

INTERNATIONAL CONGRESS ON  
POLITICAL, ECONOMIC AND SOCIAL  
STUDIES

ABSTRACTS BOOK

Uluslararası

Politik, Ekonomik ve Sosyal Araştırmalar Kongresi

Bildiri Özetleri Kitabı

9-11 November, 2017 Ankara-TURKEY

ISBN: 978-605-67821-4-5

Congress homepage: www.icpess.org

PESA homepage: www.pesa.org.tr



**Teknolojik Savaşlar: Siber Terörizm Tehditleri**  
**Technological Wars: Siber Terrorism Threats**

**Yrd.Doç. Dr. Cemalettin Hatipoğlu**

Bilecik Şeyh Edebali Üniversitesi, cemalettin.hatipoglu@bilecik.edu.tr

**ÖZET**

*Bilgi Savaşı, hem savaş hem de barış zamanında bilgi ve bilgi sistemlerinin saldırı ve savunmasını içerir. Bilgi teknolojilerinin, giderek daha karmaşık hale gelmesi ve birbirine bağlı küresel bilgi altyapısına yaygın bağımlılık nedeniyle, ortaya çıkan zayıf noktaları bulunmaktadır. Politik açıdan gündem oluşturmak amacıyla, sivilleri hedef alarak korku yaratmak için kullanılan bilişim teknolojilerinin bu tür zayıflıkları siber terörizm olarak adlandırılır bilinir. Geleneksel terörizm, hükümet politikalarını etkilemiş ve dünyadaki insanlara ve altyapıya fiziksel zarar vermiştir. Teknolojideki ilerlemeler, yazılım ve donanımın daha kolay kullanılmasını sağlamakta ve kullanıcılar tarafından daha az karmaşıklık gerektirmektedir. Terörizm grupları, siber araçlara ve yeteneklere adapte olmaya ve bunlardan yararlanmaya başladıkça, bilgisayarlar ve internet de saldırılara ile ortaya çıkardıkları tehlike de buna göre büyümektedir. Bu terör, insanları siber araçlar ile doğrudan öldürememekle birlikte, enerji hatları, su ve petrol tesisleri, ulaşım ve kamu güvenliği alanlarına kadar kritik altyapımızı yöneten tüm bilgisayar sistemlerini etkileyerek, kargaşalık ya da sosyal bozulma bu örgütün amaçları arasındadır. Siber mekânın gizliliği, terörist grupların saldırı planlarını gerçekleştirmelerine ve hemen tanımlanmasına izin vermez. Buna ek olarak, siber teröristlerin hedefleri çoğunlukla hazırlıksız yakalandığından ve siber saldırı biçimlerine karşı savunmasızdırlar. Bu ağları güvence altına almak için en iyi uygulamalara ihtiyaç duyulmakta ve birden fazla kurumun işbirliğine ihtiyaç duymaktadır. Siber terörizmin ne olduğu ve internetin açık sınırları hakkında açık bir tanım bulunmaması, bu konunun yasal bir temelde ele alınmaya çalışılmasını zorlaştırmaktadır. Bu çalışmanın amacı, siber terörle ortaya çıkan potansiyel tehditleri keşfetmek, etkin siber güvenlik ve genel olarak konuyla ilgili farkındalığı artırmak, mevcut tehditlerin yanı sıra bunları hafifletmek için neler yapılabileceğine ilişkin genel bir bakış sunmaktır.*

2017 PESA Tüm hakları saklıdır.

**Anahtar Kelimeler:**

Bilgi, Teknoloji, Ağ, Siber Araçlar, Siber Terörizm

**ABSTRACT**

*The Information War involves the attack and defense of information and information systems in both war and peace. There are weak points that arise due to the increasing complexity of information technology and the widespread dependence on interdependent global information infrastructures. Such weaknesses of information technologies used to create fear by targeting civilians in order to create an agenda in politics are known to be called cyber terrorism. Traditional terrorism has affected government policies and has physically damaged people and infrastructure around the world. Advances in technology make software and hardware easier to use and require less complexity by users. As terrorism groups become adept at using and making use of cyberapplications and talents, the danger they are exposed to attack by computers and the Internet is growing accordingly. While this terror can not kill people directly with cyberapplications, it is the purpose of these associations to confuse or disrupt social systems, affecting all computer systems that manage our critical infrastructure, from energy lines, water and oil facilities to transportation and public safety. The secret of the cyber space does not allow the terrorist groups to realize their attack plans and to immediately identify them. In addition, the targets of cyber terrorists are mostly unprepared and vulnerable to the forms of cyber attacks. Best practices are needed to secure these networks, and more than one institution needs cooperation. The lack of a clear definition of what cyber terrorism is and the open boundaries of the Internet makes it difficult to address this issue on a legal basis. The aim of this work is to explore the potential threats of cyber terrorism, to raise awareness about effective cyber security and the public in general, to present an overview of current threats as well as what can be done to mitigate them.*

© 2017 PESA All rights reserved.

**Keywords:**

Information, Technology, Network, Ciber Tools, Ciber Terrorism,