ZAKOŃCZENIE

Dzisiejsza Polska cieszy się, jak na naszą dotychczasową historię, względnie długim okresem spokoju i stabilizacji. Taka sytuacja jest w dużej mierze możliwa dzięki racjonalnym i celowym działaniom państwa. Według Publiusa Siro (cytat z pracy Andrzeja Machnacza), *wybawi się od niebezpieczeństwa jedynie ten, kto czuwa także wtedy, gdy czuje się bezpieczny.*

Andrzej Jóźwiak zdefiniował pojęcie bezpieczeństwa narodowego i strategii Biura Bezpieczeństwa Narodowego w tym zakresie i omówił istotne obszary bezpieczeństwa systemów telekomunikacji (TK) i teleinformatyki (TI). Autor rozpatrzył skutki zagrożeń dla bezpieczeństwa narodowego poprzez unieruchomienie systemów administracji publicznej na przykładzie Estonii (także Jacek Matyszczak i Dariusz Kulawik omawiali te zagadnienia).

Telekomunikacja i teleinformatyka sektora publicznego, włączając w to infrastrukturę prywatną i warstwę publiczną sektora rządowego i służb państwa, jest dzisiaj naszą codziennością. Bezpieczeństwo korzystania z sieci często w sposób nieświadomy jest przyjmowane za oczywiste.

Współpraca i wspólne określenie zagrożeń przez organ regulujący, służby odpowiedzialne za bezpieczeństwo, resorty siłowe, producentów i operatorów umożliwiają realne, w odniesieniu do konkretnej sytuacji politycznej i gospodarczej kraju, wskazanie zagrożeń w wymienionych sieciach. Pewną systematykę i przykłady zagrożeń podali Krystian Baniak i Andrzej Machnacz.

Czynnik ludzki jest zagrożeniem wskazywanym w opracowaniach Krystiana Baniaka, Andrzeja Wisza, Dariusza Bogusza i Dariusza Kulawika.

Szczególnej wagi nabiera TK i TI w zakresie infrastruktury krytycznej dla funkcjonowania państwa (krytyczna infrastruktura telekomunikacyjna – KIT, krytyczna infrastruktura teleinformatyczna – KITI). Ze względu na znaczenie KIT i KITI (Jacek Matyszczak) w skali powiązań pa-

neuropejskich, Polska podjęła prace nad wdrożeniem Dyrektywy EPCIP Unii Europejskiej w tym zakresie (Krystian Baniak). Andrzej Machnacz i Andrzej Wisz identyfikują aktywa KIT/KITI resortów siłowych i standaryzowane atrybuty bezpieczeństwa: poufności, integralności, dostępności i rozliczalności (zwanej również niezaprzeczalnością).

Odpowiednio rozróżnia Andrzej Machnacz priorytety poszczególnych atrybutów w odniesieniu do aktywów KIT/KITI, co kierunkuje analizę zagrożeń, wymagań i umożliwia celowe przeciwdziałanie.

Robert Goniacz analizuje szczegółowo wymagania technologiczne stawiane wojskowym systemom TK i TI: z jednej strony, muszą zapewnić integralność Polski, z drugiej, nieodzowna dla bezpieczeństwa jest kompatybilność sieci TK i TI NATO. Ekonomia wykorzystania i rzeczywistość sieci publicznych oraz dostępnych w nich informacji dla wojska stawiają wysoką poprzeczkę rozwiązaniom możliwych przeciwdziałań (Robert Goniacz).

Celowe są przeciwdziałania na różnych szczeblach: fizycznym i środowiskowym (Andrzej Machnacz, Dariusz Kulawik), technologicznym (Zdzisław Drzycimski, Andrzej Machnacz) i proceduralnym (Andrzej Machnacz, Dariusz Bogusz, Dariusz Kulawik).

Wspólne dla każdego opracowania elementy: sieci publiczne, infrastruktura krytyczna, współpraca sieci różnych warstw, sieci międzynarodowe, zagrożenia i przeciwdziałania, odniesione do aktywów wymienionych w opracowaniu i tych z sektora publicznego, wskazują na potrzebę doskonalenia regulacji i standardów w tym zakresie. Tylko wtedy celowe projekty publiczne, krytyczne i specjalne zapewnią wymagany poziom bezpieczeństwa kraju i jego obywateli przy optymalnym, ekonomicznym wykorzystaniu środków finansowych.

Pragnę jeszcze raz podziękować wszystkim członkom zespołu, wymienionym we wprowadzeniu, za wkład pracy, w szczególności autorom pełniącym niezwykle wymagające funkcje w życiu codziennym, za ich gotowość przyjęcia dodatkowego obciążenia związanego z terminowym przygotowaniem niniejszego opracowania. To silny, niezwykle kompetentny, oddany bezpieczeństwu zespół.

Bogdan Lent
Warszawa, 23 lipca 2007 r.

SUMMARY

By historical standards today's Poland enjoys relatively long period of stability and peace. The targeted and justified state activities determine to large extend this positive situation. We quote here Publius Siro after Andrzej Machnacz: "only the one who keep alerted, while being secure, gets out of the insecurity".

The definition of the national security and the strategy of BBN in that area has beed presented by Andrzej Jozwiak. The relevant areas and the projection of telecommunication and information systems are analysed. The Estonia collapse of the national information network illustrate well the threats in the ICT-communication (also Jacek Matyszczak and Dariusz Kulawik).

Public sector ICT-communication, including private networks and public part of governmental and state networks became our daily appliances. The security of the network, security of using it and it's deployment to secure our lives are taken for granted.

The real, concrete analysis of threats, which are placed in the actual political, economical and social situation, can be elaborated only in a close collaboration of the national security institutions, state regulators, national forces, manufacturers and ICT-networks operators.

A taxonomy and examples of threats may be found in papers by Krystian Baniak and Andrzej Machnacz. Krystian Baniak, Andrzej Wisz, Dariusz Bogusz, Dariusz Kulawik agree on human factor as one of the major risks in ICT-communication.

ICT-communication play a particular role as a part of the so called Critical Infrastructure. Critical Infrastructure (CI) defined as a key factor in sustaining the operation of the country in regular situation (Jacke Matyszczak) and under emergency conditions, can not be treated only locally: it is equally crucial to pan European security. Poland joints the works on implementation of the relevant EPCIP directive (Krystian Baniak). Andrzej Machnacz and Andrzej Wisz identify the corresponding assets of the ministry of internal

affairs and state administration MSWiA and national forces. They assign the security attributes of confidentiality, integrity, accessability and accountability to specific assets and evaluate the threats from this perspective.

Andrzej Machnacz analysed and justified the differentiating priorities between the ICT-communication assets and their attributes. This allows for better and more precise analysis of threats, requirements and countermeasures.

The specific technological requirements put on the military ICT-communication may be found in Robert Goniacz. Military ICT-communication shall as well secure the integrity of Poland as well as the fullest compatibility within the NATO ICT-communication networks. Economy and the powerful reality of the public networks and military relevant data available in those networks are the challenges, named by Robert Goniacz.

Countermeasures against threats may be taken on different levels: physical and environmental (Andrzej Machnacz, Dariusz Kulawik), technological (Zdzislaw Drzycimski, Andrzej Machnacz) and procedural (Andrzej Machnacz, Dariusz Bogusz, Dariusz Kulawik).

The omni present interaction in papers of each author of public networks, critical infrastructure, interoperability of networks, national and international issues, threats and countermeasures with regards to the relevant ICT-communication assets point at the necessity of improved regulations and standards in this area.

Only then the dedicated projects in public domain, critical infrastructure or special areas will provide the necessary level of the national security at affordable and justified cost.

I would like to thank again all members of the team, listed in the introduction for their contributions and in particular to all authors, who despite their enormous workload and high responsibility on most prominent positions, express their readiness and accepted the additional work of timely preparation of that study. Truly strong, highly competent and dedicated to the national security team.

Bogdan Lent
Warsaw, 23rd of July 2007