Komponenty systemu bezpieczeństwa państwa i ich koordynacja

*dokumenty typu non paper*

Słusznym jest powiedzenie, że państwo o tyle jedynie może uważać się za bezpieczne, o ile każdy z kluczowych elementów systemu bezpieczeństwa państwa działa, a wszystkie są odpowiednio skoordynowane. Warto więc wymienić poszczególne systemy:

1. **System szybkiego, lokalnego reagowania na sytuacje kryzysowe:**
2. Obrona Cywilna (OC) – bardzo istotny element „szybkiego reagowania”. W wielu wypadkach kluczowy dla możliwości ograniczenia strat w pierwszych chwilach po momencie wystąpienia zdarzenia. Obecnie w Polsce w dużej mierze ograniczający się do Ochotniczej Straży Pożarnej, która – choć wykonuje niesamowitą pracę – jest niewystarczająca. Należy wrócić do szerokiego włączenia społeczności lokalnych w system obrony cywilnej. Początkiem tego procesu jest trwająca obecnie budowa Wojsk Obrony Terytorialnej, które angażują się w sytuacje kryzysowe. Jednak co do zasady OT pełni funkcję odrębną do OC i jest czym innym.
3. Wojska Obrony Terytorialnej – obecnie dobrze opisane, z dużą determinacją i dobrze tworzone, nie ma potrzeby poświęcania im w tym miejscu więcej uwagi.
4. Wojska Logistyczne – oprócz zaangażowania w operacje stricte wojskowe, wspierające społeczności lokalne w sytuacjach poważnych kryzysów dzięki posiadaniu odpowiedniego sprzętu i wyszkolenia. Jednocześnie kluczowe dla skuteczności operacji wojskowej.

Należy zaznaczyć, że opisane powyżej komponenty, które w okresie komunizmu funkcjonowały w określony, zorganizowany i skoordynowany przez państwo sposób (niezależnie od negatywnej oceny samego okresu oraz tego, że ówczesny sposób organizacji był wadliwy) po 1989 roku przez 25 lat pogrążały się w coraz głębszym kryzysie i są obecnie w głęboko niezadowalającym stanie pod względem sprzętu, wyszkolenia, organizacji, koordynacji, liczebności, rozlokowania itd.

1. **Infrastruktura krytyczna i strategiczna**
2. Infrastruktura krytyczna i strategiczna – jest w bardzo złym stanie technicznym. Jednocześnie najczęściej (np. schrony) w miejscach w pełni rozpoznanych przez potencjalnych nieprzyjaciół. Wymaga kompleksowej przebudowy.
3. Służby – nie wchodząc w „twardsze” zagadnienia kontrwywiadowcze: służby nie wypełniają swojej roli względem infrastruktury krytycznej i strategicznej. Tzw. załączniki antyterrorystyczne tworzone przez ABW do planów ochrony obiektów są dokumentami fikcyjnymi, ponieważ zajmują się zagrożeniami na poziomie lat 70 i 80: przesyłane pocztą paczki z bombą, ataki uwzględniające wzięcie zakładników. Nie ma tam uwzględnienia zagrożeń cybernetycznych, nie ma uwzględnienia sabotażowych zagrożeń typu hybrydowego (nastawionych na zniszczenie / unieruchomienie infrastruktury w sposób, w którym można się wyprzeć odpowiedzialności, a nie na branie zakładników) – czyli zagrożeń, których istotność od roku 2000 nieustannie wzrasta. Sam sposób oceny zagrożenia dla poszczególnych elementów infrastruktury jest oderwany od rzeczywistości i nie obrazuje prawdziwego poziomu zagrożenia. Jest to związane m.in. z przestarzałością przepisów prawa regulujących działania służb oraz np. ustawy o ochronie informacji niejawnych.
4. Kluczowe spółki infrastruktury strategicznej – posiadają zróżnicowany poziom bezpieczeństwa, niektóre bardzo wysoki. Przy braku adekwatnego wsparcia ze strony państwa i służb funkcjonują w tym obszarze samodzielnie. Spółki nie mają więc poziomu ochrony, który wymagałby wsparcia i koordynacji, a państwo nie korzysta w odpowiedni sposób np. z informacji i doświadczeń zbieranych w obszarze zagrożeń cybernetycznych. Co do zasady, luki w systemach bezpieczeństwa spółek są bardzo duże.

Obszar infrastruktury jest podobnie zaniedbany, co opisany wcześniej system szybkiego lokalnego reagowania. Biorąc pod uwagę jedyne słuszne założenie w przypadku systemów bezpieczeństwa, zwłaszcza w obliczu zagrożeń sabotażowych – że system jest tak dobry jak jego najsłabsze ogniwo – należy uznać, że polski system infrastrukturalny w tym zakresie jest dziurawy, wystawiony na zagrożenia, przed którymi nie jest zabezpieczony i w wypadku prawdziwego testu – nie zda egzaminu.

1. **Przemysł obronny:**

Sensem posiadania własnego przemysłu obronnego, z punktu widzenia obronności a nie ekonomii, jest posiadanie takich zdolności przemysłowych, które zwiększają potencjał militarny zdolności do samodzielnej obrony kraju i są np. skalowalne w przypadku narastającego napięcia (np. produkujemy 500 dronów uderzeniowych rocznie, głównie na eksport, ale w przypadku wzrostu poziomu zagrożenia jesteśmy szybko w stanie wyprodukować 5000 na własny użytek). Jako przykład takiego działania – tyle, że ze strony agresora – posłużyć może np. hitlerowska aneksja Sudetów w 1938 roku: był tam ulokowany bardzo rozwinięty przemysł, bez którego hitlerowskie Niemcy nie przygotowałyby się w odpowiedni sposób do rozpoczęcia i prowadzenia wojny. Nie trzeba w tym miejscu dodawać, że nie ma obecnie w Polsce takiego systemu planowania zdolności przemysłowo-obronnych, który brałby pod uwagę tą celowość istnienia przemysłu obronnego dla zwiększenia zdolności obronnych państwa.

1. **Obrona cybernetyczna:**

Ulokowanie kwestii cyberbezpieczeństwa w Ministerstwie Cyfryzacji jest niewłaściwe i niezgodne z tym jak ten obszar jest rozwiązany w krajach będących liderem tego obszaru. Działanie takich instytucji jak NASK i Exatel powinno podlegać wraz z RCB bezpośrednio pod KPRM i być koordynowane z działalnością podległych Premierowi (zazwyczaj za pośrednictwem Ministra Koordynatora) służb. Tu wymagane również byłoby zaktualizowanie ustawy o ochronie informacji niejawnych oraz innych przepisów prawa do rzeczywistości cyfrowej, aby koordynacja działań w obszarze cyber była możliwa i miała swój jasny cel i sens.

Obszar cybernetyczny, jak wiadomo, zazębia się ze wszystkimi pozostałymi (można mówić o cybernetycznej obronie cywilnej i terytorialnej, cybernetycznej ochronie infrastruktury, zdolnościach przemysłu obronnego w obszarze cyber, wojskach cybernetycznych). Tylko prowadzony w taki, skoordynowany sposób, może być skuteczny.

1. **Policja, Straż Graniczna, Straż Pożarna**

W dobie zagrożeń hybrydowych (sabotażowych; poniżej progu wojny) koordynacja działania tych instytucji z pozostałymi elementami systemu staje się kluczowe. W prawidłowo funkcjonującym systemie plan ochrony elementu infrastruktury strategicznej jest skoordynowany z tym, w jakiej odległości jest najbliższy posterunek pozostających w gotowości antyterrorystów, jakiej pomocy można się spodziewać od rozlokowanej nieopodal straży granicznej, ile jednostek straży pożarnej jest dedykowanych i odpowiednio wyposażonych, i rozlokowanych do odpowiedzi na potencjalny kryzys. W Polsce odgórne procedury koordynacyjne w przepisach prawa są na poziomie kompletnie nieadekwatnym do zagrożeń. Koordynacja pomiędzy np. spółką właścicielem infrastruktury, a Policją, SG, władzami lokalnymi czy strażą pożarną zależy od dobrej woli stron na poziomie lokalnym. Skutkuje to w większości przypadków bardzo niskim poziomem odporności na potencjalne zagrożenia.

1. **Siły zbrojne:**

Obszar najbardziej „silosowo” oddzielony od pozostałych. Jednak w dobie zagrożeń hybrydowych, które nie skutkują pełnoskalową operacją obronną, bardzo zazębiający się z pozostałymi, i musi być z nimi koordynowany. Kwestie rozlokowania schronów, ich jakości, rozlokowania magazynów broni, wojsk logistycznych i ich sprzętu itd. – stają się kluczowe dla tych typów sytuacji kryzysowych, które nie wiążą się z rozpoczęciem pełnoskalowej operacji obronnej.