IX KONFERENCJA „WOLNOŚĆ I BEZPIECZEŃSTWO”, WROCŁAW, 19 -21 WRZEŚNIA 2012 R.

Opis przedsięwzięcia

Mistrzostwa Europy w piłce nożnej EURO 2012, które odbędą się w Polsce i na Ukrainie w czerwcu 2012, staną się znakomitą okazją do obserwacji jak działa nasz system zarządzania kryzysowego, zwłaszcza na tle XXX Letnich Igrzysk Olimpijskich w Londynie.

Czy wszystkie służby poradziły sobie z zadaniem? Jakie incydenty wydarzyły się podczas zawodów i czy wpłynęły na stopień bezpieczeństwa publicznego? Czy przygotowywane mozolnie systemy wsparcia teleinformatycznego spełniły swoją funkcję? Jakie wnioski płyną na przyszłość? Co nowego należy wprowadzić do systemu bezpieczeństwa pozamilitarnego po EURO 2012 zarówno od strony politycznej i organizacyjnej, ale również od strony zabezpieczenia teleinformatycznego?

Pochylimy się zarazem nad miejscem i rolą teleinformatyki na współczesnym polu walki, zastanowimy czym w rzeczywistości jest koncepcja wojny sieciocentrycznej, jakie jest miejsce na wojnie i w reagowaniu kryzysowym dla robotów – dronów.

Taka debata z udziałem specjalistów ds. bezpieczeństwa publicznego to możliwość przeprowadzenia krajowych ćwiczeń z ochrony infrastruktury krytycznej przed atakiem z cyberprzestrzeni. Ustawa z 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw wprowadziła pojęcie cyberprzestrzeni do polskiego porządku prawnego. Jeżeli Prezydent RP uzna, że np. atak cybernetyczny na system zarządzania siecią energetyczną zagraża bezpieczeństwu państwa, ma prawo wprowadzić jeden z stanów nadzwyczajnych (w zależności od okoliczności: stan klęski żywiołowej, stan wyjątkowy lub stan wojenny).

„Ustawa stwarza podstawy prawne do praktycznego uruchomienia prac planistycznych i organizacyjnych przez wszystkie organy władzy i administracji w zakresie uwzględniania w planach operacyjnych i programach przygotowań obronnych z jednej strony możliwych nowych zagrożeń w postaci cyberzagrożeń oraz z drugiej – wykorzystywania cyberprzestrzeni we własnych działaniach i systemach bezpieczeństwa na

wszystkich szczeblach funkcjonowania państwa" – czytamy w komentarzu na stronach Biura Bezpieczeństwa Narodowego.

Ćwiczenia z ochrony infrastruktury krytycznej przed atakiem z cyberprzestrzeni i z reagowania kryzysowego post factum, pozwoliłyby sprawdzić jak ta ustawa ma zadziałać w praktyce, czy służby zarządzania kryzysowego, których wysiłek skupia się na minimalizacji klasycznych zagrożeń np. podczas EURO 2012, są w stanie interweniować po ataku z cyberprzestrzeni; jak wyglądałaby współpraca w ramach krajowych instytucji, organizacji i firm sektora publicznego i prywatnego przed i w trakcie takiego ataku; wreszcie ćwiczenia umożliwiłyby koordynację działań specjalistów od bezpieczeństwa teleinformatycznego z klasycznymi służbami zarządzania kryzysowego i bezpieczeństwa narodowego jak Straż Pożarna, Policja, Straż Miejska, Straż Graniczna, Wojsko Polskie i instytucje sojusznicze.

Przebieg konferencji

Formuła konferencji, która jest główną imprezą Roku Ochrony Cyberprzestrzeni Krytycznej ROCK 2012, pozwala na opracowanie i przedyskutowanie zawczasu realnego planu ćwiczeń ochrony cyberprzestrzeni. Zajmuje się tym konwersatorium „Pięć żywiołów", które pełni zarazem zaszczytną funkcję Rady Programowej konferencji.

Jednocześnie nasi eksperci obserwują przygotowania do EURO 2012, następnie zaś skupią się na analizie stanu bezpieczeństwa podczas samej imprezy.

W rezultacie pierwszego dnia wrocławskiej konferencji zajmiemy się EURO 2012 i implikacjami na przyszłość, jednocześnie już rozpoczynając międzynarodowe ćwiczenia z ochrony cyberprzestrzeni. Najprawdopodobniej postawimy na symulację ataków na obiekty teleinformatycznej infrastruktury krytycznej. Regulamin ćwiczeń zostanie opracowany przez uczestników konwersatorium. Główne zadanie to z jednej strony podniesienie w stan gotowości bojowej całego systemu zarządzania kryzysowego, zaś z drugiej - opracowanie przesłanek, które pozwoliłyby Prezydentowi RP do ogłoszenia jednego ze stanów nadzwyczajnych.

Na bazie dyskusji o EURO 2012 oraz doświadczeń z ćwiczeń przygotowano by dwa oddzielne raporty (szczegółowe do wewnętrznych analiz oraz ogólne – dostępne publicznie). Notabene jesteśmy przekonani o konieczności przygotowania tzw. raportu otwarcia, pokazującego obecny cyberbezpieczeństwa i stanu ochrony infrastruktury krytycznej.

Zagadnienia

- Bezpieczeństwo w energetyce, telekomunikacji i sektorze bankowym – ochrony infrastruktury krytycznej
- Zarządzanie ryzykiem w instytucjach publicznych i gestorach infrastruktury krytycznej
- Ochrona infrastruktury krytycznej podczas imprez masowych
- Łączność specjalna
- Jak zadziałał nasz system zarządzania kryzysowego podczas EURO 2012?
- Czy wszystkie służby poradziły sobie z zadaniem?
- Jakie incydenty wydarzyły się podczas zawodów i czy wpłynęły na stopień bezpieczeństwa publicznego?
- Czy przygotowywane mozolnie systemy wsparcia teleinformatycznego spełniły swoją funkcję?
- Jakie wnioski płyną na przyszłość?
- Co nowego należy wprowadzić do systemu bezpieczeństwa pozamilitarnego po EURO 2012 zarówno od strony politycznej i organizacyjnej, ale również od strony zabezpieczenia teleinformatycznego?
- Wojny dronów – teleinformatyka na współczesnym polu walki i w działaniach antyterrorystycznych
- Systemy wczesnego ostrzegania przed niebezpieczeństwem
- Ćwiczenia z ochrony cyberprzestrzeni

Uczestnicy

Konferencja o charakterze międzynarodowym dla wszystkich osób zainteresowanych tematyką bezpieczeństwa i zarządzania kryzysowego ze szczególnym uwzględnieniem instytucji zabezpieczających EURO 2012 oraz zajmujących się bezpieczeństwem teleinformatycznym.

Poza tym zapraszamy przedstawicieli administracji samorządowej i rządowej, funkcjonariuszy Straży Granicznej, Służby Celnej, Policji, Wojska Polskiego, Straży Miejskiej i Państwowej Straży Pożarnej, posłów, senatorów i radnych, pełnomocników ochrony informacji niejawnych i pełnomocników bezpieczeństwa, firm zajmujących się ochroną fizyczną, specjalistów od zarządzania kryzysowego, ochrony infrastruktury krytycznej i bezpieczeństwa teleinformatycznego; łącznie ok. 200 osób.