Nasze zdanie o Raporcie z likwidacji WSI – część VIII

UZASADNIENIE DO STAWIANYCH TEZ – CIĄG DALSZY

Analiza „Raportu" pozwala wskazać kolejne nieprawdziwe informacje dotyczące kryptografii zamieszczone na stronach 145-146 w wersji elektronicznej (na stronach 147-149 w „Monitorze Polski") – niebieską kursywą – nasze wyjaśnienia i komentarz.

Analizując działania zmierzające do zakupu specjalistycznego sprzętu od z góry ustalonych firm warto przywołać zachowania zmierzające nie tylko do obejścia prawa, ale w szczególności ewentualne próby wpłynięcia na kształt przepisów ustawy. *Należy wyjaśnić, że jeśli chodzi o zakupy, to WSI realizowały jedynie zakupy na potrzeby własne – niezbędne do realizacji zadań, zaś za zakupy dla SZ RP byli odpowiedzialni gestorzy (wyznaczone przez ministra ON komórki) oraz Departament Zaopatrzenia SZ MON. W przypadku sprzętu teleinformatycznego i ochrony kryptograficznej gestorem była komórka P6 Sztabu Generalnego WP. Rolą WSI była ochrona kontrwywiadowcza zakupów oraz nadzór nad przestrzeganiem bezpieczeństwa teleinformatycznego, z tytułu realizacji zadań służby ochrony państwa (SOP) sfery wojskowej, którą były WSI z mocy ustawy o ochronie informacji niejawnych. Ponieważ za realizację zakupów w MON nie odpowiadały WSI, a jedynie gestorzy, dlatego WSI nie musiały obchodzić prawa, gdyż nie ponosiły odpowiedzialności za stan wyposażenia SZ RP w sprzęt. Natomiast, w związku z wypełnianiem funkcji SOP, WSI wraz z ABW były odpowiedzialne za ocenę projektów ustaw i rozporządzeń w obszarze ochrony informacji niejawnych i bezpieczeństwa teleinformatycznego, a tym samym jako komórki specjalistyczne w tym obszarze miały wpływ na kształt tych dokumentów, które ostatecznie uchwalał Sejm RP.*

Pierwsze starania zmierzające do zakupu sprzętu kryptograficznego firmy SILTEC podjęto już w roku 2001. ***Brak jakiegokolwiek przykładu i opisu nieprawidłowości, które miały miejsce w latach 2001 – 2004. Wszystkie poruszone w Raporcie sprawy dotyczą jedynie 2005 roku.*** Obowiązujące wówczas przepisy uniemożliwiały zakup i dopuszczenie do użytku urządzeń, które nie przeszłyby stosownej certyfikacji. *Zdanie ma charakter manipulacji informacją. Mówiąc o zakupach należy pamiętać, że zakupy mogły i mogą być dokonywane przez MON w celu realizacji zadań sojuszniczych (NATO lub UE) i narodowych, a wówczas nie jest bez różnicy o jakim prawie mówimy – sojuszniczym, czy narodowym. Autorzy Raportu nie precyzują obszaru swoich zainteresowań, tym samym fałszują istniejący obraz problemu kryptografii w MON (narodowej i sojuszniczej). Obowiązujące przepisy w Polsce (narodowe), ustawa o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz. U. 1999 Nr 11 poz. 95 z późn. zm.), umożliwiały stosowanie w narodowych systemach i sieciach teleinformatycznych urządzeń kryptograficznych do klauzuli „zastrzeżone" bez badań i certyfikatu SOP (zarówno rodzimej produkcji, jak i innych państw). Obowiązek posiadania stosownego certyfikatu SOP dotyczył jedynie urządzeń do ochrony niejawnych informacji narodowych o klauzuli „poufne" i wyższej. W niejawnych systemach NATO (też UE) zainstalowanych w Polsce i przetwarzających informacje niejawne NATO (UE) nie obowiązują wymogi polskiej ustawy, gdyż stosowanie urządzeń kryptograficznych do ochrony niejawnych informacji NATO (UE) w niejawnych systemach teleinformatycznych NATO i państw członków NATO określają dyrektywy NATO (UE). Przepisy te dotyczą również przetwarzania informacji niejawnych NATO (UE) w polskich narodowych systemach teleinformatycznych. Przepisy NATO (UE) określają również zasady i odpowiedzialność za certyfikację urządzeń kryptograficznych służących do ochrony niejawnych informacji NATO (UE) i polska ustawa nie reguluje tych obszarów. Ponadto należy przypomnieć, że obowiązek certyfikacji przez SOP narodowych urządzeń kryptograficznych stosowanych w narodowych systemach i sieciach teleinformatycznych oznaczonych klauzulą „poufne" został wprowadzony w dniu 3 lutego 2001 r. (Dz. U 2001 Nr 22 poz. 247) – art. 60 ust. 2a. Wcześniej obowiązek ten istniał tylko dla tajemnicy państwowej („ściśle tajne" i „tajne"). Ustawa z 2010 r. wprowadziła obowiązek certyfikowania przez ABW albo SKW wszystkich urządzeń kryptograficznych stosowanych w systemach teleinformatycznych do ochrony narodowych informacji niejawnych wszystkich klauzul.* W roku 2005 doszło do nowelizacji przepisów ustawy o ochronie informacji niejawnych. *Była to przynajmniej trzynasta nowelizacja ustawy o ochronie informacji niejawnych z dnia 22 stycznia*

1999 r., która miała miejsce 15 kwietnia 2005 r. (Dz. U. 2005 Nr 85 poz. 727). Ponadto, należy podkreślić, że pomimo tych wielu nowelizacji, ustawa o ochronie informacji niejawnych nadal pozostawiała wiele do życzenia w obszarze ochrony kryptograficznej i odbiega od prawa obowiązującego w NATO i państwach NATO oraz UE (problem ten dotyczy również ustawy z 2010 r.). Gruntownej zmianie uległy przepisy art. 60 i następnych. *Wprowadzone zmiany były istotne oraz poszły w dobrym kierunku i dotyczyły:*

- *wprowadzenia pojęcia „akredytacji bezpieczeństwa teleinformatycznego" – art. 60 ust. 1 i ust. 2,*
- *wzajemnego uznawania certyfikatów ochrony kryptograficznej wydawanych przez służbę ochrony państwa sfery cywilnej (ABW) i wojskowej (WSI) – art. 60 ust. 4,*
- *dopuszczenia przez szefa właściwej służby ochrony państwa na czas określony, nie dłuższy jednak niż na 2 lata niejawnego systemu teleinformatycznego (wszystkich klauzul) bez spełnienia niektórych wymagań bezpieczeństwa – art. 60 ust. 7,*
- *kierownicy jednostek organizacyjnych organów uprawnionych do prowadzenia czynności operacyjno-rozpoznawczych uzyskali możliwość podejmowania decyzji o eksploatacji niejawnych systemów i sieci teleinformatycznych (wszystkich klauzul) bez konieczności ich akredytacji i certyfikacji oraz bez konieczności badania i certyfikacji urządzeń i narzędzi kryptograficznych w nich stosowanych – art. 60 ust. 8,*
- *zmieniono nazwę jednego z dwóch dokumentów bezpieczeństwa – „procedury bezpieczeństwa" na „procedury bezpiecznej eksploatacji" i zrezygnowano z jego opracowywania w fazie projektowania – art. 61 ust. 2,*
- *zmieniono zasady opłat za badania, certyfikację i akredytację – art. 63.*

Dlaczego autorzy Raportu nie biją na alarm, że w działalności operacyjno-rozpoznawczej można było (i można nadal) eksploatować niejawne systemy i sieci teleinformatyczne bez akredytacji i certyfikacji oraz urządzenia kryptograficzne bez badań i certyfikatów? Przecież może się zdarzyć, że prokuratura prowadzi śledztwo w sprawie podejrzenia o ujawnienie informacji przetwarzanej w akredytowanym systemie teleinformatycznym (bezpiecznym), np. zabiera dysk użytkownikowi podejrzewanemu o ujawnienie informacji niejawnych i bada go w swoim nieakredytowanym (z mocy ustawy) systemie teleinformatycznym. Co będzie, jeśli podejrzenie to nie potwierdziło się, gdyż system był bezpieczny a użytkownik przestrzegał zasad bezpieczeństwa, ale przeciwnik „podsłuchiwał" system teleinformatyczny prokuratury, który nie był akredytowany i nie był bezpieczny? W bezpieczeństwie informacyjnym nie zostawia się furtek – przeciwnik analizuje system informacyjny i uderza w jego najsłabszy punkt! Z posiadanych informacji wynika, że WSI liczyły na to, iż zostanie uchwalony przepis w brzmieniu umożliwiającym wyrażenie przez Szefa właściwej służby zgody na używanie sprzętu kryptograficznego do klauzuli „poufne" bez przeprowadzania stosownych badań certyfikacyjnych. Jednakże taka redakcja przepisu spotkała się ze stanowczym oporem ekspertów sejmowych. Wskazywali oni m.in. na korupcjogenność powyższego zapisu. *WSI nie liczyły na taką zmianę w ustawie i nie zabiegały o taką zmianę. Autorzy Raportu nie zdają sobie chyba sprawy, że większą korupcjogenność generują bardziej restrykcyjne przepisy. Sprawa wyrażenia zgody na używanie sprzętu kryptograficznego do klauzuli „poufne" bez przeprowadzenia stosownych badań certyfikacyjnych dotyczył tylko sfery wojskowej. Propozycja ta wynikała z braku certyfikowanych narodowych wyrobów kryptograficznych dla wojska i braku możliwości certyfikowania przez WSI nowych wyrobów kryptograficznych wyprodukowanych przez polskie firmy (brak odpowiednich sił i środków w WSI). Należy podkreślić, że obowiązująca wówczas ustawa nie pozwalała stosować w wojskowych systemach i sieciach teleinformatycznych urządzeń kryptograficznych posiadających certyfikat służby ochrony państwa sfery cywilnej (ABW). Propozycja wprowadzenia czasowego dopuszczenia do eksploatacji niektórych certyfikowanych urządzeń kryptograficznych NATO i niezwłocznego rozwiązania istniejącego problemu braku narodowych urządzeń była pomysłem szefa CBT. Rozwiązanie to miało charakter czasowy na okres maksymalnie czterech lat. Stosowane w wojskowych narodowych niejawnych systemach i sieciach teleinformatycznych urządzenia kryptograficzne miały być certyfikowanymi urządzeniami pochodzącymi z wybranych państw NATO, które zostały wcześniej już zakupione przez wojsko do systemów NATO i były eksploatowane w MON w systemach NATO. Dotyczyło to jedynie takich urządzeń, które zostaną zastąpione narodowymi urządzeniami kryptograficznymi w ciągu najbliższych czterech lat. Bezpieczeństwo systemów i sieci teleinformatycznych z takimi urządzeniami musiały być*

bezwarunkowo oceniane i dopuszczane do eksploatacji przez WSI. Była to propozycja umożliwiająca niezwłoczne przystąpienie do budowania w MON nowoczesnych bezpiecznych systemów i sieci teleinformatycznych oraz dająca czas na rozwój laboratoriów badawczych WSI i wyprodukowanie narodowych urządzeń kryptograficznych przez polskie firmy i przeprowadzenie ich certyfikacji przez WSI. Prace w tym kierunku trwały od 26 marca 2004 r. kiedy problem ten stanął na Kolegium dowódców SZ RP. W dniu 9 listopada 2004 r. minister ON Jerzy Szmajdziński zatwierdził „Koncepcję certyfikacji wyrobów służących do ochrony informacji niejawnych przeznaczonych na cele obronności i bezpieczeństwa państwa", przygotowaną przez WSI co dało realną podstawę do wyjścia z istniejącej zapaści w obszarze narodowej ochrony kryptograficznej. Koncepcja mówiła o zwiększeniu etatu CBT o 56 etatów oficerskich (specjalności: kryptografia, informatyka i elektronika), przeznaczonych na badania i certyfikację urządzeń kryptograficznych oraz certyfikację i akredytację systemów teleinformatycznych. Koncepcja miała zostać wdrożona w ciągu 3 lat, tj. do końca 2007 roku i tym samym miały skończyć się problemy w SZ RP w obszarze narodowej kryptografii. Etaty zostały przydzielone w roku 2004, zaś w czerwcu 2006 r. zakończono przyjmowanie młodych oficerów na przydzielone etaty, głównie absolwentów WAT wymienionych specjalności. Proces kształcenia specjalistycznych kadr w latach 2005-2006, jak również w kolejnych latach, został pisemnie uzgodniony z kierownictwem dydaktycznym WAT oraz wydziałów Cybernetyki i Elektroniki w grudniu 2004 r. Do końca 2007 roku został czas na szkolenie „młodych" oficerów przez „doświadczonych" i wdrażanie procedur badawczych i certyfikacji. Paradoksem w całej sprawie, jest fakt, że o istniejących kłopotach w obszarze kryptografii meldował w lutym 2004 r. przyjmującemu obowiązki nowemu szefowi CBT (wówczas CAKiBT) płk. Krzysztofowi Polkowskiemu, główny autor notatki płk Jerzy M., szef oddziału w CBT i to on przygotowywał koncepcję oraz był jej realizatorem – jako szef oddziału otrzymał 40 etatów, typował ludzi, a następnie podpowiadał przyszłemu swojemu przełożonemu w SKW dr. Jerzemu U., kogo z nowoprzyjętych oficerów zatrudnić w BBT SKW. Likwidacja z dniem 30 września 2006 r. WSI przerwała ambitną realizację zatwierdzonej koncepcji – a na pewno zmiotła wszystkich jej ojców, z wyjątkiem autorów notatki, zaś większości przyjętym w latach 2005 i 2006 oficerom podziękowano za służbę lub stworzono takie warunki, że sami odeszli ze służby lub przeszli do innych instytucji. Stan narodowej kryptografii w MON kuleje do dnia dzisiejszego i nic nie wskazuje, że zostanie poprawiony ku uciesze naszych sojuszników, a szczególnie naszych przeciwników.

---

[277] Dyrektorem ds. wdrożeń w tej firmie jest płk rez. H.D., wieloletni oficer Zarządu II, w latach 1992-1998 Szef Oddziału Łączności i Informatyki „odpowiedzialny za szereg niejasnych i kontrowersyjnych zakupów. Został odwołany ze stanowiska w związku z podejrzeniem o korupcję, chociaż takiego zarzutu nigdy mu nie postawiono (prowadzono SOZ „A"). *W tym okresie w WSI były dwa oddziały: Oddział Łączności i Oddział Informatyki, którymi kierowali dwaj różni szefowie – Odziałem Łączności kierował płk H. D. a Oddziałem Informatyki w latach 1990-95 kierował płk Krzysztof Polkowski.* W firmie pracuje wielu oficerów Zarządu II, którzy podobnie jak H.D. rozpoczynali służbę w 2 pułku rozpoznania radioelektronicznego w Przasnyszu (Zarząd II Sztabu Generalnego)." W sprawie SILTEC postępowanie prowadzi również Żandarmeria Wojskowa. Informacja dot. zaangażowania byłych i czynnych oficerów i pracowników WSI w pracę na rzecz przedsiębiorstw realizujących usługi dla resortu ON, SO „T", k. 123-128 *Jest to fakt – w czasie opracowywania Raportu było prowadzone przez ŻW śledztwo o sygn. akt K. Śl. 19/05. Do prowadzonego przez ŻW zostało dołączone przesłane przez Przewodniczącego Komisji Weryfikacyjnej zawiadomienie nr KTKW/00-28/07 z dnia 12.02.2007 r. o podejrzeniu popełnienia przestępstwa w sprawach dotyczących kryptografii, opisanych w Raporcie. W konsekwencji prowadzenie śledztwa zostało przekazane do Wojskowej Prokuratury Okręgowej w Warszawie i było prowadzone pod sygn. akt Po.Śl. 84/05. W dniu 4 czerwca 2009 r. prokuratura wydała postanowienie o umorzeniu śledztwa, które uprawomocniło się w dniu 16 czerwca 2009 r.*

[278] Jak wynika z notatki WS „GUSTAW" (Teczka „Z" t. VII), w 2002 r. przetarg na komputery klasy TEMPEST dla Marynarki Wojennej wygrała firma DGT-System. Po ogłoszeniu tej decyzji, przedstawiciel firmy SILTEC Tadeusz Orłowski stosując szantaż wobec jednego z właścicieli DGT-System -Marka Antosza -nakazał mu wycofanie się z wygranego przetargu. Podstawą takiego żądania miała być nieformalna umowa między dwoma firmami o podziale rynku kontraktów na zakup komputerów. W efekcie tych działań DGT-System zmuszona została do złożenia protestu formalnego na wygrany przez siebie przetarg.

[279] Z Generalnego Zarządu Dowodzenia i Łączności SG WP z przedstawicielami firmy SILTEC utrzymywali także kontakt gen. bryg. Wojciech Kubiak, gen. Stanisław Krysiński oraz płk Aleksander Kuber.

Ostatecznie uchwalony został przepis, który pozwalał na dopuszczenie omawianego sprzętu do użytku warunkowo, na okres 2 lat. Przedstawiciele służb zapewniali, że takie rozwiązanie może być stosowane jedynie wyjątkowo, np. w wypadku braku odpowiednich urządzeń, w warunkach polowych, w trakcie misji zagranicznych. *Jest to argument przeczący tezie autorów o sprzeciwie ekspertów sejmowych co do takiego rozwiązania. Należy podkreślić, że WSI nie zgłaszało propozycji czasowego dopuszczenia do eksploatacji urządzeń kryptograficznych NATO jako zmian do ustawy. Uchwalony przez Sejm RP przepis (art. 60 ust. 7) dotyczył wszystkich niejawnych systemów teleinformatycznych (od klauzuli „zastrzeżone" do „ściśle tajne") i poszedł znacznie dalej niż propozycja WSI czasowego i ograniczonego stosowania urządzeń kryptograficznych NATO. Propozycja szefa CBT była bardziej restrykcyjna od rozwiązania przyjętego w ustawie przez ekspertów sejmowych, gdyż mówiła o stosowaniu jedynie natowskich certyfikowanych urządzeń kryptograficznych w systemach i sieciach teleinformatycznych do klauzuli „poufne". Ponadto należy podkreślić, że w wyjątkowych sytuacjach przepisy NATO oraz niektórych państw członków NATO dają możliwość stosowania urządzeń kryptograficznych bez certyfikatów w systemach teleinformatycznych a nawet w wyjątkowych sytuacjach bojowych pozwalają na przesyłanie niejawnych informacji NATO w jawnych systemach.* Powyższe zapewnienia w kontekście podejmowanych od 2001 r. zabiegów zmierzających do zakupu sprzętu kryptograficznego konkretnej firmy, o którym od początku wiadomo było, że nie spełnia i nie będzie spełniał wymagań ustawowych, mogą budzić poważne wątpliwości. *Brak w opisie na czym polegały te zabiegi od 2001 r. Natomiast należy mieć świadomość, że urządzenia kryptograficzne zgodnie z ustawą o ochronie informacji niejawnych mogły być stosowane bez posiadania certyfikatu do klauzuli „zastrzeżone". Ponadto, mowa jest o urządzeniach kryptograficznych posiadających certyfikat NATO, a zatem mogły być one zakupywane do systemów natowskich instalowanych w naszym kraju. Należy podkreślić, że za planowanie i zakup sprzętu kryptograficznego nie odpowiadało WSI, lecz P-6 SG WP i DZ MON.* Pełną świadomość naruszeń prawa, który nastąpiły po uchwaleniu nowelizacji ustawy, musiał mieć gen. Dukaczewski, który sporządził notatkę dotyczącą interpretacji zapisu art. 60 pkt. 7 opisywanej ustawy. *Jest to kolejna manipulacja faktami. W myśl cytowanego zapisu, po 15 kwietnia 2005 r. szef WSI otrzymał ustawowe uprawnienie dopuszczania do eksploatacji niejawnych systemów teleinformatycznych wszystkich klauzul na okres do dwóch lat. Wspomniana notatka została sporządzona i podpisana przez szefa WSI w dniu 28 stycznia 2005 r. i nie była ona interpretacją art. 60 pkt. 7, gdyż nie było go w obowiązującej wówczas ustawie (taki zapis pojawił się w ustawie ponad 3 miesiące później). Notatka określała zasady czasowego i ograniczonego dopuszczenia do stosowania certyfikowanych urządzeń NATO tylko w wojskowych niejawnych narodowych systemach i sieciach teleinformatycznych. Należy przypomnieć, że istniał wówczas w Rozporządzeniu Prezesa RM w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych z dnia 25 lutego 1999 roku (Dz. U. Nr 18, poz. 162) § 4, który mówił, że: „Służby ochrony państwa mogą dopuścić do stosowania w systemie lub sieci teleinformatycznej, bez konieczności przeprowadzania badań, urządzenie, które spełnia wymagania bezpieczeństwa określone w rozporządzeniu, jeżeli otrzymało certyfikat właściwej krajowej władzy bezpieczeństwa w państwie będącym stroną Organizacji Traktatu Północnoatlantyckiego.", które mieszało w głowach użytkowników i wywoływało spory wśród prawników, co do jego kompatybilności z ustawą, ale nikt nie próbował przez lata unormować tego problemu.* Smutnym epilogiem opisanych, acz nie w pełni skutecznych zabiegów, było podpisanie w maju 2005 r. przez min. Jerzego Szmajdzińskiego, Szefa WSI gen. Marka Dukaczewskiego oraz Szefa Generalnego Zarządu Dowodzenia i Łączności gen. Stanisława Krysińskiego „Aneksu do Koncepcji rozwoju systemów ochrony kryptograficznej w resorcie Obrony Narodowej". W dokumencie tym zatwierdzili oni de facto plan niestosowania obowiązujących przepisów w procedurze akredytacji urządzeń kryptograficznych oferowanych przez SILTEC.[280] *Cytowany Aneks, zatwierdzony przez ministra ON w dniu 27 maja 2005 r., był kolejnym krokiem uregulowania sprawy związanej z budową w MON bezpiecznych narodowych*

niejawnych systemów teleinformatycznych z czasowym i ograniczonym wykorzystaniem urządzeń kryptograficznych certyfikowanych przez NATO w narodowych systemach teleinformatycznych MON. Należy w tym miejscu również powiedzieć, że „Aneks" precyzował opracowaną i zatwierdzoną w dniu 26 marca 2004 r. przez Ministra ON „Koncepcję rozwoju systemów ochrony kryptograficznej w resorcie obrony narodowej" w związku z nowelizacją ustawy o ochronie informacji niejawnych i zaakceptowanym przez Ministra ON rozwiązaniem zaproponowanym w notatce z 28 stycznia 2005 r. przez Szefa WSI, nie mówiąc już o wspomnianej wcześniej koncepcji certyfikacji wyrobów kryptograficznych i rozpoczętym jej wdrażaniu. Zarzuty o naruszaniu prawa przez szefa WSI i podległe mu CBT oraz podane argumenty są bezpodstawne. W latach 2004-2005 WSI zrobiły wiele w celu podniesienia poziomu bezpieczeństwa w MON, na co istnieje szereg konkretnych dowodów znajdujących się w zasobach archiwalnych MON i w świadomości ludzi. Jest to przykład całkowitej instrumentalizacji prawa w celu zabezpieczenia swoich partykularnych interesów z oczywistą szkodą dla poziomu bezpieczeństwa tajemnicy państwowej, której ochroną na mocy ustawy zajmowały się właśnie WSI. *Jest to przykład kolejnego manipulowania faktami, gdyż opisywane powyżej działania WSI dotyczyły tylko tajemnicy służbowej, a nie tajemnicy państwowej.*

Opisane, nie będące wyjątkiem, działania powodowały wymierne straty dla budżetu państwa. *Jest to argument bez żadnego dowodu i po raz kolejny jest manipulowaniem opinią publiczną.* Stanowiły również, poprzez akredytowanie urządzeń kryptograficznych bez faktycznego przeprowadzenia wymaganych badań, olbrzymie zagrożenie dla bezpieczeństwa państwa. *Autorzy Raportu chcąc krytykować innych powinni posiąść chociaż minimum wiedzy – urządzeń kryptograficznych nie akredytuje się. Natomiast mówienie o olbrzymim zagrożeniu dla bezpieczeństwa państwa jest niepoważne i świadczy, że autorzy opisujący to zagadnienie chcieli czymś błysnąć u czytelnika, nie mając pojęcia o problematyce kryptografii. Do tego nie pokusili się nawet o poznanie dokumentów znajdujących się w zasobach CBT, WSI i MON, nie mówiąc już o chęci zrozumienia trudnego problemu narodowej i sojuszniczej kryptografii. Należy podkreślić, że do dnia dzisiejszego problem narodowych i sojuszniczych informacji niejawnych oraz ich ochrony kryptograficznej nie został profesjonalnie rozwiązany w polskim prawodawstwie i dalece odbiega od zasad stosowanych w NATO i państwach członkach NATO, mimo podpisania przez nasz rząd umów w tym obszarze. Istnieje szereg pisemnych dowodów, że to właśnie w latach 2004-200 nie kto inny jak WSI podjęły szereg działań mających na celu poprawienie istniejącej sytuacji w tym obszarze w resorcie ON. Działania te wspierał ówczesny Minister ON Jerzy Szmajdziński, zatwierdzając i nadzorując wdrożenie dwóch koncepcji (plus Aneksu) i zapalając zielone światło do opracowania trzeciej, która do dnia dzisiejszego nie została zatwierdzona, mimo powstania jej projektu w grudniu 2005 r., za który był odpowiedzialny autor notatki płk Jerzy M. Nie wspominamy o innych osiągnięciach międzynarodowych WSI w obszarze bezpieczeństwa informacyjnego, jak osiągnięcia wojskowej służby kurierskiej, podpisane umowy z państwami NATO, udział w międzynarodowych gremiach decyzyjnych, czy zaproszenia do wygłaszania referatów na konferencjach międzynarodowych przez oficerów CBT.* Z dopuszczonych w ten sposób do użytku urządzeń korzystały lub korzystają osoby sprawujące najwyższe urzędy państwowe w tym: Prezydent RP, Szef BBN, Minister Obrony Narodowej, Szef Sekretariatu MON, Sekretarz Stanu I Zastępca MON, Szef Sztabu Generalnego WP, Szef WSI czy Komendant Główny ŻW. *Podany przykład dotyczy niejawnego telefonu komórkowego posiadającego certyfikat „NATO Secret". Telefony tego typu zostały wykorzystane we wdrożonym w MON przez P6 SG WP narodowym niejawnym systemie teleinformatycznym do klauzuli „poufne" na okres dwóch lat (do końca 2007 r.), do czasu opracowania własnego utajnionego telefonu komórkowego. Jaki ma to związek z olbrzymim zagrożeniem dla bezpieczeństwa państwa? Chyba, że zdaniem autorów należy aż tak obawiać się NATO i nie korzystać z pomocy Sojuszu, nawet jeśli nie możemy uporać się z chwilowo istniejącymi trudnościami. Niestety problem ten nie został rozwiązany do dnia dzisiejszego w MON. Ciekawa jest odpowiedź na pytanie: „Z jakich telefonów niejawnych korzysta w obecnej chwili kierownictwo MON?" Mamy nadzieję, że Antoni Macierewicz, jako szef SKW wycofał z eksploatacji tak skrytykowane w Raporcie czasowe „natowskie rozwiązanie" zaakceptowane przez WSI.* Na uwagę zasługuje także fakt, iż gdyby zamiast wieloletnich starań zmierzających do zakupu obcych urządzeń zdecydowano się na przygotowanie własnych rozwiązań, prawdopodobnie w tym samym czasie udałoby się je wdrożyć. ***Jest to bardzo rozsądny wniosek. Kreowanie takich wniosków jest bardzo łatwe,***

ale znacznie gorzej jest z ich realizacją, o czym zapewne przekonali się autorzy notatki, którzy nie rozwiązali również tego problemu do kwietnia 2010 r., odpowiadając za ten obszar w SKW.

---

[280] Aneks ten jest zwieńczeniem działań nielegalnego lobby na rzecz firmy SILTEC. W jego skład wchodzili najwyżsi rangą oficerowie Sztabu Głównego WP oraz WSI; poza wymienionymi także gen Henryk Tacik (Polskie Przedstawicielstwo Wojskowe przy Komitecie Wojskowym Organizacji Traktatu Północnoatlantyckiego), gen. Henryk Szumski (Członek Rady Bezpieczeństwa Narodowego), gen. Maj, gen Wojciech Wojciechowski, gen. Wojciech Kubiak, płk Glonek, płk Dobrosław Mąka (dyr. Biura Bezpieczeństwa Teleinformatycznego), płk Jerzy Cichosz (autor Aneksu, dyr. WBBiŁ), płk Andrzej Dańczak (WBBŁiL), płk Marek Sobczak (CAŁiBT), płk Krzysztof Polkowski (szef CBT). *W treści Raportu nie podano żadnego dowodu, który wskazuje na zasadność takiego wniosku.* Opis poszczególnych etapów działania tej grupy znajduje się w „W notatce w sprawie dopuszczenia do eksploatacji w WP urządzeń kryptograficznych oferowanych przez firmę SILTEC w latach 2001-2006" *W treści Raportu nie wymieniono innych oficerów, którzy uczestniczyli w latach 2001-2006 w tym nagannym zdaniem jego autorów procederze: zastępcy szefa WSI, który bezpośredni był odpowiedzialny za sprawy techniki w 2005 r., szefa SG WP, któremu podlegało P-6, szefów komisji przetargowych i prawników? Dlaczego autorzy Raportu nie zweryfikowali zawartych w notatce informacji z dokumentami znajdującymi się w zasobach archiwalnych MON, a także nie wysłuchali członków rzekomego nielegalnego lobby na rzecz firmy SILTEC w procesie przeprowadzanej ustawowej weryfikacji, w tym szefa CBT, który poddał się weryfikacji i z którym komisja rozmawiała, ale nie zadała mu żadnego pytania w tej sprawie? „Notatka w sprawie dopuszczenia do eksploatacji w WP urządzeń kryptograficznych oferowanych przez firmę SILTEC w latach 2001-2006" została sporządzona przez dwóch oficerów CBT WSI płk. Jerzego M. i ppłk. Tadeusza R. Notatka z dnia 27 października 2006 r. o klauzuli „zastrzeżone" obejmuje 22 strony i załączniki (BBT SKW nr 2-10 na 214 kartach), które zostały tendencyjnie omówione przez jej autorów, jednoznacznie sugerując popełnienie przestępstw, w tym namawiania przez szefa CBT do nie przestrzegania istniejącego prawa. Szef CBT poznał treść notatki w dniu 21 lipca 2009 r. Ostatecznie autorzy notatki rozstali się z SKW w 2010 r. a następnie z mundurem. Niestety Szef SKW nie podjął żadnych działań po otrzymaniu informacji od byłego szefa CBT – musiał sam na własnej skórze przekonać się o wartości swoich podwładnych, autorach notatki.* Większość wymienionych oficerów w latach 70. lub 80. była szkolona w Moskwie *Na 14 wymienionych oficerów, rzekomych przestępców w obszarze kryptografii, 5 oficerów jest z WSI, a 3 oficerów WSI przeszło szkolenie na kursie GRU w Moskwie – z porównania z wykazem w Aneksie nr 13 w Raporcie. Jeden oficer spośród tych trzech przestępców szkolonych w GRU ukończył łącznie osiem kursów w USA i NATO oraz przesłużył w USA i strukturach NATO łącznie siedem lat otrzymując wzorowe opinie oraz wyróżnienia za służbę, o których autorzy notatki i Raportu mogą jedynie pomarzyć.*

WĄTEK DOTYCZĄCY KRYPTOGRAFII W ANTYRAPORCIE
Opinia zespołu ekspertów Platformy Obywatelskiej pod redakcją Marka Biernackiego
(strona 30 w wersji elektronicznej, *niebieską kursywą – komentarz*)

W tym rozdziale opisano również nieprawidłowości w Sztabie Generalnym WP. Jest to jednak odrębna struktura od WSI...

Jak widać z powyższego tekstu, to nie wiele do powiedzenia na temat problemów dotyczących kryptografii opisanych w Raporcie Antoniego Macierewicza mieli eksperci Platformy Obywatelskiej.

Poniżej przedstawiamy Postanowienie z uzasadnieniem (pkt 4) Wojskowej Prokuratury Okręgowej w Warszawie, która prowadziła śledztwo w sprawie zakupów sprzętu kryptograficznego dla SZ RP od firmy SILTEC .

Ocenę dotyczącą przestępczej działalności oficerów WSI w obszarze kryptografii opisaną w Raporcie pozostawiamy czytelnikom.

WOJSKOWA PROKURATURA OKRĘGOWA
W WARSZAWIE
ul. Nowowiejska 25 b
00-911 Warszawa

Po. Śl. 84/05

Warszawa, dn. 4 czerwca 2009 r.

Postanowienie
o umorzeniu śledztwa

Wizytator - Prokurator Wojskowej Prokuratury Okręgowej w Warszawie – ppłk Janusz Wójcik po rozpoznaniu materiałów śledztwa w sprawie przekroczenia uprawnień lub niedopełnienia obowiązków przez funkcjonariuszy publicznych podległych jednostkom organizacyjnym Ministerstwa Obrony Narodowej, którzy mieli niedopełnić obowiązków lub przekroczyć uprawnienia w związku z zakupem urządzeń oraz sprzętu od spółki z o.o. „SILTEC", przez co działali na szkodę interesu publicznego – resortu Obrony Narodowej, tj. o przest. z art. 231§1 kk

postanowił

na zasadzie art. 322§ 1 kpk w zw. z art.17§1pkt 2 kpk

1. umorzyć śledztwo w sprawie przekroczenia uprawnień lub niedopełnienia obowiązków przez funkcjonariuszy publicznych z Departamentu Zaopatrywania Sił Zbrojnych MON, którzy podpisując w Warszawie w dn. 23.11.2000 r. umowę nr 532/VII/KN/ZS/WR/2000/1017, w dn. 24.06.2002 r. umowę nr DZSZ/59/VII/KN/ZS/WR/B/2002/488 oraz w dn. 18.11.2004 r. umowę nr DZSZ/281/V/-5/UZ/NEG/Z/2004/791 na zakup urządzeń w postaci Systemu Laserowego Dalmierza i Oświetlacza Celów – GLTD II ze spółką z o.o. „SILTEC", działali na szkodę interesu publicznego - resortu Obrony Narodowej, tj. o przest. z art. 231§1 kk - trzykrotnie

albowiem czyn nie zawiera znamion czynu zabronionego,

2. umorzyć śledztwo w sprawie przekroczenia uprawnień lub niedopełnienia obowiązków przez funkcjonariuszy publicznych z Generalnego Zarządu Dowodzenia

i Łączności P-6 Sztabu Generalnego WP w Warszawie, którzy w roku 2005 w Warszawie formułując Specyfikację Istotnych Warunków Zamówienia w przetargu na dostawę komputerów klasy „TEMPEST" na potrzeby systemu „Secwan" mieli podejmować działania zmierzające do faworyzowania spółki z o.o. „SILTEC" a nadto w sprawie funkcjonariuszy publicznych z Departamentu Zaopatrywania Sił Zbrojnych MON, którzy prowadząc postępowanie o udzielenia zamówienia publicznego nr DZSZ/75/VII-30/UZ/PRZ/Z/2005, prowadzonego w 2005 r. w Warszawie, a dotyczącego wyżej wymienionych komputerów klasy „TEMPEST", mieli dopuścić się przekroczenia uprawnień lub niedopełnienia obowiązków poprzez podejmowanie działań będących wyrazem faworyzowania spółki z o.o. „SILTEC", czym działali na szkodę interesu publicznego – resortu Obrony Narodowej, tj. o przest. z art. 231 § 1 kk

albowiem czyn nie zawiera znamion czynu zabronionego

3. umorzyć śledztwo w sprawie przekroczenia uprawnień lub niedopełnienia obowiązków przez funkcjonariuszy publicznych z Generalnego Zarządu Rozpoznania Wojskowego P – 2 Sztabu Generalnego WP, Departamentu Zaopatrywania Sił Zbrojnych MON, Szefa Sztabu Generalnego WP, którzy w latach 2000 - 2007 w Warszawie podejmując działania związane z tworzeniem, rozwojem i nabywaniem sprzętu na potrzeby Systemu Informatycznego „SŁUŻBA" (w późniejszym okresie zwanego Systemem Teleinformatycznym) oraz wprowadzając sprzęt do Sił Zbrojnych RP, a co za tym idzie podejmując decyzje skutkujące nabyciem komputerów klasy „TEMPEST" od spółki z o.o. „SILTEC" działali na szkodę interesu publicznego – resortu Obrony Narodowej, tj. o przest. z art. 231 § 1 kk

albowiem czyn nie zawiera znamion czynu zabronionego

4. umorzyć śledztwo w sprawie przekroczenia uprawnień lub niedopełnienia obowiązków przez funkcjonariuszy publicznych z Generalnego Zarządu Dowodzenia i Łączności P-6, Wojskowego Biura Bezpieczeństwa i Łączności i Informatyki, Departamentu Zaopatrywania Sił Zbrojnych oraz Wojskowych Służb Informacyjnych, którzy w latach 2002 - 2004 r. w Warszawie podejmując działania w obszarze dostaw i implementacji urządzeń kryptograficznych oraz podpisując umowę na zakup

sprzętu kryptograficznego w postaci stacji zarządzania i generacji TCE 500B i TCE 621 ze spółką z o.o. „SILTEC", działali na szkodę interesu publicznego – resortu Obrony Narodowej, tj. o przest. z art. 231§1 kk

albowiem czyn nie zawiera znamion czynu zabronionego

na zasadzie art. 322§ 1 kpk w zw. z art.17§1pkt 1 kpk

5. umorzyć śledztwo w sprawie działającej w okresie od 01.01.2000 r. do 12.02.2007 r. w Warszawie zorganizowanej grupy przestępczej, składającej się z oficerów pełniących służbę w Sztabie Generalnym WP oraz strukturach Ministerstwa Obrony Narodowej RP oraz współdziałających z nimi osób cywilnych, którzy to mieli na celu popełnianie przestępstw w związku z nabywaniem sprzętu na potrzeby Sił Zbrojnych RP od spółki z o.o. „SILTEC", tj. o przest. z art. 258 § 1 kk

albowiem brak jest danych dostatecznie uzasadniających podejrzenie zaistnienia przestępstwa

- uzasadnienie do pkt. 5 rozstrzygnięcia z uwagi na to, że zawiera informacje stanowiące tajemnicę państwową jest niejawne i znajduje się w Kancelarii Tajnej Wojskowej Prokuratury Okręgowej w Warszawie .

U z a s a d n i e n i e

W Wojskowej Prokuraturze Okręgowej w Warszawie nadzorowano prowadzone przez Komendę Główną Żandarmerii Wojskowej w Warszawie śledztwo (z czasem przejęte do osobistego prowadzenia) w sprawie przekroczenia uprawnień lub niedopełnienia obowiązków przez funkcjonariuszy publicznych z Departamentu Zaopatrywania Sił Zbrojnych MON, którzy podpisując umowę na zakup urządzenia w postaci Systemu Laserowego Dalmierza i Oświetlacza Celów – GLTD II, działali na szkodę interesu publicznego, tj. o przest. z art. 231§1 kk.

wspomnianej spółki na rynku dostaw komputerów tempestowych oraz dążeniem do unifikacji sprzętowej, wyrastającej ze słusznego założenia, iż funkcjonując w ramach NATO Wojsko Polskie musi korzystać ze standardowych rozwiązań przyjętych w wiodących państwach wspomnianego Sojuszu.

Okoliczności przedstawione powyżej wyraźnie wskazują, iż działaniom wspomnianych osób nie można przypisać przestępnego charakteru zarówno w aspekcie podmiotowym (umyślność działania polegającego na przekroczeniu uprawnień tudzież niedopełnienia obowiązków) jak i w aspekcie przedmiotowym (działanie na szkodę interesu publicznego).

Co mając na uwadze postępowanie w tej części należało umorzyć, jak w pkt. 3 sentencji.

Kolejnym śledztwem, z czasem wątkiem, nadzorowanym a następnie prowadzonym przez Wojskową Prokuraturę Okręgową w Warszawie była sprawa dotycząca początkowo przekroczenia uprawnień lub niedopełnienia obowiązków przez funkcjonariuszy publicznych z Generalnego Zarządu Dowodzenia i Łączności P-6 w Warszawie, z czasem także funkcjonariuszy innych komórek organizacyjnych podległych MON, a to DZSZ, WBBŁiI oraz CBT WSI, którzy podejmując działania w obszarze dostaw sprzętu kryptograficznego i jego implementacji do krajowych systemów kryptograficznych działali na szkodę interesu publicznego, tj. o przest. z art. 231§1 kk.

Przedmiotowe postępowanie zostało wszczęte przez Komendę Główną Żandarmerii Wojskowej w oparciu o ustalenia, z których wynikało, że w trakcie podpisania umowy na dostawę na potrzeby Sił Zbrojnych RP norweskiego sprzętu kryptograficznego w postaci stacji zarządzania i generacji TCE 500 B i TCE 621 w dn. 09.09.2004 r. mogło dojść ze strony funkcjonariuszy publicznych z Generalnego Zarządu Dowodzenia i Łączności P – 6 w Warszawie do przekroczenia uprawnień lub niedopełnienia obowiązków. Miało to polegać na uzgodnieniu jeszcze przed etapem negocjacji ceny zakupu, zmienieniu specyfikacji w sposób preferujący firmę „SILTEC". Nadto zakupiony sprzęt miał nie spełniać wymogów, stawianych tego rodzaju urządzeniom, w dokumencie ramowym zatytułowanym *„Koncepcja rozwoju systemów ochrony kryptograficznej w resorcie Obrony Narodowej"* (k. 1664 – 1689),

gdzie wskazywano, iż Polska przy budowie systemów teleinformatycznych, interoperacyjnych z systemami sojuszu, musi uwzględniać w obszarze kryptograficznym stosowanie narodowych urządzeń do ochrony informacji w narodowym systemie łączności (k. 2459, 1824, 1825 – akt głównych, 225 – 301 mat. wydzielonych).

W trakcie prowadzonego śledztwa podjęto czynności zmierzające do weryfikacji zasadności podnoszonych zastrzeżeń, w tym opierając się na materiałach uzyskanych od Przewodniczącego Komisji Weryfikacyjnej ministra Antoniego Macierewicza, poprzez sprawdzenie przede wszystkim jakim celom miał przyświecać zakup kontrowersyjnego sprzętu, kiedy pojawiła się tego rodzaju idea i czy w związku z realizacją zakupów faktycznie dochodziło do faworyzowania firmy „Siltec".

Jak wynika z poczynionych ustaleń Siły Zbrojne RP w ramach procesów dostosowujących strukturę Wojska Polskiego do wymogów wynikających z przynależności do NATO realizowały szereg celów, w tym cel określony pierwotnie jako EG 2822 a następnie jako EG 2866 – „bezpieczeństwo systemów łączności i informatyki" (k. 1721 – 1726, 2457, 2447 - 2450)

Wiązał się on bezpośrednio z zakupem szeroko rozumianego sprzętu utajniającego i zmierzał do zbudowania struktur technicznych dla przetwarzania informacji o różnych klauzulach, tak na potrzeby Sojuszu Północnoatlantyckiego jak i krajowe (k. 1856 – 1862). Nadrzędnym zadaniem było zabezpieczenie środków technicznych na potrzeby łączności jednostek wysokiej gotowości, określanych jako HRF, które przeznaczone były do realizacji wspólnych zadań z innymi jednostkami państw NATO. Cel ten miał zostać osiągnięty poprzez zakupy aparatów telefonicznych (np. TCE 500B - telefon wokoderowy) z indywidualnym utajnianiem jak i rozwój wymiany informacji na bazie protokołu IP – tj. urządzenia o nazwie TCE 621.

Nabycie tego rodzaju urządzeń stało się koniecznością w momencie gdy niemożliwym było uzupełnienie sprzętu (z uwagi na zaniechanie jego produkcji) dotychczas wykorzystywanego, a pochodzącego z użyczenia partnerów amerykańskich w postaci aparatów telefonicznych oznaczonych jako SY 71E i KY 71.

Opóźnienia we wdrażaniu systemów ochrony kryptograficznej, zwłaszcza w zakresie narodowych systemów teleinformatycznych służących do przesyłania

informacji o klauzuli „Poufne" w resorcie Obrony Narodowej były przedmiotem krytycznych uwag Departamentu Kontroli MON, który przeprowadził kontrolę Wojskowego Biura Bezpieczeństwa i Łączności i Informatyki (k. 181 – 198 materiałów wydzielonych).

Jak ustalono, powodem dla którego zdecydowano się na zaopatrzenie w urządzenia produkcji norweskiej firmy „THALES COMMUNICATION AS Norway" był fakt, iż wymieniona firma była wiodącym dostawcą dla szeregu europejskich armii, tym samym były to urządzenia o zweryfikowanej jakości.

Na rynku polskim wyłącznym przedstawicielem firmy „THALES" była spółka z o.o. „SILTEC" (k. 1916, 1943 – 1948), stąd też oczywistym było, że tylko ten podmiot gospodarczy może dostarczyć żądane urządzenia. Pierwszą partię telefonów TCE 500B zakupiono w roku 2002. W roku 2003 i 2004 trwały zakończone niepowodzeniem negocjacje z firmą „SILTEC" na dostawę dalszych aparatów TCE 500B oraz nowocześniejszych TCE 621. Pod koniec roku 2003 przedstawiciele firmy „SILTEC" oświadczyli (k. 1878 – 1880), że ich norweski dostawca zaprzestał w międzyczasie produkcji stacji zarządzania, którą zamierzano nabyć na potrzeby Sił Zbrojnych, oddzielnie do aparatów TCE 500 B i TCE 621. Ze zweryfikowanych informacji istotnie wynikało, że „THALES" w roku 2003 i 2004 skoncentrował się na produkcji urządzeń łączących w sobie funkcje generacji materiału kryptograficznego i zarządzania materiałem kryptograficznym dla wszystkich uprzednio zakupionych urządzeń (k. 2374 – 2376,). Przedstawiciele „SILTEC" zaproponowali w zmienionej sytuacji Departamentowi Zaopatrywania Sił Zbrojnych nowy produkt firmy „THALES" określany jako EKMS (Elektronic Key Managment System – system elektronicznego zarządzania stacją generacji), który z jednej strony był nowocześniejszy i bardziej wszechstronny lecz z drugiej jego koszt był znacząco wyższy. Skutkowało to napięciami pomiędzy uczestnikami procedury przetargowej po stronie wojska, gdyż pierwotna kwota zabezpieczonych środków z około 2 mln zł został podwyższona do około 4 milionów zł. O fakcie tym w dn. 20.08.2004 r. poinformował płk Tomasz Górecki z WBBŁ i I zastępcę szefa P – 6 gen. bryg. Edmunda Smakulskiego, podnosząc wątpliwości co do zasadności zakupu urządzeń norweskich. (k. 1691 – 1700).

W tej sytuacji, na wniosek gen. Smakulskiego odbyło się w dn. 24.08.2004 r. spotkanie uzgodnieniowe z udziałem przedstawicieli CBT WSI, DZSZ, WBBŁ i I oraz Zarządu Łączności i Informatyki P6 – gdzie uczestnicy uznali celowość zakupu stacji

zarządzania i generacji, przy czym wskazali, że będzie ona wykorzystywana zarówno do celów narodowych (do klauzuli „Zastrzeżone") jak i w niejawnych podsystemach łączności NATO (k. 1676, t. IX).

Spotkanie to odblokowało procedurę przetargową i w efekcie w dn. 09.09.2004 r. zawarto umowę Nr DZSZ/414/V-4/ZS/WR/2003/595 z „SILTEC" na zakup stacji generacji i zarządzania systemu IP (protokół postępowania na k. 1916 – 1921), gdzie wartość umowy określono na 4.035.000 zł brutto.

Stacja ta miała zastosowanie do już uprzednio zakupionych urządzeń różnych generacji, ze szczególnym uwzględnieniem TCE 500B i TCE 621. Przy czym, jak pierwotnie założono, miała służyć do eksploatowania sytemu narodowego kryptograficznego o klauzuli „Zastrzeżone". Tego rodzaju zapis, w ówczesnym stanie prawnym, wynikał z tego, iż na gruncie obowiązującej podówczas *ustawy o ochronie informacji niejawnych (Dz.U.99.11.95)* oraz aktu wykonawczego w postaci *rozporządzenia Prezesa Rady Ministrów z dn. 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U.99.18.162)* obowiązującego do dn. 23.09.2005 r., przetwarzanie informacji niejawnych stanowiących tajemnicę państwową oraz tajemnicę służbową oznaczoną klauzulą „Poufne" wymagało certyfikacji systemu. Przy czym, co wyraźnie należy nadmienić, kwestia ta wiązała się z wymianą informacji narodowej, w stosunku do informacji określanej jako sojusznicza zakupione urządzenie nie doznawało tego rodzaju ograniczeń.

Uprzedzając dalszy wywód wskazać należy, iż w odniesieniu do kryptografii narodowej ramowe założenia przyjęte w *„Koncepcji rozwoju systemów ochrony kryptograficznej w resorcie obrony narodowej"* pozwalały na podwyższenia klauzuli przetwarzanych informacji w sytuacjach pilnych potrzeb doraźnych (k. 232 mat. wydzielonych).

Wskazówki dotyczące możliwości dopuszczenia w okresie przejściowym urządzeń kryptograficznych produkcji państw NATO do przetwarzania informacji o klauzuli do „POUFNE" w narodowych systemach kryptograficznych zawierał Aneks do *„Koncepcji rozwoju systemów ochrony kryptograficznej w resorcie Obrony Narodowej"* (k. 207, 211, 212 mat. wydzielonych)

Kwestia relacji ceny zakupionego urządzenia do klauzuli informacji jakie pierwotnie miały być na nim przetwarzane (chodzi o informację narodową) była

podnoszona jako argument przemawiający przeciwko celowości zakupu, za tak wysoką kwotę, urządzenia wykorzystywanego do przetwarzania informacji o klauzuli „Zastrzeżone"

Odnosząc się do wagi tego stwierdzenia nie sposób nie dostrzec, iż zakup urządzenia był w pierwszym rzędzie podyktowany koniecznością zapewnienia wymogów interoperacyjności w ramach NATO oraz wynikał z planów wieloletnich modernizacji technicznej SZ RP (k. 653, 659, 660, 694, 698, 706, 724, 737, 741, 790 mat. wydzielonych) (k. 2415 – 2421) i jako taki był uzasadniony.

Możliwość wykorzystania nabywanego sprzętu do przetwarzania informacji narodowych o klauzuli „Poufne", została zrealizowana w styczniu 2006 r. poprzez dopuszczenie do takiego przetwarzania urządzenia TCE 500B, po uprzednim dokonaniu oceny dokumentacji bezpieczeństwa oraz akredytacji urządzenia (k. 385 k. 471 - 524 mat. wydzielonych), oraz ESZDK (Elektroniczny System Zarządzania Dokumentami Kryptograficznymi), tj. stacji generacji i zarządzania systemu IP na okres 2 lat (k. 470, 525 – 644 mat. wydzielonych).

Sama idea, przeprowadzenia w ten sposób podwyższenia klauzuli przetwarzanej informacji narodowej do „Poufne", kontestowana była przez płk. Jerzego Mikołajczyka (k. 1741 – 1751, 2352 – 2355, 6609, 6610) powołującego się na opinię radcy prawnego Stanisława Prykowskiego, który stwierdził w swojej opinii z dn. 25.05.2005 r. (k. 1760), że szef służby ochrony państwa powinien mieć zagwarantowaną możliwość oceny ryzyka, w sytuacji zastosowania trybu określonego w art. 60.7 *ustawy o ochronie informacji niejawnych* (Dz.U.2005, Nr 196, poz. 1631), przy czym jednocześnie wskazywał on (tj. radca prawny) na nieaktualne już *rozporządzenie Prezesa Rady Ministrów z dn. 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych* (Dz. U. Nr 18, poz. 162), które w § 4 zawierało normę pozwalającą na zaniechanie badania urządzeń spełniających wymagania bezpieczeństwa określone w rozporządzeniu, jeżeli otrzymały certyfikat właściwej krajowej władzy bezpieczeństwa państwa, w państwie będącym stroną Organizacji Traktatu Północnoatlantyckiego, jako na ewentualny tryb dopuszczenia w uzasadnionych warunkach urządzenia pochodzącego z innego państwa NATO .

Powyższe rozporządzenie zostało zastąpione *rozporządzeniem Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego z*

dn. 25.08.2005 r., które weszło w życie w dn. 23.09.2005 r. (Dz.U.2005, 171,1433), które to w § 11 zawierało tożsamą niemalże normę w brzmieniu *„Służby ochrony państwa mogą dopuścić do stosowania w systemie lub sieci teleinformatycznej urządzenia lub narzędzia, które spełniają właściwe wymagania bezpieczeństwa, jeżeli otrzymały stosowny certyfikaty krajowej władzy bezpieczeństwa w państwie będącym stroną Organizacji Traktatu Północnoatlantyckiego lub w państwie członkowskim Unii Europejskiej".*

Odnosząc się zatem do zasygnalizowanych wątpliwości prawnych przez płk. Mikołajczyka stwierdzić należało, iż przywołany zapis rozporządzenia z 25.08.2005 r. w powiązaniu z zapisami Aneksu do *„Koncepcji rozwoju systemów ochrony kryptograficznej w resorcie Obrony Narodowej"* (k. 211 mat. wydzielonych) stwarzał przestrzeń do interpretacji prawnej uwieńczonej podwyższeniem klauzuli przetwarzanych informacji do „Poufne", jak to nadmieniono.

Podwyższenie klauzuli, do której zakupione urządzenia mogły przetwarzać informacje, nie byłoby możliwe bez stanowiska wyrażonego przez Szefa WSI gen. bryg. Marka Dukaczewskiego (pełniącego obowiązki na tym stanowisku pomiędzy 06.01.2001 a 08.12.2005 r.), który w piśmie z dn. 28.01.2005 r. (k. 2365, 2366, 2392 - 2397) stwierdził, iż Służba Ochrony Państwa może dopuścić urządzenia ochrony kryptograficznej pochodzące z państw NATO do eksploatacji (m in. komórkowe aparaty telefoniczne NSK – 200, aparaty telefoniczne i indywidualnym utajnianiem TCE - 500B oraz urządzenia IP Crypto TCE – 621) wykorzystywane do przesyłania informacji niejawnych (do klauzuli „POUFNE"), jeżeli urządzenia te będą posiadały certyfikaty właściwej krajowej władzy bezpieczeństwa w państwie będącym stroną Organizacji Traktatu Północnoatlantyckiego, o ile spełnione zostaną pozostałe warunki, a to:

- warunkiem eksploatacji, na czas określony, ww. urządzeń będzie przygotowanie dokumentacji wymaganej ustawą o ochronie informacji niejawnych, opracowanej w fazie projektowania, bieżąco uzupełnianej w fazie wdrażania i modyfikowanej w fazie eksploatacji sytemu lub sieci,
- podczas analizy ryzyka projektowanych systemów lub sieci specjaliści WSI będą brali pod uwagę wyniki procesu analizy ryzyka projektowanych systemów lub sieci w

celu identyfikacji słabości lub zagrożeń związanych z eksploatacją urządzeń oraz środków im przeciwdziałających.

Nadmienić należy, iż w toku dalszego postępowania ustalono, iż urządzenia ochrony kryptograficznej w postaci TCE-621 nabywane były na potrzeby budowy systemów wymiany informacji przez Marynarkę Wojenną, Generalny Zarząd Rozpoznania Wojskowego - P2, Siły Powietrzne i uprzednio wymieniony Generalny Zarząd Dowodzenia i Łączności – P6. I tak w ramach umowy nr DZSZ/10/V-7/UZ/NEG/Z/2005/815 zakupiono 41 sztuk urządzeń kryptograficznych TCE-621, z czego:

- z 20 sztuk zakupionych na potrzeby GZDiŁ, 10 sztuk przewidziano na uzupełnienie jednostek HRF przewidzianych do działań w Siłach Odpowiedzi NATO, pozostałe 10 urządzeń zaplanowano dla realizacji celu – „Możliwości Systemu Wideokonferencji (VTC) kompatybilnego z NATO,
- z zakupionych 9 sztuk urządzeń na potrzeby Marynarki Wojennej 7 sztuk przewidziano do wymiany informacji wg Stanagu 5066 a pozostałe do rozszerzenia systemu NATO Maritime Command Control and Information System (MCCIS),
- 2 sztuki zakupione dla Generalnego Zarządu Rozpoznania Wojskowego – P2 przewidziano do wymiany przestarzałych urządzeń kryptograficznych w ramach sojuszniczego Podsystemu Battelfield Information Collection and Explitation System (BICES),
- 10 sztuk zakupionych na potrzeby Sił Powietrznych przewidziano do rozszerzania systemu Initial CAOC Capability (ICC) i wymiany przestarzałych urządzeń kryptograficznych (BID-950) na nowe (TCE-621) zgodnie z koncepcją NATO - (k. 6705, 6706).

W tym miejscu wskazać należy, iż w świetle przytoczonych faktów wyraźnie widać, iż zarzut o niezgodności dokonywanych zakupów z dokumentem ramowym jakim była *„Koncepcja rozwoju systemów ochrony kryptograficznej w resorcie Obrony Narodowej”* jest nietrafny gdyż w niniejszej sprawie zachodziła przede wszystkim konieczność zrealizowania celu EG 2866 – rozumianego jako zapewnienie technicznych możliwości do wymiany informacji przede wszystkim na potrzeby NATO i innych celów Sił Zbrojnych, w zakresie budowy systemów wymiany

informacji z partnerami z NATO, a dopiero w dalszej kolejności do budowy narodowego systemu kryptograficznego, na bazie tak zakupionego sprzętu.

Co więcej, w świetle poczynionych ustaleń wynika, że zakup tzw. EKMS miał i ma nadal kapitalne znaczenie dla wymiany danych w systemach niejawnych NATO (k. 6190 – 6220). Kwestia ta związana jest z trwającymi od kilku lat pracami koncepcyjnymi związanymi z osiąganiem sieciocentryczności systemów informatycznych (NEC – Network Enabled Capability).

Jak wynikało z informacji udzielonej przez Departament Informatyki i Telekomunikacji Ministerstwa Obrony Narodowej zasadnicze prace planistyczne w tym zakresie zostały zakończone w III kwartale 2005 r. Realizacja programu składała się z etapów:

- I etap (od marca 2007 r.) objął Dowództwo Strategiczne i Regionalne Sojuszu,
- II etap (od grudnia 2008 r.) miał objąć kraje członkowie NATO.

W ramach II etapu we wszystkich krajach członkowskich sojuszu – Krajowych Organach Dystrybucji (w dowództwach NATO wcześniej) w ramach NSIP (Nato Secure Inwestment Programme) planowano zainstalowanie stacji roboczych wraz z urządzeniami elektronicznego przenoszenia dokumentów kluczowych dla urządzeń kryptograficznych systemu DEKMS (Dacan Electronic Key Managment System). Dalsza ewidencja i redystrybucja dokumentów do urządzeń kryptograficznych pozostawać miała w gestii narodowej. Wymagania NATO w stosunku do krajów członkowskich w tym zakresie potwierdzono Celem Sił Zbrojnych edycji 2008 E 2781. Uwzględniając powyższe Szef Sztabu Generalnego Rozkazem Nr 846/DOW/P6 z dn. 21 sierpnia 2006 r. powołał Zespół ds. opracowania koncepcji elektronicznego systemu zarządzania dokumentami kryptograficznymi – ESZDK.

Ponadto zauważyć należało, iż urządzenie w postaci EKMS (ESZDK) ma potencjalnie istotne znaczenie dla zarządzania szeregiem systemów teleinformatycznych narodowych, do klauzuli „Zastrzeżone" i pozwala na szkolenie użytkowników natowskich systemów kryptograficznych podczas ćwiczeń i operacji, w których biorą udział polskie jednostki wojskowe.

Wobec faktu, iż EKMS jest nowoczesnym systemem o architekturze otwartej, umożliwiającej podłączenie zewnętrznego narodowego generatora ciągów losowych, uznać należy, iż tym samym istnieją możliwości w zakresie jego unarodowienia (k. 6137, 6138).

W trakcie prowadzonego śledztwa ustalono także, iż urządzenia TCE 621 zostały zakupione na potrzeby JW 2305 (GROM) w roku 2006 od firmy „SILTEC" (k. 6246, 6247) i z powodzeniem wykorzystywane są w systemie teleinformatycznym wspomnianej jednostki.

Urządzenia te stosowane są do przetwarzania danych do klauzuli „Zastrzeżone" w systemach narodowych i do klauzuli „Secret" w systemach sojuszniczych.

Rekapitulując, zgromadzony materiał dowodowy nie daje podstaw do przyjęcia, iż w toku działań związanych z nabywaniem na potrzeby Sił Zbrojnych urządzeń kryptograficznych produkcji norweskiej, od spółki „Siltec", doszło do faworyzowania wspomnianego podmiotu gospodarczego, a zachowania osób funkcyjnych podejmujących decyzje związane z tym procesem podyktowane były dążeniem do urzeczywistnienia wspomnianego celu.

Kontrowersje jakie zrodziły się w związku z tymi działaniami miały swe źródło, jak się wydaje, w konieczności podejmowania decyzji, w których splatały się różne motywacje. Zasadniczo dążono do pozyskania sprawdzonego już sprzętu kryptograficznego, kompatybilnego ze sprzętem funkcjonującym w innych państwach NATO, spełniającego wymagania stawiane celem modernizacyjnym EG 2866 oraz, niejako przy okazji, dążono do pozyskania urządzenia przydatnego do wymiany informacji narodowej, w sytuacji gdy w latach 2002 – 2006, brakowało polskiego scertyfikowanego urządzenia kryptograficznego, bazującego na protokole IP (k. 6607v).

O ile ten ostatni cel udało się zrealizować jedynie w ograniczonym zakresie (wymiana informacji tylko do klauzuli „Poufne") to wymiana informacji sojuszniczej może być realizowana w pełnym spektrum przy użyciu zakupionych urządzeń.

Okoliczności przedstawione powyżej dają podstawę do stwierdzenia, iż działaniom wspomnianych osób nie można przypisać przestępnego charakteru zarówno w aspekcie podmiotowym (umyślność działania polegającego na przekroczeniu uprawnień tudzież niedopełnienia obowiązków) jak i w aspekcie przedmiotowym (działanie na szkodę interesu publicznego), co mając na uwadze śledztwo w tej części należało umorzyć, postanawiając jak w pkt. 4 sentencji.

Tytułem zauważenia wskazać należy, iż przyjęta za przedmiot rozważań kwalifikacja prawna z art. 231 § 1 kk była konsekwencją poczynionych ustaleń faktycznych, które nie dawały podstawy do przyjęcia, iż domniemane zachowania przestępne miały być podejmowane w celu osiągnięcia korzyści majątkowej lub osobistej w rozumieniu art. 231 § 2 kk.

Co więcej, w stosunku do dwóch umów wskazanych w pkt. 1 sentencji zachodziła konkurencyjna podstawa umorzenia śledztwa w postaci przedawnienia (zgodnie z art. 101 § 1 pkt 4 kk) jednakże mając na względzie, iż poczynione ustalenia dawały podstawę do umorzenia z uwagi na brak znamion czynu zabronionego przyjętą taką podstawę rozstrzygnięcia.

Odnośnie pkt. 5 postanowienia o umorzeniu śledztwa, to uzasadnienie w tym zakresie z uwagi na to, iż zawiera tajemnicę państwową ma charakter niejawny i przechowywane jest w Kancelarii Tajnej tut. Prokuratury.

WIZYTATOR-PROKURATOR
WOJSKOWEJ PROKURATURY OKRĘGOWEJ
w Warszawie
ppłk mgr Janusz WÓJCIK

Pouczenie:

Na zasadzie w art. 306§1 kpk w zw. z art. 465 § 1 i 2 kpk, art. 460 kpk w zw. z art. 122 § 1 i 2 kpk Ministrowi Obrony Narodowej przysługuje w zawitym terminie 7 dni od doręczenia postanowienia prawo złożenia zażalenia na niniejsze postanowienie do Wojskowego Sądu Okręgowego w Warszawie, za pośrednictwem tut. Prokuratury. Zażalenie złożone po upływie terminu zawitego jest bezskuteczne. Sąd może utrzymać w mocy zaskarżone postanowienie lub uchylić je i przekazać sprawę prokuratorowi celem wyjaśnienia wskazanych okoliczności , bądź przeprowadzenia wskazanych czynności /art. 330§1 kpk/.

Jeżeli prokurator nadal nie znajdzie podstaw do wniesienia aktu oskarżenia, wydaje ponownie postanowienie o umorzeniu śledztwa, wówczas pokrzywdzony, który wykorzystał uprawnienia przewidziane w art. 306 § 1 kpk może samodzielnie wnieść akt oskarżenia do Sądu w terminie 1-go miesiąca od daty zawiadomienia go o postanowieniu.

Akt oskarżenia winien spełniać wymogi określone w art. 55 § 1 kpk.

Inny pokrzywdzony tym samym czynem może do czasu rozpoczęcia przewodu na rozprawie głównej przyłączyć się do postępowania - art. 55 § 3 kpk.

Uprawnionemu do złożenia zażalenia przysługuje prawo do przejrzenia akt, które znajdują się w siedzibie Wojskowej Prokuratury Okręgowej w Warszawie przy ul. Nowowiejskiej 26b.

Zarządzenie – kopię postanowienia otrzymują:

1. **Minister Obrony Narodowej – za z.p.o.**

2, 3. aa.

WIZYTATOR-PROKURATOR
WOJSKOWEJ PROKURATURY OKRĘGOWEJ
w Warszawie
ppłk mgr Janusz WÓJCIK

Postanowienie uprawomocniło się
dnia 16.06.2009 r.

podpis prokuratora