, świadka, poszkodowanego, eksperta, co do znanych im okoliczności w postępowaniu karnym. Ma to znaczenie dla postępowanie karnego<sup>3</sup>.

Specyfika przesłuchania osoby małoletniej albo niepełnoletniej jest regulowana art.226 Kodeksu i polega na:

- przesłuchanie osoby małoletniej albo niepełnoletniej przeprowadza się w obecności prawnego przedstawiciela, pedagoga albo psychologa, a gdy jest to niezbędne lekarza;
- przesłuchanie osoby małoletniej albo niepełnoletniej nie może trwać, bez przerw, ponad jedną godzinę, a generalnie więcej niż dwie godziny na dzień;
- osobom, które nie osiągnęły szesnastu lat, wyjaśnia się obowiązek o konieczności mówienia prawdy, nie uprzedza się o karnej odpowiedzialności za odmowę zeznań i za fałszywe zeznania;



Od początku przesłuchania osobom wskazanym w części pierwszej tego artykułu, wyjaśnia się ich obowiązki obecności na przesłuchaniu, a także prawo do negocjowania pytań i zadawania pytań<sup>4</sup>. Generalnie przesłuchanie osoby małoletniej czy niepełnoletniej prowadzi się zgodnie z regułami art. 224 Kodeksu. Nabycie przez niepełnoletniego cywilnoprawnych zdolności do działania w pełnym zakresie do 18 lat (np. w przypadku pracy na podstawie umowy o pracę; zajmowanie się działalnością gospodarczą), nie zgłasza się dla stosowania ogólnych reguł przesłuchania. Przesłuchanie niepełnoletniego podejrzanego wykonuje się również w obecności adwokata (art. 490 Kodeksu). Obecność lekarza razem z prawnym opiekunem, pedagogiem czy psychologiem jest niezbędna przy posiadaniu danych o umysłowym niedorozwoju dziecka, choroby itd.

Jako prawni przedstawiciele do uczestnictwa w przesłuchaniu mogą być zaangażowani rodzice (przysposabiający rodzice), a w razie ich nieobecności opiekuni lub kuratorzy tej osoby. Mogą to być także inni pełnoletni bliscy krewni czy członkowie rodziny, a także przedstawiciele organów opieki i kuratorzy, instytucji i organizacji, pod opieką czy kuratelą których, znajduje się niepełnoletni.

Rodzice i inne prawni przedstawiciele, z reguły, posiadają autorytet i zaufanie niepełnoletniego, mogą sprzyjać ustalaniu kontaktu z dzieckiem, otrzymaniu prawdziwych informacji, a także obrony jego praw i prawnych interesów. Jeśli są podstawy aby uważać, że rodzice czy inni prawni przedstawiciele są zainteresowani w nieprawdziwych zeznaniach niepełnoletniego, wywierają na jego negatywny wpływ czy ich interesy są sprzeczne z interesami osoby, którą reprezentują, na mocy decyzji śledczego lub prokuratora tacy prawni przedstawiciele są zmieniani.

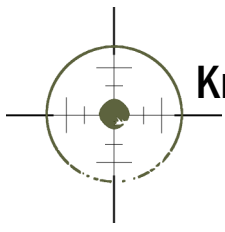
Prawo postępowania karnego wyrażenie reglamentuje prawa i obowiązki pedagoga i psychologa. Występują w tym wypadku, jako fachowcy. Pedagog

musi zajmować się edukacją i wychowaniem małoletnich czy niepełnoletnich w tym dziecka, jakie podlega przesłuchaniu. Psycholog powinien być fachowcem w dziedzinie dziecięcej i młodzieżowej psychologii. Zadanie pedagoga czy psychologa pomóc śledczemu ustanowić kontakt psychologiczny, wypracować poprawną taktykę przesłuchania, sformułować pytania z uwzględnieniem dziecięcej psychiki czy indywidualnych właściwości psychiki niepełnoletniego. Dla tego pedagog czy psycholog powinien być zaznajomiony z niektórymi okolicznościami sprawy karnej. W razie potrzeby do rozstrzygnięcia pytania o obecności u małoletniego choroby psychicznej czy opóźnienia rozwoju psychicznego i jego zdolności całkowitego lub częściowego uświadamiania znaczenia swoich działań i kierowania nimi w konkretnej sytuacji przeznaczają się kompleksowa psychologiczno - psychiatryczna ekspertyza (art. 486 ust.1 Kodeksu)<sup>5</sup>.

Przedstawiona część artykułu była pokazana z prawnego punktu widzenia Kodeksu i komentarza do niego. Kolejna część będzie przedstawiona z psychologiczno - kryminalistycznego punktu widzenia nawiązywania kontaktu z osobą niepełnoletnią, bez którego taktyka śledcza nie będzie miała sensu.

Ukraiński autor podręcznika *Kryminalistyka* V.U. Szepitko, ma następujący pogląd na ciąg taktyk dla przesłuchiwanego w postępowaniu karnym. Ustalanie psychologicznego kontaktu jest najbardziej sprzyjającym psychologicznym „klimatem” przesłuchania. Taktyczne chwytły, skierowane są na ustalanie psychologicznego kontaktu z przesłuchiwanym i znane sposoby zdobywania przychylności ludzi, zaproponowane przez Dalą Carnegie, takie jak:

- wykazuj szczerą ciekawość wobec innych ludzi;
- uśmiechaj się;
- pamiętaj, że dla człowieka dźwięk jego imienia - najśłodszy i najważniejszy dźwięk ludzkiej mowy;
- bądź dobrym słuchaczem; zachęcaj innych do opowiadania o sobie;
- prowadź rozmowę w kręgu interesów twojego



rozmówcy;

- dawaj ludziom odczuć ich ważność i czyń to szczerze<sup>6</sup>.

Ważnymi chwytami są także aktualizacja zapomnianej informacji w pamięci przesłuchiwanego, która może być istotna w karnej sprawie, wykrycie kłamstwa w zeznaniach, żeby odpowiadały one kryteriom rzeczywistości<sup>7</sup>.

Przygotowanie i przeprowadzenie przesłuchania niepełnoletnich uwarunkowane właściwościami<sup>8</sup> przesłuchiwanego, związanymi z jego wiekiem. Wiedza w tej materii ma bardzo ważne znaczenie dla ustalenia kontaktu psychologicznego.

## Okoliczności przesłuchania śledczego niepełnoletniej i małoletniej osoby

Wiek, zaczynając z jakiego niepełnoletni może występować na przesłuchaniu, jako świadek czy poszkodowanego, jest nie określony w ustawodawstwie o postępowaniu karnym.

Dzieci rekomenduje się przesłuchiwać tylko w skrajnych wypadkach, ponieważ przesłuchanie może negatywnie wpływać na ich psychikę.

Dla dzieci przedszkolnej grupy wiekowej charakterystyczna jest wyostrożona (spiczasta) spostrzegawczość, ich postrzeganie jest właściwie detalizowane, czyli przy odtworzeniu pewnego wydarzenia dzieci mogą mówić o faktach, których nie zauważyli dorośli.

W przedszkolnym i młodszym szkolnym wieku małoletni ma dużą podatność na sugestie i skłonność do fantazjowania. Te psychologiczne właściwości należy uwzględniać przy przesłuchaniu.

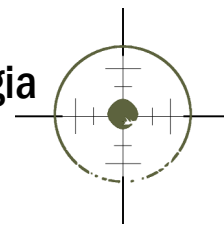
U nastolatków zasadniczo nową cechą wyróżniającą, jest w tym wieku „uczucie dorosłości”. Nastolatkom właściwy jest brak równowagi, impulsywność, szybka zmiana humoru, negatywizm.

Starszy szkolny wiek (wczesna młodość) - końcowy etap przejścia do dorosłości. Starsi uczniowie charakteryzują się dosyć wysokim rozwojem procesów psychicznych. W tym okresie krystalizują się życiowe ideały, dokonuje się wybór np. zawodu, ustala się cel i sens życia. W okresie wczesnej młodości posiada się obiekt do naśladowania, który staje się dla niepełnoletnich ważnym autorytetem. Dosyć często autorytetem są starsi przyjaciele, często, z nieprzyjaznych rodzin. W psychologii niepełnoletnich występuje charakterystyczne zjawisko konformizmu (podatność na realną czy domniemaną presję grupy)<sup>9</sup>. Na początku przesłuchania trzeba powiedzieć dziecku, że jeśli ono czegoś nie wie, to musi otwarcie mówić o tym. Jednak nie trzeba specjalnie utrwalać początku przesłuchania. Należy płynnie kierunkować rozmowę na otrzymanie zeznań o istocie sprawy. Pytania muszą się komplikować stopniowo: najpierw docelowo wyja-



Kodeks Postępowania Karnego Ukrainy  
Fot. <http://umdpl.info/index.php?id=1306951245>





ścić grono osób, które brało udział w przestępstwie, sytuację, którą dziecko dobrze zapamiętało, działania, które samo wykonywało, i dopiero potem stawiać pytania w sprawie samego wydarzenia. Można pobudzać dziecko, powtarzając na głos pytania śledczego.

Ze względu na ograniczoność objętości, stałości i podzielności dziecięcej uwagi, szybkie zmęczenie się przy jednostajnej formie przesłuchania, można zaproponować dziecku pokazywanie to, co ono widziało, nazywać kolory, formę.

Wszystkie pytania, związane z tamtymi wydarzeniami, powodującymi szkody dla psychiki dziecka, muszą przeplatać się z pytaniami neutralnymi, emocjonalnie-pozytywnymi.

W razie silnego stresu przesłuchanie powinno być czasowo przerwane, a uwaga dziecka powinna być skierowana na emocjonalnie-pozytywne rzeczy<sup>10</sup>.

Problematyka wiążąca się z niepełnoletnimi została uregulowana przez ONZ. Państwa Strony we własnym zakresie poprzez, minimalne standardowe reguły, dotyczące postępowania wymiaru sprawiedliwości w zakresie niepełnoletnich (Reguły Pekinśkie). Państwa – Strony powinny przejawiać wolę oraz chęć, aby w zgodzie ze swoimi interesami ogólnymi, sprzyjać pomyślności niepełnoletniego i jego rodziny<sup>11</sup>. Dlatego w postępowaniu karnym, w którym występuje małoletni lub niepełnoletni, jako uczestnik lub świadek, zadaniem każdego śledczego, jest także to, aby być właściwie przygotowanym w takich także dziedzinach wiedzy jak: psychologia, taktyka, logika itd.

## Przypisy

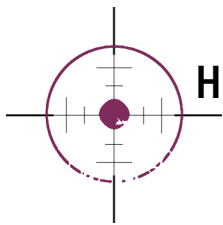
- 1 Kodeks postępowania karnego Ukrainy. Oficjalna edycja/ Wiadomości Rady Najwyższej Ukrainy № 9-10 od 08.03.2013. 20.07.2013
- 2 Tamże, art. 42 ust.1 Kodeksu, Podejrzaną osobą jest osoba, która w trybie, przewidzianym artykułami 276-279 Kodeksu, powiadomiona o podejrzeniu, albo osoba, która jest zatrzymana za podejrzeniem w dokonywaniu kryminalnego czynu zabronionego.
- 3 Art. 42 ust. 2 Oskarżonym (podsądnym) jest osoba, co, do której akt

oskarżenia jest przekazany do sądu w trybie, przewidzianym artykułem 291 Kodeksu. Prawa podejrzanego i oskarżonego są przewidziane w art.42 ust.3 Kodeksu.

- 4 Tamże, art. 95 ust.1. Podstawą dla przeprowadzenia przesłuchania jest to, że śledczy ma dostatecznie wiarygodną informację o tym, że pewna osoba ma wiedzę o okolicznościach, które mogą mieć ważne znaczenie w prowadzonym śledztwie o przestępstwo. Zaproszenie osoby dla przesłuchania wykonuje się poprzez wysłanie wezwania. Miejsce przesłuchania wyznacza śledczy samodzielnie.
- 5 Art. 226, Kodeks postępowania karnego Ukrainy. Oficjalna edycja/ Wiadomości Rady Najwyższej Ukrainy № 9-10 od 08.03.2013. 20.07.2013. W Kodeksie postępowania karnego Ukrainy wyodrębniony jest cały Rozdział 38, który stosuje się w razie postępowania karnego odnośnie niepełnoletnich.
- 6 Kodeks postępowania karnego Ukrainy. Komentarz. <http://pravo-ukraine.org.ua/resyrsi/kz/ugolovno-protsessualnyj-kodeks/5396-statya-226-osobnosti-doprosa-maloletnego-ili-nesovershennoletnego-lica> 20.07.2013
- 7 В.Ю.Шепитько. Криминалистика: Курс лекций. Издание третье.- Х.:ООО «Одиссей», 2006, s.188-189.
- 8 Tamże, s.191, 194.
- 9 Типове для tego wieku (do 18lat) procesy, stan, właściwości, które przejawiają się w zachowaniu niepełnoletniego.
- 10 В.Ю.Шепитько. Криминалистика: Курс лекций. Издание третье.- Х.:ООО «Одиссей», 2006. s.197-199.
- 11 М.И. Еникеев, В.А. Образцов, В.Е. Эминов. Следственные действия: психология, тактика, технология. [http://pravolib.com/ugolovnoe-pravo\\_815/osobnosti-doprosa-nesovershennoletnih.html](http://pravolib.com/ugolovnoe-pravo_815/osobnosti-doprosa-nesovershennoletnih.html) 20.07.2013
- 12 Минимальные стандартные правила Организации Объединенных Наций, касающиеся отправления правосудия в отношении несовершеннолетних ("Пекинские правила"). [http://zakon4.rada.gov.ua/laws/show/995\\_211](http://zakon4.rada.gov.ua/laws/show/995_211) 20.07.2013.

## Bibliografia

- В.Ю.Шепитько. Криминалистика: Курс лекций. Издание третье.- Х.:ООО «Одиссей», 2006.
- М.И. Еникеев, В.А. Образцов, В.Е. Эминов. Следственные действия: психология, тактика, технология.
- [http://pravolib.com/ugolovnoe-pravo\\_815/osobnosti-doprosa-nesovershennoletnih.html](http://pravolib.com/ugolovnoe-pravo_815/osobnosti-doprosa-nesovershennoletnih.html)
- Kodeks postępowania karnego Ukrainy. Oficjalna edycja/ Wiadomości Rady Najwyższej Ukrainy № 9-10 od 08.03.2013.
- Kodeks postępowania karnego Ukrainy. Komentarz.
- <http://pravo-ukraine.org.ua/resyrsi/kz/ugolovno-protsessualnyj-kodeks/5396-statya-226-osobnosti-doprosa-maloletnego-ili-nesovershennoletnego-lica>
- Минимальные стандартные правила Организации Объединенных Наций, касающиеся отправления правосудия в отношении несовершеннолетних ("Пекинские правила"). [http://zakon4.rada.gov.ua/laws/show/995\\_211](http://zakon4.rada.gov.ua/laws/show/995_211).



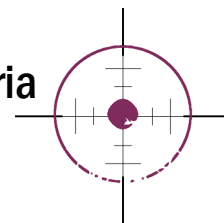
## Metody szkolenia politycznego funkcjonariuszy SB i MO

Dla poprawności wypowiedzi na temat wynikający z tytułu, kilka zdań zawiązujących do nie tak odległej historii. W systemie władzy komunistycznej instytucje bezpieczeństwa i porządku publicznego odgrywały szczególną rolę. Ich zadania nie skupiały się jedynie na zwalczaniu przestępczości kryminalnej oraz ochronie życia i zdrowia obywateli, tak jak to jest w krajach demokratycznych, ale obejmowały sferę oddziaływania ideologicznego i politycznego na społeczeństwo<sup>1</sup>.

Dekret Polskiego Komitetu Wyzwolenia Narodowego z dnia 7 października 1944 r. o Milicji Obywatelskiej, stanowił, że Milicja Obywatelska jest prawnopubliczną formacją służby Bezpieczeństwa Publicznego. W zakresie działania MO znalazły się sprawy wiążące się z: a) ochroną bezpieczeństwa, spokoju i porządku publicznego; b) dochodzeniem i ściganiem sprawców przestępstw; c) wykonywaniem zleceń władz administracyjnych, sądów i prokuratury w zakresie prawem przewidzianym. Milicja Obywatelska podlegała Kierownikowi Resortu Bezpieczeństwa Publicznego, a na jej czele stał Komendant Główny. Organizację wewnętrzną, szczegółowy zakres działania władz Milicji Obywatelskiej, stosunki służbowe, jak również prawa i obowiązki, odpowiedzialność dyscyplinarną członków MO określić miało rozporządzenie Kierownika Resortu Bezpieczeństwa Publicznego. Art. 7 dekretu stanowił, że kontrolę społeczną nad działalnością Milicji Obywatelskiej sprawują rady narodowe, terytorialnie właściwe, za pośrednictwem swoich prezydów, względnie przez wyłonione komisje. Wykonanie postanowień dekretu „porucza się Kierownikowi Bezpieczeństwa Publicznego w porozumieniu z Kierownikiem Resortu Administracji Publicznej”<sup>2</sup>. W strukturze organizacyjnej Komendy Głównej podstawowymi jednostkami organizacyjnymi były trzy oddziały:

- **Służby Zewnętrznej**, w skład, którego wchodziły wydziały: Organizacji i Nadzoru Administracyjnego; Nadzoru nad Ochroną Obiektów Państwowych i Społecznych; Bezpieczeństwa Ruchu Pieszego i Kołowego; Milicji Kolejowej i Wodnej; Organizacji Służby i Posterunków MO; Walki z Nierządem, Przestępczością Nieletnich oraz Włóczęgostwem i Żebractwem.
- **Służby Śledczej** zajmował się walką z: przemytem; bandytyzmem, kradzieżami; fałszerstwami i oszustwami; handlem walutą i narkotykami; przestępstwami urzędniczymi, przestępstwami podatkowymi oraz spekulacją. W ramach tego oddziału funkcjonowała specjalna komórka zajmująca się działalnością analityczną oraz prowadząca statystyki kryminalne przestępczości.
- **Szkoleniowo-Polityczny**, w którego gestii była praca z oficerami; praca polityczna (szkolenia); fachowe studia i wydawnictwa<sup>3</sup>.

W zasadzie można już teraz przejść do następnego wątku związanego z ustawowymi zadaniami MO, a przede wszystkim szkoleniem politycznym, na niższych szczeblach struktury organizacyjnej, ale tytułem dopełnienia wypada dodać, że w strukturze KG MO funkcjonowały: komórka do spraw ogólnych; działało Biuro Rejestracji Cudzoziemców oraz Wydział Prezydialny. Samodzielny Wydział Specjalny – komórka podporządkowana bezpośrednio Ministerstwu Bezpieczeństwa Publicznego, zajmująca się inwigilacją polityczną funkcjonariuszy Milicji pojawiła się w połowie 1946 roku<sup>4</sup>. Natomiast funkcjonowanie inspektoratu Ochotniczej Rezerwy Milicji Obywatelskiej (ORMO) w strukturze KG należy łączyć z uchwałą Rady Ministrów z 21 lutego 1946 roku o powołaniu do życia Ochotniczych Oddziałów Rezerwy Milicji Obywatelskiej (OORM). Potrzebę powołania ORMO uzasadniane było



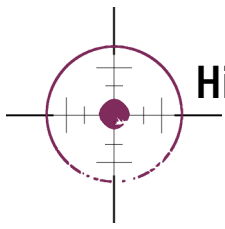
faktem, że koniecznie należy wzmóc walkę z bandytyzmem, rabunkami i innymi przestępstwami oraz wzmocnienie ochrony spokoju i i porządku publicznego<sup>5</sup>. Innymi słowy, powodem powołania tej organizacji był katastrofalny stan bezpieczeństwa w kraju, przy jednoczesnym braku możliwości powiększania korpusu MO i tak już o wiele liczebniejszego niż przedwojenny policyjny. Zwierzchnikiem ORMO był komendant główny MO. W województwach jej szefami byli zastępcy komendantów wojewódzkich, jako komendanci wojewódzcy ORMO, z pomocniczym aparatem instruktorów. Taka struktura powielona była do szczebla gminnego. Służba była bezpłatna i miała charakter społeczny, oddziały były zorganizowane na wzór wojskowy<sup>6</sup>. Nawiązanie do tej formacji, może wydawać się przypadkowe, ale tylko w tym miejscu. W dalszej części, w oparciu o materiały będące w posiadaniu autora, zostanie przekazanych kilka ciekawostek, związanych z uświadamianiem milicjantów, o konieczności współdziałania z członkami ORMO, w toku służby. Natomiast szkolenie członków odbywało się według programu milicyjnego, w oparciu o instrukcje dotyczące MO oraz obowiązujące milicjantów przepisy<sup>7</sup>.

Wróćmy jednak do spraw polityczno - wychowawczych. W komendach wojewódzkich i powiatowych MO w 1945 roku przewidziano stanowiska zastępców, w których zakresie obowiązków były sprawy polityczno-wychowawcze. Funkcjonowały też Wydziały Polityczno-Wychowawcze (w KW MO) oraz referaty będące ich odpowiednikami w KPMO. W komisariatach MO przewidziano także stanowisko zastępcy kierownika ds. polityczno-wychowawczych. Niestety w powszechniejszym obiegu nie ma przekazów, nawiązujących do pracy polityczno - wychowawczej. Nie pozostawia wątpliwości fakt, że MO oraz jej funkcjonariusze poprzez przełożonych „politycznych” byli włączani w sferę działań politycznych, przede wszystkim walkę z opozycją antykomunistyczną. Uregulowania prawne wynikające z dekretu PKWN temu sprzyjały i nie będzie przesady w stwierdzeniu, że celowo ustanowiono takie prawo.

*Ślubuję uroczyście stać na straży wolności, niepodległości i bezpieczeństwa Państwa Polskiego, dążyć ze wszelkich sił do ugruntowania ładu wewnętrznego, opartego na społecznych, gospodarczych i politycznych zasadach Polski Ludowej i z całą stanowczością, nie szczędząc swych sił, zwalczać jego wrogów. Ślubuję uroczyście strzec i dochować tajemnicy służbowej, rozkazy przełożonych wykonywać wiernie i obowiązki moje wypełniać gorliwie i sumiennie. Ślubuję uroczyście stać na straży praw Rzeczypospolitej, mieć wszystkich obywateli w równym poszanowaniu, a w postępowaniu kierować się zasadami godności, uczciwości i sprawiedliwości społecznej.*

Teksty ślubowania funkcjonariuszy, okres powojenny lata 50 – te i 60 – te zobacz: <http://www.zomoza.kgb.pl/przysiega.htm>.

Dekret z dnia 20 lipca 1954 r. o Milicji Obywatelskiej<sup>8</sup>, stanowił, że „Milicja Obywatelska działając w ramach służby bezpieczeństwa publicznego jest powołana do ochrony ludowego porządku prawnego, opartego na zasadach Konstytucji Polskiej Rzeczypospolitej Ludowej. Milicja Obywatelska strzeże porządku i ładu wewnętrznego, prowadzi nieubłaganą walkę z wszelką działalnością godzącą w ustalony wola ludu pracującego porządek prawny, ochrania własność społeczną, strzeże bezpieczeństwa, spokoju i mienia obywateli”. W świetle postanowień dekretu MO jest organizacją na wzór wojskowy i uzbrojoną formacją służby bezpieczeństwa publicznego (art. 1). Do zakresu działania należały sprawy: związane ze strzeżeniem porządku i ładu wewnętrznego; ochrona własności społecznej oraz dbać o bezpieczeństwo i mienie obywateli; przeciwdziałanie i zapobieganie przestęp-



czości; przeprowadzać postępowania przygotowawcze w sprawach karnych, wykonywać zalecenia prokuratorów i sądów oraz innych właściwych organów – w zakresie prawem przewidzianym (art. 2). Stosunek służbowy powstawał na podstawie mianowania funkcjonariuszem, w następstwie dobrowolnego zgłoszenia się kandydata. **Jednym z warunków, jaki kandydat musiał spełnić był „odpowiedni poziom polityczno-moralny”** (art. 5 pkt 2). Co w praktyce to oznaczało? Nie sposób rozważać tego w tym miejscu. Przed podjęciem służby w MO, funkcjonariusz składał wobec przełożonego ślubowanie w prezentowanej wcześniej formie.

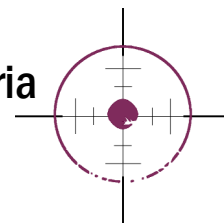
*Aparat bezpieczeństwa, specjalnie powołany Korpus Bezpieczeństwa Wewnętrznego oraz radziecki sojusznik – licząca ponad dywizję jednostka specjalna podporządkowana Moskwie – wspólnie zwalczały ruch niepodległościowy. Cała ta machina korzystała z pozyskiwanych informacji szybko rosnącej sieci agentów. W 1952 r. było ich ponad 70 tys. Organy i służby bezpieczeństwa w 1953 r. liczyły około 380 tys. funkcjonariuszy. Już w 1946 r. aresztowano, co najmniej 35 tys. osób., w walce zabito, około 10 tys. Sądy wojskowe w latach 1945-1947 skazały 17 tys. osób, w tym 2500 na karę śmierci. Jak oszacowali historycy, około 10 tys. zamordowano bez sądu. Później liczba aresztowanych wahała się od 12 tys. do 15 tys. rocznie, by w 1952 r. osiągnąć 21 tys. W końcu tego roku w więzieniach znajdowało się prawie 50 tys. więźniów politycznych. (...) System represji obejmował również zwykłych obywateli, którzy nie byli nigdy zaangażowani w działalność publiczną.*

E. Duraczyński, Stalin twórca i dyktator supermocarstwa, Pułtusk-Warszawa 2012, s. 684.

Dekret nie podawał treści ślubowania. Stanowił, m. innymi, że funkcjonariusz powinien ze wszystkich sił służyć Ojczyźnie, stać na straży ustalonego przez prawo ludowe ładu i porządku wewnętrznego; działać w ścisłej zgodności z przepisami prawa; strzec własności społecznej oraz bezpieczeństwa i mienia obywateli; wykonywać dokładnie rozkazy i polecenia władz przełożonych oraz przestrzegać ściśle przepisów regulaminowych; **w postępowaniu swym kierować się zasadami godności i uczciwości, stale podnosić poziom swojego uświadczenia politycznego** oraz wiedzy ogólnej i zawodowej (art. 23). Szczegółowe obowiązki funkcjonariusza określały zarządzenia Ministra Bezpieczeństwa Publicznego.

Funkcjonariusz w myśl postanowień dekretu podlegał odpowiedzialności dyscyplinarnej za naruszenie dyscypliny służbowej. Najłagodniejszą karą było upomnienie, natomiast najsurowszą wydalenie ze służby. Art. 33 przewidywał, odpowiedzialność przed oficerskimi sądami honorowymi za czyny, które godziły w honor i godność oficera Milicji Obywatelskiej. Za takie samo postępowania podoficerowie i szeregowcy ponosić mogli odpowiedzialność przed sądami koleżeńskimi, funkcjonującymi dla tych korpusów. Sądy mogły orzekać kary, lub wnioskować o wymierzenie kary dyscyplinarnej przez właściwego przełożonego. W ten sposób przyczyniały się do kształtowania właściwych, czy odpowiednich postaw polityczno - moralnych.

W świetle tego, co wynika z przytoczonych przepisów dekretu, ma pełne uzasadnienie teza, że przyjęte w dekrecie rozwiązania stanowiły krok w kierunku uwolnienia milicji od zadań w charakterze politycznym. Absolutnie nie oznacza to, że na funkcjonariuszy nie oddziaływało polityczne. Nadal obowiązywała zasada, że formacja jest częścią służby bezpieczeństwa publicznego<sup>9</sup>. Patrząc na tę zmianę należy uwzględnić wydarzenia historyczne. Terror, którego doznało społeczeństwo, powodował



**Protokół**  
**Z zebrania POP\* Komendy Powiatowej MO**  
**w (...) odbytego w dniu 19.07.1968 r**

Porządek zebrania:

1. Informacja światopoglądowa,
2. Dyskusja,
3. Sprawy organizacyjne,
4. Wolne wnioski.

Zebranie zagań sekretarz POP tow. K. J., zapoznając towarzyszy z porządkiem zebrania.

**Ad. 1.** Informacja światopoglądowa na temat: „Struktura religii” przeprowadził tow. A. C. Informacje przeprowadził w oparciu o skrypt dla słuchaczy Wyższej Szkoły Nauk Społecznych.

**Ad. 2.** Zabierając głos w dyskusji tow. E. K. skoncentrował swoją wypowiedź na funkcjach religii. Tow. F. K. omówił przeobrażenia wsi polskiej pod względem praktyk religijnych.

**Ad. 3.** Sprawy organizacyjne.

– W tym punkcie zebrania sekretarz POP tow. K. J. przedstawił zebranych prośby tow. tow. o przyjęcie w poczet kandydatów PZPR, a to: 1) J. T., 2) A. K., 3) J. P. Ubiegającym się o przyjęcie w poczet kandydatów PZPR zadano pytania i tak: tow. T. pytał kol. J. T. dlaczego wcześniej nie ubiegał się o przyjęcie w poczet kandydatów a dopiero od chwili odejścia tow. W. Kol. T. odpowiedział, że czynił starania wcześniej, lecz później zaniedbał ostatecznego załatwienia czynności związanych z przyjęciem. Tow. K. J. zwrócił się z pytaniem do kol. K., czy chodzi do kościoła – na to kol. K. oświadczył, że nie chodzi i sprawę tą zupełnie ma uregulowaną. Tow. C. poddał wniosek przyjęcia kol. J. T. w poczet kandydatów PZPR do przegłosowania. W wyniku głosowania jednogłośnie przyjęto wymienionego w poczet kandydatów PZPR. Tow. M. P. podał wniosek przegłosowania kol. kol. A. K. i J. P. w poczet kandydatów PZPR. W wyniku głosowania, wymienieni jednogłośnie przyjęci zostali na kandydatów PZPR.

– Zatarcie kary tow. C. Tow. K. J. odczytał podanie tow. C. o zatarcie wymierzonej mu kary w roku ubiegłym. W wyniku głosowania kara wymienionemu została zatarta.

**Ad. 4.** Wolne wnioski.

– W wolnych wnioskach, komendant powiatowy tow. S. P. zapoznał zebranych z planem zabezpieczenia Świąta 22 lipca.

– Tow. M. zastępca komendanta powiatowego odczytał rozkazy personalne MSW, KW MO, KP MO o przyznanych awansach i nagrodzeniu funkcjonariuszy, MO z okazji 22 lipca. Nagrody i odznaki wręczył komendant powiatowy mjr S. P.

– Tow. M. przedstawił zebranych sprawę opłacania rachunków za przejazdy świadków oraz powoływanych biegłych sądowych.

– Tow. T. D. przedstawił trudności związane z kupnem różnych towarów w sklepie „Konsumy”. W związku z tym zebrani wyrazili zgodę na wybór nowej Komisji Pracowniczej KP MO, która zajmie się między innymi tą sprawą. W skład nowej komisji pracowniczej weszli: 1. T. D., 2) T. P., 3) E. J., 4) D. S., 5) Z. B. Przewodniczącym komisji wybrano tow. K. P.


Na zakończenie zebrania tow. K. J. zwrócił się do zebranych tow. o chętnie wykonywania prac związanych z przeprowadzką do nowych biur budynku, jako prac wchodzących w zakres podjętego czynu społecznego.

\*POP - skrót od Podstawowa Organizacja Partyjna. Najmniejsze (najniższe usytuowane w strukturze) ogniwo organizacyjne Polskiej Zjednoczonej Partii Robotniczej, partii hegemonicznej, w systemie sprawowania władzy w PRL. Na jego czele stał I Sekretarz POP, mający do pomocy innych funkcyjnych członków.

**Protokółował:**  
**E. J.**

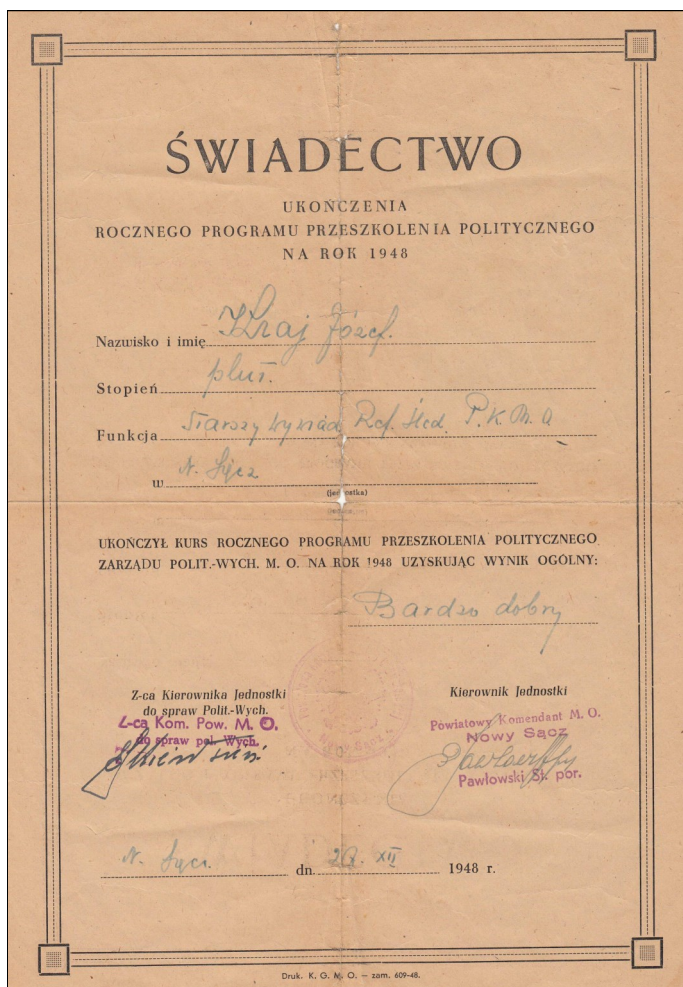
głębokie i trwałe zmiany zachowań społecznych. Gotowość do stawiania oporu zmalała niemal do zera, rozbite zostały więzi społeczno-środowiskowe, lokalne, rozpowszechniła się nieufność do obcych, a nawet bliskich, w rozmowach unikano drażliwych tematów<sup>10</sup>. Po drugie przyjęcie 22 lipca 1952 r. Konstytucji Polskiej Rzeczypospolitej Ludowej, do projektu, której wcześniej Józef Stalin własnoręcznie naniósł poprawki (było ich ponad 50). Prawdopodobnie z projektu wypadł punkt o kierowniczej roli Polskiej Zjednoczonej Partii Robotniczej (PZPR) i przyjaźni polsko-radzieckiej. Wydaje się, że znaczenie miała także śmierć J. Stalina 5 marca 1953 r., w następstwie, której nastąpiły zmiany personalne w kierownictwie partyjnym ZSRR.

Wracając do wątku związanego ze szkoleniem politycznym, stwierdzić należy, że zainteresowanie autorów, poruszających problematykę milicyjną w tym obszarze, o którym traktuje ten materiał jest praktycznie niezauważalne. Pozostawmy na uboczu przyczynę takiego stanu rzeczy. Przenieśmy się do lat sześćdziesiątych ubiegłego wieku do jednej z komend powiatowych MO w województwie rzeszowskim. Oto fakty wiążące się z interesującą nas problematyką, którą odzwierciedla zamieszczony wcześniej protokół.

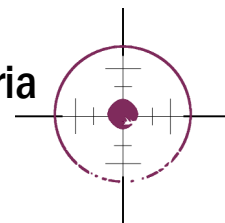
O innych zebraniach oraz poruszanej problematyce będzie okazja jeszcze napisać, jeżeli będzie zainteresowanie. W następnej części, natomiast przedstawione zostaną uwarunkowania oraz przyczyny powołania pionu polityczno – wychowawczego, a także jego zadaniach oraz metodach szkolenia funkcjonariuszy MO i SB. 

### Przypisy

- 1 A. Misiuk, Historia Policji w Polsce. Od X wieku do współczesności, Warszawa 2008, s. 171
- 2 Dekret Polskiego Komitetu Wyzwolenia Narodowego z dnia 7 października 1944 r. o Milicji Obywatelskiej, Dz. U. 1944, nr 7, poz. 33.
- 3 A. Misiuk, Historia ..., wyd. cyt., s. 174-175.
- 4 P. Majer, Historiografia i stan badań nad dziejami aparatu bezpieczeństwa i porządku publicznego oraz wojsk wewnętrznych, Warszawa 1984, za: A. Misiuk, Historia ..., s. 175.
- 5 R. Socha, A. Letkiewicz, P. Guła, Policyjne oddziały i pododdziały zwarte w Polsce. Historia i teraźniejszość, Szczytno 2010, s. 96.
- 6 P. Sykut, Ochotnicza Rezerwa Milicji Obywatelskiej (ORMO), [http://www.kujawsko-pomorska.policja.gov.pl/\\_portal/12650211694b66b0f13c6a2/Ochotnicza\\_Rezerwa\\_Milicji\\_Obywatelskiej\\_\(ORMO\).html](http://www.kujawsko-pomorska.policja.gov.pl/_portal/12650211694b66b0f13c6a2/Ochotnicza_Rezerwa_Milicji_Obywatelskiej_(ORMO).html) – dostęp 22.08.2013 r.
- 7 R. Socha, A. Letkiewicz, P. Guła, Policyjne oddziały i pododdziały ..., wyd. cyt., s. 97.
- 8 Dz. U. z 1954, nr 34, poz. 134.
- 9 A. Misiuk, Historia ..., wyd. cyt., s. 178.
- 10 E. Duraczyński, Stalin twórca i dyktator supermocarstwa, Pułtusk-Warszawa 2012, s. 685.



Świadectwo przeszkolenia politycznego.



## Cichociemni

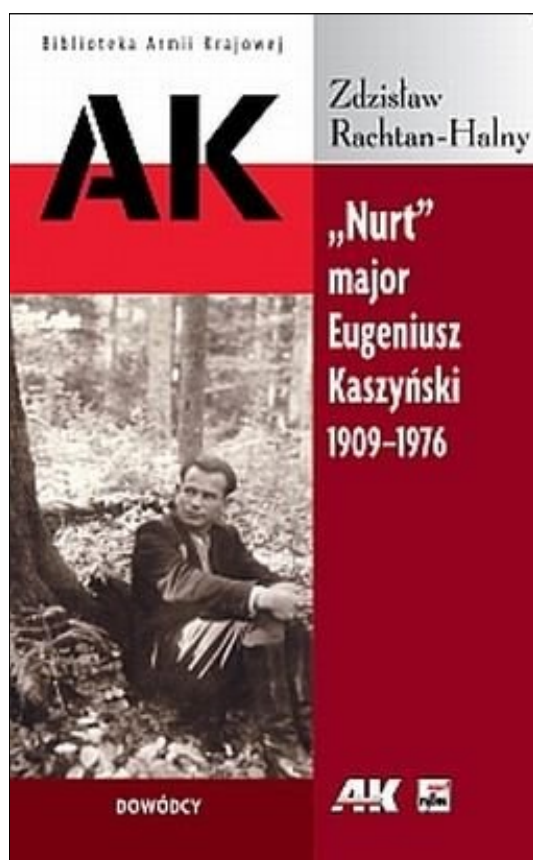
### *- Kiedy gadzina ukąsi Żmudzina, od jadu Żmudzina ginie gadzina*

Powyzsza sentencja w tytule, nawiązująca do pseudonimu jednego z najbardziej znanych cichociemnych Bolesława Kontryma, ps. Żmudzina celnie oddaje kwalifikacje i umiejętności pierwszych polskich komandosów – dywersantów, znanych, jako cichociemni.

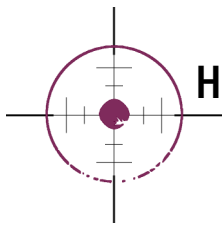
Ideę zorganizowania polskich jednostek spadochronowych, które miały wspierać konspirację w okupowanej Polsce stworzyli dwaj oficerowie dyplomowani, saperzy, kapitanowie Maciej Kalenkiewicz oraz Jan Górski. Obydwaj zresztą zginęli, jako cichociemni.



Standardowe wyposażenie cichociemnego.



Pierwsze swoje propozycje przygotowali już we Francji na potrzeby generała Kazimierz Sosnkowskiego, przełożonego Związku Walki Zbrojnej w Polsce. Po klęsce Francji już październiku 1940 r. rozpoczął pracę pięcioosobowy specjalny wydział studiów i szkolenia wojsk spadochronowych, znajdujący się w składzie III Oddziału (operacyjny) Sztabu Naczelnego Wodza w Londynie. Jego naczelnikiem został ppłk dypl. Wilhelm Heinrich, a oprócz Jana Górskiego i Macieja Kalenkiewicza innymi członkami zespołu byli lotnicy: ppłk Stefan Olszewski i kpt. naw. Lucjan Fijuth. Wydział przygotowywał założenia łączności lotniczej z Polską, planami werbunku i szkolenia przyszłych dywersantów - cichociemnych oraz problematyką lotów do kraju. Zrzućni spadochroniarze mieli być oficerami łącznikowymi odpowiednio przeszkolonymi do zadań bieżących. Dla wykonania tego typu misji miała funkcjonować pol-



ska eskadra specjalna, wyposażona w samoloty przystosowane do operacji desantowych odbywających się w nocy. Opracowano koncepcję polskich wojsk powietrzno-desantowych. Po zakończeniu prac studialnych dzięki staraniom kpt. dypl. Macieja Kalenkiewicza zorganizowany został pierwszy polski kurs spadochronowy, w brytyjskim ośrodku w Ringway. Kurs ukończyło 12 uczestników, którzy wykonali po kilka skoków ćwiczebnych w dzień i jeden nocny. Werbunkiem przyszłych cichociemnych zajmował się VI Oddział Sztabu Naczelnego Wodza. Oddział był organem łącznikowym Naczelnego Wodza z Komendantem Głównym AK. Utrzymywał stałą łączność radiową i kurierską z Polską. Wspierał operacje KG AK lub wykonywane z rozkazu przez Naczelnego Wodza. Utrzymywał,

## Cichociemni

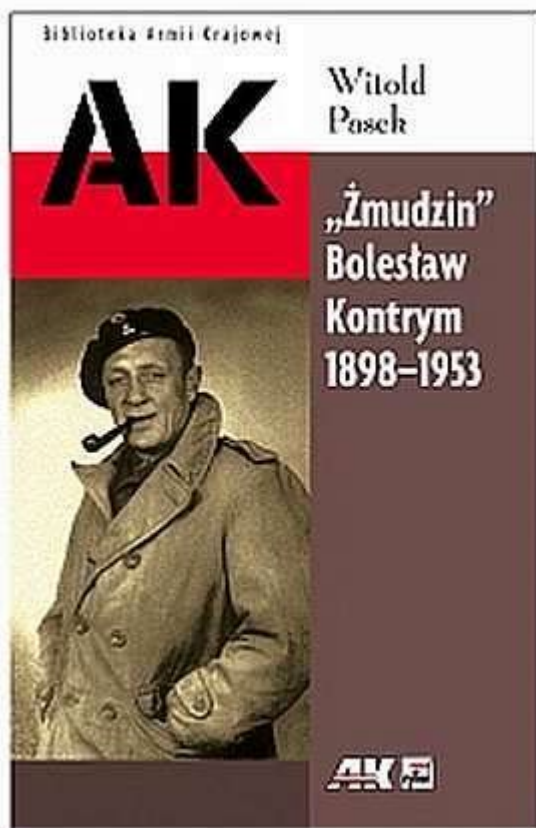


ppor. Stefan Bałuk ps. Starba w kombinezonie bojowym

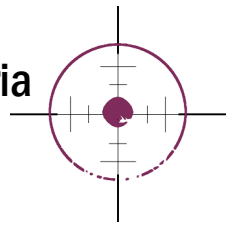
więc łączność lotniczą wysyłając cichociemnych, pieniądze i inne walory oraz sprzęt niezbędny do walki. Współpracował z innymi oddziałami Sztabu Naczelnego Wodza w sprawach dotyczących Armii Krajowej oraz angielskim SOE (Special Operation Executive). Zarządzał środkami finansowymi przeznaczonymi dla AK i wykonywał wiele innych czynności np. pośrednicząc przy nadawaniu przez BBC zakodowanych haseł na potrzeby AK.

Już w nocy z 15 na 16 lutego 1941 r. pierwsza ekipa skoczków znalazła się w kraju. Byli to: mjr Stanisław Krzymowski "Kostka", rtm. Józef Zabielski "Żbik" i bomb. Czesław Raczkowski "Orkan", "Włodek" - kurier Delegatury Rządu na Kraj. Operacja nosiła kryptonim „Adolphus”.

Osiągnięcia VI Oddziału najlepiej przedstawią statystyki dotyczące przeszkolonych skoczków, wysłanego sprzętu i sumy zrzuconych pieniędzy. W wyniku prowadzonej rekrutacji zgłosiło się do pracy w kraju: 1 generał, 112 oficerów sztabowych, 894 oficerów młodszych, 592 podoficerów, 771







## Cichociemni

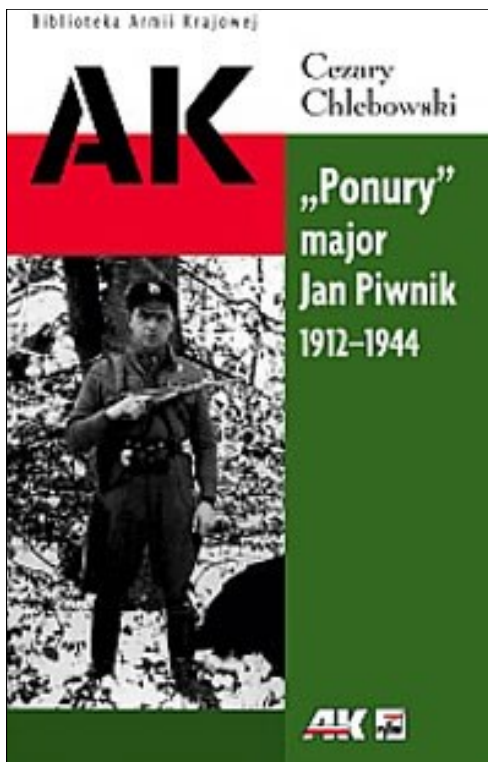
szeregowych, 15 kobiet i 28 kurierów cywilnych. Łącznie było 2410 kandydatów na cichociemnych. Z tej liczby 606 ukończyło pomyślnie szkolenie, a 579 zostało zakwalifikowanych do skoku do kraju. Do końca 1944 zrzucono do 316 cichociemnych oraz 28 cywilnych kurierów MSW. Wyślano ok. 670 ton wyposażenia wojskowego (broń i amunicja, materiały dywersyjne, sprzęt radiowy oraz bardzo zróżnicowane materiały specjalne, medyczne, umundurowanie itp.). Sprzęt pochodził z kilku źródeł. Angielski sprzęt wojskowy dostarczała polska sekcja SOE. Niemiecki i włoski pobierano z magazynów z bronią zdobyczną. Dokonywano zakupów w Wielkiej Brytanii, Szwecji, USA, a nawet Portugalii. Były to m.in. ubrania i drobiazgi dla skoczków, lekarstwa i trucizny, sprzęt fotograficzny i optyczny oraz elementy i półfabrykaty radiowe. Skoczkowie zabrali ze sobą znacznie środki finansowe przeznaczone dla AK. Było to: 26 299 375 \$ w banknotach i zło-

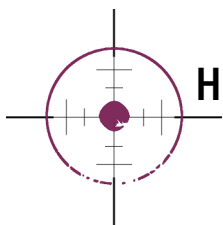
cie, 1755 funtów w złocie, 3 578 000 marek, 10 000 peset, 40 869 800 złotych okupacyjnych, tzw. młynarek (fałszywych). Delegatura Rządu z otrzymała: 8 593 788 \$ w banknotach, 1644 funtów w złocie, 15 911 900 marek, 400 000 młynarek.

VI Oddział ściśle współpracował ze wspomnianym wyżej brytyjskim Special Operations Executive. Oddział VI prowadził główną bazę przerzutową oraz dysponował stacjami wyczekiwania dla cichociemnych wysyłanych do Polski. Innymi ogniwami organizacyjnymi Oddziału były: komórki organizujące kursy wyszkolenia dla cichociemnych oraz bazy i placówki łączności lądowej

Warto podkreślić, że zrzut cichociemnych w nocy z 15 na 16 lutego 1941 roku, był także pierwszą operacją SOE na kontynencie europejskim połączoną z desantowaniem spadochroniarzy.

Cichociemni odbywali niezwykle intensywne szkolenie, nabywając zróżnicowanych i szerokich umiejętności bojowych. Programy były cały czas doskonałe, na podstawie uwag napływających z Polski. M.in. rozszerzono programy zajęć z zakresu akcji na komunikację oraz naukę wytwarzania środków wybuchowych domowym sposobem. Jedną z początkowych słabości cichociemnych, była niedostateczna znajomość broni niemieckiej. W szkoleniu kładziono nacisk na praktykę, mniej na teorię. Nieszablonoowo szkolono przyszłych wywiadowców, dywersantów czy oficerów do zadań sztabowych. Wszyscy cichociemni musieli przejść kurs spadochronowy i odprawowy. Każdy z kandydatów na cichociemnego przechodził kilka kursów. Były to m.in. takie kursy jak: zaprawy dywersyjno minerskiej, strzeleckiej i fizycznej stanowiącej selekcję fizyczną kandydatów i przygotowywał do dalszego szkolenia dywersyjnego. Podstawowymi zajęciami na tym kursie była zaprawa fizyczna, uczone strzelania z różnych pozycji, terenoznawstwa, walki wręcz oraz posługiwania się prostymi środkami minerskimi. Nie ukończenie tego kursu powodowało





powrót do jednostki macierzystej; kurs badań psychotechnicznych, kurs spadochronowy (szkolenie trwało tydzień); lotnicy przechodzili lotniczy kurs specjalny na temat niemieckich samolotów; prowadzono kursy pancerne, przeciwpancerne i kierowców, radiotelegrafistów i radiomechaników; kurs *The E & Sphon* specjalizował się w środkach łączności ziemia-lotnik stosowanych przy odbiorach zrzutów; kurs wyrobu materiałów wybuchowych i środków zapalających metodami domowymi; kurs informacyjno-wywiadowczy dawał znajomość kodów, szyfrów, wyrobu atramentów sympatycznych, pogłębiał znajomość pracy podziemnej i propagandy, zaznajamiał ze strukturami niemieckimi; kurs mikrofotografii; miesięczny kurs dla komandosów dostarczał fachowców wyspecjalizowanych umiejętność w dywersji i sabotażu na obiekty przemysłowe, komunikację kolejową, linie telefoniczne itp.; kurs czarnej propagandy, obejmujący teorię propagandy, drukarstwo i fotografię. Pozostałe kursy to: zmiany wyglądu zewnętrznego oraz tzw. kurs korzonkowy, polegający na bytowaniu przez dłuższy czas na łonie natury i korzystanie tylko z jej zasobów.



Kurs walki wręcz.

## Cichociemni

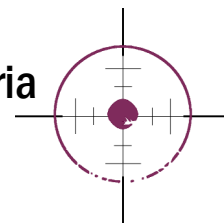


Ćwiczenia w tzw. małym gaju.

Każdy cichociemny przygotowywał własną legendę i miał dopasowany do niej zawód.

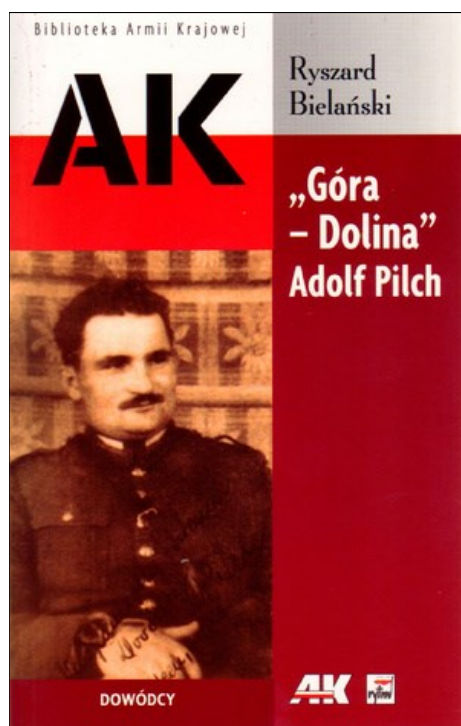
Cichociemni wyszkoleni dywersji działali w „Wachlarzu”. Do „Wachlarza” przydzielono 27 cichociemnych, jednak tylko 26 zgłosiło się do służby, pierwszym z nich był kpt. Alfred Paczkowski, ps. „Wania”.

Cichociemnym, który nie wykonał rozkazu (zdezercerował) i nie stawiał się do służby w „Wachlarzu” był por. Leonard Zub -Zdanowicz, ps. „Dor” przeszedł do NSZ. Do dziś sprawa budzi wiele kontrowersji. Cichociemni-dywersanci kierowani byli nie tylko do „Wachlarza”, ale również do innych organizacji potrzebujących dywersantów. Były to Związek Odwetu oraz Organizacja Specjalnych Akcji Bojowych „Osa”. W wyniku scalenia wyżej wymienionych organizacji powołano Kierownictwo Dywersji „Kedyw”. Cichociemni pełnili




## Cichociemni

w nim często role kierownicze. Cichociemni przeszkoleni w specjalności wywiadowczej, byli powołani do pełnienia funkcji organizatorów i inspektorów sieci wywiadu. Byli kierowani przede wszystkim do Wywiadu Ofensywnego Oddziału II KG AK oraz na różnorakie stanowiska dowódcze w centrali oraz w terenie. Zadania legalizacyjne prowadziło trzech cichociemnych. Po skoku skierowano ich do Wydziału Techniczno-Legalizacyjnego Oddziału I KG AK. Rozbudowywana sieć łączności AK, wymagała dobrze przygotowanych technicznie fachowców i organizatorów radiołączności, a także radiotelegrafistów. Cichociemny radiotelegrafistów było wyszkolonych ok. 30. Skoczkowie – pancernicy przeszkoleni w obsłudze niemieckiego sprzętu pancernego, mieli stanowić kadrę jednostek pancernych h po wybuchu powstania powszechnego. Ponieważ ich drugą specjalnością była dywersja, kierowano ich do Kedywu lub do oddziałów leśnych. Wyszkolono grupę cichociemnych przeznaczoną do pracy w konspiracyjnych sztabach. Kierowano ich zgodnie z przeznaczeniem do pracy w sztabach KG AK, obszarów lub okręgów.



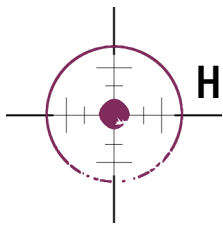
Z zrzuconych do Polski 316 cichociemnych zginęło lub zaginęło 112 (38% ogółu zrzuconych). Straty te obejmują zabitych przez Niemców, Rosjan oraz w wyniku działań po wojnie Urzędów Bezpieczeństwa. Ponadto w trakcie lotu zginęło 6 cichociemnych, a śmiercią spadochroniarza trzech. Ponadto do innych państw europejskich (Francja, Jugosławia, Albania, Grecja) zrzucono 46 polskich skoczków – cichociemnych.

Do najbardziej znanych cichociemnych należą: Alfred Paczkowski, ps. Wania; Bolesław Kontrym, ps. Żmudzin; Jan Piwnik, ps. Ponury; Adam Borys, ps. Pług, Stanisław Jankowski, ps. Agaton; Michał Fijałka, ps. Kawa, Wieśniak, Sokół; Ryszard Nuskiewicz, ps. Powolny; Adolf Pilch, ps. Góra, Pistolet, Waldemar Szwiec, ps. Robot i wielu innych.

Warto o nich pamiętać, znać ich niebanalne drogi życiowe oraz osiągnięcia, które na ogół nie są znane szerszemu ogółowi. Dlatego warto zapoznać się choćby z częścią proponowanych pozycji książkowych oraz portalami internetowymi poświęconymi cichociemnym: J. Tucholski, Cichociemni, tenże Powracali nocą i Cichociemni i spadochroniarze 1941 – 1956; P. Bystrzycki, Znak cichociemnych; I. Valentine, Baza 43, C. Chlebowski, Pozdróćcie Góry Świętokrzyskie i Odłamki granatu oraz Saga o Bohaterach „Wachlarz IX 1941 – III 1943; J. Szatsznejder, Cichociemni z Polski do Polski, A. Paczkowski, Ankieta cichociemnego lub Lekarz nie przyjmuje; C. Leżeński, Żołnierskie drogi; M. Gordon, Cichociemni; K. Śledziński, Cichociemni, Elita polskiej dywersji; W. Pasek, „Żmudzin” Bolesław Kontrym 1898 – 1953; R. Bielański, „Góra – Dolina” major Adolf Pilch; C. Chlebowski, „Ponury” major Jan Piwnik 1912 – 1944; Z. Rachtan – Halny, „Nurt” major Eugeniusz Kaszyński 1909 – 1976, K. Kraj, Cichociemny „Wróbel” – mój nauczyciel [w:] MMS Komandos nr 3/2011. 

KPK

Zdjęcia pochodzą z książki M. Olton, Zanim uderzył GROM, Historia jednostek specjalnych i wojsk powietrznodesantowych Wojska Polskiego, Warszawa 2010, w której były wykorzystywane zdjęcia z prywatnego archiwum cichociemnego, generała Stefana "Starby" Bałuka.



## 31 października 1984 r.

Zabójstwo Indiry Gandhi, było jednym z nietypowych, niespodziewanych zamachów terrorystycznych. Pięć lat wcześniej przez funkcjonariuszy ochrony został zamordowany Nur Mohammad Taraki, prezydent Afganistanu. Został uduszony przez dwóch oficerów straży przybocznej. Jednak zabicie Tarakiego, wynikało z rozgrywek w łonie najwyższych władz Ludowo – Demokratycznej Partii Afganistanu, z konfliktu pomiędzy dwoma frakcjami *Chalk i Parczam*. Indira Gandhi była premierem demokratycznego, nuklearnego mocarstwa, zamieszkiwanego przez ponad 700 mln. mieszkańców, której mandat sprawowanej władzy pochodził z wyborów.

W dniu swojej śmierci premiera Indira Gandhi miała w swojej rezydencji udzielić wywiadu znanemu aktorowi Peterowi Ustinowowi. Oczywiście w tym rejonie świata zginęło w zamachach wielu politycznych przywódców, aby wymienić kilku: Mahatma Gandhi (Indie), prezydent Pakistanu Ali Khan, premier Cejlonu (Sri Lanka) Solomon Bandaranaike czy przywódca Bangladeszu Mudżibur Rahman oraz Ziaur Rahman. Wcześniej obiektem zamachów (nieudanych) był jej ojciec Jawaharlal Nehru oraz ona sama. Również jej następcą na stanowisku premiera, a zarazem syn Rajiv zginął, w samobójczym ataku terrorystycznym.

W Indiach, w tym okresie panowała napięta sytuacja związana z wydarzeniami w Pendżabie. Zdobyciem przez armię indyjską, na rozkaz Indiry Gandhi – Złotej Świątyni – miejsca otoczonego czią przez Sikhów. W Pendżabie i nie tylko rozszerzała się działalność terrorystyczna. W walce prowadzonej przez sikhijskich radykałów, ofiarami padali również umiarkowani Sikhowie, zwolennicy porozumienia z rządem Indii.



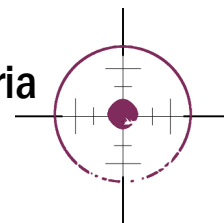
Indira Gandhi i Lyndon B. Johnson w marcu 1966 roku.  
Fot. commons.wikimedia.org

Zamachowcami byli Sikhowie służący w ochronie osobistej premiera. Inspektor Beant Singh i konstabl Satwant Singh. Beant Singh chronił Indirę Gandhi od dziesięciu lat. Jeździł wraz z nią w podróże zagraniczne. Niewątpliwie przyczyną, która pchnęła obydwu Sikhów do zabójstwa Indiry Gandhi, były wydarzenia związane ze zdobyciem Złotej Świątyni oraz wcześniejszą działalnością charyzmatycznego Jarnaila Bhindranwale.

Ale wróćmy do przebiegu samego zamachu, który miał miejsce na terenie oficjalnej siedziby premiera Indii.

**Godzina 9.05** - Indira Gandhi opuszcza hall swojej rezydencji w towarzystwie osobistego sekretarza oraz oficera policji D. K. Bhatta, którego zadaniem była bezpośrednia ochrona pani premier (zasłonięcie własnym ciałem). Na terenie rezydencji, jak się wydawało, była bezpieczna i Bhatt nosił wtedy parasol przeciwsłoneczny.

**Godzina 9.08** - Rorry O'Farrell z ekipy przygotowującej wywiad z Indirą Gandhi prosi o sprawdzenie mikrofonów.



31 października 1984 r.

Idącą dobrze sobie znaną alejką Indira Gandhi, za którą w odległości kilku metrów podążali Bhatt i osobisty sekretarz zbliża się do zamachowców patrolujących przydzielony im odcinek. Pozdrawia ich. W tym momencie Satwant Singh podnosi do góry rękę ze Stenem, a będący w odległości 3 metrów od pani premier Beant Singh wyciąga służbowy rewolwer i pierwszy oddaje do strzały. Do leżącej na ziemi Indiry serię ze Stena oddaje Satwant Singh. Odgłosy strzałów powodują pojawienie się komandosów straży granicznej pilnujących niedalekiej bramy. Beant i Satwant odkładają broń.

**Godzina 9.11** – Pierwszy, że coś się dzieje zorientował się Peter Ustinov i próbował się dostać na miejsce zamachu, lecz drogę zagroził mu komandos.

Z zamachowców ginie Beant Singh, ciężko ranny zostaje Satwant Singh. Tutaj jest kilka wersji, jak to się stało, że komandos zabili i zranili zamachowców, mimo że ci się poddali. Ale to nie temat na ten artykuł.


**Godzina 9.15** – Synowa Sonia oraz Bhatt i sekretarz wkładają do limuzyny marki Ambassador ciężko ranną Indirę Gandhi i wyruszają do Wszechindyjskiego Instytutu Nauk Medycznych. Samochód wjeżdża bez eskorty. Nie jest konwojowany przez policję na motorach, co utorowałoby drogę przez zatłoczone ulice Delhi (7 km) do szpitala,

**Godzina 9.35** – Samochód dociera do szpitala, po 20 minutach jazdy. Kierowca i Bhatt na rękach przenoszą ranną do gabinetu lekarskiego. Nikt nie tamował krwi.

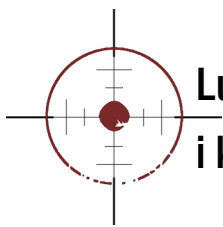
**Godzina 10.09** – rozpoczyna się operacja i zabiegi reanimacyjne trwające ok. 2 godzin.

W międzyczasie do szpitala dodał dyżurny ambulans z rezydencji premiera oraz jej osobisty lekarz. Dyżurny ambulans, jego kierowca i osobisty lekarz odnaleźli się kilka minut po odjeździe samochodu z ranną Indirą Gandhi. Przywieziono nim rannego Satwanta Singha. Ambulans był eskortowany przez policję na motocyklach.

### Konkluzje:

- Zamach był dokładnie opracowany od strony organizacyjnej.
- Jego przebieg i sposób przeprowadzenia był nowatorski i zaskakujący (członkowie ochrony zabijają swojego podopiecznego).
- Zamachowcy byli zdecydowani na śmierć, gdyż w takiej sytuacji trudno było przewidzieć ich ucieczkę.
- Zawiodły służby policyjne i kontrwywiadowcze, nie wykrywając wcześniej spisku i dopuszczając nadal do służby Sikhów, po wydarzeniach w Złotej Świątyni. Nie bez wpływu było tu prawdopodobnie, stanowisko w tej kwestii, samej Indiry Gandhi. Wcześniej ze służby dyplomatycznej w Norwegii zdezerterował kuzyn Beanta Singha, co powinno zaalarmować służby specjalne.
- Brak nadzoru kontrwywiadowczego nad funkcjonariuszami ochrony.
- Służby ochronne nie przewidziały potrzeby większej eskorty na terenie rezydencji.
- Na całej linii zawiodła pomoc medyczna, w tym system ewakuacji.
- Zawiodły, także procedury i cały system dowodzenia, który dopuścił do wyjazdu samochodu z ranną panią premier, bez eskorty.
- Decyzję o ewakuacji rannej podjęła synowa Sonia.
- Bhatt oraz inni, nie byli w stanie udzielić pomocy medycznej (paramedycy), prawdopodobnie z powodu braku wykształcenia. Być może zatamowanie upływu krwi uratowałoby życie Indiry Gandhi. 

KPK



## Pułkownik Geоргij Mordwinow

Geоргij Iwanowicz Mordwinow, był dwukrotnie przedstawiany do odznaczenia Gwiazdą Bohatera Związku Radzieckiego. Obydwa razy wniosek był odrzucany przez Ławrientija Berię. Geоргij Iwanowicz odszedł do rezerwy w 1949 r., w stopniu pułkownika, chociaż w czasie wojny zajmował stanowiska odpowiadające stopniowi generała lejtnanta.

Nasz bohater urodził 5 maja 1896 r., we wsi Burnaszowo w jednym z rejonów Obwodu Zabajkalskiego, obecnie Republika Buriatria, w rodzinie parobka. Wcześniej osierocony, początkowo trafił pod opiekę byłego pracodawcy ojca (na prośbę dziadka). W wieku dwunastu rozpoczął pracę w fabryce szkła w Wierchnieudińsku, jako goniec, a następnie w Czycie, jako ślusarz – hydraulik.

W 1915 roku został wcielony do armii. Ponieważ był znakomitym jeźdźcem służył w zespole konnych zwiadowców 75 sybirskiego pułku strzeleckiego na południowo zachodnim froncie. Był ranny. W 1917 r. uczestniczył w likwidacji sztabu (kwatery) generała Nikołaja Duchonina (głównodowodzącego armią rosyjską) w Mohylewie.



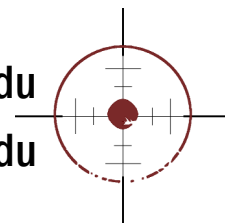
Płk. G. Mordwinow



Legitymacja płk. G. Mordwinowa

Po demobilizacji i powrocie do Czyty wstąpił do Czerwonej Gwardii. W grudniu 1917 roku był uczestnikiem likwidacji rewolty junkrów w Irkucku.

W kwietniu 1918 roku został przyjęty do służby w Zabajkalskiej Komisji Nadzwyczajnej, w dwa miesiące później wstąpił do Rosyjskiej Komunistycznej Partii (bolszewików). W sierpniu tegoż roku wykrył, z innym czekistą, spisek białogwardyjski, którego celem było wywołanie powstania w Czycie. Po wkroczeniu wojsk japońskich i upadku władzy radzieckiej został partyzantem. Sformował i dowodził oddziałem partyzanckim w walkach z japońskimi interwentami. W 1920 roku został dowódcą I Amurskiej Brygady Kawalerii, jednocześnie był szefem wywiadu frontu. Po utworzeniu Republiki Dalekowschodniej został w 1921 roku mianowany naczelnikiem wydziału transportowego Państwowej Ochrony Politycznej republiki. W końcu 1921 roku został komisarzem Specjalnego Pułku Amurskiego i uczestniczył w walkach na Dalekim Wschodzie. Między innymi podporządkował sobie garnizon Nerczyńska, tym sposobem przyczyniając się do rozbięcia wojsk interwencyjnych na Zabajkalu. Latem 1922 r. z zadaniem dowództwa frontu przeszedł na tyły wojsk japońskich i sformował chiński i koreański



ski oddziały partyzanckie. Oddziały ochraniały linie kolejowe oraz przeciwdziałały akcjom dywersyjnym ze strony Mandżurii.

Lata 1923 – 1924 spędził ucząc się w tzw. *rabfaku*, czyli fakultecie przygotowującym do studiów. Jednocześnie do 1929 roku służył na stanowiskach kierowniczych w oddziałach wojsk pogranicznych i organach Głównego Zarządu Politycznego (GPU). Uczestniczył w likwidacji oddziałów białogwardyjskich działających w okolicach rzeki Arguń. Od 1926 był naczelnikiem samodzielnej komendantury wojsk pogranicznych oraz naczelnikiem Fiedosijsko – Sudakskiego Oddziału OGPU na Krymie. W roku 1929 został skierowany na kursy doskonalenia kadr w Wyższej Szkole Pogranicznej. Za działania prowadzone na Syberii oraz na Krymie był trzykrotnie nagradzany bronią oraz cennymi pamiątkami. W roku 1929 rozpoczął studia na chińskim fakultecie Instytutu Orientalistyki. Odwołany ze studiów, ponownie rozpoczął służbę w OGPU i został wysłany w 1930 r. do Mongolii, a następnie do Chin. Prowadził działalność wywiadowczą. Po powrocie z Chin w 1935 roku zdał egzaminy końcowe w Instytucie Orientalistyki i został skierowany na naukę do Instytutu Czerwonej Profesury, do sekcji chińskiej wydziału historycznego.




W 1937 r. napisał raport do szefa NKWD Nikołaja Jeżowa w sprawie swojego aresztowanego przyjaciela i towarzysza N. I. Toropowa, zna-


nego mu z pracy w Chinach. W wyniku raportu został zwolniony ze służby w organach bezpieczeństwa. Ukończywszy Instytut pracował w Komitecie Wykonawczym Kominternu, gdzie był referentem i kierownikiem wschodniego sektora tej instytucji. Jednocześnie uczestniczył w studiach doktoranckich (aspirantura)

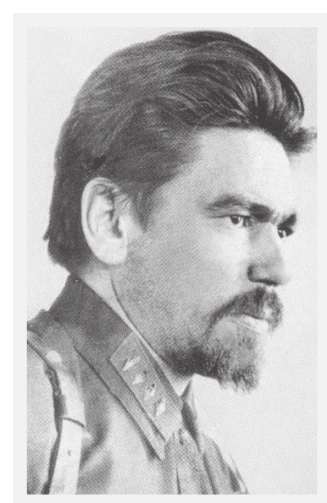
Moskiewskiego Uniwersytetu Państwowego.

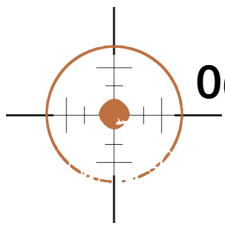
Na początku Wojny Ojczyźnianej Gieorgij Mordwinow został zmobilizowany i wcielony do Grupy Specjalnej NKWD, gdzie zajmował się formowaniem oddziałów partyzanckich wysysanych na tyły niemieckie. W październiku 1941 r. został oddelegowany, jako Gieorgij Pawłow - wicekonsul, do Stambułu w Turcji. Wraz z Naumem Eitingonem przygotowywał zamach na niemieckiego ambasadora w Turcji Franza von Papena. Został aresztowany w marcu 1942 roku i skazany na 20 lat więzienia, zredukowanych następnie do lat 16. Podczas śledztwa i rozprawy sądowej zachowywał się godnie. Po zerwaniu przez Turcję stosunków z Niemcami został w sierpniu 1944 roku uwolniony z więzienia na mocy amnestii dla obywateli radzieckich. Powrócił do ZSRR. Rozpoczął pracę w centralnym aparacie wywiadu, lecz już w październiku 1944 r. został skierowany na tyły niemieckie – uczestnik sławnej operacji *Bierezino*.

Od początku działań na froncie radziecko – japońskim był naczelnikiem Wydziału Wywiadowczego Zarządu NKGB Obwodu Czytyński. Prowadził działania wywiadowcze w Mandżurii. Od 1946 r. był rezydentem wywiadu w Mandżurii posługując się legendą zastępcy naczelnika Kolei Chińsko – Czuncinskiej i nazwiskiem Karłow. W związku z chorobą przeszedł do rezerwy. Pracował na kolei w Jarosławiu, a następnie od 1952 roku w Instytucie Orientalistyki i Instytucie Narodów Azji Akademii Nauk ZSRR.

Zmarł 7 kwietnia 1966 r. Za swoje zasługi był uhonorowany Orderem Lenina, dwoma Orderami Czerwonego Sztandaru, Orderem Wojny Ojczyźnianej I stopnia i wieloma medalami. 

Zmarł 7 kwietnia 1966 r. Za swoje zasługi był uhonorowany Orderem Lenina, dwoma Orderami Czerwonego Sztandaru, Orderem Wojny Ojczyźnianej I stopnia i wieloma medalami. 





## Model działań bezpieczeństwa teleinformatycznego z punktu widzenia Ustawy o ochronie informacji niejawnych

**W polskim systemie prawnym bezpieczeństwo informacji niejawnych jest regulowane przede wszystkim przez Ustawę o ochronie informacji niejawnych (Dz. U. 2010 nr 182 poz. 1228), zwaną dalej UOIN. Poprzez taką informację niejawną należy rozumieć taką, której ujawnienie spowodowałoby szkodliwe skutki dla funkcjonowania państwa.**

Informacje tego typu są odpowiednio klasyfikowane, według czterech kategorii klauzul: ściśle tajne (najwyższa), tajne, poufne, zastrzeżone (najniższa). Klauzula ściśle tajne może dotyczyć informacji, które ujawnione mogłyby doprowadzić do np. identyfikacji funkcjonariuszy tajnych służb, zagrożić świadkom koronnym lub ich rodzinom. Informacje tajne to takie które ujawnione mogą m. in. pogorszyć stosunki z innymi krajami, zakłócić przygotowania obronne, utrudnić czynności operacyjno-rozpoznawcze i śledcze. Informacje poufne grożą natomiast w przypadku ujawnienia np. zakłóceniem porządku publicznego, utrudnieniem prowadzenia bieżącej polityki zagranicznej, utrudnić wykonywanie zadań służbom ochrony państwa. Najniższa klauzula, zastrzeżone, dotyczy ogólnie ujętego szkodliwego wpływu na działanie organów władzy publicznej, realizacji polityki wewnętrznej i zagranicznej, itd. Klauzule odpowiednio do wrażliwości danej informacji nadaje osoba odpowiadająca za podpisanie dokumentu zawierającego tę informację.

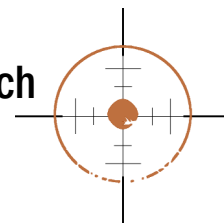
Ogólnie, to od tego momentu (a nawet już od rozpoczęcia tworzenia informacji) zaczyna się jej ścisła ochrona. Ustawa przewiduje kontrolę dostępu do niej na podstawie przydzielania odpowiednich zezwoleń przez ABW/SKW (tzw. poświadczenia bezpieczeństwa uzyskiwane po wnikliwym sprawdzeniu osoby). W miejscu jej przechowywania wymagane

stają się zabezpieczenie fizyczne informacji (m. in. kancelarie tajne) oraz szkolenia w zakresie ochrony informacji oraz kontrolę stanu ich zabezpieczenia przez odpowiedzialne za nie jednostki. Ustawa zajmuje się również problematyką bezpieczeństwa teleinformatycznego.

Z systemami teleinformatycznymi spotykamy się codziennie. Są to zarówno komputery osobiste jak i serwery, urządzenia przesyłowe (np. służące sieci Internet, czy telefonii komórkowej) i towarzyszące im dodatkowe wyposażenie elektroniczne. Razem stanowią one określony system, który wykorzystywany jest do pewnych działań. Ponieważ systemy wykonując swoje funkcje nie pozostają wolne od zagrożeń, niezbędne staje się zapewnienie im bezpieczeństwa.

Bezpieczeństwo nazywane jest niekiedy stanem i procesem. Niektórzy autorzy określają bezpieczeństwo jako „obiektywną pewność gwarancji nienaruszalnego przetrwania i swobód rozwojowych”<sup>1</sup>. Stanisław Koziej dodaje, że w bezpieczeństwie rozumianym jako dynamiczne zjawisko, działalność podmiotu którego ono dotyczy „zmierza do zapewniania możliwości przetrwania, rozwoju i swobody realizacji własnych interesów w konkretnych warunkach, poprzez wykorzystanie okoliczności sprzyjających (szans), podejmowanie wyzwań, redukcja ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów”<sup>2</sup>. Naruszenie bezpieczeństwa systemów teleinformatycznych godzi więc w gwarancję swobód przetrwania i rozwoju podmiotu, w którym urządzenia funkcjonują lub dla którego mają one istotne znaczenie. W przypadku przechowywania informacji niejawnych w systemie komputero-





wym może oznaczać to sprowadzenie zagrożenia zarówno dla jednostki organizacyjnej (np. starostwo, przedsiębiorstwo) jak i na podmioty trzecie, bądź nawet całe państwo, w zależności od rodzaju przechowywanych informacji. Informacje niejawne mogą trafić do niepowołanych rąk, być publicznie ujawnione, zmodyfikowane bez uprawnień lub zniszczone albo niedostępne<sup>3</sup>. Zagrożenie może przyjść ze strony celowej działalności ludzkiej (służby wywiadowcze innych państw, przestępczość), błędów ludzkich (w oprogramowaniu, użytkowaniu), błędów techniki czy nawet zagrożeń naturalnych (szczególnie dla paraliżu całych systemów poprzez działania żywiołów). Zwiększanie bezpieczeństwa można tu osiągnąć poprzez stosowanie odpowiednich środków w celu wykorzystania szans (np. technologicznych), przeciwdziałanie i zapobieganie (np. szkolenia personelu) i redukcję ryzyka (np. ochrona fizyczna, kontrola dostępu).

### **Prawne środki bezpieczeństwa teleinformatycznego**

Ochrona prawna systemów teleinformatycznych organizowana jest w Polsce przez szereg powiązanych ze sobą ustaw i rozporządzeń. Wśród najważniejszych ustaw, oprócz Ustawy o ochronie informacji niejawnych, należy wymienić także: Ustawę prawo telekomunikacyjne (z dnia 16 lipca 2004 roku), Ustawę o ochronie baz danych (z dnia 27 lipca 2001 roku), czy Ustawę o podpisie elektronicznym (z dnia 18 września 2001 roku). Rozporządzeń związanych z bezpieczeństwem teleinformatycznych jest kilkadziesiąt<sup>4</sup>. Dochodzą do nich także zarządzenia i wytyczne, w tym np. „Wytyczne służby kontrwywiadu wojskowego w sprawie powoływania i odwoływania kancelarii kryptograficznych (z 22 maja 2012 roku)”. Nie można pominąć też norm obronnych, wyznaczających standardy ochrony. Jednak na potrzeby tematu tego opracowania oprócz UOIN najistotniejszym dokumentem jest Rozporządzenie Prezesa Rady Ministrów w

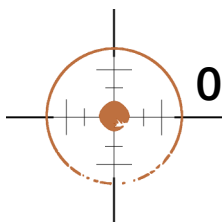
sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (z dnia 20 lipca 2011 roku, Dz.U.2011.159.948). Wraz z Ustawą o ochronie informacji niejawnych oba dokumenty tworzą pewien model działań które zapewniają bezpieczeństwo teleinformatyczne w kontekście ochrony niejawnych informacji. W artykule zostanie podjęta próba opisanie zarysu modelu, na podstawie analizy wymienionych i innych dokumentów.

### **Model działań zapewniających bezpieczeństwo teleinformatyczne**

Za ochronę systemów teleinformatycznych przetwarzających informacje niejawne w jednostce organizacyjnej odpowiedzialni są inspektor bezpieczeństwa telekomunikacyjnego oraz administrator. Pewne role pełnią też kierownik jednostki organizacyjnej i nadzorujące całość Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego<sup>5</sup>. Zadaniem osób w jednostce organizacyjnej (kierownika i powołanych przez niego inspektora i administratora) jest dbanie o bezpieczeństwo informacji niejawnych w systemie teleinformatycznym, poprzez zapewnienie temu systemowi poufności, dostępności oraz integralności<sup>6</sup>. Bezpieczeństwo powinno zostać zapewnione w sferze fizycznej, personalnej, elektromagnetycznej, kryptograficznej oraz technicznej<sup>7</sup>. Zagłębiając się w funkcjonowanie systemu teleinformatycznego można jeszcze wyróżnić poszczególne elementy ochrony, składające się na całość systemu informatycznego.

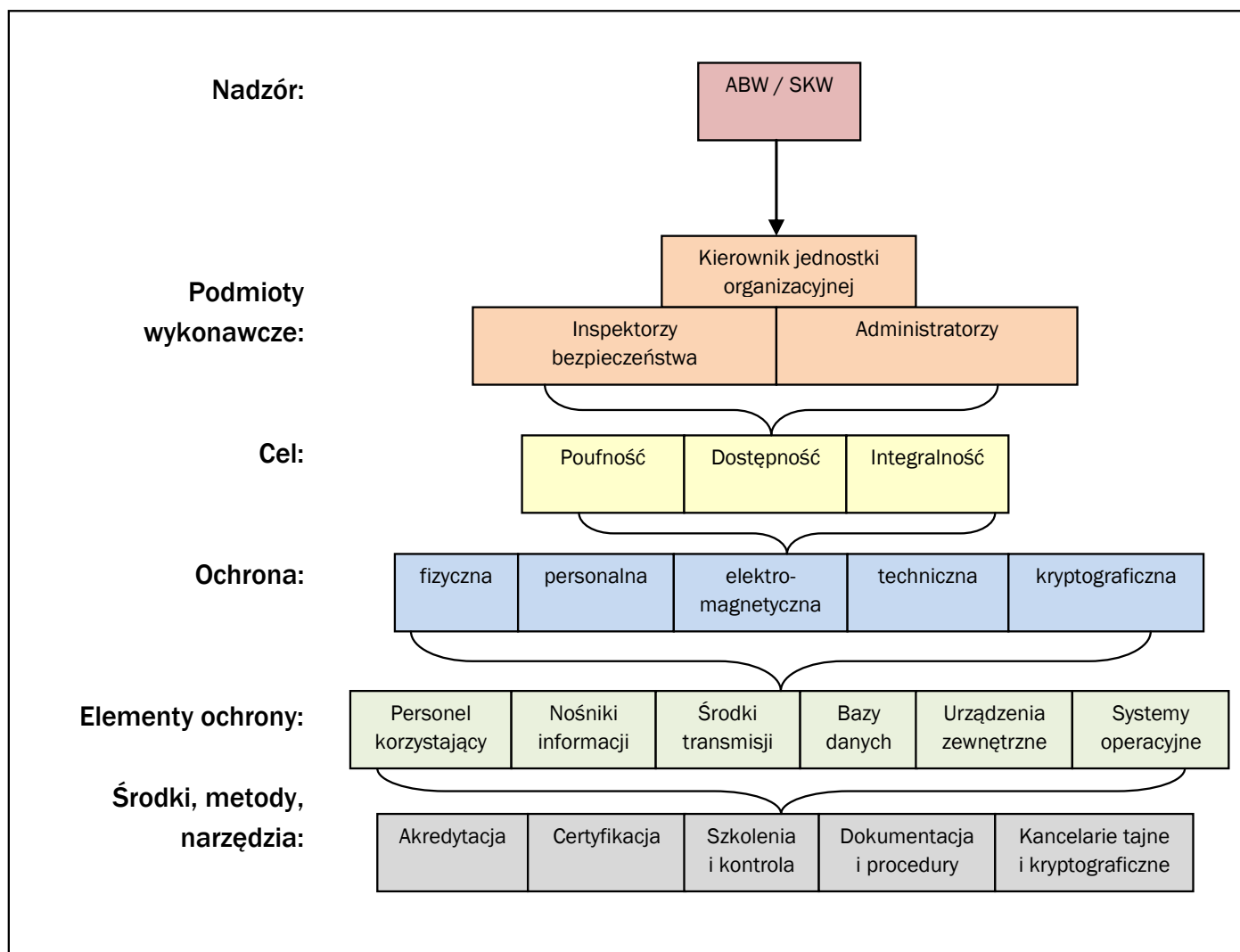
### **Proces bezpieczeństwa teleinformatycznego i jego etapy**

Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (z dnia 20 lipca 2011 roku) wymienia pięć etapów zapewnienia bezpieczeństwa teleinfor-



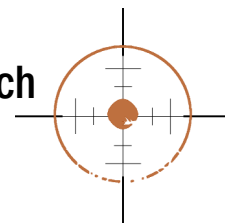
matycznego. Są to kolejno<sup>8</sup> planowanie, projektowanie, wdrażanie, eksploatacja i wycofywanie. Etap planowania służy określeniu przeznaczenia tego systemu, maksymalnej klauzuli do jakiej ma być dopuszczony, trybu bezpieczeństwa jego pracy, szacunkowej liczby jego użytkowników oraz lokalizację, gdzie ma być umieszczony<sup>9</sup>. Na etapie projektowania szacuje się ryzyko, dokonuje odpowiedniego wyboru zabezpieczeń, uzgadnia się z podmiotem akredytującym (ABW/SKW lub kierownik jednostki organizacyjnej) plan dopuszczenia tego systemu do danej klauzuli,

rodzaj i ilość odpowiednich urządzeń kryptograficznych oraz opracowuje się dokument szczególnych wymagań bezpieczeństwa<sup>10</sup>. Etap wdrażania dotyczy pozyskania i uruchomienia potrzebnych urządzeń i elementów wchodzących w skład systemu, przeprowadzanie testów bezpieczeństwa, dalsze szacowanie ryzyka, tworzy się dokument procedur bezpiecznej eksploatacji i uzupełnia dokument szczególnych wymagań bezpieczeństwa<sup>11</sup>. Następnie system poddaje się akredytacji. Etap eksploatacji to utrzymanie systemu w zgodności z jego dokumentacją, dalsze szaco-



Schemat modelu działań zapewniających bezpieczeństwo teleinformatyczne w świetle Ustawy o ochronie informacji niejawnych (z dnia 5 sierpnia 2010) i Rozporządzenia Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (z dnia 20 lipca 2011 roku).

Opracowanie własne.



wanie ryzyka, okresowe przeprowadzanie testów bezpieczeństwa, wprowadzanie koniecznych zmian do systemu i dokumentacji - za zgodą ABW/SKW jeśli są to modyfikacje istotne dla bezpieczeństwa<sup>12</sup>. Ostatnim etapem jest wycofywanie systemu – zaprzestaje się jego eksploatacji, powiadamia ABW/SKW, oddaje im wydane przez nich świadectwo akredytacji, i usuwa informacje niejawne przechowywane w wycofanym systemie<sup>13</sup>.

### Akredytacja bezpieczeństwa teleinformatycznego

Podstawą dopuszczenia systemu teleinformatycznego do przetwarzania informacji niejawnych jest udzielenie mu akredytacji bezpieczeństwa. Jeśli system ten ma współdziałać tylko z informacjami o klauzuli „zastrzeżone”, to akredytację taką przyznaje sam kierownik jednostki organizacyjnej, któremu dany system podlega<sup>14</sup>. Wymogiem jest analiza oraz akceptacja dokumentacji bezpieczeństwa przez kierownika i następnie przekazanie dokumentacji do ABW/SKW. Służby mogą przedstawić, co do dokumentacji, własne zalecenia dotyczące wprowadzenia zmian polepszających bezpieczeństwo<sup>15</sup>. Jeśli kierownik nie dostosuje się do tych zaleceń w wystarczającym stopniu, służby mogą nakazać wstrzymanie przetwarzania informacji niejawnych w systemach<sup>16</sup> pomimo udzielenia im akredytacji przez kierownika. Pozwala to zapobiec sytuacji, kiedy dopuszczony do informacji „zastrzeżonych” zostanie system niespełniający minimalnych wymogów bezpieczeństwa. Natomiast, aby system informatyczny mógł przetwarzać informacje niejawne o wspomnianych klauzulach „poufne” i wyższe, niezbędne jest wydanie akredytacji przez ABW/SKW. Odbywa się to po spełnieniu dwu wymogów.

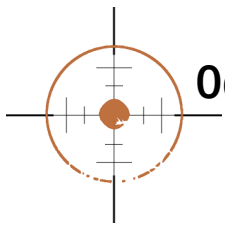
Pierwszym wymogiem udzielenia akredytacji przez ABW/SKW jest pozytywna ocena dokumentacji, a drugim warunkiem jest pozytywny wynik przeprowadzonego w jednostce audytu. Akredytacja przyznawana jest na czas 5 lat. Powodem takiego okresu jest m.

in. fakt, że elektronika oraz oprogramowanie wchodzące w skład systemów teleinformatycznych z roku na rok pozostają powoli w tyle za nowszymi ich wersjami, okres ten wystarczy, aby system stał się przestarzały, co negatywnie odbiłoby się na jego bezpieczeństwie. Ustawodawca zatem z góry przewidział konieczność przeprowadzania ponownej procedury udzielania akredytacji po 5 latach od jej przyznania<sup>17</sup>.

### Zadania kierownika, inspektora oraz administratora

Za ochronę informacji niejawnych w jednostce organizacyjnej odpowiada jej kierownik. Jego podstawowym zadaniem jeśli chodzi o bezpieczeństwo teleinformatyczne jest określenie, czy w podległych mu systemach teleinformatycznych lub sieciach są przetwarzane informacje niejawne, albo będą takie w przyszłości. Otrzymuje od ABW/SKW niezbędną pomoc do realizacji swoich zadań, w postaci zaleceń w zakresie bezpieczeństwa teleinformatycznego. Powiadamia te służby o incydentach zagrożenia bezpieczeństwa. Kierownik zapewnia również szkolenie osób przeznaczonych do pracy z systemem teleinformatycznym przed ich dopuszczeniem do pracy. Udziela akredytacji bezpieczeństwa systemom przeznaczonym do klauzul „zastrzeżone” - po spełnieniu wcześniej omawianych warunków. Odpowiada za przekazanie ABW/SKW dokumentacji bezpieczeństwa teleinformatycznego, akceptuje wyniki procesu szacowania ryzyka (o samym procesie analizy ryzyka będzie mowa dalej). Kierownik wyznacza pracowników pionu ochrony, którzy będą pełnić odpowiednio: funkcję inspektora bezpieczeństwa teleinformatycznego oraz administratora systemu. Przy czym, te osoby nie mogą piastować obu funkcji jednocześnie.

Inspektor bezpieczeństwa teleinformatycznego jest odpowiedzialny za „weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa



oraz przestrzegania procedur bezpiecznej eksploatacji<sup>18</sup>. Inspektor bierze też udział w procesie szacowania ryzyka, weryfikując poprawność realizacji zadań administratora, „właściwe zarządzanie konfiguracją oraz uprawnieniami przydzielanymi użytkownikom<sup>19</sup>, „znajomość i przestrzeganie przez użytkowników zasad ochrony informacji niejawnych<sup>20</sup> oraz weryfikuje „stan zabezpieczeń systemu teleinformatycznego, w tym analizując rejestry zdarzeń systemu teleinformatycznego<sup>21</sup>.

Zadaniem z kolei administratora jest odpowiedzialność za „funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego<sup>22</sup>. Administrator bierze też udział w tworzeniu dokumentacji bezpieczeństwa oraz w procesie zarządzania ryzykiem<sup>23</sup>. Realizuje szkolenia użytkowników systemu, utrzymuje zgodność systemu z jego dokumentacją i wdraża zabezpieczenia systemowe.

### Uprawnienia dostępu do informacji niejawnych w systemie teleinformatycznym

Z systemu teleinformatycznego będą korzystał użytkownicy, przetwarzając za jego pomocą informacje niejawne. Z tego powodu, systemy powinny działać w różnych trybach swojej pracy, charakteryzujących się różnym poziomem bezpieczeństwa. Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (z dnia 20 lipca 2011 roku) wymienia trzy takie tryby, i są to kolejno tryb dedykowany, systemowy, i wielopoziomowy<sup>24</sup>.

Tryb dedykowany oznacza, że wszyscy użytkownicy „posiadają uprawnienie do dostępu do informacji niejawnych o najwyższej klauzuli tajności, jakie mogą być przetwarzane w tym systemie teleinformatycznym<sup>25</sup>, przy jednocześnie posiadanej ku temu uzasadnionej potrzebie. Uprawnienie to poświadczenie bezpieczeństwa.

Tryb systemowy to spełnienie pierwszego powyższego warunku, ale zakłada się, że nie wszyscy z tych użytkowników posiadają taką uzasadnioną konieczność<sup>26</sup>.

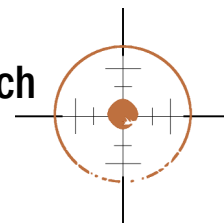
Tryb wielopoziomowy całkiem odwraca sytuację. Użytkownicy mają różne poziomy uprawnień, i różnią się w uzasadnieniu swoich potrzeb<sup>27</sup>. Jeśli więc system przetwarza informacje zastrzeżone, poufne i tajne, w tej konfiguracji niektórzy użytkownicy mogą mieć dostęp tylko do informacji zastrzeżonych i to w niewielkim zakresie potrzeb. System musi więc być tak skonstruowany, aby nadal zapewniał poufność, integralność i dostępność.

### Ochrona fizyczna i elektromagnetyczna

Ochrona fizyczna i elektromagnetyczna dotyczy bezpieczeństwa systemu pod kątem fizycznego dostępu (nieuprawnionego, kradzieży, zniszczenia) oraz jego podsłuchu lub zakłócania za pomocą różnych środków technicznych. Bezpieczeństwo fizyczne opisywane jest w dokumencie szczególnych wymagań bezpieczeństwa, który przedstawia m. in. granice i lokalizacje stref kontrolnych i inne środki ochrony<sup>28</sup>. Dokument precyzuje sposoby ochrony elektromagnetycznej. Środki stosowane w tym celu dobiera się na podstawie przeprowadzonej analizy ryzyka, po uwzględnieniu zaleceń<sup>29</sup>. Środki takie podlegają również certyfikacji i badaniom bezpieczeństwa<sup>30</sup> prowadzonym przez ABW/SKW. Certyfikaty takie wydawane są na okres nie krótszy niż 3 lata, a od odmowy wydania takiego certyfikatu nie służy odwołanie.

### Analiza, ocena i szacowanie ryzyka

Ryzykiem nazywa się kombinację skutków oraz ich prawdopodobieństwa. Jeśli skutki zdarzenia są wysokie, lecz prawdopodobieństwo nikłe, ryzyko przyjmuje postać niską. Lecz już średnie prawdopodobieństwo przy średniej wagi skutkach daje średnie ryzyko -



jednocześnie, skutki pomijalnej wagi przy wysokim prawdopodobieństwie nie czynią ryzyka wysokim. Ryzyko to bierze się z możliwych zagrożeń dla systemu informatycznego. Proces analizy, oceny i szacowania ryzyka zajmuje ważne miejsce w zadaniu zapewnienia bezpieczeństwa tym systemom.

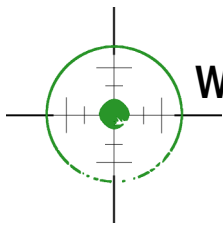
Wyniki procesu szacowania tego ryzyka powinny znajdować się w dokumencie szczególnych wymagań bezpieczeństwa teleinformatycznego<sup>31</sup>. Szczególną uwagę zwraca się na możliwości wykrycia, przechwycenia lub zakłócenia transmisji danych w tym systemie. Identyfikuje się posiadane zasoby, możliwe zagrożenia, stopnie podatności, potrzebne zabezpieczenia oraz skutki wystąpienia danych zagrożeń<sup>32</sup>. Ryzyko należy kontrolować poprzez wdrażanie nowych zabezpieczeń i obniżanie zidentyfikowanego ryzyka, pozostawianie go bez zmian, jeśli jest to ryzyko akceptowalne, unikanie go w drodze nie podejmowania działań będących jego źródłem, bądź też w drodze przenoszenia odpowiedzialności i ryzyka na inny podmiot<sup>33</sup>.

### Uwagi końcowe

Zaprezentowany w artykule model działań zapewniający bezpieczeństwo teleinformatyczne to zaledwie wycinek całości zagadnienia. Zagłębiając się w nie, wiele miejsca poświęcić można praktycznie każdemu z jego elementów, z których nie wszystkie zostały, nawet ogólnie nakreślone. W artykule skupiono się poza tym na procesie zabezpieczenia informacji na podstawie Ustawy o ochronie informacji niejawnych oraz rozporządzeń wydanych do niej. Warto odnotować, iż nie jest to jedyny dokument dotyczący tych kwestii. Przykładem jest norma ISO/IEC 27001 regulująca tworzenie SZBI (Systemu zarządzania bezpieczeństwem informacji), mająca szerokie zastosowanie w przedsiębiorstwach zainteresowanych ochroną swoich wrażliwych informacji, choć nie będących niejawnymi z punktu widzenia omawianej Ustawy.

### Przypisy

- 1 R. Jakubczak, J. Flis, *Bezpieczeństwo narodowe Polski w XXI w.* Warszawa 2006, s. 16.
- 2 S. Koziej, *Między piekłem a rajem: szare bezpieczeństwo na progu XXI w.*, Toruń 2006, s. 7.
- 3 K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, s. 13. Warszawa 2008.
- 4 Zob. *Systemy teleinformatyczne - przepisy*, strona [www. Źródło online: \[http://www.iniejawna.pl/przyciski/tele\\_info.html\]](http://www.iniejawna.pl/przyciski/tele_info.html), dostęp: 2013-08-04. Autorzy strony wymieniają ponad 50 ustaw i rozporządzeń jako związanych z bezpieczeństwem teleinformatycznym.
- 5 Agencja Bezpieczeństwa Wewnętrznego odpowiada za jednostki cywilne, a Służba Kontrwywiadu Wojskowego za jednostki wojskowe. Dzieje się tak, ponieważ ABW można uznać za kontrwywiad cywilny, a ABW - za kontrwywiad wojskowy. Pod ABW podlegają więc w ochronie informacji niejawnych takie podmioty jak starostwa, gminy, urzędy miejskie, ale także Policja. Pod SKW podlegają jednostki wojskowe, ale też Żandarmeria Wojskowa.
- 6 Rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego. § 5. 1. (Dz.U.2011.159.948)
- 7 Zob. K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych...*, wyd. cyt., s. 14. Autor wymienia sferę fizyczno-techniczną, sprzętowo-programową, i organizacyjno-kadrową.
- 8 Rozporządzenie... § 18. 1.
- 9 Tamże, § 18. 2.
- 10 Tamże, § 18. 3.
- 11 Tamże, § 18. 4.
- 12 Tamże, § 18. 5.
- 13 Tamże, § 18. 6.
- 14 Ustawa o ochronie informacji niejawnych, art. 48, ust. 9 (Dz.U. 2010 nr 182 poz. 1228)
- 15 Tamże, art. 48, ust. 11-12.
- 16 Tamże, art. 48, ust. 12.
- 17 Tamże, art. 48, ust. 2.
- 18 UOIN, art. 52. ust. 1, p. 1.
- 19 Rozporządzenie... § 14. p. 1.
- 20 Tamże, § 14. p. 2.
- 21 Tamże, § 14. p. 3.
- 22 UOIN, art. 52. ust. 1, p. 2.
- 23 Rozporządzenie... § 13.
- 24 Tamże, § 3.
- 25 Tamże, § 3, ust. 1.
- 26 Tamże, § 3, ust. 2.
- 27 Tamże, § 3, ust. 3.
- 28 Rozporządzenie... § 25, ust. 3, p. 5.
- 29 tamże, § 8, ust. 1.
- 30 UOIN, art. 50. Ust. 1. Tutaj jak z rozporządzeniem
- 31 Tamże, art. 49, ust. 1.
- 32 Rozporządzenie... § 20. ust. 1.
- 33 Rozporządzenie... § 21. ust. 1.

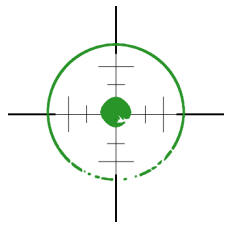


# Droga ku jakości i odpowiedzialności policji

Na początek kilka zdań o Autorze interesującego opracowania „Społeczna odpowiedzialność Policji. Teoria i praktyka” - Dominiku Hryszkiewiczu. Jest policjantem pełniącym służbę w Wyższej Szkole Policji w Szczytnie od 2004 roku. Stopień doktora w dyscyplinie nauki wojskowe uzyskał w 2011 roku w Akademii Obrony Narodowej w Warszawie. Jego zainteresowania naukowe ukierunkowane są na problematykę zastosowania nowoczesnych narzędzi zarządzania do rzeczywistych możliwości instytucji zorganizowanych, o charakterze publicznym. Jest autorem bądź współautorem publikacji poświęconych zarządzaniu kapitałem ludzkim, zarządzaniu strategicznemu oraz problematyce konstruowania nowoczesnych kryteriów oceny efektywności pracy instytucji publicznych w Polsce. Od 1 sierpnia 2013 roku, kom. dr Dominik Hryszkiewicz jest dyrektorem Instytutu Nauk Społecznych Wydziału Administracji Wyższej Szkoły Policji Szczytnie.

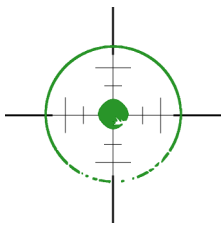
Opracowanie to warto polecić do przeczytania, a niekiedy do przestudiowania niektórych jego części z wielu względów. Pozycję tę przede wszystkim powinni obowiązkowo zainteresować się nie tylko policjanci czy ich policyjni przełożeni. Formacje umundurowane i uzbrojone w ramach polskich rozwiązań ustrojowych to także, np. Agencja Bezpieczeństwa Wewnętrznego oraz Agencja Wywiadu, Służba Kontrwywiadu Wojskowego oraz Służba Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Żandarmeria Wojskowa, Służba Więzienna, Biuro Ochrony Rządu, Inspekcja Transportu Drogowego. To instytucje, które ponoszą, każda w swoim zakresie, odpowiedzialność wobec społeczeństwa za podejmowane działania. Nie od dziś wiadomo, że kierowanie taką instytucją jak Policja jest zagadnieniem trudnym i złożonym.

Policja jest instytucją działającą na terenie całej Polski, posiadającą dość złożoną strukturę organizacyjną przy pomocy, której realizuje zadania wynikające z ustawy o Policji i innych ustaw. Ogólnie można powiedzieć, że Policja, jako umundurowana i uzbrojona formacja utworzona została, aby służyć społeczeństwu. Jest przeznaczona do ochrony bezpieczeństwa ludzi oraz do utrzymania bezpieczeństwa i porządku publicznego<sup>1</sup>. Podstawowym obowiązkiem Policji, nałożonym na mocy ustawy, jest ochrona życia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra, ochrona bezpieczeństwa i porządku publicznego (w tym zapewnienie spokoju w miejscach publicznych oraz środkach publicznego transportu i komunikacji publicznej, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania). Poczesne miejsce zajmują działania mające na celu zapobieganiu popełniania przestępstw i wykroczeń oraz zjawiskom kryminogennym. Warunkiem skuteczności działania, jest nie tylko pełna realizacja przez Policję podstawowych zadań, lecz również właściwa koordynacja działań i ścisła współpraca z instytucjami ochrony prawnej<sup>2</sup>. Jak zauważa S. Pieprzny, ogólny charakter zadań został określony w art. 1 ustawy o Policji, ale treść tego artykułu wskazuje na brak możliwości dokładnego określenia granic tych zadań<sup>3</sup>. Zakres zadań wykracza, w odniesieniu do służebnej roli tej formacji, poza ochronę bezpieczeństwa i porządku publicznego. Jak dalece, trudno o precyzyjną odpowiedź. Z tego wynika, że każda sprawa, która służy społeczeństwu, winna leżeć w zakresie zadań Policji. Z praktyki wiadomo, że tak oczywiście nie jest, bo zadania służące społeczeństwu powierzane są także innym podmiotom. Wszelkie działania Policji, zmierzające do ochrony bezpieczeństwa ludzi oraz do utrzymania na akcep-



towanym przez społeczeństwo poziomie poczucia bezpieczeństwa i porządku publicznego, nie mogą być jednak realizowane w każdych warunkach i za każdą cenę. Każdy człowiek, każda osoba ma konstytucyjnie zagwarantowane prawa, których w toku podejmowanych czynności służbowych, czy ogólniej w działalności instytucji, należy przestrzegać. Działania te absolutnie muszą być zgodne z obowiązującym prawem, a jeśli stanowią w tym zakresie wyjątek (np. działania w ramach kontratypu), to muszą zachowywać wszelkie te warunki, pod którymi prawo zezwala na wyjątkowe odstępstwa od swych postanowień<sup>4</sup>. Nie wchodząc głębiej w zadania tej formacji, można powiedzieć, że społeczne oczekiwania stale rosną i obejmują coraz to nowe obszary. Wymaga to umiejętnego dostosowania się do zmieniających się warunków otoczenia oraz doskonalenia systemu zarządzania w kierunku podnoszenia efektywności. Recenzowane opracowanie wzbogaca ten proces. Odpowiedzialność społeczna także tej instytucji (organizacji), wymaga określenia tego, co jest dobre, a co złe. Oznacza to konieczność wywiązywania się ze zobowiązań prawnych, ale również troskę o moralne postępowanie, inwestowanie w kapitał ludzki a także dbanie o poprawne relacje ze społeczeństwem. Czym zatem jest „społeczna odpowiedzialność”? **To całokształt zobowiązań danej organizacji wobec otoczenia, w którym funkcjonuje, zmierzających do budowania dobrobytu całego społeczeństwa oraz korzystnych relacji z tym społeczeństwem poprzez przestrzegania w procesie zarządzania obowiązujących zasad etycznych<sup>5</sup>**. Biorąc pod uwagę definicję zaproponowaną przez D. Hryszkiewicza zagadnienie społecznej odpowiedzialności jawi się, jako wielowątkowe a zarazem złożone. Osoby zainteresowane problematyką społecznej odpowiedzialności w procesie zarządzania organizacją wypada odsłać do rozdziału pierwszego recenzowanego opracowania. Pojęcie to funkcjonuje w praktyce w biz-

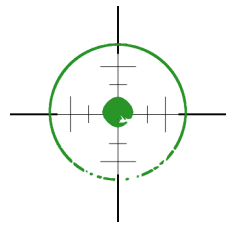
nesie od około trzydziestu lat. Natomiast w odniesieniu do Policji, jest to pionierska próba wprowadzenia tego pojęcia do problematyki i specyfiki działania służb mundurowych. Autor ma zresztą tego świadomość pisząc: *Model społecznej odpowiedzialności Policji musi zawierać kryteria i wskaźniki uwzględniające charakter prowadzonej działalności. Nie można oceniać tej organizacji, opierając się na założeniach identycznych jak w przypadku przedsiębiorstw prywatnych. (...) Zaproponowany model zawiera obszary kluczowe dla funkcjonowania Policji, choć ze względu na zakres poruszanej problematyki z pewnością nie wyczerpuje on wszystkich możliwych parametrów definiujących określone kryterium<sup>6</sup>*. W ramach **kryterium etycznego** w odniesieniu do Policji, zainteresowania Autora kierunkowane były na: posiadanie kodeksu etycznego; problem szkolenia i edukacji; motywowanie oraz zwalczanie korupcji w policyjnych szeregach. To ostatnie zagadnienie szczególnie bulwersuje. W październiku 2012 r. mogliśmy przeczytać informację o 13 policjantach z drogówki zatrzymanych za łapówki. Pełnili służbę w Wydziale Ruchu Drogowego Komendy Wojewódzkiej Policji w Poznaniu. W lipcu 2013 r. usłyszeliśmy, że 10 policjantów Wydziału Ruchu Drogowego Komendy Powiatowej Policji w Łowiczu zostało zatrzymanych na polecenie łódzkiej prokuratury okręgowej. Policjanci w wieku od 28 do 47 lat, zostali przesłuchiwanii pod zarzutami przyjmowania korzyści majątkowych i przekroczenia uprawnień. Według śledczych policjanci z łowickiej „drogówki” podczas patroli mieli przyjmować pieniądze w kwotach od 20 do 500 zł lub do 100 euro, bądź prezenty rzeczowe. Poszczególnym funkcjonariuszom zarzucono popełnienie od pięciu aż do 54 tego rodzaju przestępstw korupcyjnych<sup>7</sup>. Problematyka korupcyjna i nie tylko ma odzwierciedlenie w badaniach ankietowych. Pytania kierowane do respondentów wraz z opracowanymi danymi statystycznymi znajdziemy w części



drugiej monograficznego opracowania (Aneks zawierający załączniki nr 1 i nr 2). Pytania obejmujące problematykę postaw etycznych oraz korupcji i innych przestępstw policjantów wraz z opracowanymi odpowiedziami warto gruntownie przestudować. Zresztą, badania z uwagi na problematykę są interesujące w sensie poznawczym. Ponieważ o recenzji nie można napisać wszystkiego, co jest zawarte na 333 stronach, toteż w telegraficznym skrócie. **Kryterium społeczne** obejmuje problematykę: zatrudnienia i stosunku pracy; stosunki z interesariuszami oraz ze społecznością lokalną; świadczenie usług; zarządzanie. Trzecie z przyjętych przez Autora kryteriów, to **kryterium ekologiczne**. W ramach tego omówione zostały kwestie: zarządzanie ukierunkowane na przestrzeganie zasad związanych z ochroną środowiska naturalnego; świadczone usługi; szkolenie i edukację. Autor proponuje także kolejne wyznaczniki ekologiczne. Dzieło dla bardziej przejrzystego przybliżenia podzielone zostało przez recenzującego na dwie części. Aneks, o których była już mowa wraz z załącznikami, zawiera opracowane wyniki badań ankietowych zamieszczonych w rozdziałach: czwartym i piątym. Na część pierwszą, składają się: Wstęp; problematyka dotycząca społecznej odpowiedzialności oraz o zarządzaniu strategicznym Policji (rozdziały pierwszy i drugi); przedstawienie metodologii przeprowadzonych badań (rozdział trzeci); przedstawienie charakterystyki respondentów w ramach badań weryfikujących model społecznej odpowiedzialności polskiej policji (rozdziały czwarty i piąty); problematyka funkcjonowania modelu odpowiedzialności społecznej w działalności Policji według trzech przyjętych kryteriów (etyczne, społeczne, ekologiczne), czynniki wpływające na realizację modelu społecznej odpowiedzialności oraz zakres tej realizacji (rozdział szósty); wnioski końcowe; bibliografia; spis rysunków; spis tabel; spis wykresów. Po tym hasłowym przybliżeniu części pierw-

szej, pora podjąć próbę zainteresowania innych odbiorców aniżeli przedstawiciele służb mundurowych. Mam na myśli studentów, którzy zainteresowani są problematyką bezpieczeństwa, zarządzania w formacjach zmilitaryzowanych i nie tylko. Jak napisał prof. J. Klimek, *Autor w sposób dojrzały, przemyślany i metodologicznie konsekwentny analizuje zagadnienia dotyczące polskiej Policji i to, w jakim stopniu faktycznie wypełnia ona oczekiwania, które są formułowane pod jej adresem przez społeczeństwo*. Przytaczając zdanie z recenzji wydawniczej jednego z recenzentów tego opracowania, czuję się zwolniony z potrzeby przybliżania czy rozwijania myśli w nim zawartej. Stwierdzenie to ma oczywiście uzasadnienie w treści recenzowanego dzieła. Ponieważ doświadczenie podpowiada mi, że studentów bardziej przekonują przykłady, toteż dla zachęcenia po sięgnięciu po tę pozycję, kilka zdań o badaniach. Przedmiotem przedstawionych w opracowaniu badań była instytucja polskiej Policji, a w ramach niej zjawisko społecznej odpowiedzialności. Podmiotem badań były dwie grupy reprezentatywne, po 300 osób każda. Autor przeprowadził badania w środowisku cywilnym (pracownicy przedsiębiorstwa Totalizator Sportowy) oraz wśród policjantów, z co najmniej trzyletnim stażem służby. Cel i przedmiot badań został przedstawiony w punktach 1-4 (s. 99-100), a cele te mają charakter poznawczy. Problemy badawcze i hipotezy natomiast przedstawione nieco dalej (s.101-105). D. Hryszkiewicz podzielił się też wiadomościami na temat metody, techniki i narzędzi badawczych. Dla niektórych te pojęcia mogą być znane, chociażby z problematyki badań kryminologicznych zjawiska przestępczości. Oczywiście w omawianym opracowaniu jest także informacja z organizacji procesu badawczego. Ponieważ celem badań było: 1. Poznanie pożądanego przez społeczeństwo modelu odpowiedzialności społecznej polskiej Policji; 2. Poznanie funkcjonowania powyższego modelu





## Droga ku jakości i odpowiedzialności policji

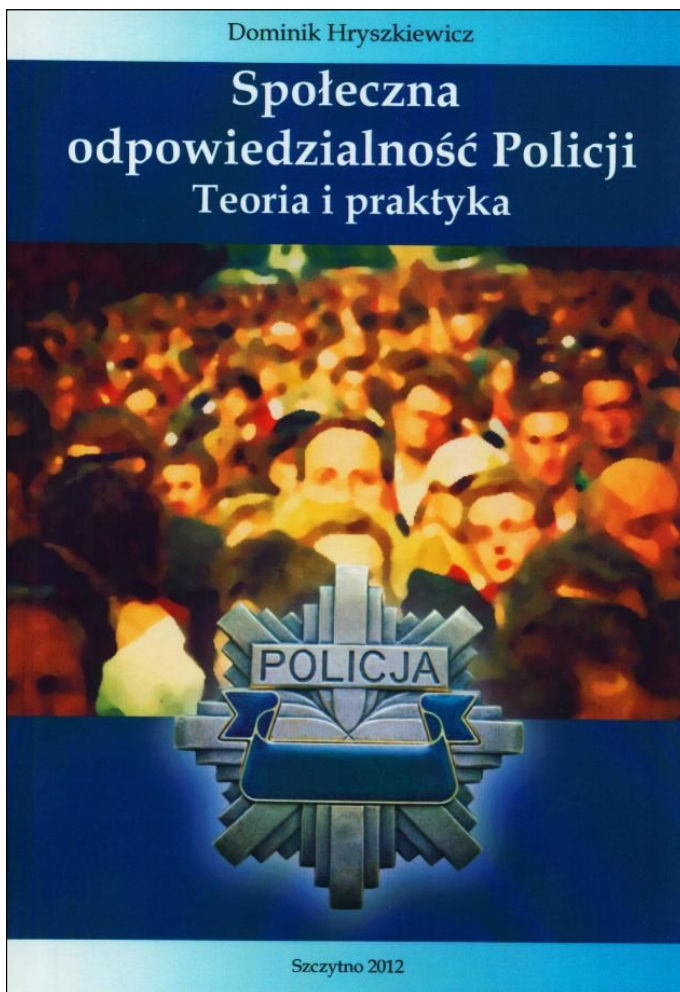
w działalności Policji; 3. Określenie czynników warunkujących (ograniczających i stymulujących) jego funkcjonowanie w Policji; 4. Określenie zakresu realizacji powyższego modelu w działalności Policji<sup>8</sup>, toteż po tak metodycznie poprawnie przeprowadzonych badaniach, łatwiej jest formułować wnioski. W chwili pisania tekstu, jeden z nich przykuwa uwagę. Policja jest organizacją, która nie zawsze funkcjonuje efektywnie w obszarach, które są przecież kluczowe z punktu widzenia jej ustawowej roli – zauważa Autor. Ostatnie wydarzenia na plaży w Gdyni również to zaświadcza. Działania Policji post factum to przedsięwzięcia, które nie do

końca przekonują, biorąc chociażby pod uwagę nakłady finansowe i koszty społeczne tych spóźnionych działań. Należy zgodzić się, że dziś nie wystarczy tylko badać i diagnozować sytuacje w organizacji. Należy na tej podstawie podejmować rzeczywiste decyzje, oczywiście w granicach prawa, w zakresie rozwiązań poprawiających efektywność zarządzania i prowadzonej działalności. W przeciwnym razie nastąpi spadek wiarygodności Policji w oczach społeczeństwa. Bez społecznej akceptacji działań, każda policja na świecie staje się bezradna, ślepa i głucha. Ponieważ tę część recenzji ukierunkowałem głównie dla studentów, toteż jedno zdanie, w zasadzie praktyczna rada. Nawet ukierunkowanie zainteresowania jedynie na problematykę badawczą, przyniesie taki pozytywny skutek, że stojąc przed problemem przeprowadzenia badań ankietowych do pracy licencjackiej czy magisterskiej, można skorzystać ze sprawdzonego wzorca. Wszystkim, którym udało się autorowi recenzji zainteresować monograficznym opracowaniem *Spółeczna odpowiedzialność Policji. Teoria i praktyka* wypada życzyć przyjemnej lektury i owocnych przemyśleń. ☺

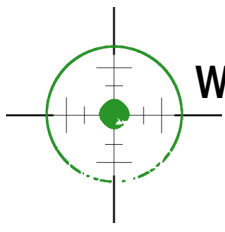
Jan Swół

### Przypisy

- 1 Zob. art. 1 ust. 1 ustawy z dnia 6 kwietnia 1990 roku o Policji (t.j. Dz. U. z 2011, nr 287, poz. 1687 ze zm.)
- 2 W. Kotowski, Ustawa o policji. Komentarz, LEX a Wolters Kluwer business, Warszawa 2012, s. 143-144.
- 3 S. Pieprzny, Policja. Organizacja i funkcjonowanie, Warszawa 2011, s. 28.
- 4 T. Hanausek, Ustawa o Policji. Komentarz, Kraków 1996, s. 17.
- 5 D. Hryszkiewicz, *Spółeczna odpowiedzialność Policji. Teoria i praktyka*, Szczytno 2012, s. 30.
- 6 Tamże, s. 69.
- 7 Zatrzymali 2/3 policjantów łowickiej „drogówki”, <http://niezalezna.pl/43494-zatrzymali-23-policjantow-z-lowickiej-drogowki>, dostęp 15 sierpnia 2013.
- 8 D. Hryszkiewicz, *Spółeczna odpowiedzialność ...*, wyd. cyt., s. 185.



**D. Hryszkiewicz, Spółeczna odpowiedzialność Policji. Teoria i praktyka, Szczytno 2012, ss. 333.**



## Bezpieczeństwo międzynarodowe - współczesne koncepcje

W 2012 roku, nakładem wydawnictwa PWN ukazała się najnowsza książka dra hab. Jacka Czaputowicza *Bezpieczeństwo międzynarodowe. Współczesne koncepcje*, autora takich publikacji, jak m.in. *System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku (1998)* oraz *Teorie stosunków międzynarodowych. Krytyka i systematyka (2007)*.

Autor – dyrektor Krajowej Szkoły Administracji Publicznej, przewodniczący grupy roboczej ds. bezpieczeństwa w International Institute of Administrative Sciences (IIAS), w swojej ostatniej książce skupił się na tematyce związanej z bezpieczeństwem międzynarodowym. Jacek Czaputowicz zawarł w niej nie tylko opis współczesnych koncepcji, takich jak realizm, liberalizm, konstruktywizm i krytyczne studia nad bezpieczeństwem, ale także poruszył kwestie, które pojawiają się w większości publikacji z zakresu bezpieczeństwa i nauk strategicznych, rzadko jednak są rozwijane lub przedstawiana jest ich geneza. Wyjaśnił m.in., czym są badania nad pokojem (*peace research*) i instytucje naukowe, takie jak Peace Research Institute Oslo (PRIO) oraz Stockholm International Peace Research Institute (SIPRI). Opisał również istotę odstraszenia nuklearnego i broni atomowej, prywatyzację bezpieczeństwa czy różnice między wojnami „starymi” i „nowymi” (koncepcja autorstwa Mary Kaldor). Przedstawił ponadto proces rozszerzania bezpieczeństwa, jaki miał miejsce po upadku systemu dwubiegunowego, odwołując się przy tym do głośnej publikacji Barry’ego Buzana.

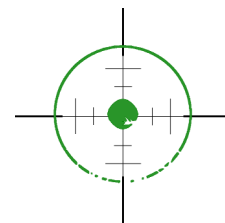
Całość książki składa się z wprowadzenia, siedmiu rozdziałów merytorycznych, zakończenia, bibliografii, indeksu nazwisk, spisu tabel, spisu rysunków oraz spisu ramek.

We wstępie autor zaznaczył, iż dyskusja na temat teoretycznych podstaw bezpieczeństwa trwa już sześćdziesiąt lat, a zapoczątkował ją artykuł Arnolda Wolfer-

sa *National Security as an Ambiguous Symbol*. Od tamtej pory do dnia dzisiejszego bezpieczeństwo było postrzegane różnie, w zależności od zagrożenia dla państwa. Tradycyjne bezpieczeństwo dotyczyło obrony (państwa) przed atakiem zewnętrznym, podbojem czy wręcz unicestwieniem. Oznaczało wolność od zagrożeń stwarzających niebezpieczeństwo dla przetwarzania. Same studia nad bezpieczeństwem (*security studies*), wyodrębniły się natomiast ze stosunków międzynarodowych po drugiej wojnie światowej, a w czasie zimnej wojny skupiły się na kwestiach takich, jak zmiany technologiczne, strategia i teoria odstraszenia nuklearnego, ekonomia obrony i system decyzyjny.

Rozdział pierwszy zatytułowany *Rozwój studiów nad bezpieczeństwem* zapoznaje czytelnika ze stanem studiów nad bezpieczeństwem po zimnej wojnie, naturą bezpieczeństwa, typologią bezpieczeństwa oraz epistemologią studiów nad bezpieczeństwem. Autor wyjaśnił, jaka jest równica między studiami strategicznymi a bezpieczeństwem narodowym, stwierdzając, że studia strategiczne związane są z amerykańskim podejściem do kwestii militarnych okresu zimnej wojny, bezpieczeństwo narodowe natomiast obejmuje zagrożenia niemilitarne, odnoszące się do – jak to ujął autor – aktorów niepaństwowych. Przedstawił możliwe typologie bezpieczeństwa, wymieniając kryteria podmiotowe, przedmiotowe, zakresu, przestrzenne oraz sposobu organizacji. W epistemologii słowa „bezpieczeństwo” wyróżnił natomiast trzy podejścia: obiektywne, subiektywne i dyskursywne.

Drugi rozdział nosi tytuł *Bezpieczeństwo militarne* i dotyczy kilku kwestii – przyczyn wojen, broni nuklearnej i odstraszenia, rozróżniania broni ofensywnej od defensywnej, bezpieczeństwa prywatnego, różnic między wojnami „starego” i „nowego” typu, sojuszy militarnych oraz Wspólnej Polityki Bezpieczeństwa i Obrony UE. Autor wymienił m.in. monoprzyczynowe teorie woj-



ny, odwołując się do publikacji Secerova, Morgenthau'a, Klingberga, McClellanda, Ardreya, Lorentza, White'a, Fornary'ego, Chource'a czy Gilpina. Opisał wzrastającą rolę sektora prywatnego dla bezpieczeństwa, a szczególnie PMCs – prywatnych przedsiębiorstw zajmujących się świadczeniem usług związanych z bezpieczeństwem. Wśród sojuszy militarnych najwięcej uwagi poświęcił WPBiO UE, opracowując m.in. dysproporcję w wydatkach na obronę poszczególnych państw.

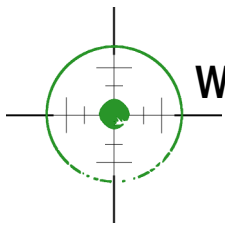
W trzeciej części publikacji, zatytułowanej *Rozszerzenie bezpieczeństwa* autor przybliżył tezy pracy Barry'ego Buzana *People, State and Fear. An Agenda for International Security Studies in the Post-Cold War Era*, tzn. wyróżnia pięć sektorów bezpieczeństwa: militarny, polityczny, społeczny, ekonomiczny i ekologiczny. Opisuąc bezpieczeństwo polityczne, Czaputowicz przybliżył czytelnikowi problematykę państw upadłych, terroryzmu, proliferacji broni masowego rażenia oraz przestępczości zorganizowanej. Przechodząc do bezpieczeństwa społecznego skupił się na tożsamości i migracji, odwołując się do publikacji Ole Waevera, Jefa Huysmansa czy Artura Gruszcza (*Bezpieczeństwo wewnętrzne w Unii Europejskiej*). W bezpieczeństwie ekonomicznym wskazał na bezpieczeństwo żywnościowe, bezpieczeństwo energetyczne oraz metody przeciwdziałania im. W opisie bezpieczeństwa ekologicznego, skupił się natomiast na interpretacji tego rodzaju bezpieczeństwa oraz kwestiach przeciwności bezpieczeństwa i środowiska.

W kolejnych rozdziałach mamy do czynienia z prezentacją poszczególnych koncepcji bezpieczeństwa międzynarodowego. W rozdziale czwartym autor scharakteryzował realizm – zdefiniował pojęcie potęgi, równowagi sił oraz dylematu bezpieczeństwa, a także przedstawił różnice między realizmem klasycznym a realizmem strukturalnym oraz realizmem ofensywnym i defensywnym, przywołując dzieła Hansa Morgenthau'a, Kennetha Waltza, Johna Mearsheimera, czy Christophera Layne'a. Kończąc rozdział, odwołał się do

WPBiO, prezentując jej realistyczne wytłumaczenie. Stwierdził, iż słabością realizmu jest niemożność wyjaśnienia, dlaczego państwa europejskie zdecydowały się na integrację w dziedzinie bezpieczeństwa i obrony wtedy, gdy ich bezpieczeństwo nie było zagrożone i korzystały z „parasola” NATO.

W rozdziale piątym autor skupił się na liberalizmie. Przedstawił najważniejsze założenia i postulaty liberałów, takie jak np.: współzależność, demokratyczny pokój i bezpieczeństwo zbiorowe. W liberalnej nauce o bezpieczeństwie wyróżnił trzy nurty: liberalizm handlowy, społeczny i instytucjonalny. Opisał różnice między *hard power* a *soft power* i odmienne podejście do tych zagadnień przez realistów i liberałów. W części dotyczącej demokratycznego pokoju odwołał się do Michaela W. Doyle'a, który stwierdził, że liberalne demokracje nie prowadziły wojen z innymi liberalnymi demokracjami. Przedstawił, czym jest „wieczny pokój” Immanuela Kanta oraz Organizacja Bezpieczeństwa i Współpracy w Europie. Podobnie jak w poprzednim rozdziale, scharakteryzował WPBiO, tym razem jednak pod kątem teorii liberalnych – liberalnego podejścia międzyrządowego, funkcjonalizmu i instytucjonalizmu.


W rozdziale szóstym autor opisał konstruktywizm. W przeciwieństwie do liberałów i realistów, zwolennicy konstruktywizmu nie zaliczają się do tradycyjnego nurtu studiów nad bezpieczeństwem. Ich zdaniem bezpieczeństwo jest warunkowane nie tylko przez rozkład zdolności militarnych, lecz także przez dominującą w systemie kulturę. Czaputowicz nawiązał w tym miejscu do kultury strategicznej – bardzo istotnej kwestii w naukach o bezpieczeństwie i naukach strategicznych. Odwołał się do badań prowadzonych przez Jacka Snydera, Elizabeth Kier, Thomasa U. Bergera czy Kerry Longhurst. Jak zaznaczył, konstruktywiści przekonują, że kulturę strategiczną definiuje system wspólnych znaczeń, który wpływa na postrzeganie, komunikację i działanie państw w sferze bezpieczeństwa. Rozdział kończy się spojrzeniem na Wspólną Politykę Bezpieczeństwa i Obrony z punktu widzenia konstruktywizmu.



Zdaniem konstruktywistów, WPBiO zmienia tożsamość i interesy państw w niej uczestniczących. Powstaje europejska kultura bezpieczeństwa, której cechą jest delegitymizacja polityki siły i desekurytyzacja życia politycznego i społecznego.

Rozdział siódmy – *Krytyczne studia nad bezpieczeństwem*, dotyczy nietradycyjnych teorii bezpieczeństwa, jakie pojawiły się w debatach uniwersyteckich w połowie lat 90. XX wieku. Zdaniem autora, zaliczają się do nich: szkoła kopenhaska, szkoła walijska, szkoła paryska, poststrukturalistyczne studia nad bezpieczeństwem, postkolonializm i feministyczne podejście do bezpieczeństwa. Słowo „krytyczność” wyraża niemożność oddzielenia podmiotu badającego od przedmiotu badania i spojrzenia na bezpieczeństwo spoza istniejących struktur. Badacz nie dąży do odkrycia uniwersalnej prawdy, lecz do lepszego zrozumienia dominujących postaw i zachowań w celu ich naprawienia. Badacze krytyczni koncentrują się w dziedzinie bezpieczeństwa na analizie państwa i polityki, badaniu wojska, policji, europejskiej biurokracji, prywatyzacji bezpieczeństwa, działaniach antyterrorystycznych, migracji i polityce azylowej.

W zakończeniu autor stwierdził, że studia nad bezpieczeństwem są dynamicznie rozwijającą się dziedziną nauki, a bezpieczeństwo zapewniane jest na wszystkich poziomach. W sektorze militarnym przedmiotem referencyjnym jest państwo, w sektorze politycznym chroniona jest suwerenność wewnętrzna państwa, stabilność polityczna i porządek społeczny. Przedmiotem referencyjnym bezpieczeństwa społecznego jest zaś tożsamość, kultura i język wspólnoty, bezpieczeństwa ekonomicznego rynki, finanse i zasoby, ekologicznego natomiast środowisko naturalne, biosfera i gatunki. Zmienia się także zainteresowanie bezpieczeństwem. O ile realizm był dotychczas dominującą koncepcją w nauce amerykańskiej, w ostatnim czasie spotyka się coraz więcej badań prowadzonych w ramach innych paradygmatów.

Publikacja Jacka Czaputowicza bez wątpienia ułatwia czytelnikowi zapoznanie się z poglądami głównych współczesnych myślicieli zajmujących się bezpieczeństwem i stosunkami międzynarodowymi. Ze względu na fakt, iż większość esejów i artykułów traktujących o tej tematyce napisana jest w języku angielskim, *Bezpieczeństwo międzynarodowe* może być idealnym wprowadzeniem do problematyki dla czytelnika polskojęzycznego. Książka ta jest kolejną pozycją autora, którego zainteresowania koncentrują się wokół stosunków międzynarodowych, bezpieczeństwa i Unii Europejskiej. Połączenie tych elementów, jak widać na powyższym przykładzie, umożliwia opracowanie i wydanie wartościowej, pomocnej w procesie dydaktycznym zarówno dla studentów, jak również nauczycieli akademickich publikacji. 

**Tomasz Wójtowicz**



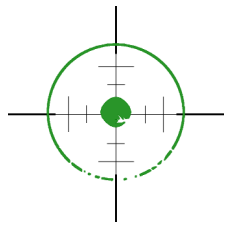
**Bezpieczeństwo międzynarodowe.**

**Współczesne koncepcje**

Czaputowicz Jacek

Warszawa 2012

ss. 260.



## Elita szpiegów - Guido Knopp (seria Kulisy Wywiadu i Kontrwywiadu)

Książka składa się z sześciu rozdziałów. W każdym z rozdziałów przedstawione są struktury wywiadowcze poszczególnych krajów. Na końcu pomocny słownik rozwijający skróty. Opowiada historię sześciu szpiegów. To mężczyźni różnego pokroju. Łączy ich jedno: każdy zdradził swoją ojczyznę. Pozostawili po sobie niezagojone rany. Zostali potępieni, muszą pamiętać o ludziach, których wydali na śmierć. Zapewne tłumią w sobie wspomnienia z przeszłości, lecz nie mogą się ich pozbyć. Ich tajemnica to żal, smutek i wyrzuty sumienia. Postaram się przybliżyć czytelnikom krótki opis poszczególnych rozdziałów.

W rozdziale *Podwójny Agent* poznamy historię Olega Anatoljewicza Gordijewskiego, niedoszłego rezydenta KGB w Londynie odwołanego do Moskwy. Udało mu się zbiec prawdopodobnie przez Finlandię do Wielkiej Brytanii.



Oleg Gordievsky (z prawej) i Ronald Reagan  
Fot. CIA, commons.wikimedia.org

Przez 11 lat współpracował z wywiadem brytyjskim. Przyczynił się do wydania wielu agentów współpracujących z KGB. Należeli do nich Norweżka Gunvor Haarvik i norweg Arne Treholt. Z rozdziału tego dowiemy się co sądzi o Gordijewskim nieżyjący już dzisiaj Władimir Aleksandrowicz Kriuczukow (szef I Zarządu Głównego KGB w latach 1974-1988, a w etapie końcowym przewodniczący KGB). W rozdziale struktura KGB i struktura I Zarządu Głównego KGB (wywiad zagraniczny).

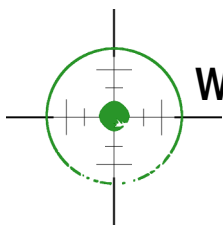
*Szpieg atomowy* - na początku tego rozdziału poznamy tajemnicze przedsięwzięcie *Manhattan Project*. Dowiemy się o zdradzie Klausa Fuchsa (na zdj.), który sprzedał Moskwie tajemnice budowy bomby jądrowej.



Klaus Fuchs, Fot. Department of Justice  
USA, commons.wikimedia.org

W efekcie ujawnienia szpiegowskiej działalności Fuchsa doprowadziło to do zatrzymania Juliusa i Ethel Rosenbergów i skazania ich na śmierć, tzw. „polowania na czarownice” w USA, przystąpienia USA do wojny koreańskiej. Klaus Fuchs to komuniści nie akceptujący granic państwowych - widział i dostrzegał tylko bariery między klasami społecznymi. Poznamy życie słynnych fizyków jak Max Born, Enrico Fermi, Robert Oppenheimer, Leo Szilard, którzy prowadzili badania w tajnej bazie Los Alamos oraz motywy „zdrady stulecia” którymi kierował się wybitny naukowiec. Według prawa angielskiego nie zdradził tajemnicy wrogowi tylko sprzymierzeńcowi, za co nie został skazany na karę śmierci.

*Kret* - mający obecnie 91 lat George Blake przez siedemnaście lat pracował dla MI 6. Przez dziesięć lat służył dla KGB jako podwójny agent. Dzięki jego pomocy zidentyfikowano we wschodniej Europie ponad czterystu zachodnich szpiegów. Był



najskuteczniejszym podwójnym agentem zimnej wojny. Dostarczył min. informacji o tunelu podsłuchowym w Berlinie. Poznamy kulisy operacji „Gold” oraz spektakularną akcję ucieczki G. Blake’a z więzienia. W rozdziale struktura MI 5 w latach pięćdziesiątych.

**Referent** to tytuł rozdziału poświęcony agentowi NRD na usługach STASI Günterowi Guillaume. Wysyłając go w sekretną misję nawet jego przełożony Markus Wolf (szef wschodnioniemieckiego wywiadu HVA) nie podejrzewał, że zajdzie tak wysoko i zostanie współpracownikiem kanclerza RFN Willy’ego Brandta. W 1972 roku zostaje jego osobistym sekretarzem. Wydział IV/A1 odpowiedzialny za opracowanie i ocenę danych przechwycił w roku 1956 i 1957 radiotelegramy i to właśnie one przyczyniły się do skierowania śledztwa na właściwe tory. Guillaume stał się podejrzany i od tego momentu pętla coraz mocniej zaciskała się na jego szyi. W rozdziale struktura BND.

**Dealer** to rozdział poświęcony Johnowi Walkerowi. Ten oficer marynarki wojennej przez ponad 18 lat szpiegował dla

KGB. Przekazał dokumenty dotyczące głównie marynarki wojennej USA, które zawierały najważniejsze informacje strategiczne. Był dla KGB żyłą złota. Za informacje które dostarczył mianowano go admirałem floty ZSRR. Zdradził plany maszyn




John Anthony Walker. Fot. US Government, commons.wikimedia.org

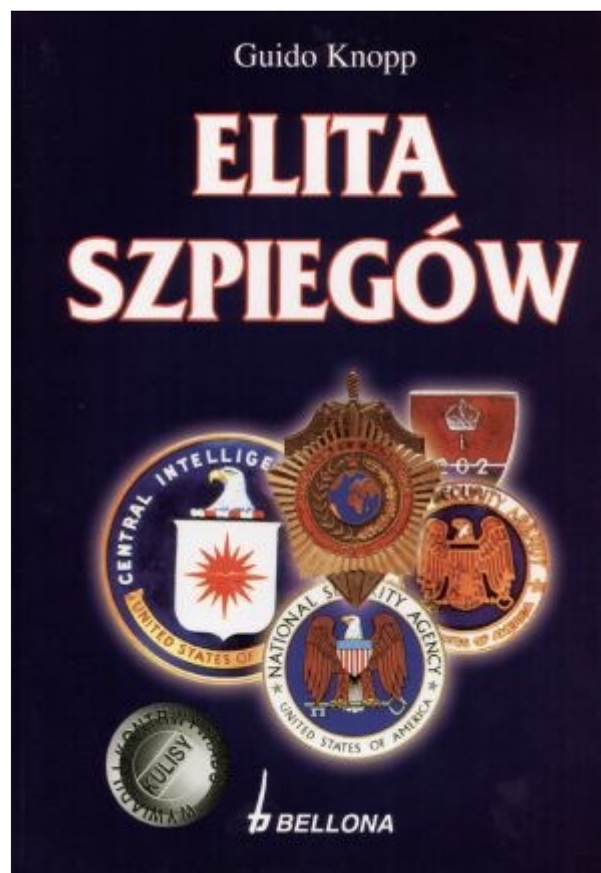
szyfrujących dzięki czemu odszyfrowano ponad milion tajnych informacji. Przez ponad 18 lat żył ponad stan

## Elita szpiegów - Guido Knopp

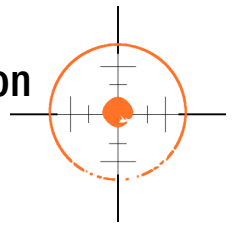
(podobnie jak Aldrich Ames) - służby odpowiedzialne za bezpieczeństwo nie zwróciły na to uwagi i pokazały w jakim są miejscu. Do swojej gry wciągnął brata, syna oraz żonę. W rozdziale struktura CIA.

**Dezertjer** to ostatni rozdział poświęcony Wernerowi Stillerowi. Dzisiaj Peter Fischer. Agent Głównego Urzędu Wywiadowczego byłego NRD (HVA) zdradza sekrety swojej organizacji dla Federalnej Służby Wywiadowczej RFN (BND) wraz ze swoją kochanką Helgą Michowską. Następnie ucieka z kraju. Objęty programem „Resettlment program” zaczął nowe życie. W rozdziale struktura HVA. 

Przemysław Bacik



Elita szpiegów,  
Guido Knopp,  
Warszawa 2004,  
ss. 216.



## Od redakcji

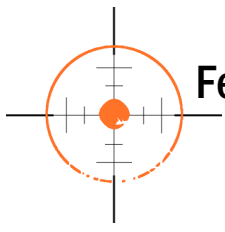
Pomysł kącika zrodził się podczas praktyk studenckich w Katedrze Bezpieczeństwa Wewnętrznego. Dwie studentki kierunku bezpieczeństwa wewnętrznego, zainteresowały się felietonami „Starszego dzielnicy”, które mają swoją historię nie tylko dlatego, że pokryte były grubą warstwą kurzu. Najpierw odkurzyły zbiór tych felietonów, a następnie utrwaliły w formie umożliwiającej ponowną ich publikację. Niekiedy sformułowały pytania, w kwestiach, które je najbardziej zainteresowały. W naszej ocenie, z uwagi na specyficzny czas, w jakim się ukazywały te felietony oraz poruszaną problematykę, poprzez fakt, że mimo upływu lat, niektóre felietony pozwalają poszerzyć wiedzę jak zwalczano przestępczość kiedyś, warto kontynuować podjętą próbę edukacji na przykładach. Materiały mogą okazać się pomocne w utrwalaniu wiedzy z zakresu szeroko rozumianego bezpieczeństwa uwzględniając dzisiejsze realia. Okoliczność, że do poruszanych kwestii, uwarunkowań prawnych i społecznych uzupełniają nie raz komentarze, do publikowania takich materiałów jeszcze bardziej przekonuje. Zatem zapraszamy do lektury, refleksji i poszukiwaniu innych źródeł informacji odnoszące się do tej problematyki. Redakcja zaprasza do współredagowania kącika, nie tylko studentów związanych z bezpieczeństwem wewnętrznym. Zapraszamy i zachęcamy także tych, którym marzy się dziennikarstwo śledcze oraz inne osoby. Poniższy felieton, jest kontynuacją cyklu felietonów poświęconych problematyce demoralizacji i przestępczości nieletnich. Pod wspólnym tytułem „Zaradne dzieci” ukaże się pięć części. Dzisiaj część piąta, która ukazała się 15 czerwca 1990 roku. Zapraszamy do lektury, a zarazem do delektowania się spostrzeżeniami, uwagami oraz opiniami, nie tylko w wymiarze historycznym. Zachęcamy do podjęcia takiej próby, życząc połamania pióra. Próba wypowiedzenia się w obrębie omawianej problematyki, może być dla niektórych studentów doskonałym treningiem, przed większym wyzwaniem, to jest pisaniem pracy dyplomowej z takiej lub zbliżonej problematyki.

## Dębica (nie) spokojna (Zaradne dzieci, cz. 5)

**Po serii włamań do sklepów podejrzenia skierowano na nieletnich. Ustalono, że w grupie wieku od dziewięciu do czternastu lat przewodzi 12-letni Januszek ps. „Wisiuła”. Znany był milicji z wcześniejszych 15 włamań i kradzieży. Sprawa trafiła do sądu dla nieletnich, który miał znaleźć środki wychowawcze i dyscyplinujące wobec chłopca.**

Nie wiadomo dlaczego, wokół tamtej sprawy zrobiła się cisza, a zdemoralizowany Januszek coraz częściej postępował niezgodnie z prawem. Milicja mająca ograniczone możliwości w stosunku do nieletnich, nie wiele mogła również działać. W zasadzie rola milicji sprowadza się do profilaktyki, ale jak można mówić o niej, gdy bardzo często chłopaka nie było w domu, a rodzice nic o nim w zasadzie nie wiedzieli. Może nie chcieli wiedzieć lub mówić. W czasie poszukiwania w domu skradzionych towarów, matka starała się ukryć, że maszynki do mięsa przyniósł syn. Twierdziła, że kupiła je w sklepie. Jak w takim wypadku sąd lub milicja może wpływać na postępowanie nieletniego?

Nie dziwi więc, że chłopak dopuścił się wraz z innymi, od połowy grudnia, ubiegłego roku do chwili zatrzymania 18 włamań. Część towarów przyniósł do domu, przekazując matce, a także obdarowując rodzeństwo. Czy matka niczego nie podejrzewała? Czy ślepcami były osoby, które kupowały od nieletnich wódkę obok „Kaprysu”? Wyjątkowa bezduszność. Czy



nikt nie wiedział, że chłopak długie godziny przebywa w salonie gier, przegrywając w ciągu trzech dni prawie 100 000 zł. Jeżeli właściciel jest obojętny (ze zrozumiałych względów) nie powinni być obojętni rodzice.

Po zatrzymaniu i przesłuchaniu, Januszek został przekazany rodzicom. Nikt poza milicją nie chciał z nim rozmawiać, a kompetencje tego organu na tym się kończyły.

W tydzień po pierwszym zatrzymaniu, nastąpiło następne. Na pytanie co robił, odpowiedział, że to co zwykle, z niecierpliwością oczekując o co funkcjonariusze będą pytać. Pytania były o stosunek rodziców do niego. Czy chodzi do szkoły, czy odwiedził go kurator itp. Bez większego skrępowania przyznał, że postępowania nie zmienił, bo w dwa dni po pierwszym przesłuchaniu, dokonali włamania, kradnąc głównie słodycze.

W następnym dniu, a właściwie w nocy kolejne włamanie w nieco zmienionym składzie. Skradli słodycze, soczki dla niemowląt, trochę bilonu, po czym rozeszli się do domów. On sam ponownie wrócił do miejsca przestępstwa, tym razem z plecakiem, do którego włożył więcej towaru. Zaniósł go do domu, część rozdał rodzeństwu, część sam zjadł.

Wieczorem następnego dnia odwiedził go kolega. Postanowili okraść kiosk z papierosami. Odstąpili jednak od tego ze względu na duży ruch. Grupa podzieliła się. Część poszła „zrobić” restaurację, a on wraz z innymi na dyskotekę. Po drodze wybili szybę w kiosku, do którego weszli po dyskotece. Z tego włamania przyniósł kosmetyki, które podarował siostrze.

## Dębica (nie) spokojna...

Tej samej nocy, z kolegą, którego spotkał na dyskotece włamał się do restauracji. O starszym koledze wie tyle, że w przeszłości dokonał kilku rozbojów i kradzieży, często widzi go na dyskotece oraz wie, że nie uczy się, podobnie, jak on. Z tego włamania przyniósł wino i wódkę. Na drugi dzień butelkę pożyczył wczorajszym współnikom, a po południu, gdy sam chciał się napić stwierdził, że najprawdopodobniej został przez nich okradziony.

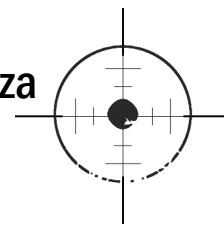
Co można dodać do tego wszystkiego? Chyba tylko tyle, że chłopiec ze łzami w oczach prosił o umieszczenie w Pogotowiu Opiekun-czym! Po dramatycznej prośbie i interwencji milicji sąd wydał tymczasowe zarządzenie w sprawie Januszka. Chłopiec był z tego zadowolony, przynajmniej część problemów rozwiązał sobie sam. Jakie nasuwają się wnioski? Co z pozostałymi z tej grupy? Pytania jak na razie pozostają bez odpowiedzi. O dalszych losach zadecydują rodzice i sąd, do którego niebawem trafi sprawca.

Gdy rozmawiałem z Januszkiem i pytałem, co będzie dalej, odpowiedział, jak w tytule: „Dębica spokojna”. Kiedy zagadnąłem, czy przypadkiem nie chce zostać „młodym Najmrodzkiem” - uśmiechnąłem się, zaprzeczał, kręcąc głową. Jest więc nadzieja na poprawę.

Dębica będzie spokojna pod warunkiem sprawnego działania nie tylko policji. Rodzice, sąd i sami mieszkańcy muszą mieć również w tym udział. 🚔

**Starszy Dzielnicowy**





## 1 sierpień

- 2000** – **Indie:** Podejrzani bojownicy islamscy w Kaszmirze zabijają 102 indyjskich pielgrzymów w drodze do sanktuarium, dziesiątki rannych.

## 2 sierpień

- 2003** – **Irak:** samochód pułapka eksploduje przed ambasadą Jordanii w Bagdadzie zabijając 19 i raniąc 50 osób.

## 3 sierpień

- 2001** – **Wielka Brytania:** Eksplozja samochodu pułapki blisko dworca kolejowego w Londynie rani 6 osób, odpowiedzialna IRA.

## 4 sierpień

- 2002** – **Izrael:** Bomba w autobusie zabija 10 pasażerów i rani ponad 40- tu, za zamachem stoi HAMAS.

## 5 sierpień

- 2003** – **Indonezja:** w Dżakarcie przed hotelem Marriott eksploduje samochód pułapka zabijając 13 i raniąc 149 osób, odpowiedzialna Dżimah Islamija (JI).

## 6 sierpień

- 2009** – **Demokratyczna Republika Konga:** 100 cywilów porwanych i zamordowanych w Niangara – odpowiedzialna Armia Bożego Oporu.



Fot. D. Vignoni / Stannered, commons.wikimedia.org

## 7 sierpień

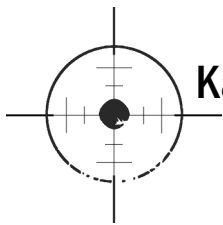
- 1998** – **Kenia, Tanzania:** zamach na amerykańskie ambasady spowodował śmierć 224 osób, 5000 zranień w Nairobi (Kenia) i 224 w Dar es Salaam (Tanzania).

## 8 sierpień

- 2008** – **Irak:** samochód pułapka eksploduje na rynku w Tall' Afar zabijając 28 i raniąc 71 osób.

## 9 sierpień

- 2008** – **Algieria:** w Zemmouri w samobójczym ataku ginie 8 osób, rannych zostaje 17, odpowiedzialna Al-Ka'ida Islamskiego Maghrebu (AQIM).



### 10 sierpień

**2006 – Wielka Brytania:** policja przeciwdziała atakowi na samoloty lecące do USA, aresztowano ponad 20 osób, odpowiedzialna odpowiedzialna Al-Ka'ida.

### 11 sierpień

**2006 – Indonezja:** ekstradycja z Pakistanu Umara Pateka ponoszącego odpowiedzialność za zamachy bombowy w Bali w październiku 2002 roku w których zginęło ponad 200 osób.

### 12 sierpień

**2001 – Izrael:** samobójczy atak bombowy w restauracji w pobliżu Hajfy zranił 20 osób; odpowiedzialność ponosi JIHAD.

### 13 sierpień

**2009 – Irak:** 21 osób zginęło podczas podwójnego samobójczego ataku na kawiarnię w Kala.

### 14 sierpień

**1994 – Sudan:** aresztowanie i ekstradycja do Paryża Ilicha Ramíreza Sáncheza, pseudonim Carlos odpowiedzialnego za wiele ataków terrorystycznych na terenie Europy.

### 15 sierpień

**2001– Indie:** w Handwarze atak bombowy zranił 18 osób, odpowiedzialna Lashkar-e-Toiba.

### 16 sierpień

**2002 – Irak:** Abu Nidal, mózg operacji z 1985 roku na lotniska Wiednia i Rzymu ginie w tajemniczych okolicznościach w Bagdadzie.

### 17 sierpień

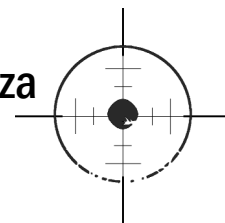
**2010 – Irak:** W Bagdadzie zamachowiec-samobójca zabił 57 cywilów i ranił 118 innych w dodatku zabijając i raniąc wielu rekrutów, odpowiedzialna organizacja Islamskie Państwo w Iraku i Levancie.

### 18 sierpień

**2011 – Izrael:** w trzech atakach w Eliacie terroryści zabili sześć i zranili 25 osób.

### 19 sierpień

**2003 – Izrael:** zamachowiec-samobójca detonuje bomby na pokładzie autobusu w Jerozolimie, zabijając 20, w tym pięciu obywateli USA i raniąc 140, odpowiedzialny HAMAS.



## 20 sierpień

**2008** – **Algieria:** dwa zsynchronizowane ataki samochodów pułapek zabiły 11 osób w Bouira, podejrzana Al-Ka'ida.

## 21 sierpień

**1995** – **Izrael:** ataki bombowe zabijają pięć i ranią ponad 100 osób w zamachu bombowym na autobus w Jerozolimie, odpowiedzialność ponosi HAMAS.

## 22 sierpień

**2007** – **Irak:** w Bayji samochód pułapka zabija 25 policjantów i 20 cywili.

## 23 sierpień

**2001** – **Kolumbia:** samochód pułapka na zewnątrz komisariatu policji w Marintilla zabija jedna i rani 25 osób, odpowiedzialna Armia Wyzwolenia Narodowego.

## 24 sierpień

**2010** – **Somalia:** dwa samobójcze ataki na hotel Nuna w Mogadiszu powodują śmierć 33 osób (ginie 4 członków parlamentu), odpowiedzialność Asz-Szabab.

## 25 sierpień

**2009** – **Afganistan:** Ginie blisko 40 osób a 60 zostaje rannych w zamachu bombowym samochodu pułapki w Kandaharze.

## 26 sierpień

**2011** – **Nigeria:** wybuch samochodu pułapki w Kwaterze Głównej ONZ w Abuji zabija 23 osoby i rani ponad 80, odpowiedzialna Boko Haram.

## 27 sierpień

**2006** – **Irak:** wybuch dwóch bomb samochodowych i ataki granatników przeciwpancernych zabijają w Diyala, Bagdadzie i Kirku 50 osób.

## 28 sierpień

**1999** – **Jemen:** bomba samochodowa zabija 6 i rani 12 osób, odpowiedzialna Islamska Armia Aden-Abyan.

## 29 sierpień

**1995** – **Gruzja:** Prezydent Eduard Szewardnadze zraniony podczas ataku bombowego.

## 30 sierpień

**2001** – **Sri Lanka:** bomba na zewnątrz budynku komunalnego w Kalunai zabiła 3 i zraniła 7 osób, odpowiedzialność ponoszą Tamiłskie Tygrysy.

## 31 sierpień

**2004** – **Izrael:** dwa zamachy na autobusy w Beer Szewa spowodowały śmierć 16 osób, odpowiedzialny HAMAS.



„Publishing School” funkcjonuje już 15 lat (od maja 1998 roku). Jest formalnie szkołą policealną ponieważ minimalny poziom wykształcenia aplikujących kandydatów to średnie, ale maksymalnym jest doktorat z różnorodnych dziedzin. Ze względu na wyspecjalizowanie się w nauczaniu dorosłych, którzy pracują, przygotowują się do pierwszej pracy lub ją zmieniają, zajęcia odbywają się w trybie zaocznym.

Główny nacisk szkoła kładzie na kształcenie umiejętnościowe i praktyczne. Wykładowcami są praktycy z poszczególnych obszarów grafiki, mediów i reklamy. Patronat nad szkołą sprawuje Apple ATC SAD z Warszawy.

Szkoła współpracuje z Akademią Sztuk Pięknych w Krakowie, Wojewódzkim Urzędem Pracy w Krakowie, wieloma firmami branży, z absolwentami prowadzącymi własne wydawnictwa, drukarnie, firmy graficzne i reklamowe.

Motto szkoły: **Uczymy nowoczesnych zawodów, które umożliwiają pracę!**

„Publishing School“ stara się maksymalnie wzbogacić i ukierunkować wiedzę Słuchaczy, wyzwalać ich kreatywność, poszerzać zainteresowania i umiejętności praktyczne zgodnie z aktualnymi wymaganiami rynku pracy w obszarze ze mediów 2D i 3D, poligrafii oraz reklamy.

Szkoła prowadzi pięć specjalistycznych kierunków w ramach ujętego w Klasyfikacji Zawodów i Specjalności zawodu grafik komputerowy. Są to:

- kierunek poligraficzny (ze specjalnością poligraf operator DTP)
- kierunek multimedialny (ze specjalnością grafik stron www i prezentacji multimedialnych)
- kierunek reklamowy (ze specjalnością kreowanie kampanii reklamowych)
- kierunek animacja (ze specjalnością animacja komputerowa)
- kierunek grafika 3D (ze specjalnością grafika 3D i wizualizacje)

**Policealna Szkoła Poligraficzna Multimedialna  
i Projektowania Reklam „Publishing School”  
ul. Grzegórzecka 79, 31-559 Kraków**

[www.publishingschool.pl](http://www.publishingschool.pl)

[www.facebook.com/publishingschoolpl](https://www.facebook.com/publishingschoolpl)



**WYŻSZA SZKOŁA  
INFORMATYKI I ZARZĄDZANIA**  
z siedzibą w Rzeszowie

Policjanci  
Strażacy  
Urzędnicy  
Żandarmi  
Żołnierze

Pragniesz awansów? Rozwoju?  
Kariery? Wyższej pensji? Pewnej pracy?


# Podejmij studia

na kierunku Bezpieczeństwo Wewnętrzne  
w Wyższej Szkole Informatyki i Zarządzania

Bezpieczeństwo wewnętrzne to wszechstronny kierunek. Polecany przedstawicielom służb mundurowych ale i także przyszłym ekspertom w zakresie: **bezpieczeństwa systemów i sieci informatycznych, cywilnego zarządzania zagrożeniami i sytuacjami kryzysowymi** oraz **zapewnienia bezpieczeństwa podmiotów gospodarczych.**

[www.wsiz.rzeszow.pl](http://www.wsiz.rzeszow.pl)

Dział Rekrutacji WSliZ, pok. RA 8, ul. Sucharskiego 2  
35-225 Rzeszów, tel 17 866 11 88, 17 866 11 99  
rekrutacja@wsiz.rzeszow.pl



Zapraszamy  
na stronę  
internetową:

[www.e-terroryzm.pl](http://www.e-terroryzm.pl)

Zobacz także  
archiwalne  
numery

Internetowy Biuletyn  
e-Terroryzm.pl  
wydawany jest  
od stycznia 2012 r.

Czasopismo tworzą studenci  
Wyższej Szkoły Informatyki  
i Zarządzania w Rzeszowie,  
pracownicy Instytutu Studiów  
nad Terroryzmem  
i zaprzyjaźnieni entuzjaści  
poruszanej problematyki