HORYZONTY BEZPIECZEŃSTWA

UNIWERSYTET OPOLSKI

Opole

Nr 8(3) 2017

ISSN 2543-6090

HORYZONTY BEZPIECZEŃSTWA

Nr 8 (3) 2017

---

pod redakcją

Tomasza Dukiewicza

Opole 2017

Wydział Prawa i Administracji

ISSN 2543-6090

Wersją pierwotną czasopisma jest wersja elektroniczna

Contents

Mariusz Czyżak[1]

Legal protection of the state's cyberspace

Abstract

Cyberspace is a virtual component of the space, in which the country performs its jurisdiction. It is shaped by the nature of physical phenomena used in the teleinformatics and the structure of IT systems. It constitutes a source of threats directed against an entity and the state whose elimination is facilitated by legal regulations concerning in particular the rules for introducing the states of emergency, crisis management as well as prevention of various forms of cybercrime, including those directed against armed forces and terrorist cybercrime

Key words: ***cyberspace, legal protection, state***

1. Uwagi wstępne

Pojęcie *cyberprzestrzeni* stanowi od dosyć dawna przedmiot zainteresowania doktryny nauk o bezpieczeństwie oraz doktryny nauk prawnych. Na trwałe zagościło również na gruncie przepisów powszechnie obowiązującego prawa oraz różnego rodzaju dokumentów o charakterze doktrynalno-strategicznym opracowywanych przez instytucje publiczne odpowiedzialne za wykonywanie zadań z zakresu obrony narodowej, bezpieczeństwa powszechnego i porządku publicznego. Mając na względzie jej status prawny wynikający z treści aktów normatywnych oraz wagę, jaką tak ustawodawca, jak i organy władzy publicznej, przywiązują do jej ochrony, pokusić można się o sformułowanie poglądu, że stanowi ona na tyle integralną część struktury państwa, jakkolwiek nie w pełni materialnej natury, iż podlega ochronie prawnej na równi z innymi jego atrybutami.

[1] Dr Mariusz Czyżak, Urząd Komunikacji Elektronicznej Warszawa, dyrektor generalny

2. Pojęcie cyberprzestrzeni i jej „granice"

Rozpocząć wypada zatem od przybliżenia istoty i cech *cyberprzestrzeni*. Obszernego przeglądu definicji pojęcia *cyberprzestrzeń* dokonał Janusz Wasilewski, podsumowując swe rozważania w sposób następujący: *(...) cyberprzestrzeń to nie tylko suma fizycznych składników – systemów, sieci, oprogramowania oraz przetwarzanych w nich informacji. To nie proste odwołanie do Internetu – choć niewątpliwie to właśnie Internet jest obecnie ilościowo najistotniejszym składnikiem cyberprzestrzeni, mieszczącym się w każdej omawianej definicji oraz będącym wymienianym wprost w części z nich. Cyberprzestrzeń to również nie suma operacji wykonywanych przez użytkowników w sieciach. Istotę cyberprzestrzeni tworzy koncepcja powołania do życia swojego rodzaju równoległego środowiska, które jest nowym wymiarem dla ludzkich działań. Wymiar ten, z uwagi na sposób budowy, jest jednak obszarem wymykającym się opisowi za pomocą typowych, fizycznych miar, nie poddaje się zatem prostemu podziałowi geograficznemu pomiędzy państwa. Cyberprzestrzeń – z uwagi na swoją budowę – ma swoistą fizykę, w której zamiast atomów, istnieją bity, środowisko naturalne zaś jest zastąpione środowiskiem programowym. Cyfrowy zapis danych to nie tylko sposób odzwierciedlania dóbr prawnych użytkowników cyberprzestrzeni, ale także wyłączny budulec dla niektórych z nich, nieistniejących w ogóle w innej postaci – np. informacji przetwarzanych wyłącznie w sieciach komputerowych. (...) O ile intuicyjne uchwycenie szczególnych cech cyberprzestrzeni nie wydaje się nastręczać zbyt wielu problemów, o tyle z punktu widzenia funkcjonowania organów administracji publicznej, szczególnie organów wymiaru sprawiedliwości, jakiekolwiek działania podejmowane w cyberprzestrzeni muszą być poddawane kwalifikacjom prawnym jako czynności znane prawu oraz przez to prawo dopuszczalne.*[2]. Przywołać wypada również katalog cech cyberprzestrzeni wskazany przez Tomasza r. Aleksandrowicza, tj. niezależność od miejsca, odległości, czasu i granic, względna anonimowość oraz możliwość ustalenia sprzętu, a nie osoby operującej w cyberprzestrzeni[3].

Jak przedstawia się zatem definicja legalna cyberprzestrzeni sformułowana przez polskiego ustawodawcę? W myśl postanowień art. 2 ust. 1b ustawy z 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyj-

[2] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, Przegląd Bezpieczeństwa Wewnętrznego 2013, Nr 9, s. 233-234.

[3] T. r. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, Przegląd Bezpieczeństwa Wewnętrznego 2016, Nr 15, s. 12.

nym organom Rzeczypospolitej Polskiej[4] (dalej: *u.s.w.k.N.D.S.Z.*), rozumie się przez nią bowiem *przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne*. Systemy teleinformatyczne to, mając na względzie odesłanie do treści przepisu art. 3 pkt 3 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[5], zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego. W świetle art. 2 pkt 42, 43 i 46 ustawy z 16 lipca 2004 r. Prawo telekomunikacyjne[6], telekomunikacyjne urządzenie końcowe to *urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci", zaś samo urządzenie telekomunikacyjne to „urządzenie elektryczne lub elektroniczne przeznaczone do zapewniania telekomunikacji", czyli do zapewnienia „nadawania, odbioru lub transmisji informacji, niezależnie od ich rodzaju, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną.*

Cyberprzestrzeń ma zatem w świetle definicji sformułowanych przez doktrynę nauk o bezpieczeństwie, a także na gruncie przepisów prawa, co prawda charakter przestrzeni wirtualnej służącej komunikowaniu się, a nie zmaterializowanej przestrzeni fizycznej, ale jej istnienie i wykorzystywanie jako obszaru wymiany informacji uzależnione jest przecież od istnienia urządzeń technicznych o charakterze fizycznym, zlokalizowanych w określonym miejscu, na terytorium określonego kraju, obsługiwanych przez istniejące w rzeczywistości osoby będące obywatelami konkretnego państwa. Co więcej, skoro inicjujące powstanie i istnienie cyberprzestrzeni urządzenia techniczne zostaną pozbawione obsługi oraz energii podtrzymującej ich pracę, tym samym cyberprzestrzeń rozumiana jako wymiar wirtualny przestanie istnieć, nawet wówczas, gdy obecne będzie środowisko fizyczne służące wymianie informacji, np. widmo radiowe. Pewnego rodzaju punkty graniczne w cyberprzestrzeni wyznaczają chociażby *routery* służące do łączenia określonych sieci komputerowych i *firewalle* tj. zapory sieciowe służące filtrowaniu danych przychodzących do komputera i wychodzących z komputera za pośrednictwem sieci lub Internetu. Mając na względzie posiadaną funkcjonalność wskazane powyżej elementy sieci komputerowych wytyczają w konsekwencji granice pomiędzy siecią lokalną a Internetem lub pomiędzy poszczególnymi

[4] Tekst jedn. Dz.U. z 2016 r., poz. 851, ze zm.
[5] Tekst jedn. Dz.U. z 2014 r., poz. 1114, ze zm.
[6] Tekst jedn. Dz.U. z 2016 r., poz. 1489, ze zm.

sieciami lokalnymi, a nawet wyizolowanymi elementami sieci lokalnej.

3. Cyberprzestrzeń jako element składowy państwa

Czym jest samo państwo i czy cyberprzestrzeń jest jego częścią składową? Przywołać tutaj należy definicję odzwierciedlającą klasyczne postrzeganie instytucji państwa, w myśl której jest ono *wielką społeczną grupą, sformalizowaną, wyposażoną w organy władztwa publicznego i opartą na sformalizowanym członkostwie (obywatelstwo). Jest ono organizacją społeczeństwa z tego względu, że obejmuje całą ludność zamieszkałą na danym terytorium*[7].

W tradycyjnym ujęciu pojęcie terytorium państwa obejmuje natomiast *obszar ziemi wraz z wodami śródlądowymi, przyległy pas wód morskich oraz przestrzeń powietrzną nad obszarem lądowym i morskim państwa aż do strefy przestrzeni kosmicznej*[8]. Analogicznie traktuje pojęcie terytorium ustawodawca, chociażby przy okazji uregulowania materii ochrony granic państwa. Zgodnie z art. 6 ustawy z 12 października 1990 r. o ochronie granicy państwowej[9], *Rzeczpospolita Polska wykonuje swoje zwierzchnictwo nad terytorium lądowym oraz wnętrzem ziemi znajdującym się pod nim, morskimi wodami wewnętrznymi i morzem terytorialnym oraz dnem i wnętrzem ziemi znajdującymi się pod nimi, a także w przestrzeni powietrznej znajdującej się nad terytorium lądowym, morskimi wodami wewnętrznymi i morzem terytorialnym..*

Jak podejść należy zatem do zagadnienia władztwa państwowego nad cyberprzestrzenią, która na trwałe zadomowiła się nie tylko w świadomości użytkowników narzędzi teleinformatycznych (w tym i instytucji publicznych), ale również na gruncie obowiązującego ustawodawstwa i podlega równocześnie w pewnej mierze ochronie prawnej? Czy przez sam fakt nadania cyberprzestrzeni statusu pojęcia prawnego pozostającego w swoistej relacji z instytucją państwa, nie uczynił z niej ustawodawca swego rodzaju elementu tego państwa? Jest ona z pewnością pewnego rodzaju kategorią przestrzeni. Sama przestrzeń ma przy tym również swoje znaczenie potoczne i może być traktowana jako: *nieograniczony obszar trójwymiarowy*, *zamknięta, ograniczona część tego obszaru*, *pusta, rozległa powierzchnia bez wyraźnie oznaczonych, widocznych granic* lub *odległość między czymś a czymś*[10]. Terytorium zaś to m.in. *teren wyodrębniony ze względu na cechy charakterystyczne*[11].

[7] T. Stawecki, P. Winczorek, *Wstęp do prawoznawstwa*, Warszawa 1999, s. 31.
[8] Ibidem, s. 34.
[9] Tekst jedn. Dz.U. z 2015 r., poz. 930, ze zm.
[10] *Słownik języka polskiego PWN* (red. E. Sobol), PWN, Warszawa 2006, s. 77.
[11] Ibidem, s. 1038.

Cyberprzestrzeń określić można zatem mianem swoistego komponentu przestrzeni państwa, w której – analogicznie jak na lądzie, wodzie i w powietrzu – państwo sprawuje swoje funkcje, o ile wspomnianą cyberprzestrzeń tworzą systemy teleinformatyczne podlegające jurysdykcji tego państwa z racji na ich rozmieszczenie na terytorium tego państwa lub chociażby fakt, iż stanowią jego własność pozostająca w dyspozycji organów władzy publicznej. Dodać trzeba, że w świetle *Doktryny cyberbezpieczeństwa Rzeczypospolitej Polskiej* z 22 stycznia 2015 r., cyberprzestrzeń RP opisana została jako *cyberprzestrzeń w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji)*[12].

4. Zagrożenia wypływające z cyberprzestrzeni

W myśl postanowień art. 5 Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 r.[13] (dalej: *Konstytucja RP*), *Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju.*. Przepis art. 5 Konstytucji RP wyznacza zatem funkcje państwa, tj. „zasadnicze kierunki i cele jego działania", które determinują z kolei konkretne kompetencje i zadania poszczególnych organów władzy publicznej. Kluczową spośród tych funkcji jest strzeżenie niepodległości i nienaruszalności terytorium państwa, ponieważ dopiero w następstwie jej realizacji możliwe staje sie wykonywanie kolejnych funkcji państwa, w szczególności zapewnienia przestrzegania wolności i praw człowieka i obywatela, a także zapewnienia mu należytego bezpieczeństwa[14], w tym i zagwarantowania odpowiedniego poziomu bezpieczeństwa w cyberprzestrzeni, z której tak instytucje publiczne, komercyjne podmioty korporacyjne, jak i jednostki korzystają.

Zagrożenia pochodzące z cyberprzestrzeni, a adresowane odpowiednio do instytucji państwowych, przedsiębiorców i człowieka przybierają różnoraką postać. Na płaszczyźnie militarnej działalności państwa, ukazuje się cyberprzestrzeń jako piąty (obok lądu, wody, powietrza i przestrzeni kosmicznej)

[12] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, s. 7.
[13] Dz.U. Nr 78, poz. 483, ze zm.
[14] W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, LEX, 2013, komentarz do art. 5 Konstytucji RP.

wymiar prowadzenia działań wojennych[15], ale stanowi także źródło cyberprzestępczości i cyberterroryzmu, których obowiązek zwalczania spoczywa na organach władzy publicznej. Dla podmiotów wykorzystujących w swojej działalności gospodarczej technologie teleinformatyczne zagrożenia tego rodzaju generują dodatkowe koszty związane z przeciwdziałaniem szeroko rozumianej przestępczości komputerowej, przybierającej w szczególności postać – ataków komputerowych, niszczenia danych i programów komputerowych, sabotażu i szantażu komputerowego, włamań do systemów informatycznych, szpiegostwa komputerowego, itp[16].

Zjawisko cyberprzestępczości odznacza się m.in. tym, że: narzędzia teleinformatyczne służyć mogą zarówno popełnianiu przestępstw tradycyjnych (np. oszustwo), jak i tych, które zaistniały wraz z pojawieniem się cyberprzestrzeni; czynnościom technicznym służącym ich popełnianiu towarzyszy równocześnie zastosowanie metod socjotechnicznych; systemy i sieci teleinformatyczne mogą być tak narzędziem, jak i celem działania sprawców; zaistnienie cyberprzestrzeni skutkuje powstaniem nowego środowiska działalności przestępczej, a w konsekwencji zmiana postrzegania dóbr podlegających ochronie prawnej (cyberatak skierowany jest równocześnie przeciwko wielu dobrom społecznie istotnym – np. bezpieczeństwu systemów, bezpieczeństwu danych i mieniu); skutek przestępny stanowić może zarówno konsekwencje działania człowieka, jak i zautomatyzowanego narzędzia teleinformatycznego; ściganie cyberprzestępstw wymaga zastosowania czynności technicznych[17].

Jeszcze inaczej rzecz się przedstawia w przypadku oddziaływania cyberprzestrzeni na jednostkę, nie zawsze sprowadzając się do działań podlegających reakcji prawnokarnej, ale również dolegliwych społecznie. Andrzej Pieczywok wyodrębnia trafnie wśród zagrożeń egzystencjalnych związanych z cyberprzestrzenią, a wymierzonych w człowieka m.in.: zagrożenia edukacyjne, skutkujące wręcz biologicznymi zmianami neurologicznymi, ograniczeniem kreatywności i zaburzeniami emocjonalnymi; zagrożenia osobowościowe, powiązane z kształtowaniem fałszywego obrazu innych w oczach użytkownika Internetu (np. uprzedmiotowienie człowieka), powstawaniem niewłaściwych relacji pomiędzy człowiekiem a maszyną, nowymi formami tradycyjnych patologii i dysfunkcji oraz marginalizacją rodziny; zagrożenia społeczne, stanowiące konsekwencję braku zachowania równowagi pomię-

[15] J. Dereń, A. Rabiak, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni* (w:) *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku* (red. M. Górka), Difin, Warszawa 2014, s. 206-210.

[16] M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, CeDeWu Sp. z o.o., Warszawa 2016, s. 127 i n.

[17] J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, Przegląd Bezpieczeństwa Wewnętrznego 2016, Nr 15, s. 171-172.

dzy rozwojem sfery mentalności człowieka i wszechotaczającym go rozwojem technologicznym, konsumpcjonizmu, kryzysu kultury wysokiej, itp.[18]

5. Reakcja na zagrożenia w cyberprzestrzeni i ich zwalczanie

Mając na względzie różnorodność i złożoność zjawisk towarzyszących cyberprzestrzeni ustawodawca odnosi się na gruncie wielu aktów normatywnych do zagrożeń z niej wypływających bądź stanowiących nieodłączny element jej wykorzystywania.

W pierwszej kolejności wypada dokonać pobieżnego przeglądu postanowień ustawodawstwa dotyczącego stanów nadzwyczajnych odnoszących się do zagrożeń wynikających z cyberprzestrzeni. Zewnętrzne zagrożenie państwa spowodowane w szczególności *działaniami w cyberprzestrzeni* stanowi przesłankę wprowadzenia stanu wojennego (art. 2 u.s.w.k.N.D.S.Z.). Działania w cyberprzestrzeni powodujące szczególne zagrożenie konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego stanowią również powód dla wprowadzenia stanu wyjątkowego (art. 2 ust. 1 z dnia 21 czerwca 2002 r. o stanie wyjątkowym[19]). Stan klęski żywiołowej to natomiast stan nadzwyczajny, który może zostać wprowadzony dla zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej, jak również w celu ich usunięcia, przy czym zjawiska te mogą wywołać również zdarzenia w cyberprzestrzeni (art. 2 i 3 ust. 2 ustawy z 18 kwietnia 2002 r. o stanie klęski żywiołowej[20]).

W świetle ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym[21] (dalej: *u.z.k.*) zarządzanie kryzysowe rozumiane jako *działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej* (art. 2 u.z.k.), odnosi się do infrastruktury krytycznej, na którą składają się systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty (obiekty budowlane, urządzenia, instalacje), usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

[18] A. Pieczywok, *Cyberprzestrzeń a zagrożenia egzystencji człowieka* (w:) *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku* ..., s. 118-129.

[19] Tekst jedn. Dz.U. z 2016 r., poz. 886, ze zm.

[20] Tekst jedn. Dz.U. z 2014 r., poz. 333, ze zm.

[21] Tekst jedn. Dz.U. z 2017 r., poz. 209.

Obejmuje ona przy tym systemy: zaopatrzenia w energię, surowce energetyczne i paliwa; łączności; sieci teleinformatycznych; finansowe; zaopatrzenia w żywność; zaopatrzenia w wodę; ochrony zdrowia; transportowe; ratownicze; zapewniające ciągłość działania administracji publicznej; produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych (art. 3 u.z.k.), a zatem zarówno systemy teleinformatyczne w ścisłym tego słowa znaczeniu, jak i te elementy infrastruktury technicznej, których funkcjonowania w chwili obecnej nie sposób sobie wyobrazić bez zarządzania nimi za pośrednictwem systemów teleinformatycznych.

Wspomnieć należy również o ochronie prawnokarnej w sferze cyberprzestrzeni. Poza wymienianymi często tzw. *przestępstwami komputerowymi*, umieszczonymi w rozdziale XXXIII k.k. ustawy z dnia 6 czerwca 1997 r. - Kodeks karny[22] (dalej: k.k.), zatytułowanym skądinąd *Przestępstwa przeciwko ochronie informacji* (np. sabotaż komputerowy), czy też czynu zabronionego, o którym mowa w przepisie art. 165 § 1 pkt 4 k.k., którego istotą jest sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach, o ile dojdzie do niego przez zakłócenie, uniemożliwienie, lub wpływanie w inny sposób na automatyczne przetwarzanie, gromadzenie bądź przekazywanie danych informatycznych[23], zwrócić należy uwagę na przepis art. 140 k.k. Poddano w nim bowiem penalizacji dopuszczenie się gwałtownego zamachu na jednostkę Sił Zbrojnych Rzeczypospolitej Polskiej, niszczenie lub uszkadzanie obiektu albo urządzenie o znaczeniu obronnym, w celu osłabienia mocy obronnej Rzeczypospolitej Polskiej, które podlega karze pozbawienia wolności od roku do lat 10. Jeśli następstwem tego czynu jest śmierć człowieka lub ciężki uszczerbek na zdrowiu wielu osób, sprawca podlega karze pozbawienia wolności od lat 2 do 12, zaś jeśli sprawca czyni przygotowania do takiego przestępstwa, podlega karze pozbawienia wolności do lat 3. Dla wyjaśnienia dodać trzeba, że zgodnie z przepisem § 2 pkt 9 rozporządzenia Rady Ministrów z 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony[24], do obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa zalicza również obiekty infrastruktury łączności, w tym m.in. obiekty przedsiębiorców telekomunikacyjnych, przeznaczone do realizacji zadań na rzecz bezpieczeństwa i obronności państwa.

[22] Tekst jedn. Dz.U. z 2016 r., poz. 1137, ze zm.

[23] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem* [w:] *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna* (red. A. Podraza, P. Potakowski, K. Wiak), Difin, Warszawa 2013, s. 155.

[24] Dz.U. z 2003 r. Nr 116, poz. 1090, ze zm.

Sam zamach na jednostkę wojskową przybierać może natomiast również postać tzw. *cyberataku*.

Ze względu na istniejący współcześnie poziom zagrożeń o charakterze cyberterrorystycznym przywołać w tym miejscu należy także ustawę z 10 czerwca 2016 r. o działaniach antyterrorystycznych[25] (dalej: u.dz.a.), która określa zasady prowadzenia działań antyterrorystycznych, w tym w cyberprzestrzeni, oraz współpracy między organami właściwymi w zakresie prowadzenia tych działań (art. 1 u.dz.a.), polegających na *zapobieganiu zdarzeniom o charakterze terrorystycznym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć, reagowaniu w przypadku wystąpienia takich zdarzeń oraz usuwaniu ich skutków, w tym odtwarzaniu zasobów przeznaczonych do reagowania na nie* (art. 2 pkt 1 u.dz.a.). Szef Agencji Bezpieczeństwa Wewnętrznego (dalej: Szef ABW) jest organem odpowiedzialnym za zapobieganie zdarzeniom o charakterze terrorystycznym tj. takim sytuacjom, co do której istnieje podejrzenie, że powstały one na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 k.k. lub zagrożenie zaistnienia takiego czynu (art. 3 w zw. z art. 2 pkt 7 u.dz.a.). W celu realizacji przypisanych w tym zakresie zadań, Szef ABW koordynuje czynności analityczne lub informacyjne, podejmowane przez służby specjalne (art. 5 u.dz.a.). W celu rozpoznawania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym może m.in. zarządzić wobec osoby niebędącej obywatelem polskim, na okres nie dłuższy niż 3 miesiące, niejawne prowadzenie czynności polegających m.in. na: uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych; uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych (art. 9 u.dz.a.). Odrębnej kategoryzacji poddano na gruncie ustawy o działaniach antyterrorystycznych również stopnie alarmowe odnoszące się do zagrożeń terrorystycznych w cyberprzestrzeni. W razie zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, które dotyczyłoby systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej albo w przypadku wystąpienia takiego zdarzenia, może zostać wprowadzony jeden z 4 stopni alarmowych CRP (ALFA-CRP, BRAVO-CRP, CHARLIE-CRP, DELTA-CRP), w zależności

[25] Dz.U. z 2016 r., poz. 904.

od poziomu zagrożenia cyberterrorystycznego (art. 15 u.dz.a.).

6. Uwagi końcowe

W dobie rozwoju technologicznego obejmującego wszystkie sfery życia społecznego i gospodarczego jednostki, jak i struktury organizacyjne oraz działalność państwa, nieodłącznym przedmiotem zainteresowania nauki i ustawodawcy stała się cyberprzestrzeń. Przyczyn takiego stanu rzeczy upatrywać należy zarówno w powszechnym wykorzystaniu komunikacji elektronicznej, jak i potrzebie wypracowania skutecznego mechanizmu ochrony dóbr społecznie istotnych przed *cyberzagrożeniami* godzącymi w suwerenność i nienaruszalność struktur państwa, działalność organów władzy publicznej, działalność gospodarczą, życie i zdrowie człowieka, itd. Wydaje się jednakże, że przyjęcie wyłącznie pojęcia cyberprzestrzeni za punkt wyjścia dla rozważań o pożądanej postaci systemu bezpieczeństwa personalnego i strukturalnego państwa w tym obszarze, jest zabiegiem dosyć ułomnym. Jest ona bowiem jedynie wirtualnym komponentem przestrzeni, w której państwo, przedsiębiorcy i poszczególne jednostki prowadzą działalność za pomocą infrastruktury teleinformatycznej zlokalizowanej w fizycznym komponencie przestrzeni. Podkreślić trzeba przy tym również, że cyberprzestrzeń ma swoje ograniczenia oraz mniej lub bardziej klarowne i trwałe granice zarazem. Ograniczenia wynikają z jednej strony z natury zjawiska elektromagnetyzmu stanowiącego źródło i narzędzie do wymiany informacji, z drugiej zaś z kształtu systemu wchodzącego w skład infrastruktury teleinformatycznej, który może być w mniejszym lub większym stopniu autonomiczny. Pozwalają one w konsekwencji przypisać konkretnemu państwu (a nawet poszczególnym instytucjom publicznym i podmiotom prywatnym posiadającym własne sieci teleinformatyczne) pewną odrębną cyberprzestrzeń podlegającą jego ochronie, tak jak chociażby krajowa administracja łączności jest dysponentem widma radiowego na terytorium danego państwa, gospodarując nim poprzez licencjonowanie przedziałów częstotliwości, uprawnień do używania urządzeń radiowych, kontrolując emisje radiowe, itd.

Bibliografia

1. Aleksandrowicz T. R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, Przegląd Bezpieczeństwa Wewnętrznego 2016, Nr 15.
2. Białkowski M., *Ocena prawna i kryminalistyczna przestępczości komputerowej*, CeDeWu Sp. z o.o., Warszawa 2016.
3. Dereń J., Rabiak A., *NATO a aspekty bezpieczeństwa w cyberprzestrzeni* [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku* (red. M. Górka), Difin, Warszawa 2014.
4. *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015.
5. Pieczywok A., *Cyberprzestrzeń a zagrożenia egzystencji człowieka* [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku* (red. M. Górka), Difin, Warszawa 2014.
6. Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, LEX, 2013, komentarz do art. 5 Konstytucji RP.
7. *Słownik języka polskiego PWN* (red. E. Sobol), PWN, Warszawa 2006.
8. Stawecki T., Winczorek P., *Wstęp do prawoznawstwa*, Warszawa 1999.
9. Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem* [w:] *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna* (red. A. Podraza, P. Potakowski, K. Wiak), Difin, Warszawa 2013.
10. Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, Przegląd Bezpieczeństwa Wewnętrznego 2013, Nr 9, s. 233-234.
11. Wasilewski J., *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, Przegląd Bezpieczeństwa Wewnętrznego 2016, Nr 15, s. 171-172.

Dominika Kosárová, M.A.[1]

Information warfare and the contemporary security environment[2]

Abstract

Contemporary security environment is influenced by massive informatization of the society where information becomes a powerful instrument with the capacity to influence public opinion. This leads states to use information as a strategic weapon to enforce their national and foreign policy objectives by means of propaganda and manipulation with people's perceptions.

The aim of this article is to evaluate nowadays security environment in terms of information operations with a particular focus on the European and Slovak context. The major player within the European and Slovak information space is the Russian Federation hence the article will focus exclusively on the information „warfare" led by Russia. The article claims that Russian information operations focus on the proliferation of propaganda with the aim to influence electoral results in foreign states, legitimize its foreign-policy steps on the domestic scene and finally to undermine cohesion and trust in the state and Euro-Atlantic institutions especially in Central and Eastern Europe.

Key words: ***nformation war, propaganda, security environment, Russia***

[1] Mgr. Dominika Kosárová, M.A. is a PhD. Candidate at the Faculty of Political Science and International Relations, Matej Bel University, Kuzmányho 1, 974 01 Banská Bystrica, Slovak Republic, e-mail: dominika.kosarova@umb.sk.

[2] This article was written within the project VEGA 1/0545/17 Transformácia bezpečnostného prostredia: aplikácia skúseností štátov Vyšehradskej štvorky na príklade Ukrajiny

Introduction

The ongoing technological development, progress in the communication infrastructure and informatization of the society have raised the importance of information to the level of a strategic weapon, which is able to enforce national interests and political objectives of a state on the international scene. Consequently, the means of leading wars as well as the meaning of a *war* itself have changed. While in the past military operations aimed to gain control over the territory, sea and airspace, today, states strive to control information channels and ultimately to influence people's mind and perceptions of a particular situation often by means of propaganda. Given the enormous amount of data and diversity of information resources, it is difficult to categorize information and differentiate between the true ones and those that have been deliberately biased. Hence, the modern tactics of *war* include manipulation with facts in order to influence public opinion or decision-making process in the target state. The warfare enters thus to a new – information or cyber dimension. This article aims to evaluate the threat that the information warfare represents in the contemporary security environment with a particular focus on the European level. Russia is considered to be the major actor in this *warfare*, therefore the analysis will be focused on Russian activities in the information space. The article is based on the analysis of recent development within the European security environment, while the final part focus more specifically on the case of the Slovak Republic as one of the target states of Russian information operations. This issue required accurate analysis of media including pro-Russian internet portals, such as international websites of Russia Today and Sputnik. Out outcomes have been enriched by expert opinions and analysis elaborated within the Slovak as well as foreign security community.

1 Conceptualization of the issue

Information warfare is not a warfare in its strict sense. It is not preceded by official declaration of war, neither does it include the use of physical force. Moreover, it does not necessarily lead to causalities. Information when used as a weapon is aimed to interfere with opponent's perceptions, to gain control over his information resources and thus to influence the psyche of the population by means of deception, manipulation or propaganda. Method used to interfere with enemy's mind consists of *a reflexive control* which is

based on *conveying to an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action.* (Snegovaya, 2015, 10) The method of reflexive control leads the opponent to unintentionally make a decision that is bad for himself yet convenient for the opponent. Hence the information warfare is a contactless war that occurs *in the human consciousness and in the cyberspace.* (Pomerantsev, 2015, 46)

On the one hand, information operations may occur as a collateral phenomenon to a conventional war. In such a scenario, belligerents do not fight only by the armed forces, but they use various strategies to gain access to the opponent's information systems in order to either abuse or distort information or they deliberately spread disinformation in order to gain strategic advantage. Given the importance that information plays in the contemporary military strategies, wars obtained hybrid character based on other than exclusively armed operations. The decisive factor in hybrid warfare is not the strength or equipment of the army, but rather a control over the flows of information and access to the opponent's information systems. In these circumstances *whose story wins is more important than whose army wins.* (Pomerantsev, 48) On the other hand, information channels and cyber space are becoming themselves the modern battlefield, where information has become a strategic weapon. According to this logic, arms race can potentially gain form of race for control over the flows of information.

There are two main types of information operations, according to where they take place: cyber and non-cyber. Cyber attack in general is considered to be any disruption, cancellation, or modification of computer data without right. Cyber attack may occur in two basis forms. On the one hand, it may cause that targeted source will no longer be able to carry a specific information. In this case the attack disrupts the access to information displayed by the source and eventually provokes the breakdown of communication infrastructure. On the other hand, the attack may *only* alter the information carried by its source while the access to the source will remain undamaged. Yet the information provided by the source would be different as the one originally encoded. In this case the cyber attack alters information into disinformation and leads to the spread of false misleading facts. (Durante, 2015, 371) in other words, the aim of a cyber attack may be either to steal or change data.

However, the most common mean of disseminating fake news and propaganda are traditional media including print media, television and radio.

Both strategies – cyber and non-cyber – are on the rise with the increasing informatization of the society and all aspect of human lives and they have become strategic instruments of enforcing national interests and foreign-policy objectives of states. Regarding the contemporary European security environment, including the one of the Slovak Republic, the major challenge is posed by information operations launched by the Russian Federation.

2 Russian information warfare

The subsequent analysis will stem from the two above-determined strategies of information war led in the international security environment. On the one hand, it deals with cyber attacks aimed at stealing and abusing data from an enemy state and on the other hand it concentrates on traditional propaganda spreading disinformation. It will be focused on Russia – today one of the most influential actors in the information area, and given the victory of Donald Trump in the US presidential elections, probably also the most successful one. The concept of hybrid warfare was presented by Valerij Gerasimov, the Chief of General Staff of the Armed Forces of the Russian Federation, already in 2013 and it makes part of the contemporary military doctrine of Russia adopted in 2014. (Military Doctrine..., 2014, Lídl, 2015, Snegovaya, 2015) One year later, Kremlin published the National Security Strategy which points to the intensification of the global information struggle by claiming that beside political and economic tools also *informational instruments have been set in motion in the struggle for influence in the international arena*. (The Russian National..., 2015) The perception of information as a strategic instrument of the Russian foreign policy can be observed also in the speech of Andrei Krutskikh from the Ministry of Foreign Affairs of the Russian Federation. In February 2016, he declared that Moscow was preparing a new strategy for information area which he compared in terms of its significance to the test of a nuclear weapon as it would enable Russia to communicate with the USA as peer to peer. (Ignatius, 2017) Russia perceives information space as a perpetual battlefield.

Three different directions can be distinguished in the contemporary Russian information war. First of all Russia interferes in internal issues of Western states – especially when it comes to elections – by denigrating candidates inconvenient for Moscow. Secondly, Russian information operations has been targeting Ukraine and Syria in order to portray both countries in a negative light and thus to legitimize Russian engagement in the eyes

of Russian citizens. Last but not least Russian propaganda aims to shape public opinion also in the states of central and Eastern Europe by discrediting the European Union and NATO.

2.1 Influencing electoral results

The first of above-enumerated features of the Russian information war manifested itself during the US presidential campaign in 2016. On January 6, 2017, the US government released a report where it assesses Russian cyber activities and its interference into the course of the American presidential elections. According to the report, Russia is responsible for Putin-ordered cyber campaign against the USA aimed at sabotaging elections, undermining trust of citizens into the American democratic system and denigrating democratic candidate Hillary Clinton. Russian intelligence agencies allegedly gained access to the network of the Democratic National Committee already in July 2015 and they are accused of having stolen a great amount of data. Since March 2016 they focused on email accounts of members of the Democratic Party and other politicians. The report also points out that the cyber attack, which led to the leakage of thousands of emails from the computer network of the Democratic Party, was also allegedly committed from Russia. (Assessing Russian Activities..., 2017, Miller, Entous, 2017) The subsequent release of these emails on WikiLeaks ultimately weakened the position of Hillary Clinton and at the same time they contributed to the victory of Donald Trump. However, Russia denies any responsibility for the leaked emails and on the contrary, Moscow blames the USA from publishing classified documents known as Panama Papers, which revealed that Russian money was laundered in the tax haven. In this context, Krutskikh stated in February 2016 that the USA attacked in the information war first, and it was Russia's turn to retaliate. According to him, we are in the information warfare, were hidden soldiers fight with weapons including false news and hacking. (Ignatius, 2017)

Moreover, speculations about an attempt of a foreign power to manipulate with electronic counting systems gained ground. (Belam, 2016)
The report states that besides hacking, Russia used also other information operations including the spread of propaganda via Moscow-controlled media. The key role was played by the broadcasting of Russia Today, which portrayed Hillary Clinton in a negative light (Clavel, 2017) or by social media. If Clinton was to win, pro-Russian bloggers were prepared to launch Demo-

cracyRIP campaign on Twitter in order to undermine Clinton's legitimacy. (Miller, Entous, 2017)

Cyber attacks and propaganda reveal much about the wider geopolitical context as well as national and foreign-policy interests of states that conduct these operations. In case of the US presidential elections, preferences of Moscow reflected its relation to NATO. Kremlin perceives NATO enlargement to the East and its presence in the East European countries as a threat, as was recognized also in Gerasimov's report. (Lídl, 2015) Donald Trump expressed negative attitude towards NATO during the presidential campaign and he openly criticized the deployment of American units in the states of Eastern Europe, therefore he was a more suitable and acceptable candidate for Moscow when compared to Hillary Clinton. Moreover, Trump expressed will to establish friendly relations with the Russian president Vladimir Putin, that he did not perceive in a negative light by contrast to other presidential candidates.

Even though, information operations were targeted in this particular case primarily against the USA, they represent increasing threat also to the European security environment. The success of Russian operations to manipulate with the US elections might have encouraged Moscow's endeavour to influence in a similar way internal affairs also in other states. This issue concerns especially France, where a new president of the Republic will be elected in April/May 2017 and Germany, where the Federal elections will be held in September 2017.

In France, the threat of cyber attacks has increased[3] with approaching presidential elections[4]. Despite the fact, that there is no electronic voting which decreases the chance of direct manipulation with results, the General Secretariat for Defence and National Security called upon political parties to protect their data against potential attacks. (Clavel, Boudet, Herreros, 2016) After the US presidential elections, France has recognized increased risk of potential external interference into the presidential campaign either in form of illegal seizure and exploitation of data or by means of propaganda. The latter is already significant when it comes to the leading candidates, Marine Le Pen and Emmanuel Macron. While Le Pen refuses sanctions against Russia and she advocates the recognition of Crimea as a part of Russia, hence earning Putin's favour, her opponent Macron is portrayed in Kremlin-financed media

[3] Only in 2016 there were allegedly about 24000 revealed attacks coming from outside. (Clavel, 2017)

[4] The article reflects the situation until mid-April 2017, shortly before the first round of the presidential elections.

(especially Sputnik International and Russia Today[5]) as the US agent who collaborates with Hillary Clinton[6], as well as a homosexual leading a secret live and supported by a rich gay lobby. (Blachère, 2017, Assange: des révélations..., 2017, Assange: WikiLeaks a trouvé..., 2017) These compromising information came from sources revealed at WikiLeaks and they dominated in Russian media despite the fact, that the team of Assange published also more than 1100 documents about Marine Le Pen and over 3600 others concerning François Fillon, another pro-Russian candidate. (Blachère, 2017) The overview of how French versions of Russia Today and Sputnik were informing about French elections revealed that by contrast to information provided about Marine Le Pen and François Fillon, news about Emmanuel Macron were usually degrading, tendentious and mocking. (Ako Sputnik zaujato..., 2017, La Guyane..., 2017) This is an exemplary case of propaganda based on selectively chosen information that are further manipulated and interpreted in a way to serve predetermined purposes.

Germany faces a similar situation. Angela Merkel claims that the state deals with hacker attacks and disinformation campaigns on daily basis and it has been pointed to Russia as their alleged perpetrator. (AFP, 2016) at the beginning of 2016 German secret services accused Russia from international cyber espionage including hacking computers of the German parliament in 2015 which was attributed to Russian hacking group APT28[7]. The German intelligence services have recorded also an unprecedented online proliferation of fake news, which are associated with the Russian propaganda aimed at destabilizing German government and influencing the results of upcoming election, where Angela Merkel is hoping to be re-elected to the position of Chancellor. However, this would not be suitable for Kremlin because of Merkel's criticism of Moscow for its interference in Ukraine and her support for sanctions against Russia. (Reuters, 2017)

[5] RT and Sputnik are important tools of Russian propaganda with global reach. RT is established in 100 states while Sputnik broadcasts in 30 local languages and the number of its international offices is on the rise. (Nicolini, 2017a)

[6] This allegation stem from the fact, that Clinton's emails contained information about the French candidate Macron. One of the emails contained also invitation to dinner organized by Emmanuel Macron and Manuel Valls. (Assange: des révélations..., 2017, Assange: WikiLeaks a trouvé..., 2017)

[7] The same group was suspected from the cyber attack against the OSCE in December 2016. (Reuters, 2017)

2.2 Legitimizing foreign-policy decisions

Another goal of Russian propaganda is to gain support of the Russian audience for its foreign-policy decisions, that are rather controversial and in terms of international law also disputed. This is especially the case of the annexation of Crimea but also the Russian engagement in Syria. As regards Syria, propaganda had started to proliferate four weeks before Russia intervened in the conflict, while in the case of Ukraine it had appeared at least two years before the annexation. In both cases, propaganda is based on the negative portraying of either Syria or Ukraine in the Kremlin-controlled media, which represents about 90% of all Russian media (Szabolcs, 2017), with the aim to shift public opinion against both countries. Kremlin had been thus preparing ground for intervention and had tried to gain support within Russian society for actions, that were later condemned on the international level.

Ukraine drew attention to the activities of Russian hackers already in 2010, when governmental websites were attacked by espionage malwares. There was also a Distributed Denial of Services Attack and a disruption of government and intelligence portals which resulted in information blackout. Hackers allegedly gained access to the phone records and electronic communication between Ukraine, the European Union and the USA when Ukraine was preparing to sign the Association agreement with the EU. (Jaitner, 2015) After the outbreak of the conflict, Russian media have depicted Ukraine as a fascist state committing war crimes[8] and supported by *the corrupt US government*. Kremlin-controlled state television broadcasted in Russia an interview with alleged Russian victims to Ukrainian *fascists*, yet as it turned out, these *victims* were in reality hired actors. Chaos in Ukraine is portrayed in the Russian television in contract to the stability in Russia and Putin himself is depicted as a national hero[9]. In addition, after the shooting down of MH-17, Russian media came up with a number of conspiracy theories[10] providing alternative versions of why the aircraft had fallen down. There stories were significantly different from the official outcomes

[8] Russian servers released a hoax that Ukrainians remove organs from war victims at illegal transplantation stations despite the fact that the OSCE refuted that any such stations existed. Beside this, another fake new appeared about Ukrainian soldiers who allegedly were to crucify a 3-year-old child. (Šnídl, 2015)

[9] Russian media often show pictures of Putin riding a horse, a Harley or stroking tigers, which contributes to build personal cult of Putin as a powerful statesman. (Pomerantsev, 2015)

[10] Some theories claim that the plane was shut down either by the Ukrainian army or by Americans, who according to conspirators had planned to target Putin's plane. Another theory stated that passengers had lost their lives already before the plane took off, eventually, that the fall of the plane was conspired by a pharmaceutical enterprise in order to prevent scientists on board from discovering a medicament to cure AIDS. (Kullová, 2015)

of investigators who pointed out that the plane had been shut down from the area under the control of pro-Russian separatists. Hence, people can easily find themselves in a network of some kinds of pseudo-realities where false narratives serve to direct their mind far from the true ones.

2.3 Weakening of the European and transatlantic security architecture

The integration structures across the Euro-Atlantic area have become the third object of the Russian propaganda. in case of the European Union, it seems that Kremlin seeks to affect weak places in the internal policy of the EU member states in order to disrupt and destabilize the Union from inside. At the present time, these weaknesses stem from migration crisis, distrust towards Schengen, Brexit, Greek indebtedness, crisis of legitimacy and increasing number of terrorist attacks. Russian portals often misuse these issues in exaggerated and often misinterpreted way in order to emphasize inefficacy of the Union and its failure to deal with its own internal problems. This can be illustrated by the release of a hoax about the rape of a 13-years-old Russian speaking Lisa in Berlin allegedly perpetrated by Muslim immigrants. (Knight, 2016) This fake news abused the issue that divides the European countries probably the most – migration. It was to further aggravate tensions and polarization of the society and to contribute to already steep rise of islamophobia and xenophobia as well as to the discreditation of already disputed Merkel's migration policy.

The EU currently faces increase in extreme right-wing populism that sympathizes with Russian media and to a large extent it has adopted Kremlin's narrative, eventually some of these movements may directly collaborate with Moscow. Several nationalistic right-wing parties and politicians gained ground including National Front of Marine Le Pen who allegedly receives funds directly from Moscow, British anti-EU politician Nigel Farage, Hungarian party Jobbik (Pomerantsev, 2015) and Alternative for Germany. These parties identify themselves with several Kremlin's allegations: they doubt in the effectiveness of the European integration, they criticize the commitments stemming from NATO collective defence, they depict migrants as a security threat and regard them as terrorists, eventually, they openly support friendly relations with Moscow and refuse sanctions against Russia. (Nicolini, 2017b) Disinformation and propaganda provoke two-fold implications. First of all they influence public opinion, undermine people's trust in the state

and its ability to solve problems and they lead to the polarization of society. Secondly, this manipulated public opinion may have impact also on the political decision-making, which in democratic societies should reflect the opinion of the majority.

Pro-Russian propaganda disseminating across Western states do no target exclusively the EU, but it is directed also against NATO with the USA at the head[11]. Its goal is to point out to the so called crisis of the West and meanwhile to create a positive image of Russia. Anti-American narrative influence especially far left-wing parties that strictly refuse the US hegemony and as it can be illustrated by the case of the German party Die Linke, instead they are willing to support Moscow. (Pomerantsev, 2015)

While the propaganda spread on the domestic scene aims to achieve support for intended actions of the government, as it was illustrated by the case of Syria and Ukraine, the propaganda proliferated abroad strives to achieve quite the opposite – to undermine the trust of citizens in their own state, as well as in the European and transatlantic institutions. The purpose of disinformation spread by pro-Russian media across the continent is to weaken the institutional framework of the security architecture in Europe and across Atlantic, to provoke internal cleavages within the EU and NATO, deteriorate cooperation among member states, and last but not least to make people distrustful. Its main premises are: alleged effort of the USA to rule over the whole world, the support of terrorist groups from the part of Washington, depiction of NATO as aggressor approaching Russian border with intention to threaten the Russian national security, while American troops in East European countries are depicted as occupants. The narrative depicts the EU decision-making as a dictate of Brussels that makes the EU member states devoid of their sovereignty. On the other hand, Russia itself is portrayed as a victim that has to deal with aggressive Western states – members of the EU and NATO – eventually as the only rational actor that has been misunderstood by the West. (Čížik, 2015)

The Russian propaganda against the EU and NATO has increased in its magnitude and significance especially during 2014 and 2015 after the outbreak of migration crises and the annexation of Crimea. Since then, it can be alleged that Kremlin leads an undeclared *war* against the West personified in the EU and NATO. This hybrid warfare reflects also in the increasing number of propaganda-oriented facebook pages and raising activity of in-

[11] Anti-American disinformation campaign was launched for instance in Spain, when the local RT broadcasted an emission according to which the USA caused the outbreak of Ebola. This reminds the Soviet propaganda from 1980s' when the USSR accused the USA from the outbreak of AIDS epidemy.

ternet trolls with false identities on social networks. (Šuplata, Nič, 2016) A non-negligible role is played also by international news portals of RT and Sputnik, the later established also in the Czech Republic and Poland.

2.4 Russian propaganda and the Slovak security environment

The issue of the Russian propaganda concerns directly also the Slovak Republic which may be explained by the geopolitical context. Slovakia, as a member state and external border of both the EU and NATO and a state of the former Soviet bloc, falls to the sphere of interest of the Russian information war. Historical nexus between Slovakia and Moscow is quite firm and it reflects in the inconsistent public opinion, which is not so overtly inclined in favour of the European or transatlantic integration, but instead there are also strong pro-Russian oriented voices. This part of population is the most vulnerable to the Russian propaganda or to opinions that reflect the narrative proliferated by Russian servers. The spreading disinformation contribute to the polarization of the society, they bolster anti-European tendencies and weaken the trust of the Slovak people in the EU and NATO, as well as in the core European values. Many people consider Russia to be a more suitable alternative to the cooperation within the EU, eventually they incline towards neutrality and refuse the so called dictate of Brussels or Washington – popular terms among propagandists. The survey conducted by Globsec Policy Institute points out that contemporary support for pro-Western orientation of Slovakia has dropped to 23%. Only 30% of respondents view the membership in NATO in the positive light and as much as 47% of respondents believe that neutrality would be more convenient for Slovakia in comparison to its membership in NATO. The survey revealed also a strong anti-Americanism within the Slovak society. It showed that as much as 59% of respondents perceive the US role in Europe negatively and 60% think that the USA use NATO to gain control over small states such as Slovakia. (Šuplata, Nič, 2016)

Decline in trust in the European and transatlantic institutions and search for alternatives do not have to be result of Kremlin-directed propaganda, but a significant role is played also by alternative media that have taken over the opinions from Russian propagandistic pages and hence they contribute to the spread of Russian narrative. There are several webpages[12] in Slovakia

[12] In 2015 Slovak activist Juraj Smatana published a list of 42 Czech and Slovak webpages that spread Russian propaganda. (Šnídl, 2015, Lucas, Pomerantsev, 2016)

and pages on social networks, that incline towards Russian interpretation of events especially in relation to the EU and NATO membership, the contemporary situation in Ukraine or migration crisis (they claim for instance that conflict in Ukraine or migration crisis were both caused by the USA). (Šnídl, 2016) Moreover, several of these subjects maintain connections with pro-Russian non-governmental organizations (including Slovak-Russian Association, Institute of Slavic Strategic Studies) and they often simply take over articles or arguments directly from Russian portals. (Lucas, Pomerantsev, 2016)

This narrative stemming from disinformation had not only found supporters within the Slovak society, but what is even more alarming, it has been adopted also by some political subjects such as Kotleba's People's Party Our Slovakia, which has even assumed seats in the National Council of the Slovak Republic after the last Parliamentary elections in March 2016. The agenda of Kotleba's party is based on strong anti-Americanism and rejection of Slovakia's membership in the EU and NATO as can be evidenced also by the party's effort to gather signatures required to trigger referendum on the Slovak membership in both structures. The seriousness of the situation regarding the infiltration of anti-system forces in the state institutions and the proliferation of alternative information was acknowledged also by the Ministry of Interior in 2016, when it stated that the Slovak Republic is exposed to operations launched through information channels that under the influence of the Russian Federation spread misleading news and manipulated facts. According to the statement: *The issue of Russian propaganda as a part of hybrid threats destabilizing state order and its political system is one of the major challenges that face many EU states including Slovakia.* (Šnídl, 2016)

The proliferation of fabricated facts, conspiracy theories and disinformation that are either directly spread or supported by Kremlin, eventually they may be inspired by Russian propagandistic resources, provokes several other threats that negatively influence stability of the Slovak security environment. These threats include especially the rise of radicalism and extremism in form of distrust in the state and in the transnational institution that Slovakia is a part of and the search for alternatives in form of anti-system movements and parties. Young people represent one of the most vulnerable groups hence Slovakia should fight against propaganda by enhancing the development of critical thinking that would enable people to distinguish in the massive influx of information those that are biased.

Conclusion

The era of informatization represents unprecedented opportunity as it enables to communicate a message on the global scale, yet at the same time due to the vulnerability of information systems and massive influx of all kind of information it may become a fatal weakness as well. Increasing informatization has enabled states to use information operations to achieve political ends. Primary actors of such operations are great powers, yet in terms of the contemporary European and especially Slovak security environment the major challenge is posed by information operations launched by Kremlin. Russia leads a kind of undeclared *war* against the West by means of propaganda, while important role is played by Kremlin-financed and supported media as well as cyber attacks that enable to get access to information that may be afterwards manipulated and released in misinterpreted form in order to achieve strategic goals. The danger of information war stems also from the fact that it does not recognize borders and it is launched on the global scale as it can reach every place covered by communication infrastructure.

In the Slovak context, the implications of Russian information warfare can be evidenced by increasing number of pro-Russian oriented websites and media – usually conspiracy and alternative ones – which ultimately influence public opinion and decrease state legitimacy and trust in the European and transatlantic security structures in the eyes of citizens. Pro-Russian propaganda exploits weak places and offers alternative facts and solutions that please to a part of society frustrated by the inability of the state and transnational institutions to deal with the contemporary problems such as migration, corruption or terrorism. Information warfare represents a security risk, all the more that it provokes side-effects in form of radicalization of particular groups that search for alternative solutions that are often in violation with the traditional state policy. Therefore, it is a multidimensional phenomenon threatening stability of the security environment of the Slovak Republic and other European states that struggle with the proliferation of alternative facts in line with the Russian propaganda.

References

1. *Ako Sputnik zaujato píše o francúzskych vol'bách.* 2017. [online] antipropaganda, 7.4.2017 [cit. 16.4.2017]
   Available at: http://antipropaganda.sk/ako-sputnik-zaujato-pise-o francuzskych-volbach/
2. AFP. 2016. *Russian cyber-attacks could influence German election, says Merkel.* [online] The Guardian, 8.11.2016 [cit. 14.2.2017]
   Available at: https://www.theguardian.com/world/2016/nov/08/russian-cyber-attacks-could-influence-german-election-says-merkel
3. *Assange: des révélations sur Macron dans les mails de Clinton.* [online] Sputnik France, 3.2.2017 [cit. 14.2.2017]
   Available at: https://fr.sputniknews.com/international/ 201702031029930563-wikileaks-revelations-macron/
4. *Assange: WikiLeaks a trouvé des informations sur Macron dans des emails de Clinton.* [online] RT en francais, 3.2.2017 [cit. 14.2.2017]
   Available at: https://francais.rt.com/france/33403-wikileaks-macron-clinton-email-assange
5. *Assessing Russian Activities and Intentions in Recent US Elections* [online] Intelligence Community Assessment, 6.1.2017 [cit. 14.2.2017]
   Available at: https://www.intelligence.senate.gov/sites/default/files/ documents/ICA_2017_01.pdf
6. BELAM, M. 2016. *We're living through the first world cyberwar – but just haven't called it that.* [online] The Guardian, 30.12.2016 [cit. 14.2.2017]
   Available at: https://www.theguardian.com/commentisfree/2016/dec/ 30/first-world-cyberwar-historians
7. BLACHERE, F. 2017. *Présidentielle: l'arrière- goût russe des rumeurs visant Emmanuel Macron.* [online] Le Parisien, 7.2.2017 [cit. 14.2.2017]
   Available at: http://www.leparisien.fr/elections/presidentielle/candidats-et-programmes/presidentielle-l-arriere-gout-russe-des-rumeurs-visant-emmanuel-macron-07-02-2017-6662109.php
8. CLAVEL, G. 2017. *L'élection présidentielle française est-elle exposée à une déstabilisation russe comme aus Etat-Unis?*
   [online] Le Huffington Post, 7.1.2017 [cit. 14.2.2017] Available at: http://www.huffingtonpost.fr/2017/01/07/lelection-presidentielle-francaise-est-elle-exposee-a-une-desta/
9. CLAVEL, G., BOUDET, A., HERREROS, R. 2016. *Hacking, déstabilisation...Le spectre de la cyberguerre plane sur l'élection présidentielle*

de 2017. [online] Le Huffington Post, 3.12.2016 [cit. 14.2.2017] Available at: http://www.huffingtonpost.fr/2016/12/03/hacking-destabilisation-le-spectre-de-la-cyberguerre-plane-s/

10. ČÍŽIK, T. 2015. *Informačná vojna – nová bezpečnostná hrozba pre Európu*. [online] DenníkN, 18.12.2015 [cit. 14.2.2017] Available at: http://zahranicnapolitika.dennikn.sk/informacna-vojna-nova-bezpecnostna-hrozba-pre-europu/
11. DURANTE, M. 2015. Violence, Just War and information. In *Philosophy & Technology*. No. 28/2015. ISSN 2210-5441. pp. 369-385.
12. IGNATIUS, D. 2017. *Russia's radical new strategy for information warfare*. [online] The Washington Post, 18.1.2017 [cit. 14.2.2017] Available at: https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/?utm_term=.07d87ee9bb4a
13. JAITNER, M. 2015. Russian Information Warfare: Lessons from Ukraine. In GEERS, K. (ed.) *Cyber War in Perspective: Russian Agression Against Ukraine*. Tallin: NATO Cooperative Cyber Defence Centre of Excellence, 2015. 169 p. ISBN 978-9949-9544-5-2.
14. KNIGHT, B. 2016. *Teenage girl admits making up migrant rape claim that outraged Germany*. [online] The Guardian, 31.1.2016 [cit. 14.2.2017] Available at: https://www.theguardian.com/world/2016/jan/31/teenage-girl-made-up-migrant-claim-that-caused-uproar-in-germany
15. KULLOVÁ, Z. 2015. *Aj Slovákov zaplavuje ruská propaganda*. [online] Hospodárske noviny, 23.6.2015 [cit. 14.2.2017] Available at: http://dennik.hnonline.sk/svet/519076-aj-slovakov-zaplavuje-ruska-propaganda
16. *La Guyane, une île? La géographie selon Macron fait rire le Web*. [online] Sputnik News, 27.3.2017 [cit. 16.4.2017] Available at: https://fr.sputniknews.com/insolite/201703271030635137-guyane-bourde-macron-reaction-internautes/
17. LÍDL, V. 2015. *Nová vojenská doktrína Ruska: na pokraji studené války?* [online] NATO Information Portal, 25.1.2015 [cit. 14.2.2017] Available at: http://www.natoaktual.cz/nova-vojenska-doktrina-ruska-na-pokraji-studene-valky-ppm-/na_analyzy.aspx?c=A150125_161034_na_analyzy_m00
18. LUCAS, E., POMERANTSEV, P. 2016. *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*. [online] Center for European Policy Analysis,

August 2016 [cit. 14.2.2017] Available at: https://cepa.ecms.plfiles/?id_plik=2773

19. *Military Doctrine of the Russian Federation.* 2014. [online] December 2014 [cit. 14.2.2017] Available at: https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf
20. MILLER, G., ENTOUS, A. 2017. *„Declassified report says Putin "ordered" effort to undermine faith in U.S. election and help Trump".* [online] Washington Post, 6.1.2017 [cit. 14.2.2017] Available at: https://www.washingtonpost.com/world/national-security/intelligence-chiefs-expected-in-new-york-to-brief-trump-on-russian-hacking/2017/01/06/5f591416-d41a-11e6-9cb0-54ab630851e8_story.html?utm_term=.8893ba15ab5e
21. NICOLINI, M. 2017a. *Informačná vojna: ako Putin manipuluje realitu (1. časť')* [online] antipropaganda, 12.1.2017 [cit. 14.2.2017] Available at: http://www.antipropaganda.sk/informacna-vojna-ako-putin-manipuluje-realitu-1/
22. NICOLINI, M. 2017b. *Informačná vojna: ako Putin manipuluje realitu (2. čas')* [online] antipropaganda, 29.1.2017 [cit. 14.2.2017] Available at: http://www.antipropaganda.sk/informacna-vojna-putin-manipuluje-realitu-2-cast/
23. POMERANTSEV, P. 2015. The Kremlin's Information War. In *Journal of Democracy.* Vol. 26, no. 4. ISSN 1086-3214, pp. 40-50.
24. REUTERS. 2017. *Germany investigating unprecedented spread of fake news online* [online] The Guardian, 9.1.2017 [cit. 14.2.2017] Available at: https://www.theguardian.com/world/2017/jan/09/germany-investigating-spread-fake-news-online-russia-election
25. SNEGOVAYA, M. 2015. *Russia Report I. Putin's Information Warfare in Ukraine.* Washington, D.C.: Institute for Study of War, 2015. [online] [cit. 14.2.2017] Available at: http://understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare
26. SZABOLCS, P. 2017. *Orbán is a tool in Putin's information war against the West.* [online] Index, 4.3.2017 [cit. 14.2.2017] Available at: http://index.hu/kulfold/2017/02/04/orban_is_a_tool_for_putin_in_his_information_war_against_the_west/
27. ŠNÍDL, V. 2015. *Proruskú propagandu o zhýralom Západe u nás šíri 42 webov.* [online] DenníkN, 26.2.2015 [cit. 14.2.2017] Available at: https://dennikn.sk/57740/prorusku-propagandu-o-zhyralom-zapade-u-nas-siri-42-webov/

28. ŠNÍDL, V. 2016. *Štát prvý krát priznal, že ruská propaganda útočí na prozápadné smerovanie Slovenska.* [online] DenníkN, 8.6.2016 [cit. 14.2.2017] Available at: https://dennikn.sk/481082/stat-prvykrat-priznal-ze-ruska-propaganda-utoci-prozapadne-smerovanie-slovenska/
29. ŠUPLATA, M., NIČ, M. 2016. *Russia's Information War in Central Europe: New Trends and Counter-Measures.* Bratislava: Globsec Policy Institute, 2016. 17 p.
30. *The Russian National Security Strategy.* 2015. [online] 31.12.2015 [cit. 14.2.2017] Available at: http://www.ieee.es/Galerias/fichero /OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf

Michal Kopuletý[1]

The role of Military Robots in the Explosive Threat Management

Abstract

Text introduces reader into problematics of application of robots into broad spectrum of activities connected to minimizing risk of Explosive Threat. First chapter briefly introduces reader into problematics. Second chapter deals with general characteristics and roles of current military robotic systems. Third chapter is dedicated to relationship between Military Engineering and Explosive Threat Management, followed by the last chapter that focuses on current role of robotic systems in Explosive Threat Management and identifies and predicts their future roles and capabilities.

The main aim of the text is to provide a general overview of the use of robotic systems within the Explosive Threat Management, identify their current role and predict their future capabilities and possible development.

Key words: ***Robotic Systems, Autonomous Systems, Explosive Threat Management, Ordnance Disposal***

Introduction

Robotic automation is an inevitable process of human civilization development and modern armies already react to this reality. The military robots are one of the most promising technology of future warfare and offer broad spectrum of opportunities. Unique features of these systems make them very suitable for conducting wide variety of tasks. What is more, current domestic and foreign publications together underline the need of implementing of robotic and automated systems into military. All these needs are connected to force protection (especially minimization of human losses) and sustainment of own troops in the military operations. Resistibility and force protection are

[1] npor. Ing. Michal Kopuletý, 153. engineer battalion Olomouc

extremely important in the sense of survivability and minimization of forces and means losses. One way of reducing risk to human life is to implement unmanned/robotic systems into military practise. Additionally, according to military publications and analysis, robots can reduce workload and save time.

But what is their role in Explosive Threat Management (ETM)? What are their current capabilities? Can military robots really save human lives when neutralizing explosive devices? What capabilities will have military robots within ETM in the future?

1. General characteristics of the advanced robotic systems used in military

Specific features of robotic/unmanned systems contribute to possible replacement of soldiers by robots in military operations and can be very usefully converted into military. These systems differ from classic manned (organic) systems in many ways. Unmanned systems provide persistence, versatility, survivability, and reduced risk to human life, and in many cases are the preferred alternatives especially for missions that are characterized as 3D - dull, dirty, or dangerous[2].

- Dull missions are ideal for unmanned systems because they involve long-duration undertakings with tasks that are ill suited for manned systems. Good examples are reconnaissance missions; Robotic systems can permit the realization of repetitive and fastidious tasks.
- Dirty missions have the potential to unnecessarily expose personnel to hazardous conditions. A primary example is CBRN (chemical, biological, radiological and nuclear) missions. Robotic systems can perform these dirty missions with less risk exposure to the operators.
- Dangerous missions involve high risk. With advances in capabilities in performance and automation, unmanned systems will reduce the risk exposure to personnel by increasingly fulfilling capabilities that are inherently dangerous. Robotic systems can increase the survivability of the troops in contact.

[2] *Unmanned Systems Integrated Roadmap 2013 - 2038.* Washington, D.C.: Government Printing Office, 2007.

According to US DoD (United States Department of Defence) publications, robotic and autonomous systems can contribute to:[3]

- Reducing the number of warfighters in harm's way;
- Increasing decision speed in time-critical operations;
- Performing missions impossible for humans.

What is more, actual Robotic and Autonomous Systems (RAS) Strategy declared main capabilities for these systems. They must increase situational awareness, lighten the Soldiers' physical and cognitive workloads, sustain the force with increased distribution, throughput and efficiency, facilitate movement and manoeuvre and protect the force[4].

Robotic systems are capable of executing a number of repetitive, mechanically-oriented and possibly automated tasks conducted routinely by Soldiers thereby potentially freeing them for other missions. Robots have proven very efficient and cost effective in tasks that are repetitive and dangerous. They are well suited to perform tasks where Soldier lives are at great risk and they can do much to mitigate that risk with little or no reduction to the successful execution of the task[5]. The final goal of military use of robotic systems is to increase military capability and security of forces and allow soldiers to concentrate on specific tasks which can only be fulfilled by manpower[6]. Military robot is a mechanical device, which is autonomous or remotely controlled. It can replace or strengthen the soldiers and its activity is related to military operations. NATO countries currently use terminology, which is widely acknowledged. In NATO countries, military robots are frequently defined as unmanned systems. These systems are divided into:[7]

- UAS (Unmanned Aerial System);
- UGS (Unmanned Ground System;
- UMS (Unmanned Marine System).

Each unmanned system has its own specific characteristics and is suitable for performing different tasks. For example, UAS have advantages in speed, navigation, remote control response time, range and possible stealth technologies application. They are suitable for penetrating, long-term and tactical

[3] The US Army Robotic and Autonomous Systems Strategy. Fort Eustis: TRADOC, 2016.

[4] Ibid.

[5] *Robotics Strategy White Paper*. Department of the army, 2009.

[6] *Relevance and possible future role of robotic/unmanned systems for FINABEL land forces* [online]. Brusel: European land forces interoperability center FINABEL, 2013 [cit. 2015-12-30]. Available from: https://goo.gl/U6EnyL.

[7] *Unmanned Systems Integrated Roadmap 2013 – 2038*. Washington, D.C.: Government Printing Office, 2007.

tasks. UAS are predestined to fulfil tasks from air domain. This allows them to move significantly faster than other systems. Flying at the height allows them to observe battlefield from the bird's eye view. On the other hand, their operational deployment is largely influenced by weather conditions, which seems to be a significant disadvantage. UGS are versatile, relatively fast and capable of off-road travel. UGS use tires, tracks or legs to move on the battlefield and its ground mobility is sometimes very limited because of rough terrain. It negatively affects its payload capacity, operational range and navigation. UMS have typically greatest endurance and payload capacity. UMS conduct tasks like maritime security - ISR, port surveillance, SOF support, electronic warfare etc.

Generally, unmanned systems have many advantages compared to man-

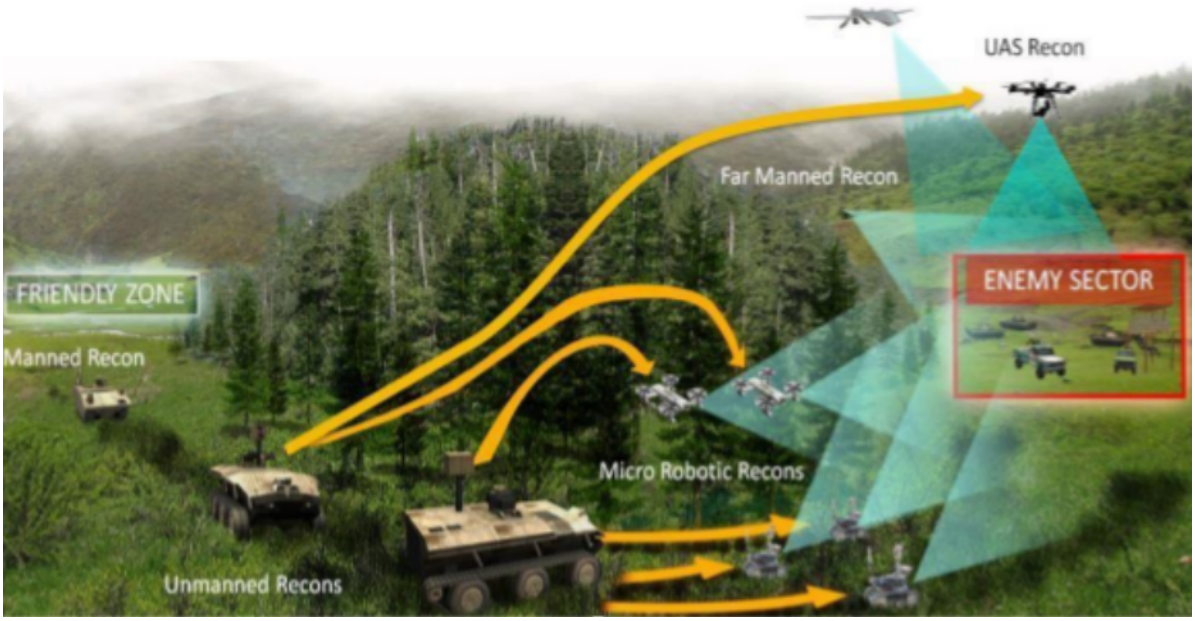

Figure 1: Manned Unmanned Teaming *

** The US Army Robotic and Autonomous Systems Strategy. Fort Eustis: TRADOC, 2016.*

ned systems and that makes them very suitable for conducting 3D missions within MUM-T (Manned Unmanned Teams) in order to support and expand capabilities of manned systems – see Figure 1.

Application of robotic systems within MUM-T can lead to synergic effect. A combination of individual benefits of organic and inorganic systems creates opportunity to increase overall efficiency of own troops and allows operations to be performed with less human effort and lowered risk of human casualties. Robotic systems within MUM-T enable organic systems to extend capabilities of their sensing and also interacting with the environment.

2. Military engineering and Explosive Threat Management

Explosive Threat Management (ETM) is one of the most important and complex task of Military engineering (MILENG) which interferes with two main MILENG roles – mobility support and survivability of own troops.

In the case of mobility support and survivability, ETM is related to minimizing the risk of explosive ordnance, both manufactured and improvised, to friendly forces (including civilians). It includes all actions from the provision of advice and engineer intelligence to deliberate actions to dispose of specific explosive threats, such as disposal, search and EOD (Explosive Ordnance Disposal), IEDD (Improvised Explosive Devices Disposal) and C-IED (Counter Improvised Explosive Device) tasks. This task can also be executed by different branch specialist. In fact, for some nations, the functions to mitigate explosive threat can be assigned to non-engineers (logistics or others). Nonetheless, this task is a MILENG responsibility as defined in the Alliance[8].

ETM is task dealing with Explosive Threats. Improvised Explosive Devices (IEDs), Unexploded Explosive Ordnance (UXOs, including mines), Abandoned Explosive Devices (AXOs) and CBRN Explosive Ordnance (CBRN EO), including Toxic Industrial Materials (TIM) and Petrol/Oil/Lubricants (POL) can be all considered as Explosive Threat. ETM manages the three MILENG tasks involved in countering explosive threats: Military Search, Explosive Ordnance Disposal and Support to Intelligence[9].

- Military Search is executed by military engineers and/or EOD units and is used to find explosive threats when executing Breaching and/or Area/Route Clearance tasks;
- Explosive Ordnance Disposal (EOD) is the final detection, identification, on site evaluation, render safe and final disposal of an Unexploded Explosive Ordnance;
- Support to Intelligence builds understanding of all aspects concerning the physical operational environment. Explosive Threats are a fundamental risk for the own troops in that physical operating environment.

All in all, it means that ETM involves broad spectrum activities that are focused on minimizing the risk of explosive ordnance that can cause human and material losses. According to military operations experience,

[8] ATP-3.12.1. *Allied doctrine for Military Engineering.* Brusel: NSA, 2016.
[9] Ibid.

we can assume that ETM tasks are time consuming, very dangerous and dirty and conducted by high-skilled specialists who need special equipment. In other words, ETM involves broad spectrum of dangerous, dirty and dull (3D) activities.

3. The current role of Military Robots within ETM

In current security environment Explosive Threat is one of the biggest issues. By 2013, 2550 U.S. service members had been killed by IED explosions in Operations Iraqi Freedom and Enduring Freedom. This number, however, is only a fraction of global IED casualties. According to the Joint Improvised Threat Defeat Agency (JIDA), between August 2010 and August 2012 there was an average of 600 IED incidents per month across the globe[10]. And not only IEDs but other types of Explosive Threats cause hundreds of human losses around the globe every year. Insurgents, terrorist and other hostile groups plan and realize attacks using explosives in order to injure or kill as many humans as possible and not only on the battlefield, but also in the heart of the world capitals.

After 2001 rapidly grew operational requirements for introducing remotely controlled means designed for EOD (Explosive Ordnance Disposal) and IEDD (Improvised Explosive Devices Disposal) activities in foreign military operations. For example, in years 2004-2006 the number of engineer EOD robots used in Afghanistan grew from 160 to more than 4000[11]. Since that, robots are being deployed by western armies very often in military operations. Estimated numbers of EOD/IEDD robots deployed by US are listed in the Table 1. Approximately 8,000 systems of various types have seen action in Operation Enduring Freedom and Operation Iraqi Freedom. As of September 2010, these deployed UGVs have been used in over 125,000 missions, including suspected object identification and route clearance, as well as to locate and defuse improvised explosive devices (IEDs). During these counter-IED missions, Army, Navy, and USMC (United States Marine Corps) explosive ordnance teams detected and defeated over 11,000 IEDs using UGVs[12].

[10] *Using Unmanned Systems to Counter the Improvised Explosive Device Threat* [online]. [cit. 2017-05-02]. Available from: http://droneanalysis.blogspot.cz/2016/07/using-unmanned-systems-to-counter.html

[11] emphUnmanned Systems Integrated Roadmap 2013 - 2038. Washington, D.C.: Government Printing Office, 2007.

[12] Ibid.

Table 1. Estimated numbers of EOD/IEDD robots in US military[*]

Name of EOD/IEDD Robotic System	Numbers deployed (year)
PackBot family of systems	1372 (2007)
TALON family of systems	
Mini-EOD	320+ (2011)
MARCbot (IV and IV-N)	811 (IV; 2011) 496 (IV-N; 2011)
Bombot	1842+ (2007)
Dragon Runner	10 (2007)

[*] *Unmanned Ground Systems Roadmap [online]. Robotic Systems Joint Project Office, 2011 [cit. 2017-05-02]. Available from: http://www.dtic.mil/ndia/2011/MCSC/Thompson_ UGSRoadmap.pdf*

In these days, military robots are common equipment of modern armies worldwide. Vast numbers of EOD/IEDD robots are incorporated in organizational structures of NATO armies. These means are able to support and enhance soldiers in wide variety of tasks including countering Explosive Threats. Current robotic systems can provide two main benefits – attack prevention and effects mitigation. Attack prevention means providing an early warning by continuous and persistent reconnaissance, surveillance and intelligence (ISR) activities. For example, group of insurgent preparing road-side IED is detected by UAV performing its mission. A Threat is detected so friendly forces can avoid human losses. Second benefit - effect mitigation is for substitution of human crew by unmanned/robotic systems that can provide stand-off capability. A common objective of the automation of land forces at the tactical level is to guarantee a tool to detect, predict and neutralize enemy threats maintaining a safe standoff for soldiers. The immediate effect is a reduction of casualties and wounded soldiers[13].

Currently, almost all military EOD teams or elements possess the same basic tools and equipment to employ techniques and perform procedures to defeat, render safe/neutralize, and dispose of hazardous explosive ordnance. These tools include, but are not limited to, portable x-ray equipment, unmanned systems, specialized demolition charges, and specialized

[13] emphRelevance and possible future role of robotic/unmanned systems for FINABEL land forces [online]. Brusel: European land forces interoperability center FINABEL, 2013 [cit. 2015-12-30]. Available from: https://goo.gl/U6EnyL.

tools for removing fuses[14].

It means that robotic systems are standard equipment of EOD teams identifying, defeating/neutralizing explosive ordnance. The main objective of implementing these technologies is to provide stand-off capability which enable locating, identifying and finally neutralizing Explosive Threat from safe distance to avoid human losses. Unmanned systems are versatile, adaptable and perform operations that would otherwise endanger the lives of service members.

The majority of land forces have already small UGS EOD/IED manipulator vehicles. The capability platforms for the EO protective task in the Army (Corps of Engineers/Army Logistic Services) consist of a remote-controlled, ground-based platform for standoff-capable EO reconnaissance, clearance and disposal, including the manipulation of objects.

Current military robots can fulfil variety of tasks connected to ETM – see Table 2. In recent military operations, UAVs are very successfully used to collect relevant information for battlespace, to provide an early warning on Explosive Threat to friendly forces. UGVs are used for reconnaissance of dangerous and inaccessible places (for example tunnels, houses), locating and identifying Explosive Threat and its neutralization using special equipment.

Table 2. Current capabilities of EOD/IEDD UAVs and UGVs

Selected ETM Tasks	UAV	UGV
Persistent ISR missions	X	
Detecting and identifying Explosive Threat	X	X
Material handling		X
Clearance and disposal of Explosive Threat		X
Inaccessible areas reconnaissance		X
Potential CBRN hazard detection	X	X

Current robotic systems used for ETM are electronic devices, that only remotely-controlled with no autonomous capability. Key part of these systems is still a human. It means that these means are not intelligent and cannot emulate human thinking. However, these systems are very effective and even necessary but relatively primitive tools to support specialist during ETM missions. Unmanned Systems provide a capability for coun-

[14] *Joint Publication 3-42: Joint Explosive Ordnance Disposal* [online]. 2016 [cit. 2017-05-02]. Available from: http://www.dtic.mil/doctrine/new_pubs/jp3_42.pdf

tering the Explosive Threat. Although not capable of (at least partially) emulate human thinking, current military robots are persistent, versatile, adaptable and perform operations that would otherwise endanger the lives of service members.

4. The future roles and capabilities of Military Robots within ETM

Although robotic automation is inevitable process of human development, massive application of autonomous and intelligent robotic systems for ETM missions is not real in a short-term according to existing research. However, what is more important, their contribution will rise in near future. As the future enables greater automation with respect to both navigation and manipulation, unmanned systems will be able to perform advanced tasks like sophisticated and complex EOD and IEDD support.

Future robotic technologies and unmanned ground systems (UGS) will augment Soldiers and increase unit capabilities, situational awareness, mobility, and speed of action. Artificial intelligence will enable the deployment of autonomous and semi-autonomous systems with the ability to learn and leverage decision aids to enable Soldiers to make rapid decisions using all available information, while reducing the cognitive burden. Robotics will enable the future force by making forces leaner and contributing to force protection, making the force expeditionary and providing increased capabilities to maintain overmatch[15].

ETM is almost always man power intensive, time-consuming, logistically demanding and dangerous. Always will be insufficient number of specialist on the battlefield but automated or autonomous military robots could solve (at least partially) this problem in the future. These systems can replace human (soldier) even in complex decision-making in the future. That can cause that soldiers would concentrate on the task, which can be fulfilled only by human power, so application of the advanced robotic systems would save scarce resources.

We can assume, that future robotic systems will have much better sensing and will be able of thinking (for example choosing optimal course of action) similar to human. For example, realising an automation effect of specific regularly repetitive work steps (e.g. approaching an object in easy

[15] TRADOC Pamphlet 525-3-1: Win in a complex world 2020-2040 [online]. 2014. Available from: http://www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf

terrain and in direct view, picking up tools carried), it should become possible to relieve the specialist operating the system[16].
According to existing research, development of these systems is mainly focused on:

- Better sensing through advanced sensors;
- Better acting with sophisticated manipulators that enable wide varieties of action;
- Advanced persistence in order to enable performing long-duration ETM tasks;
- Autonomous or semi-autonomous behaviour enabling automatic/autonomous locating, identifying and neutralizing Explosive Threat.

A need for development also exists in the following areas:[17]

- Remote-controllable and modifiable explosive charge with arming system and ignition device for radio-triggered systems and adaption for various explosive charges;
- 3D capture of the work area (outrigger range of manipulator arm) and around the tools (higher resolution) to avoid collisions;
- Integration of sensors to detect explosives, ignition components (electronic components) and jackets of explosive ordnance (geometry) and their automatic use throughout the area and space, displaying any anomalies detected;
- Uncover explosive ordnance or parts thereof buried in the ground, and system compatibility of sensors and jammers.

US military currently develops Unmanned ground systems (UGS) to support EOD/IEDD operations – MTRS, MTRS Incr. II, AEODRS and CRS-I. According to UIR, many other systems for managing Explosive Threat are being developed – for example HMDS and new family of Area Detection/ Clearance systems. All of these systems should have certain level of autonomy in the future.

[16] *Relevance and possible future role of robotic/unmanned systems for FINABEL land forces* [online]. Brusel: European land forces interoperability center FINABEL, 2013 [cit. 2015-12-30]. Available from: https://goo.gl/U6EnyL.
[17] Ibid.

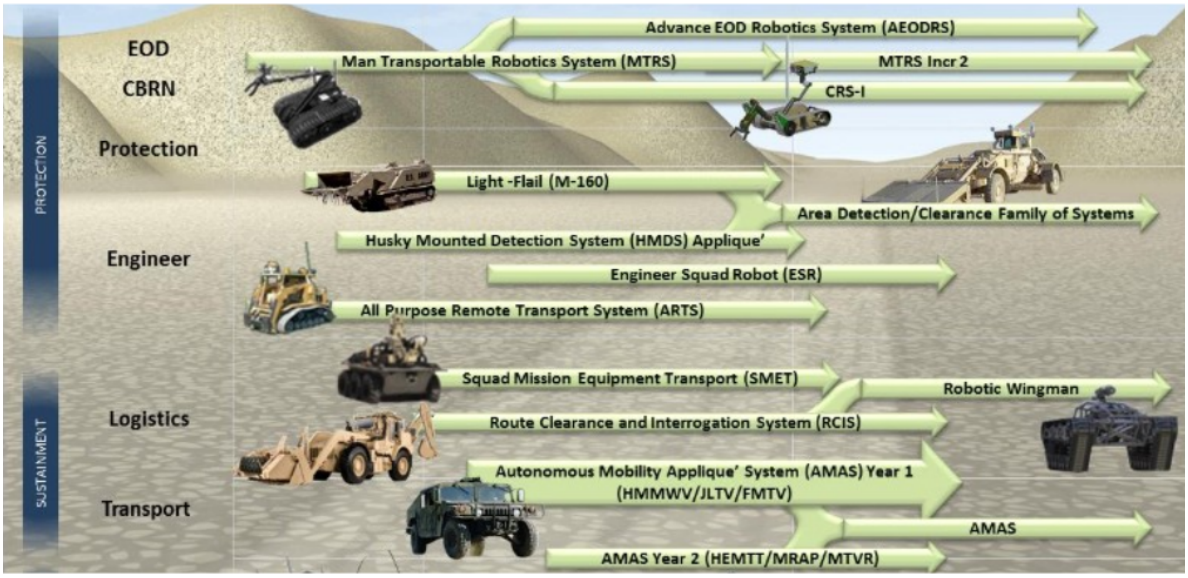

Figure 2: EOD UGVs development in US military *

* Unmanned Systems Integrated Roadmap 2013 - 2038. *Washington, D.C.: Government Printing Office, 2007.*

According to Robotics Strategy White Paper[18] we can await fully-autonomous robots capable of detecting and removing Explosive Threat in high-term horizon ($>$ 5 years). Feasibility of robotics solutions relates to the suite of sensors and delicate robotic manipulation of explosives during removal.

We can also predict not only existence of advanced robotic systems, but also multi-robotic systems (UAS, UGS and UMS together) able to cooperate in many ways (sharing information, advanced sensing etc.) with each other. It will create cooperative robotic systems (or even swarms) which will replace, augment, support and enhance soldiers when defeating Explosive Threat. In the future, the military robots will play very important role thanks to many objective reasons. As the Global War On Terrorism wages on, insurgent groups and terrorism organizations will continue to modify their tactics, techniques and procedures. An adaptive threat requires an adaptive response[19].

[18] *Robotics Strategy White Paper*. Department of the army, 2009.

[19] *Using Unmanned Systems to Counter the Improvised Explosive Device Threat* [online]. [cit. 2017-05-02]. Available from: http://droneanalysis.blogspot.cz/2016/07/using-unmanned-systems-to-counter.html

Conclusion

These systems confirmed that can improve situational awareness, situational understanding, reduce manpower, increase performance of own forces, minimize risks for civilians and reduce overall costs in the past operations. Current robotic systems used for ETM are indispensable helpers and necessary part of countering Explosive Threat. These remotely-controlled assistants can provide attack mitigation and effects mitigation to own troops (including civilians) thanks to their unique features.

Role of robotic systems will rapidly increase and expand in the future. We can await implementation of multi-robotic, intelligent, autonomous EOD/IEDD unmanned systems able to perform wide variety of task connected to locating, identifying and neutralizing Explosive Threat in hostile environment. They will perform these task autonomously, precisely and accurately and specialist will only oversee their work. This could save scarce resources, decrease costs, increase capabilities of EOD teams and finally save human lives. All in all, future will belong to robotic systems and safe managing of Explosive Threat will not be able without them. This is the final and fundamental reason that raises the need to study this issue further and deeper.

References

1. ATP-3.12.1. *Allied doctrine for Military Engineering.* Brusel: NSA, 2016.
2. *Joint Publication 3-42: Joint Explosive Ordnance Disposal* [online]. 2016 [cit. 2017-05-02]. Available from: http://www.dtic.mil/doctrine/new_pubs/jp3_42.pdf
3. *Relevance and possible future role of robotic/unmanned systems for FINABEL land forces* [online]. Brusel: European land forces interoperability center FINABEL, 2013 [cit. 2015-12-30]. Available from: https://goo.gl/U6EnyL.
4. *Robotics Strategy White Paper.* Department of the army, 2009.
5. *The US Army Robotic and Autonomous Systems Strategy.* Fort Eustis: TRADOC, 2016.
6. TRADOC Pamphlet 525-3-1: Win in a complex world 2020-2040 [online]. 2014. Available from: http://www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf

7. *Unmanned Ground Systems Roadmap* [online]. Robotic Systems Joint Project Office, 2011 [cit. 2017-05-02]. Available from: http://www.dtic.mil/ndia/2011/MCSC/Thompson_UGSRoadmap.pdf
8. *Unmanned Systems Integrated Roadmap 2013 - 2038*. Washington, D.C.: Government Printing Office, 2007.
9. *Using Unmanned Systems to Counter the Improvised Explosive Device Threat* [online]. [cit. 2017-05-02]. Available from: http://droneanalysis.blogspot.cz/2016/07/using-unmanned-systems-to-counter.html

Erik Görner[1]

National defense education in the Slovak Republic as an important feature of the nation's readiness for crisis situations[2]

Abstract

The today's security environment in Europe took a dramatic turn. Uncontrolled migration, the war in Eastern Ukraine and acts of terrorism that are difficult to predict became the features of the contemporary security environment. The main aim of this article is to evaluate the current state of national defense education nad preparedness of the nation for crisis situations. Evaluation is based on a comparison of national defense education in Slovakia in periods before and after gaining independence. We also briefly evaluate compulsory military service, voluntary military service, and other military training practices in Slovakia as we consider them part of the education of the nation in the sphere of the military. We found out that there is space for improvement regarding national defense education in the Slovak Republic. Also, out-of-school activities and broader military participation might be useful in the effort to maximize nation's readiness for crisis situations.

Key words: ***National defense education, the Slovak Republic, state of readiness, crisis situations***

[1] Mgr. Erik Görner is a PhD. Candidate at the Faculty of Political Science and International Relations, Matej Bel University, Kuzmányho 1, 974 01 Banská Bystrica, Slovak Republic, e-mail: erik.gorner@umb.sk.

[2] This article was written within the project VEGA 1/0545/17 Transformácia bezpečnostného prostredia: aplikácia skúseností štátov Vyšehradskej štvorky na príklade Ukrajiny.

Introduction

The contemporary security environment is much different from the one that prevailed most of the period of the Cold War. The simple bipolar confrontation between the United States of America and the North Atlantic Treaty Organization on one side and the Union of Soviet Socialist Republics and The Warsaw Pact on the other was gradually replaced by a complex set of the relation between independent states and other entities enjoying international sovereignty. Today's security environment became less clear. It is described by blurring of boundaries between war and peace, offense and defense. There are no more standing armies on the front. Heavily populated areas have become a war zone. Civilian casualties are on regular basis.

European security environment took a dramatic turn. From the end of the Second World War, there was no significant armed conflict in Europe. Nowadays we are witnesses of deep and profound security crisis. The war in Ukraine has started 2014 and still, there is no final peaceful resolution. The influx of migrants coming from the war-torn regions of the Middle East and Northern Africa is one of the major security challenges for Europe. Another important feature of such described security environment is terrorism. Acts of terrorism are difficult to predict, difficult to locate and it is almost impossible to prevent them. Terrorists usually attack soft targets, especially civilians and thus trying to spread fear or achieve their goals.

All the threats posed by today's security environment require much higher readiness of the societies in European states to react to crisis situations. The Slovak Republic is not an exception. Threats seem to be less immediate as in other European countries but as we mentioned it is very difficult to predict them. The Slovak Republic must prepare and educate its citizens how to act in crisis situations and take care of themselves in times of need.

The main aim of this article is to evaluate the current state of national defense education nad preparedness of the nation for crisis situations. Evaluation is based on a comparison of national defense education in Slovakia in periods before and after gaining independence. We also briefly evaluate compulsory military service, voluntary military service, and other military training practices in Slovakia as we consider them part of the education of the nation in the sphere of the military. In this research, we omit professional armed forces and military education because it is meant to educate soldiers and does not directly affect today's civil society and its readi-

ness. After evaluating the system of national defense education we mention the risks of the current state of such an education and try to propose a policy that could enhance it.

1. Comparison of national defense education in the Slovak Republic before and after gaining independence

In the first part of this chapter, we will describe and evaluate a national defense education[3] in Slovakia as it was from 1973 until 1991. After introducing old practice we will introduce and evaluate a new form of national defense education and finish the chapter with a comparison of past and present praxis.

Protection of the Czechoslovak Socialist Republic was according to a piece of legislation from 1973 the responsibility of the whole society. National defense education was understood as an inseparable part of the preparation of citizens for protection o their country. This education was based on class and international grounds. It should have enhanced the unity of armed forces and society. The protection of socialism and state were supposed to become one thing and the top priority of citizens as well (Predpis č. 73/1973).

The content of military training is on basis of Marxism-Leninism consistently shape, deepen and consolidate the socialist patriotism, proletarian internationalism and awareness of citizens to defend the Czechoslovak Socialist Republic and the necessary professional and technical knowledge, skills and habits, physical fitness and mental resilience (Predpis č. 73/1973, § 3/1).

National defense education started already in primary schools and further continued on high schools. There were also university subjects that provided national defense education for future teachers what secured that there would be enough professionals to teach young generations. National defense education was also a part of other subjects and different forms of education.

Citizens were not only prepared physically. National defense education was rather complex and provided also psychological education and substantive knowledge. There were different demands required from children, youth, and adults. National defense education changed according to the development of the society. There was also a requirement for scientific exploration

[3] The National Defense Education in the Slovak Republic before the Velvet Revolution in 1989 was called *branná výchova*. Later it was called *Ochrana človeka a prírody* (eng. *Protection of man and nature*). Current name is *Ochrana života a zdravia* (eng. *Protection of life and health*).

of the military education for society. National defense education was divided into four sections. Moral-political section ensured the belief of individual in favor of active engagement in countries defense. Professional-technical section was designed in a way it taught individuals to be able to act adequately in emergency situations. Physical education was aimed at providing physical ability. Last section, psychological, was aimed at providing knowledge and skills to react in crisis situations (Pavlík, 1980).

National defense education did not exist in first five of primary school as an autonomous subject. It was part of the curriculum of other subjects, namely: fundaments of civics and natural science, homeland study, physical education, and technical education (Ministerstvo školstva, 1971). Later on, in primary schools, it mainly dealt with non-military aspects of national defense education. As we already mentioned it was strongly based on the ideology of Marxism–Leninism, and one's obligations to protect its country and regime. In high schools, the content of national defense education was much different. It was designed in a way it taught basic military skills necessary to protect the country. As an example of what was taught, we may mention shooting, the study of military weapons, throwing a grenade, and protection against weapons of mass destruction (Soukup, 1985).

In school year 1991/1992 national defense education (branná výchova) as an autonomous subject was ended. It was replaced by *Protection of man and nature* which ceased to be autonomous subject. Education in the sphere of civic defense became just part of other subjects and exercises.

The main aim of new defense education was to prepare pupils for the protection of health, society, nature, for the education of safe behavior on workplace and in leisure time. Protection of man and nature is an inseparable part of the curriculum of following subjects: fundaments of civics and natural science, homeland study, physical education, natural science, technical education, natural history, geography, physics, and chemistry. As there is no program on universities for future defense education teachers, education for teachers takes a form of took one-day professional courses. The curriculum was thematically divided into five issues: resolution of emergency situations – civil defense; medical training; movement and the stay in nature and its protection; traffic education; and education for safe behavior. The education starts in the first year of primary school (1-9) and continues until the end middle schools (1-4). In each higher grade education becomes more and more complex. In first four years of primary schools, pupils were taught how to safely live in their local environment and how to react to local

non-military threats. In last five years, the education became more professional and there was also education about military threats- mainly weapons of mass destruction. In middle school, few more issues were added to the curriculum: technical activities and sport; workplace safety; current problems of humanity and their resolution (Modrák – Betuš- Lacko, 2007).

The curriculum containing issues of national defense has undergone its renaissance after September 11, 2001. Primary school teachers could attend courses providing knowledge from population protection, international humanitarian law, anti-radiation and chemical protection, civil defense, and civil defense organization and management. Most of the practical skills were taught at exercise which took place outside. Also, some of the military skills were part of such a curriculum – throwing a grenade at the target, air gun shooting. It was stressed that all the citizens have to take their part in civil defense (Modrák, 2007).

The compulsory curriculum of *Protection of man and nature* has been replaced by *Protection of life and health.* The basic difference between these two cross-section topics is that the later omits the protection of nature and traffic education which became the part of the curriculum of other subjects. The main aim of civil defense education stays the same: pupils should be able to cope with crisis situations which arose as a consequence industrial and ecological catastrophes, traffic accidents, natural disasters, foreign power actions, and terrorism (Ochrana života a zdravia, 2017).

Formative and informative components of the curriculum present the activities of students:

- *moral, which form the basis of their patriotic and national feeling*,
- *professional, which allow them the acquisition of knowledge and skills of self-protection and providing assistance to the others in the case of a threat to health and life*,
- *psychological, which helps them in process of adaptation in case of difficult situations*,
- *physical, which is characterized by the formation of preconditions to achieve higher physical fitness and overall body resistance to physical and mental workload in intense life situations* (Slezák, 2009, p.3).

Comparison of National defense education on one side and Protection of man and nature and Protection of life and health on the other is very difficult. to our knowledge, there has been no complex sociological research of readiness of society to react in crisis situations in past and present allowing

us to compare empirical data. Even though there is a space for comparison based on well-known facts.

The great difference between pre-1991 education and one after is that National defense education was a real subject not just a part of the curriculum of other subjects combined with exercises. It allowed National defense education to be much more complex and to deal with both military and non-military threats. Also, skills and knowledge gained from the subject were convincing. Another important fact is that future teacher could study National defense education at universities what means they became experts in this field. Today teachers gain knowledge only through educational courses.

Also, Melicher writes that education of Protection of man and nature is educated in a way that is completely in contrast with aims and content of its curriculum. The main flaw of such an education is it is understood just as a formality and teachers are far from being sufficiently prepared to teach such a curriculum (Melicher, 2006).

On the other hand, National defense education was highly politicized. Ideological ballast formed a huge part of all education. In 2003 there was an article in Slovak newspaper SME. It stated that the autonomous subject teaching national defense education would still probably be interesting for pupils. Ideology formed just one-fourth of education of this subject and could be easily transformed or erased from the curriculum. Many schools discussed the return of such a subject that would prepare the student for crisis situations. Part of the curriculum of National defense education was also sports shooting and topography. Headmaster of Evangelical High School in Tisovec after practicing school evacuation said that come back of National defense education wold be welcome. Another reason for the comeback of this subject were terrorist attacks in New York 2001 which showed a need for society to be prepared for crisis situations (Horáková, 2003).

National defense becomes an interesting subject only in a time when there is an immediate threat to society. Nevertheless, terrorist attacks still haven't convinced Slovak policymakers to incorporate an autonomous subject dealing with national security into the curriculum. The article also notes that some of the teachers see that pupils are not prepared for crisis situations sufficiently.

In 2012 an interesting research on defense education was published. Authors write that results of the research should not be generalized. Its value is just orientational. Nevertheless, the results are of certain value because as

we wrote there has been no complex research conducted regarding the topic of this paper. The research was conducted in 18 primary schools on pupils in ninth grade. The cross-section subject Protection of man and nature in ninth grade was carried out through one exercise in fall (September or October). Only 219 out of 456 pupils attended exercises what was proved by a class register of particular classes. That means that more than half of pupils didn't attend either subjective or objective grounds. According to the research, Protection of man and nature itself is an unpopular subject. 54% of respondents told they find curriculum of Protection of man and nature unattractive (Bendíková - Kopecký 2011).

All this illustrates the real state of education of national defense in Slovakia. We don't want to suggest that nowadays the education of national defense is non-existent or totally unsuitable. What we want to suggest is that there is a rather broad space for improvements in such an education.

2. Short evaluation of out-of-school defense education

It is common knowledge that in states of the former Eastern Bloc were mass armies manned by the means of compulsory military service. It provided military skills and military education for the most of the male population. However, 2006 compulsory military service has been suspended and might be applied only during the war of state of war. Conscription not only guaranteed the higher state of readiness and military preparedness of nation but it also provided a link between civilians and soldiers which many times shrinks after the adoption of all volunteer force.

There are several reasons why compulsory military service in peacetime was suspended. Since we don't want to go into details we will just briefly describe these reasons.

One of the reasons is the compulsory military service acceptance across the society. In 1993 the research of public opinion took place. Only 19,4% of respondents were in favor of all volunteer force. When people were asked whether it is important to educate the society in the sphere of national defense 88% of respondents said yes. When the question was asked whether the professionalization of armed forces is a correct step 68,4% responded positively. Shortened time of compulsory military service was also accepted by most of the respondents (Ministerstvo obrany Slovenskej republiky, 1993).

Ten years later in 2003 2/3 of respondents were in favor of the full profes-

sionalization of armed forces. Only 18,2% taught that keeping of compulsory military service was a good idea. More than 65% of respondents had no interest in serving in professional armed forces (Ministerstvo obrany Slovenskej republiky. 2004).

Public opinion clearly shows that Slovak society has moved from quite broad acceptance of compulsory military service towards its suspension. It also says that Slovaks mostly don't want to serve in armed forces. They want to be passive recipients of security.

Second reason why peacetime compulsory military service was finally suspended is accession of Slovak republic into NATO and standards of an army required by the alliance. Also, one part of the reason is the long period of peace in Europe that has been ended challenged by new forms of a threat at least from September 11. 2001.

Last of the major reasons to abolish peacetime conscription is financial. Since there has been no need for mass armed forces it is inefficient for a state to keep compulsory military service. See for example articles written by Friedman (1967); Garfinkel (1990); Poutvaara and Wagener (2007) that prove our statement.

In the history of the Czechoslovak republic and the Czechoslovak Socialist Republic, there were paramilitary organizations preparing Czechs and Slovaks for national defense. These organizations attracted many citizens. In 1938 national guards together with *Sokol* paramilitary organization armed with light weaponry supported the regular army in its tasks (Stejskal, 2014).

Nowadays the only program that is similar to past praxis of voluntary activism in militias and paramilitary organizations is Voluntary military service organized by Ministry of Defense of the Slovak Republic.

Only 129 persons were interested in completing first voluntary military training that lasted for 12 weeks. As Minister of Defense told: *One of the aims of voluntary military preparation is to enhance patriotism and national defense awareness of citizens because defense is not a concern of an individual rather it concerns all of us. Among our priorities which we want to push through in upcoming period is an enhancement of readiness of armed forces reserves. The key element for the creation of armed forces reserves might be the voluntary military service. Volunteers might also be the great source of manpower for security forces.* In first 9 weeks of military training, recruits get basic knowledge in tactics. They are also trained in orientation in nature, shooting, topography, and medical training. Other skills and abilities one gets throughout the training are enhanced mental physical and

psychological readiness and self-discipline. Last three weeks of training are dedicated to professional training for four military proficiencies: gunner, engineer, radio operator, and decontaminator (Dobrovoľná vojenská príprava neláka, 2016).

A public opinion poll showed that Voluntary military service is accepted by the most of the society. More than 72% of respondents told that it should continue also in the future. Alo 56,3% thought that each able-bodied young person should complete voluntary military service. Nevertheless, when young citizens were asked whether they want to serve only 18,3%, responded positively while 76,8 negatively (Prieskum ukázal jasne, 2016).

Today's situation with civic organizations dealing with national defense is very chaotic. There are few organizations dealing with national defense, sports activities, and official support of Armed Forces of the Slovak Republic and professional soldiers. to be specific: The Slovak Union of Reserve Soldiers; Union of Soldiers of the Slovak Republic; Union of War Veterans of the Slovak Republic; Club of General of the Slovak Republic[4]. On the other hand, there is some organization dealing with issues of national defense that are not supportive for Armed Forces of the Slovak Republic and have slightly or even very different beliefs than official policy of the Slovak Republic.

According to Radovan Braník, an expert on extremism, there are more extremist paramilitary organizations in Slovakia. One of the well-known is called Slovak Recruits[5]. One of the leaders of these organization used to fight for separatists in Ukraine. Nowadays Slovak Recruits tend to deradicalise. The organization got rid of the most extreme members. According to Braník one of the most radical organizations is Resistance Kysuce[6]. Members are trying to infiltrate into police and armed forces. The group is still rather small. Another one is Association of Slovak soldiers[7]. The core of the group is mainly formed by professional soldiers in reserves. They were trained by state and state still pays them military retirement pensions. Association has political goals and part of these goals represent political extremism. Organization forms and opposition against the North Atlantic Treaty Organization and the European Union and inclines towards Russian interests. The chairman of Association of Slovak soldiers Jozef Žarnovičan said that democracy was a dead ideology. He even threatened with coup de that if his ideas will not be materialized (Marcišiak, 2017).

[4] Original names in Slovak language respectively: *Slovenský zväz vojakov v zálohe, Zväz vojakov Slovenskej republiky, Únia vojnových veteránov Slovenskej Republiky, Klub Generálov Slevenskej republiky.*

[5] Original name in Slovak language: *Slovenský branci.*

[6] Original name in Slovak language: *Vzdor Kysuce.*

[7] Original name in Slovak language: *Asociácia slovenských vojakov (ASV).*

Conclusion

State of readiness for crisis situations of the Slovak nation is not totally insufficient. School education provides basic knowledge in this area. However, there is a rather broad space for enhancement in the area of national defense education in primary and middle schools. In our opinion, National defense education courses and programs should be reintroduced on universities to train a future teacher. In the meantime, there are still teachers who finished such courses during the time of socialism. They might be reeducated during short courses and continue to teach National defense education as an autonomous subject. Also, it should be supervised whether the education of subject National defense education is carried out properly together with mandatory exercises.

Regarding further possibilities to prepare society for crisis situations, the praxis of Voluntary military service should be continued. Also, the similar praxis of creating active reserves might be a solution. It is important thought to change legislation in a way it would not be a barrier for civilians to join reserves. They should be allowed to miss some time at the workplace in order to train. Voluntary military service should also try to attract people because of their patriotism and voluntarism, they should not be motivated just financially.

New legislation seems to be necessary also in the field of civic associations. It is highly undesirable to have uncontrolled paramilitary organizations with ideas against the interest of the state of origin. It might be very beneficial to create citizen based militias, which would cooperate with police and armed forces, organized on the level of lower administrative units as suggested by Pernica (2007).

Nevertheless, current security environment suggests that new military and non-military threats like for example terrorism will put a strain on civil society. There will be a high need for readiness of whole nation to keep the country safe from irregular threats and immune of foreign propaganda.

References

1. BENDÍKOVÁ, E. – KOPECKÝ, M. 2011. *Obsahová náplň, úroveň vedomostí a zručností žiakov základných škôl z učiva Ochrana človeka a prírody.* Olomouc: Univerzita Palackého v Olomouci, 2012. 111 s. ISBN 9788024431796
2. *Dobrovo'ná vojenská príprava neláka: Prihlásilo sa do nej iba to'koto záujemcov.* In topky.sk [online]. 2016 [cit.15.04.2017], Available at: http://www.topky.sk/cl/10/1541281/Dobrovolna-vojenska-priprava-nelaka–Prihlasilo-sa-do-nej-iba-tolkoto-zaujemcov
3. FRIEDMAN, M. 1967. *Why Not a Voluntary Army?* In New Individualist Review, 1967. p 3-9.
4. GARFINKEL, M. R. 1990. *The Role of the Military Draft in Optimal Fiscal Policy.* In Southern Economic Journal, 1990. P. 718-731.
5. HORÁKOVÁ, J. 2003. *Vráti sa branná výchova do škôl?* In SME.sk [online]. 2003 [cit.14.04.2017], Available at: https://www.sme.sk/c/863910/vrati-sa-branna-vychova-do-skol.html
6. MARCIŠIAK, M. 2017. Bránik: *Skutočnou hrozbou pre Slovensko sú frustrovaní bývalí vojaci, hrozia vojenským pučom* In tvnoviny.sk [online]. 207 [cit.18.04.2017], Available at: http://www.tvnoviny.sk/exkluzivne/1858496_branik-skutocnou-hrozbou-pre-slovensko-su-frustrovani-byvali-vojaci-hrozia-vojenskym-pucom
7. MELICHER, A. 2006. *Overovanie štandardov učiva Ochrana človeka a prírody v stredných školách. In Pedagogické spectrum*, 2006, nr. 3 – 4, ISSN 1335-5589
8. Ministerstvo obrany Slovenskej republiky. 1993. Armáda 93. Harmanec: SESOS MO SR, 1993. 135 p ISBN 80 – 88842 – 69 – 7
9. Ministerstvo obrany Slovenskej republiky. 2004. *Ročenka ministerstva obrany Slovenskej Republiky 2003.* Bratislava: Ministerstvo obrany Slovenskej republiky, 2004. 164 p.
10. Ministerstvo školstva slovenskej socialistickej republiky. 1971. Učebné osnovy pre 6.-9. ročník základnej deväťročnej školy. Bratislava: Slovenské pedagogické nakladateľstvo, 1971. 12 p.
11. MODRÁK, M. – BETUŠ, Ľ. – LACKO, N. 2007. *Cvičenia CO, účelové cvičenia, ochrana človeka a prírody v ZŠ a SŠ 2. časť.* Prešov: Metodicko-pedagogické centrum, 2007. 76 p. ISBN 978-80-8045-482-1
12. MODRÁK, M. A kol. 2007. *Cvičenia CO, účelové cvičenia, ochrana*

človeka a prírody v ZŠ a SŠ 1. Časť. Prešov: Metodicko-pedagogické centrum, 2007. 66 p. ISBN 978-80-8045-481-4
13. Ochrana života a zdravia. In Statpedu.sk [online]. 2017 [cit.14.04.2017], Availabalbe at: http://www.statpedu.sk/clanky/statny-vzdelavaci-program-svp-pre-prvy-stupen-zs-prierezove-temy/ochrana-zivota-zdravia
14. PAVLÍK, L. A kol. 1980. *Branná výchova pro studující učitelství na I. stupni základní školy.* Praha: Karlova univerzita, 1980. 176 p.
15. PERNICA, B. 2007. *Dobrovolná milice – doplněk zajištění bezpečnosti územně samosprávných celků.* In Increasing Competitiveness or Regional, National, and International Markets Development – New Challenges. 1. vyd. Ostrava: VŠB-TUO, 2007. ISBN 978-80-248-1458-2. [CD+proceedings p. 281] [international conference Increasing Competitiveness or Regional, National, and International Markets Development – New Challenges, Ostrava, Ekonomická fakulta VŠB-TUO 4 – 6. 2007]
16. POUTVAARA, P. – WAGENER A. 2007. *To draft or not to draft? Inefficiency, generational incidence, and political economy of military conscription.* In European Journal of Political Economy, 2007, p. 975–987.
17. Predpis č. 73/1973 Z. z. Zákon o brannej výchove
18. Prieskum ukázal jasne: Dobrovoľná vojenská príprava je dôležitá, občania chcú brániť vlasť. In topky.sk [online]. 2016 [cit.15.04.2017], Available at: http://www.topky.sk/cl/10/1596855/Prieskum-ukazal-jasne--Dobrovolna-vojenska-priprava-je-dolezita–obcania-chcu-branit-vlast
19. SLEZÁK, J. 2009. *Ochrana života a zdravia. Bratislava: Štátny pedagogický ústav*, 2009. 19 p.
20. SOUKUP, J. 1985. Branná výchova pre druhý ročník stredných škôl. Bratislava: Slovenské pedagogické nakladateľstvo, 1985. 128 p.
21. STEJSKAL, L. 2014. *Dobrovolná občanská participace při zajišťování obrany: Koncept, zkušenosti a perspektivy.* In Obrana a strategie, 2014, vol. 14, nr. 2, s. 119-133. ISSN 1802-7199

Bartosz Maziarz[1]

Polish military missions in the public perception

Abstract

Poland since the beginning of the twenty-first century, and was involved in several military operations of great significance in the political and military for the whole world. The fight against global terrorism in Afghanistan, the implementation of the provisions allied to the US and military involvement in Iraq, the obligation to NATO allied partners from the Baltic countries are just a few of the examples of Polish military involvement on the map of global risks. How to take part in military interventions, military operations and fulfill its alliance commitments approached Polish society?
This article is an attempt to approximate public sentiment towards Polish military engagement in the world after 2001.

Key words: ***polish military mission, public opinion, Afghanistan, Iraq, CBOS, TNS OBOP***

Polskie misje wojskowe w odbiorze społecznym po 2001 r.

Opinie polskiego społeczeństwa na temat udziału naszych żołnierzy w misjach wojskowych rozpoczętych po 2001 r., były od samego początku negatywne. Tuż po zamachach z 11 września 2001 r., Polacy w większości popierali interwencję Stanów Zjednoczonych w Afganistanie. W badaniu TNS OBOP z października 2001 r., aż 69% ankietowanych Polaków uważało za słuszną interwencję USA w Afganistanie. W podobnym badaniu przeprowadzonym przez CBOS - odsetek głosów popierających działania Stanów Zjednoczonych w Afganistanie wynosił 61%[2]. Jednakże na pytanie dotyczące ewentualnego udziału polskich żołnierzy w operacji afgańskiej, odpowiedzi polskiego społe-

[1] Dr Bartosz Maziarz, Pracownia Polityki Bezpieczeństwa, Instytut Politologii Uniwersytetu Opolskiego ul. Katowicka 89, 45-061 Opole, e-mail: bartosz.maziarz@uni.opole.pl

[2] TNS OBOP, *Polacy o akcji zbrojnej w Afganistanie i terroryzmie*, Warszawa, listopad 2001; CBOS, *Poparcie dla akcji w Afganistanie*, Warszawa 2001.

czeństwa były podzielone. 45% respondentów opowiadało się za poparciem udziału w wojnie afgańskiej, przeciw było 44% badanych[3]. Taka tendencja utrzymywała się do przełomu lat 2002-2003, kiedy tempa nabierały międzynarodowe negocjacje dotyczące udziału w planowanej wojnie irackiej. Dynamicznie rozwijająca się sytuacja w Zatoce Perskiej, popieranie polityki USA przez polskie władze spowodowały, że opinia publiczna zaostrzyła swoje sądy odnośnie trwającej już misji afgańskiej, jak również planowanego udziału w wojnie w Iraku.

Ciekawym jest fakt, że opinie sprzeciwiające się udziałowi polskich żołnierzy w misjach w Iraku i Afganistanie, były odwrotnie proporcjonalne do zapatrywania się obywateli na czynny udział Polski w polityce międzynarodowej. Według TNS OBOP w czerwcu 2003 r. 64% ankietowanych wskazywało, że Polska powinna angażować się w politykę międzynarodową[4]. W tym samym okresie, w badaniu CBOS, 55% badanych sprzeciwiało się udziałowi Polski w operacji w Iraku[5]. W grudniu 2007 r., nieco ponad połowa Polaków opowiadała się za zwiększonym zaangażowaniem naszego kraju w światową politykę[6]. W badaniu z października 2007 r., przeprowadzonym przez CBOS, sprzeciw wobec polskiej obecności wojskowej w Iraku wyrażało aż 81% ankietowanych. W kontekście misji afgańskiej - 77% badanych nie popierało udziału Polski w wojnie w Afganistanie[7]. Interesującym jest fakt, że w przypadku tego badania, nie uwidaczniają się różnice w poglądach politycznych respondentów. Większość badanych nie aprobowała wojskowych działań Polaków w tych państwach, niezależnie od prezentowanych sympatii politycznych, wykształcenia, pochodzenia oraz statusu majątkowego[8].

Malejące poparcie dla polskiej obecności wojskowej w Afganistanie (w grudniu 2007 r., tylko 14% ankietowanych popierało udział polskich żołnierzy w operacji NATO w Afganistanie, wobec aż 83% badanych będących przeciw temu udziałowi - spowodowane było wydarzeniami związanymi z ostrzałem afgańskiej wioski przez polskich żołnierzy, podczas którego zginęli cywile), w połączeniu z wysoką dezaprobatą dla polskiej obecności w Iraku

[3] Dane z grudnia 2001 r. Zob. CBOS, *Opinia publiczna o udziale polskich żołnierzy w misjach poza granicami kraju oraz ostatnich wydarzeniach w Iraku*, Warszawa, luty 2007.

[4] TNS OBOP, *Po zapowiedzi wycofania wojska z Iraku*, Warszawa, grudzień 2007, s. 4.

[5] CBOS, *Opinia publiczna o udziale polskich żołnierzy w misjach poza granicami kraju oraz ostatnich wydarzeniach w Iraku...* .

[6] 51% ankietowanych wskazywało, że Polska powinna angażować się w politykę międzynarodową. Zob. TNS OBOP, *Po zapowiedzi wycofania wojska z Iraku....*

[7] CBOS, *Stosunek do obecności żołnierzy polskich w Iraku i Afganistanie*, Warszawa, październik 2007, s. 2-3.

[8] Odnośnie opinii dotyczącej zaangażowania militarnego w Iraku, przeciw było 76% wyborców PO, 79% wyborców PiS, 80% PSL i aż 87% elektoratu SLD. W kwestii dotyczącej Afganistanu, swój sprzeciw wyrażało 69% wyborców PO, 74% elektoratu PiS, 76% wyborców PSL i 88% głosujących na SLD. Zob. CBOS, *Stosunek do obecności żołnierzy polskich w Iraku i Afganistanie*, Warszawa, październik 2007, s. 4.

w latach 2003-2008 spowodowało, żePolacy byli jednym z najbardziej pacyfistycznie nastawionych społeczeństw na świecie[9]. Sprzeciw wobec misji NATO w Afganistanie był w Europie niższy niż w Polsce. W lipcu 2009 r., 59% ankietowanych Polaków, uważało, żeAfgańczycy chcieliby, aby wojska NATO opuściły ich kraj. W Niemczech, odsetek takich głosów wynosił 55%, w Wielkiej Brytanii - 47%, we Francji - 46%, a w Stanach Zjednoczonych tylko 39%. Na pytanie dotyczące natychmiastowego zakończenia misji ISAF w lipcu 2009 r., za opowiedziało się 65% naszych rodaków, 52% obywateli Niemiec, 47% Brytyjczyków, 38% Francuzów i tylko 30% Amerykanów[10]. We wrześniu 2009 r. polski udział w operacji afgańskiej popierało 20% ankietowanych a 76% respondentów było przeciwnych[11]. Podobne wyniki sondaży, zanotowano w listopadzie 2010 r., kiedy poparcie dla misji ISAF i udziału w niej Polaków spadło do 17%, przy jednoczesnym sprzeciwie 79% rodaków[12]. W badaniach przeprowadzonych w listopadzie 2011 r., przez Fundację na Rzecz Studiów Europejskich wespół z TNS OBOP, przeciw obecności polskich żołnierzy w Afganistanie było 69% badanych, „za" opowiedziało się 17%[13].

Sprzeciw wobec udziału Wojska Polskiego w misji w Afganistanie od 2003 r., oscylował na poziomie ok 70%. Taka tendencja widoczna była przez cały okres wypełniania mandatu ISAF przez polskich żołnierzy. Należy podkreślić, żezarówno misja iracka, jak i afgańska polskiego wojska, nieczęsto była obiektem zainteresowania ośrodków zajmujących się badaniem opinii publicznej, mediów, jak również samego społeczeństwa. Polacy pomimo wyraźnego sprzeciwu wobec obu wojen toczonych po 2001 r., nie przejawiali głębszej refleksji na ich temat. Wykazana wyżej sprzeczność w opiniach naszych rodaków dotyczących zaangażowania Polski w politykę światową przy jednoczesnym sprzeciwie wobec obecności wojskowej w Afganistanie i Iraku, dobitnie świadczy o fakcie, żepercepcja środowiska międzynarodowego przez polskie społeczeństwo nie jest najlepsza. Głównymi powodami wyrażania sprzeciwu przez Polaków wobec misji polskich żołnierzy w Iraku i Afganistanie, były niechęć do ponoszonych ofiar przez polską armię, brak wiary w skuteczność i sensowność obu misji, koszty związane z wyekspediowaniem

[9] CBOS, *Stosunek do obecności polskich żołnierzy w Afganistanie i ostatnich wydarzeń związanych z tą operacją*, Warszawa, grudzień 2007, s. 1.

[10] CBOS, *Światowa opinia publiczna o polityce Stanów Zjednoczonych i operacji NATO w Afganistanie*, Warszawa, lipiec 2009, s. 10-11.

[11] CBOS, *Opinia publiczna wobec misji NATO w Afganistanie*, Warszawa, wrzesień 2009, s. 1.

[12] CBOS, *Udział Polski w operacji NATO w Afganistanie i jego konsekwencje*, Warszawa, listopad 2011, s. 1.

[13] Sg, *OBOP: tylko 17 proc. Polaków popiera misję w Afganistanie*, Portal internetowy Polskiego Radia, źródło: http://www.polskieradio.pl/5/3/Artykul/477987,OBOP-tylko-17proc-Polakow-popiera-misje-w-Afganistanie (10.03.2017).

żołnierzy oraz doniesienia o zwiększaniu liczebności polskich kontyngentów wojskowych.

Powody te przypominają sprzeciw amerykańskiego społeczeństwa wobec wojny wietnamskiej na przełomie lat 60. i 70. XX wieku - na co wskazuje Klaus Bachmann[14]. W przeciwieństwie do Stanów Zjednoczonych czasów wojny w Wietnamie i Europy w 1968 r., w Polsce nie spotykaliśmy się z wielotysięcznymi manifestacjami antywojennymi czy innymi przejawami jawnie wyrażanego sprzeciwu Polaków wobec wojen w Afganistanie i Iraku. Powodem takiego stanu rzeczy niewątpliwe jest fakt, żezarówno Irak, jak i Afganistan są odległymi krajami i wydarzenia mające w nich miejsce - pozornie - nie dotyczą bezpośrednio mieszkańców Polski. Potwierdzeniem tej tezy są badania dotyczące poczucia zagrożenia zamachami terrorystycznymi, przeprowadzone przez CBOS w maju 2011 r. (po zabiciu Osamy bin Ladena przez amerykańskich komandosów w Pakistanie), oraz w czerwcu 2013 r. (po zamachu bombowym w Bostonie). Wyniki obu badań jasno wskazują, że Polacy nie odczuwają zagrożenia terroryzmem. W maju 2011 r. 69% ankietowanych odpowiedziało, że ryzyko zamachu terrorystycznego w Polsce nie zwiększyło się po śmierci przywódcy Al-Kaidy. Zaś 63% badanych na pytanie o obawy związane z atakiem terrorystycznym w Polsce odpowiedziało, że takiego ataku się nie obawia. Swoje obawy wyraziło 35% ankietowanych, spośród których, tylko 7% wskazało, że obawia się bardzo takiego ataku[15]. W 2013 r. różnice w percepcji zagrożenia terroryzmem w Polsce uległy zwiększeniu, ponieważ na pytanie o obawy wystąpienia aktów terroryzmu w Polsce, twierdząco odpowiedziało 26% badanych, z czego tylko 5% obawiało się ataków w znaczący sposób. Brak obaw wskazało 72% uczestniczących w badaniu[16].

Kolejnymi badaniami opinii publicznej, potwierdzającymi brak zainteresowania oraz odczuwania zagrożenia ze strony np. Afganistanu, są raporty CBOS dotyczące poczucia zagrożenia bezpieczeństwa Polaków w kontekście wydarzeń na Krymie i polityki Rosji. W badaniu przeprowadzonym w kwietniu 2014 r. aż 47% ankietowanych wskazało, żeodczuwa zagrożenie dla niepodległości Polski. Brak zagrożenia wskazało 41% badanych. Co trzeci Polak uważał, że potencjalne zagrożenie dla Polski ma charakter militarny. Jako kraj, który stanowi największe zagrożenie dla naszego państwa, Polacy wskazują Rosję - 80% odpowiedzi. Kraje arabskie/islamskie/muzułmańskie, bez wyszczególniania, o jakie kraje konkretnie chodzi, stanowiące zagrożenie dla

[14] K. Bachmann, *Chwiejne procenty*, Polska Zbrojna nr 1/2012, s. 28-29.
[15] CBOS, *Poczucie zagrożenia terroryzmem po śmierci Osamy bin Ladena*, Warszawa, maj 2011.
[16] CBOS, *Zagrożenie terroryzmem*, Warszawa, czerwiec 2013.

Polski i jej mieszkańców, wskazał tylko 1% badanych. w 2014 r. większy odsetek Polaków obawiał się zagrożenia ze strony USA (2% wskazań), niż ze strony krajów muzułmańskich czy Korei Północnej (obie odpowiedzi uzyskały 1% głosów). Świadczy to o braku zainteresowania Polaków odległymi konfliktami, pomimo przeszło 10-letniego udziału w wojnach w Afganistanie i Iraku[17]. W październiku 2014 r. obawy Polaków dotyczące zagrożenia militarnego wzrosły o 12%. 42% badanych uważało, że realne jest wkroczenie obcych wojsk na terytorium Rzeczypospolitej. Ogólne poczucie zagrożenia wśród Polaków, związane z wydarzeniami mającymi miejsce na Ukrainie, wzrosło do 67%[18].

W odniesieniu do pozostałych misji wojskowych w których udział brali polscy żołnierze po 2001 r., poza misją w Czadzie, brakuje badań opinii publicznej dotyczących misji w Mali, na Morzu Śródziemnym, jak również misji Baltic Air Policing. Jedynym badaniem, przeprowadzonym w 2008 r. dotyczącym innej misji wojskowej poza Afganistanem i Irakiem, było pytanie o poparcie udziału polskich żołnierzy w misji UE w Czadzie. Poparcie wyraziło wówczas 30% badanych, wobec 60% będących przeciwnymi udziałowi Polaków w tej misji[19].

Koszula bliższa ciału, niż sukmana - to stare polskie przysłowie najlepiej oddaje stosunek Polaków do zagranicznych misji polskiego wojska. Polskie społeczeństwo nie wykazuje większego zainteresowania sferą polityczną problematyki międzynarodowej, nie wspominając już o międzynarodowym bezpieczeństwie, jako elemencie składowym polityki zagranicznej. Zdecydowanie więcej uwagi, Polacy przykładają do zagadnień gospodarczych, społecznych czy polityki krajowej, niż do wojen w odległych zakątkach świata. Sytuacja ta uległa zmianie wraz z aneksją Krymu przez Rosję oraz wojną domową trwającą na Ukrainie. Głównym powodem zainteresowania Polaków kwestiami bezpieczeństwa i wzrostu poczucia zagrożenia w 2014 r. był aspekt geopolityczny - Rosja i Ukraina są najbliższymi sąsiadami naszego kraju.

Widoczne wieloletnie wyrażanie sprzeciwu wobec dwóch największych misji polskiej armii: afgańskiej i irackiej, spowodowane było w większości brakiem zainteresowania międzynarodową polityką oraz niewiedzą Polaków, niż faktycznym zainteresowaniem omawianą tematyką. Percepcja polskiego społeczeństwa nt. misji wojskowych była i jest niewielka. Polacy w tej materii operują głównie stereotypami oraz powielanymi przez media, częstokroć

[17] CBOS, *Polacy o bezpieczeństwie narodowym i NATO*, Warszawa, kwiecień 2014, s. 1-4.

[18] CBOS, *Zainteresowanie sytuacją na Ukrainie i poczucie zagrożenia w październiku*, Warszawa, październik 2014, s. 3-7.

[19] CBOS, *O udziale polskich żołnierzy w operacjach militarnych za granicą, tarczy antyrakietowej i zagrożeniu terroryzmem*, Warszawa, luty 2008, s. 11.

błędnymi, informacjami i ocenami. Powodem niewiedzy Polaków, nt. udziału polskich żołnierzy w misjach poza granicami kraju jest brak odpowiednio prowadzonej polityki informacyjnej Ministerstwa Obrony Narodowej oraz specyfika polskich mediów. Priorytetem Ministerstwa Obrony Narodowej było wykonywanie zadań i wywiązywanie się z sojuszniczych zobowiązań w Afganistanie i Iraku, przez co działania PR dotyczące polskich kontyngentów wojskowych były niewystarczające i źle prowadzone. Media zaś informowały społeczeństwo o wojskowej misji zagranicznej zazwyczaj przy okazji ataku na polskich żołnierzy, śmierci polskich żołnierzy czy też w związku z nieprawidłowościami związanymi z działalnością polskich żołnierzy poza granicami kraju (braki sprzętowe w wyposażeniu, kwestie dotyczące wynagrodzeń żołnierzy, wysokości polis ubezpieczeniowych wykupionych przez MON dla żołnierzy służących poza granicami kraju w rejonach konfliktu, etc.). Te czynniki w połączeniu z nieregularnymi badaniami opinii publicznej (badania zazwyczaj organizowane były przy okazji jakiegoś wydarzenia związanego z wojną w Iraku lub Afganistanie, np. zamach w którym zostali ranni lub zginęli polscy żołnierze), doprowadziły do takiego a nie innego postrzegania polskiego zaangażowania w misje wojskowe.

Bibliografia

1. Bachmann K., *Chwiejne procenty*, Polska Zbrojna, nr 1/2012.
2. CBOS, *O udziale polskich żołnierzy w operacjach militarnych za granicą, tarczy antyrakietowej i zagrożeniu terroryzmem*, Warszawa, luty 2008.
3. CBOS, *Opinia publiczna o udziale polskich żołnierzy w misjach poza granicami kraju oraz ostatnich wydarzeniach w Iraku*, Warszawa, luty 2007.
4. CBOS, *Opinia publiczna wobec misji NATO w Afganistanie*, Warszawa, wrzesień 2009.
5. CBOS, *Poczucie zagrożenia terroryzmem po śmierci Osamy bin Ladena*, Warszawa, maj 2011.
6. CBOS, *Polacy o bezpieczeństwie narodowym i NATO*, Warszawa, kwiecień 2014.
7. CBOS, *Poparcie dla akcji w Afganistanie*, Warszawa 2001.
8. CBOS, *Stosunek do obecności polskich żołnierzy w Afganistanie i ostatnich wydarzeń związanych z tą operacją*, Warszawa, grudzień 2007.
9. CBOS, *Stosunek do obecności żołnierzy polskich w Iraku i Afganistanie*, Warszawa, październik 2007.
10. CBOS, *Światowa opinia publiczna o polityce Stanów Zjednoczonych i operacji NATO w Afganistanie*, Warszawa, lipiec 2009.

11. CBOS, *Udział Polski w operacji NATO w Afganistanie i jego konsekwencje*, Warszawa, listopad 2011.
12. CBOS, *Zagrożenie terroryzmem*, Warszawa, czerwiec 2013.
13. CBOS, *Zainteresowanie sytuacją na Ukrainie i poczucie zagrożenia w październiku*, Warszawa, październik 2014.
14. Sg, *OBOP: tylko 17 proc. Polaków popiera misję w Afganistanie*, Portal internetowy Polskiego Radia, źródło: http://www.polskieradio.pl/5/3/Artykul/477987,OBOP-tylko-17proc-Polakow-popiera-misje-w-Afganistanie (10.12.2014).

Tomáš Novotný[1]

Contemporary Terrorism Manifestations (Simple Causal Model Analysis)

Abstract

This article briefly describes and puts together conclusions of the Copenhagen Peace Research Institute' key publications, which were released within the transformation of the Security Studies at the turn of the millennium, with conclusions of the UN Human Security Concept that was successfully institutionalized in 2012. Afterwards, the Copenhagen School *methodology was applied on the UN Human Security Concept to identify a set of human security challenges and threats, which have been - after analysis of their causal relationship - supplemented by a causal classification. Most security threats create a causal link with one or more other security threats. This fact implies that there is a possibility to create a causal model (mental, graphic, etc.) of any security threat to simulate or to predict the consequences and successfulness / efectivity of a suggested security solution (securitizating or de-securitizating). As a practical subject of a security threat causal analysis was used the model of processes on the way* from a state failure to a terrorism manifestation *adapted to contemporaty situation in the European Union.*

Key words: ***security, human security, security threats, security sectors, securitization, causal analysis, causal model***

[1] Col. Tomáš Novotný Col, PhD. Director Education Centre Armed Forces Academy of General M. R. Stefanik (Akadémia ozbrojených síl generála M. R. Štefánika) Demänová 393, 031 06 Liptovský Mikuláš, Slovakia tomas.novotny@aos.sk

Introduction

The state policy [has] to protect life, liberty, and property from acts of terrorism, [has] to condemn terrorism as inimical and dangerous to the national security of the country and to the welfare of the people, and [has] to make terrorism a crime against the people, against humanity, and against the law of nations[2].

1. The Copenhagen School theory

By the collapse of the Soviet Union in the early 1990's, the mostly bi-polar system of international relations dramatically changed to the uni-polar one with the U.S. as the only global power. That substantial change initiated both the expansion and the transformation in area of the Security Studies. The new, complex perception of security has enlarged the traditional framework of hard (military – political) security, and embodied new economic, societal and environmental sectors of the soft (non-military) security.

One of the think tanks participating in this transformation of Security Studies was the Copenhagen Peace Research Institute (COPRI), where the so-called *Copenhagen School* had been established. Members of that think-tank – Barry Buzan, Ole Waever and Jaap de Wilde – elaborated a new theoretical concept of security in their writing Security: *A New Framework for Analysis*, edited in 1998. The writing examined in details all security sectors inclusive of those newly identified, and *rejected the traditionalists' case for restricting security to one sector*[3].

The second significant benefit of the Copenhagen School Project was the expansion of the term security by implementing the new notion *securitization*[4]. The distinctiveness of the securitization approach rests in broader perception of security. While traditionally, the term security is contemplated in light of its status, securitization is considered a process – *a more extreme version of politicization*[5].

In theory, any public issue can be located on the spectrum ranging ***from non-politicized*** *(meaning the state does not deal with it, and it is not in any other way made an issue of public debate and decision),* ***through politicized***

[2] HUMAN SECURITY ACT OF 2007 (RA 9372) - a Philippine law, Manila, 19. 02. 2007, http://jlp-law.com/blog/ra-9327-human-security-act-of-2007-full-text/

[3] BARRY BUZAN, OLE WAEVER, JAAP de WILDE, Security, vii

[4] OLE WAEVER, *Securitization and Desecuritization*, in Lipschutz, R. D. (ed.) *On Security* (Colombia University Press, 1995)

[5] BARRY BUZAN, OLE WAEVER, JAAP de WILDE, Security, 23

(meaning the issue is part of public policy, requiring governmental decision and resource allocation) ***to securitized*** *(meaning the issue is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedures)*[6].

The significance of this approach consists in the possibility „to evaluate whether one finds it good or bad to securitize a certain issue ... and ... to ask whether it is a good idea to make this issue a security issue meaning to transfer it to the agenda of panic politics, or whether it is better handled within normal politics"[7].

Securitization is essentially an intersubjective process. The sense of threat, vulnerability, and (in)security are socially constructed rather than objectively present or absent ...Paranoia (the securitization of nonexistent threats) and complacency (the non-securitization of apparent threats) are both possible[8].

Partial implication I.

Understandig this Copenhagen School's academic approach of the 1990's through *the eyes* and practical experience of European citizens of the 2010's, it is possible to identify many analogies between Buzan's theory and the Europe's *(un)practical* solutions of the rampant migration wave and especially one of its direct consequences – a series of terrorist attacks in Western Europe.

2. The Human Security Story

Since the fall of the Iron Curtain, in parallel with the transformation of Security Studies, the idea of *Human Security* has gradually grown under the UN umbrella, even if the notion of human security has been latently used since the creation of the United Nations in 1945. The beginning of a serious research and development of human security is therefore dated in the early 1990's, when the United Nations Development Programme (UNDP) released its *1994 Human Development Report* whose one whole chapter (out of five) was dedicated to and focused on the analysis of human security as a new security paradigm.

Moreover, the UN Human Security Concept, unlike security concepts of modern states (which are basicly focused on defending borders from exter-

[6] Ibid., 23 - 24
[7] BARRY BUZAN, OLE WAEVER, JAAP de WILDE, 34
[8] BARRY BUZAN, OLE WAEVER, JAAP de WILDE, 34 Ibid., 57

nal military threats) is concerned with the security of individuals. The founders of the United Nations had always given equal importance to people's security and to territorial security.

> The battle of peace has to be fought on two fronts. The first is the security front where victory spells ***freedom from fear***. The second is the economic and social front where victory means ***freedom from want***. Only victory on both fronts can assure the world of an enduring peace[9].

In the area of particular threats to human security, the Human Development Report 1994 provided a detailed layout of following seven new security categories (sectors) - economic security, food security, health security, environmental security, personal security, community security and political security; however, without any closer analysis of a particular threat. In retrospect, a very visionary part of the report was dedicated to the identification of following six emerging threats to human security for the 21^{st} century that *will arise more from the actions of millions of people than from aggression by a few nations*[10]:

- Unchecked population growth;
- Disparities in economic opportunities;
- *Excessive international migration*;
- Environmental degradation;
- Drug production and trafficking;
- *International terrorism.*

In January 2001, then UN Secretary General (UN SG), Kofi Annan, established the Commission on Human Security (CHS) in response to the UN SG's call at the 2000 Millennium Summit for a world ***„free of want" and „free of fear"***[11]. In 2003, CHS presented to Kofi Annan the Final Report *Human Security Now*, which clarified and further developed the vague definition of the human security paradigm specified in the Human Development Report 1994 as follows: Human security means protecting fundamental freedoms – freedoms that are the essence of life. It means protecting people from critical (severe) and pervasive (widespread) threats and situations. It means creating political, social, environmental, economic, military and cultural systems that together give people the building blocks of survival, livelihood and

[9] STETTINIUS, E. R. Jr., The US Secretary of State report to the US government on the results of the San Francisco Conference, June 1945, in Human Development Report 1994, 3

[10] UNITED NATIONS DEVELOPMENT PROGRAMME, 1994 Human Development Report, 34

[11] From: Commission on Human Security web site, http://www.humansecurity-chs.org/

dignity[12].

The next important step on the way to a broader utilization and institutionalization of the new security paradigm was the Report of the UN Secretary General's High-level Panel on Threats, Challenges and Change - *A More Secure World: Our Shared Responsibility.* The report addressed both threats and challenges and, for the first time, explicitly enumerated and prioritized the following human security threats:

1. Economic and social threats, including poverty, infectious disease and environmental degradation;
2. Inter-state conflict;
3. Internal conflict, including civil war, genocide and other large-scale atrocities;
4. Nuclear, radiological, chemical and biological weapons;
5. Terrorism;
6. Transnational organized crime[13].

Contemporary security threats are being caused by both the state - as well as non-state actors, as current security threats do not recognize any borders. Furthermore, most of security threats have causal conditionality. They create a causal link(s) with other security threat(s).

> *Civil war, disease and poverty increase the likelihood of state collapse and facilitate the spread of organized crime, thus also increasing the risk of terrorism and proliferation due to weak states and weak collective capacity to exercise the rule of law*[14].

A significance of that report rested also in the fact that it suggested a new UN definition of terrorism, which was absent. That deficiency constantly *prevents the United Nations from exerting its moral authority and from sending an unequivocal message that terrorism is never an acceptable tactic, even for the most defensible of causes*[15]. The report argues that:

In addition to actions already specified by the existing conventions on aspects of terrorism

– the Geneva Conventions and UNSC Resolution 1566 (2004) - Terrorism should be described as „any action, that is intended to cause death

[12] COMMISSION ON HUMAN SECURITY, Human Security Now (UN CHS, 2003), 4
[13] UNSG HIGH-LEVEL PANEL ON THREATS, CHALLENGES AND CHANGE, *A more secure world: Our shared responsibility* (United Nations, 2004), 23
[14] Ibid., 16
[15] Ibid., 51

> or serious bodily harm to civilians or non-combatants, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act"[16].

However, it is necessary to note that in spite of all Kofi Annan's personal efforts, the subsequent 60^{th} jubilee UN General Assembly in 2005 failed once again to approve a mutual definition of terrorism. Until today, no universal convention on terrorism has been adopted! Concerning the emerging Human Security Concept, the only reference to the broader understanding of human security was the very general paragraph 143 of the General Assembly Resolution 60/1 of 24 October 2005:

> We stress the right of people to live in freedom and dignity, free from poverty and despair. We recognize that all individuals, in particular vulnerable people, are entitled to **freedom from fear and freedom from want**, with an equal opportunity to enjoy all their rights and fully develop their human potential.
> To this end, we commit ourselves to discussing and defining the notion of human security in the General Assembly.

However, this paragraph ensured the continuation of the human security institutionalization process of the 2010's. The United Nations member states finally agreed to start formal/official discussions on the notion of human security.

After a formal debate, the consequential General Assembly Resolution 66/290 from September 10, 2012 finally agreed the human security common understanding. Institutionalization of the concept of human security in the official UN documents represents a significant victory and accomplishment after two decades' effort of governmental, non- governmental organizations and informal UN bodies.

> The common understanding on human security, agreed by the General Assembly in resolution 66/290 in September 2012, provides a useful way of thinking about how we respond to 21^{st}-century challenges. By focusing on the interconnected pillars of peace and security, development and human rights, human security provides a comprehensive, integrated and people-centred approach for generating tangible improvements

[16] UNSG HIGH-LEVEL PANEL, *A more secure world: Our shared responsibility* (United Nations, 2004), 52

in the daily lives of the men, women and children this Organization exists to serve[17].

Partial implication II.

Evaluating the UN Human Security approach of the 1990's through *the eyes* and practical experience of European citizens of the 2010's, it is possible to identify many analogies between *visionary conclusions* of the above mentioned UN Reports concerning the emerging human security threats for the 21^{st} century and the real situation e. g. in Syria, Libya and consequently in Europe about 20 years later.

It can be assumed that the most of human security threats have a causal conditionality. They create causal links with one or more other security threats. Tracing the causality between particular threats to human security, it is posible to complete their classification by labeling particular human security threats as either primary (source) or secondary (induced) ones. Manytimes both assessments are possible – in case of a *double-meaning* security threat. It is possible to expect that taking into account chiefly the primary security threats may narrow down the number of security threats, which should principaly draw attention of security analysts.

3. Human security threats' causal analysis

The need of a causal *analysis of contexts* in favour of an effective solution logically arises from a broader perception of security as a multi-level process - politicization, securitization and de-securitization. The starting point is a simple logical reasoning that the essence of an effective and lasting solution to any problem *does not lie in the „removal of consequences"*, which that problem caused, but *in focusing on elimination of its „root (source) causes"*.

Most security threats create a causal link with one or more other security threats. This fact implies that there is a possibility to create *a causal model* (mental, graphic, etc.) of any security threat to simulate or to predict the consequences and successfulness / efectivity of a suggested security solution (*securitizating or de-securitizating*).

By analyzing a simple mental causal model of a general *secondary security threat*, the conclusion is that, such a threat can be effectively addressed

[17] HUMAN SECURITY UNIT, Strategic Plan 2014 – 2017, 3, from https://docs.unocha.org/sites/dms/HSU/HSU%20Strategic%20Plan%202014-2017%20Web%20Version.pdf

(or reduced its acuity) by actively acting on one or more *primary security threats* - should their causal relationship has been identified. Otherwise, it is highly probable that the direct securitization of any secondary security threat will only cause *a security dilemma* (spiral)[18], because the source of a negative phenomenon will not be removed, only its consequences will be securitized - what (in most cases) can generate negative effects in the form of further deterioration of the primary security threat's severity, consequently creating additional secondary security threats and worsening the overall security situation.

For that reason, in the context of a secondary security threat's causal model, it is necessary to look for (or to simulate) a suitable *causal loop*, which would allow not only the required removal (reduction in severity) of a particular secondary security threat, but also - principally - to address its source: the primary security threat (or threats).

Partial implication III.

A flagrant example would be a causal model of *a state failure as the primary security threat* – in relation to which it might be possible to identify a large number of causal links with secondary security threats. Therefore, a timely international support and assistance to weak or failing states might be considered the most effective tool capable of preventing multiple secondary threats to human security such as, for example, intra-state conflict, state bankruptcy transnational organized crime or mass migration and terorrism. In addition, that causal model could demonstrate correctness of the EU approach that considers the state failure as a major security threat with a critical role in an uncertain global security environment[19].

[18] Complete security cannot be obtained within periodic situations called the security dilemma (spiral) when the security of one state (or a protected interest) is being achieved at the expense of security of the other and vice versa.

[19] JAVIER SOLANA, *European Security Strategy - A Secure Europe in a Better World* (EU, 2003), 10, from http://ue.eu.int/uedocs/cmsUpload/78367.pdf

4. Simple causal model - *from a state failure to a terrorism manifestation*

This causal model (see below) is not an elementary model of a single causal relationship between one primary and one secondary security threats. The reason is that the state failure subsequently creates more secondary security threats. While looking for a suitable *causal loop*, which would enable not only the required removal (or reduction in severity) of the threat of terrorism manifestations in Europe, but also to address systemically its sources (e.g. the mass migration), it is possible to find both opposing approaches – securitizing and de-securitizing ones.

An official statement of the Slovak Government, expressed in the National Action Plan of Combating Terrorism for 2015-2018, represents the securitization tendencies of the mass migration solution.

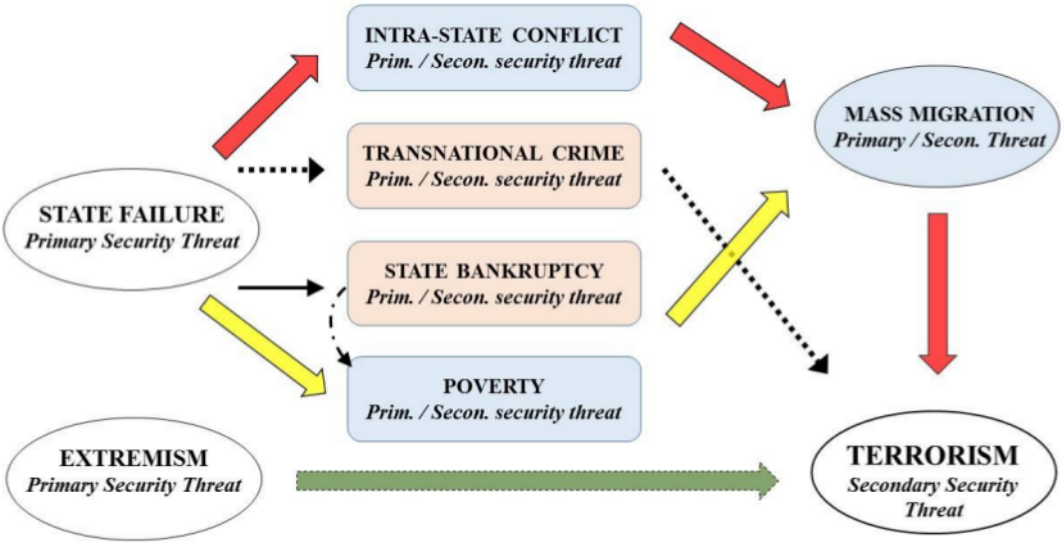

Figure 1: Simple causal model of the way *from a state failure to a terrorism manifestation*

Terrorism and radicalization have increased in recent years. Open borders within Europe and the resulting freedom of movement within the Schengen Area pose a potential threat in the form of uncontrolled flows of illegal migrants, including those with criminal backgrounds and experience of fighting in crisis areas. For this reason, it is now very important - within the fight against illegal migration - to strengthen the security controls of the external Schengen borders and to prevent Euro-

pean fighters from travelling to crisis areas, as well as to prevent suspects traveling from these areas from entering to the Schengen area[20].

Opposing, de-securitizating trend holds the International Organization for Migration (IOM), which promotes the idea that human and organized migration is beneficial to both migrants and society[21].

Migration in the twentieth century has irreversibly changed the developed western countries and brought unprecedented cultural diversity to the nationally defined countries without which these societies could no longer exist. Migrants have greatly helped the growth of advanced economies after the Second World War and the rise in the living standards of the local population, whether as highly qualified professionals, but more often as cheap labor in low-skilled and low-paid jobs[22].

These two opposing views on the migration wave represent the current deep division of views among EU Member States. Buzan (1991), in this context, offers a possibility of a comprehensive evaluation, whether it is good or bad to securitize the issue of mass migration = *whether it is a good idea to make this issue a security issue - meaning to transfer it to the agenda of panic politics, or whether it is better handled within normal politics*[23] Expected result is the exclusion of one (or both) possible extreme(s): *the (over)securitization of a nonexistent threat AND/OR the de-securitization of an imminent threat (complacency).*ANSWER OF THIS „KEY QUESTION" SHOULD DRAW HIGH ATTENTION OF TOP EU POLITICIANS.

Mapping of this causal model needs to start with the basic, initial statement that the mass migration is a secondary (induced) security threat, the source of which is in this particular case in the failing states - nowadays especially in Syria. Since 2011, the civil war in this country has gradually grown into an obscure, complicated regional armed conflict, exhaling millions of people from their homes, and forced them to leave their native land and property for the sole purpose of saving their bare life. Based on the United Nations General Assembly Resolution on Human Security, 66/290 of 10

[20] National Action Plan of Combating Terrorism for 2015-2018 (approved by the Government of the Slovak Republic on April 29, 2015), from http://www.rokovanie.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=24497

[21] IOM has been active in Slovakia since 1996, where it has implemented various projects and activities in the area of migrant integration and coordination of the activities of the European Migration Network - http://www.iom.sk/en

[22] ANDRÁŠOVÁ, S, Na čo je nám dobrá migrácia? (What is migration good at for us?), 34, from http://www.cpep.sk/fileadmin/Dokumenty/publikacie/migracia/Andrasova-Migracia.pdf (translated by author)

[23] ANDRÁŠOVÁ, S, Na čo je nám dobrá migrácia? (What is migration good at for us?), 34, from http://www.cpep.sk/fileadmin/Dokumenty/publikacie/migracia/Andrasova-Migracia.pdf (translated by author)

September 2012, this group of migrants, which utilize the Balkan migration route, has also the right *to live in freedom and dignity, without misery and despair ... free from fear and from want, with an equal opportunity to enjoy all their rights and fully develop their human potential*[24].

It should be remembered that the primary security threats to Syria (as a security actor) - the state failure and the resulting regional conflict - can also be characterized as *general* security threats to its population = Human Security Threats. However, mass migration, which is (also) a secondary security threat, now threatens - in case of its mishandling - the EU.

Within the presented causal model, it is possible to identify the increased risk of terrorism manifestations as a secondary security threat deriving from mass migration of Islamic population into Europe. The interconnection of individual terrorist attacks and their actors with terrorist organizations is another of the complex issues whose knowledge is important in terms of their investigation and subsequent repression and possible prevention. Many times, in the common media environment, the association of terrorist groups with the Islamic State (IS) is reported, but Europol, in its report of 20 July 2016[25], stated that most attacks in the EU are linked to jihadists, and the association of these terrorist attacks with IS is weak. In addition, Europol has highlighted alarming trends in the number of homecoming terrorists and a ignificant increase in anti-Semitic, xenophobic and racist moods in the EU and their gradual increase.

Conclusion

The simple causal model of processes *from a state failure to a terrorist attack* is possible to divide into three levels (layers). The first level is formed by the primary security threats that have been identified as the original cause of mass migration from Syria - in our case, the state failure and the intra-state / regional conflict.

The second level is represented by the mass migration as a secondary security threat, derived from the primary ones (it is necessary to point out here that the mass migration is not the only secondary security threat derived from these two particular primary threats).

[24] Resolution adopted by the General Assembly on 10 September 2012 - 66/290. Follow-up to paragraph 143 on Human Security, of the 2005 World Summit Outcome. http://www.un.org/humansecurity/sites/www.un.org.humansecurity/files/hsu%20documents/GA%20Resolutions.pdf

[25] EUROPOL, EU Terrorism Situation and Trend Report (TE-SAT), 2016, https://www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-te-sat-2016

The third level of the causal model is created by secondary security threats, which are consequently derived from the real interaction of the EU security environment with the mass migration as a new immediate security threat - namely extreme nationalism and Islamic extremism, terrorism and some other threats (not mentioned at the Figure 1) such as the horizontal competition (possible unfavorable demographic development) and impending new epidemics or pandemics.

References

1. AXWORTHY L. Human, *Security in the Era of Terrorism: The Responsibility to Protect*, Center for Globalization and Policy Research Center for Civil Society and Canadian Studies Endowed Fund, UCLA, Working Paper No 14, 2003
2. BALDWIN D. A., *Concept of Security*, Review of International Studies 23, No. 1, 1997
3. BUZAN B. People, *States and Fear – An Agenda for International Security Studies in the Post- Cold War Era*, Lynne Rienner Publishers, 1991 (Second Edition)
4. BUZAN B., WAEVER, O., de WILDE, J., *Security: A New Framework for Analysis*, Lynne Rienner Publisher, 1998
5. BUZAN B., *The United States and the Great Powers, World Politics in the Twenty-First Century*, Polity Press, 2004
6. COMMISSION ON HUMAN SECURITY, Human Security Now, UN CHS, 2003 EUROPOL, EU *Terrorism Situation and Trend Report* (TE-SAT), 2016
7. HUMAN SECURITY UNIT, *Strategic Plan 2014 – 2017*, 2014
8. LEGRAIN P., *Immigrants. Your Country Needs Them*, London 2007
9. SOLANA J., *European Security Strategy - A Secure Europe in a Better World*, EU 2003
10. SOLANA J., *Report on the Implementation of the European Security Strategy - Providing Security in a Changing World*, EU, 2008
11. UNSG High-level Panel on Threats, Challenges and Change, *A more secure world: Our shared responsibility*, United Nations, 2004
12. UNITED NATIONS DEVELOPMENT PROGRAMME *Challenges to Human Security in the Arab Countries*, Arab Human Development Report 2009
13. WAEVER O., *Securitization and Desecuritization*, in Lipschutz, R. D. (ed.) On Security, Colombia University Press, 1995