Journal of Defense Management

ISSN: 2167-0374

Review Article

Open Access

Modern Terrorism as Hybrid Threat and Digital Challenge

Zlatogor Minchev*

Institute of Information and CommunicationTechnology, Sofia, Bulgaria

Abstract

Nowadays the world is facing a new security challenge - the hybrid threats and war. Whilst this idea could be addressed as an extension of the Alliance Comprehensive Approach, the combination of conventional and non-conventional methods towards modern warfare is already a fact. The key idea behind is the hybrid nature of the modern conflicts, feeding in the terrorism context. The paper outlies a general model of the terrorism hybrid nature, accentuating on the modern cyber space role and is targeting our authors to go deeper in the problem from both technological and human part, supporting in this way a more secure future world.

Keywords: Modern terrorism; Hybrid threat; Digital challenge

Nowadays the world is facing a new security challenge – the hybrid threats and war [1]. Whilst this idea could be addressed as an extension of the Alliance Comprehensive Approach, the combination of conventional and non-conventional methods towards modern warfare is already a fact. The key idea behind is the hybrid nature of the modern conflicts, feeding in the terrorism context [2].

Generally, the idea of todays' terrorism as a hybrid threat could be summarized as self-feeding social engineering system (Figure 1). Evidently, this is a combination of 'Armed' and 'Informational' activities for achieving chaos, stress, fear and disorder, providing in this way – useful conditions for world social change [3]. The 'Armed activities' are assumed in the common understanding for conventional weapons and use of force operations. The 'Informational activities' could be discussed and in the broader 'Cyber activities' sense, but the accent here is given to the information in itself. The hidden roles are for 'Non-state Actors' and 'Radical Ideology', being consecutively – a gear and accumulator for modern terrorism. Here it should be noted that organized crime is considered to be part of the 'Non-state Actors' together with non-formal organizations and hidden societies. 'Radical Ideology' is encompassing religious or political beliefs that claim primary values or rules but do not follow the common social wellbeing, but only non-formal groups' ones. Moreover, this requires a dynamic multiple target, focusing for successful terrorism coping on the problem and is quite complex and ambiguous. The possible control here lies behind the very organizational idea of dual system self-feeding, i.e. no possibility for terrorism self-existence without hybrid (dual) fueling from underground and official sources. Following the above idea, a successful fighting against terrorism is expected to emerge because of underground economy and informational space controlling.

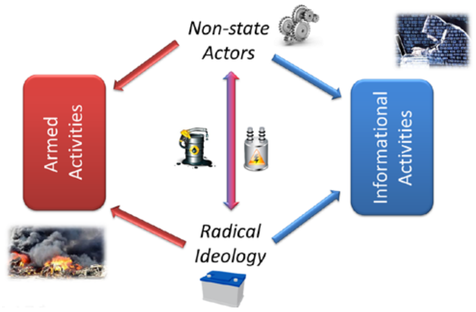

Figure 1: Terrorism as hybrid threat and self-feeding social engineering system.

Further on, an accent will be given to the informational ones, being a more innovative, fast evolving and young generation users' breeding. Todays' Internet Web 3.0 technologies and services are addressing mobile devices, social networks and Internet with expected by CISCO near future – 'Internet of Everything' boom [4]. The natural ancestor – Web 4.0 is currently believed to encompass within Web 3 and real environment actuators, i.e. involving somehow advanced 'mutated AI' and smart robots. Another generalized approach in this sense is mixing virtual and real environment in multiple senses, producing an evolutional augmented reality [5]. Talking in this direction for fighting terrorism, an expectation for immediate focusing towards social engineering and propaganda is emerging. According to our recent survey (amongst 300 young and educated people, averaged age 27 years, +/- 5) the key advantage in present social networks is related to Sharing of information, followed by Entertainment in-between Internet users.

Apart from these, the most expected web technologies and services trends are addressing Virtual Entertainment, E-market Progress and Augmented Realities. These beliefs however are just outlining studied users' hopes for the future. But, discussing the terrorism context, another dual consideration should be made: between human factor and technologies (Figure 2). As new technologies are hiding a number of expected and unexpected cyber threats, the human factor stays for greatest importance together with Radical Ideology and Non-state Actors. Psychologically, the phenomenon could be considered in several directions: terrorism motivation, alienation and sensation seeking caused from depression or other social phenomenon like poverty or social denial. Being a rather broad topic, the psychological side of the problem requires also the physiological human factor response observation. In this sense the digital world is opening numerous possibilities, providing a capability for terrorism prevention and societal resilience, using the Internet environment and human factor emotions and behaviour non-formal monitoring [6]. Finally, meeting the modern terrorism hybridization is rather challenging and requires cooperative approach encompassing: public and private sector cooperation, sharing common values for social wellbeing. A natural

***Corresponding author:** Zlatogor Minchev, Institute of Information and Communication Technology, Sofia, Bulgaria, Tel: (+359 2) 979 6631; E-mail: zlatogor.minchev@gmail.com

Received May 16, 2015; **Accepted** July 27, 2015; **Published** July 29, 2015

Citation: Minchev Z (2015) Modern Terrorism as Hybrid Threat and Digital Challenge. J Def Manag 5: 129. doi:10.4172/2167-0374.1000129

follow-up combination in this context is the digital world interaction clash with human factor, producing numerous challenges. With this short introduction we are welcoming our authors to go deeper in the problem from both technological and human part, supporting in this way a more secure future world.

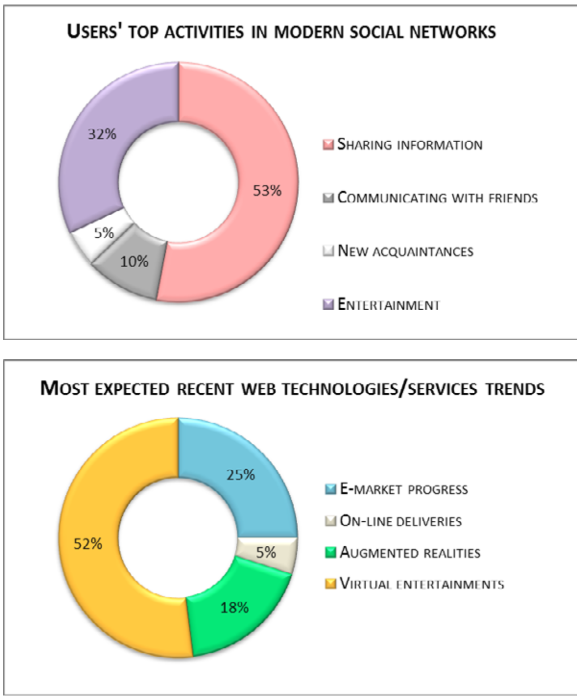

Figure 2: Users top activities in modern social network.

References

1. Dilipraj E (2015) Hybrid Warfare: Re-Innovating the Concept, CAPS.
2. Zakrzewska J (2014) NATO after 2014, NATO Parliamentary Assembly Report.
3. Miller M (2013) The Foundations of Modern Terrorism: State, Society and the Dynamics of Political Violence, Cambridge University Press.
4. Vermesan O, Friess P (2014) Internet of Things - From Research & Innovation to Market Deployment, River Publishers.
5. Meyerson B (2015) Top 10 Emerging Technologies of 2015, World Economic Forum.
6. Minchev Z (2015) Human Factor Role for Cyber Threats Resilience, In: Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare, IGI Global.