OPUS
Uluslararası Toplum Araştırmaları Dergisi
International Journal of Society Researches

ISSN:2528-9527
E-ISSN : 2528-9535
Yıl *Year* :11
Cilt *Volume*:18
Sayı *Issue* :42
Ekim *October* 2021
Makalenin Geliş Tarihi *Received Date*: 23/03/2021
Makalenin Kabul Tarihi *Accepted Date*: 30/05/2021

# Türkiye'de Siber Terörizme Karşı Bilişim Teknolojilerinin Kullanımı

DOI: 10.26466/opus.901520

*

Ahmet Doğan * – Furkan Abacı **
* Dr. Öğr. Üyesi, Osmaniye Korkut Ata Üniversitesi, Osmaniye/Türkiye
**E-Posta**: ahmetdogan@osmaniye.edu.tr **ORCID:** 0000-0002-7116-3558
**Jandarma Teğmen, Jandarma Genel Komutanlığı, Ankara /Türkiye
**E-Posta**: furkanabaci@jandarma.gov.tr **ORCID:** 0000-0003-3044-203X

**Öz**

*Bilgi ve iletişim teknolojilerinin dünya çapında yaygın bir şekilde kullanılması siber terörün kapsamını genişletmektedir. Bilgisayar ve internet ağlarının yoğun olarak kullanıldığı ulaşım, enerji yönetimi, hastane yönetimi, milli savunma, finans vb. alanlar ile ilgili faaliyet gösteren kurum ve kuruluşlar siber terörizme açık alanlardır. Faaliyetlerini bu şekilde sürdüren kurumların bilişim sistemlerine erişim sağlayarak, bu kurum/kuruluşların işleyişini aksatmak veya engellemek terör örgütlerinin asıl amacını oluşturmaktadır. Bu çalışmanın amacı, Türkiye'de siber terörizme karşı bilişim teknolojilerinin etkin kullanımı konusunun tespit edilerek, bu alanla ilgili ne gibi iyileştirmeler yapılması gerektiğini ortaya koymaya çalışmaktır. Bu amaçla, öncelikle nitel araştırma yöntemlerine dayalı olarak yarı yapılandırılmış görüşme tekniğiyle veriler toplanmıştır. Alan uzmanları (ağırlıklı akademisyen) ile yapılan mülakatlar aracılığıyla, uzmanların Türkiye'de siber terörizme karşı bilişim teknolojilerinin kullanımı ile ilgili görüşleri alınmıştır. Görüşleri alınan uzman katılımcıların bilgileri, nitel araştırma yöntemlerinde kullanılabilen NVivo 12 paket programı ile analiz edilmiş ve bulgular aktarılmıştır. Araştırma bulgularına göre, siber terörizme karşı koymada bilişim teknolojilerinin etkin kullanımı için vurgulanan en önemli konunun bu alana yönelik farkındalığın oluşturulması olduğu tespit edilmiştir. Bu farkındalığın oluşturulmasında ise, eğitim, bilimsel çalışmalar, sivil toplum kuruluşları ve medyanın önemi üzerinde durulmuştur. Son olarak, Türkiye'de siber güvenlik alanı ile ilgili çalışmaların yeterli düzeyde olmadığı ve bu alana yönelik çalışmalara ağırlık verilmesi gerektiği sonucu elde edilmiştir. Bu açıdan çalışmanın alana ilgi duyan araştırmacılara katkı sağlayabileceği düşünülmektedir.*

**Anahtar Kelimeler:** *Güvenlik, Terörizm, Siber Güvenlik, Siber Terörizm, Siber Saldırı.*

OPUS
Uluslararası Toplum Araştırmaları Dergisi
International Journal of Society Researches

ISSN:2528-9527
E-ISSN : 2528-9535
Yıl *Year* :11
Cilt *Volume*:18
Sayı *Issue* :42
Ekim *October* 2021
Makalenin Geliş Tarihi *Received Date*: 23/03/2021
Makalenin Kabul Tarihi *Accepted Date*: 30/05/2021

# Cyber Terrorism against the Use of Information Technology in Turkey

*

**Abstract**

*The widespread use of information and communication technologies extends the scope of cyber terrorism worldwide. Institutions and organizations; where computer and internet networks are used intensely; operating in areas such as transportation, energy management, hospital management, national defense, finance etc. are areas responsive to cyber terrorism. The main purpose of terrorist organizations is to provide access to the information systems of institutions that continue their activities in this way and to disrupt or prevent the operation of these institutions / organizations. The aim of this study is to determine the effective use of information technologies against cyber terrorism and trying to put forward as to what needs to be done to improve it. For this purpose, data were collected using semi-structured interview technique based primarily on qualitative research methods. Opinions of experts in Turkey have been taken regarding the use of information technologies against cyber terrorism, through the interviews with field experts (mainly academicians). The information gathered from the participants was analyzed with the NVivo 12 software, which is widely used in qualitative research methods, and the findings were presented. According to the research findings, it has been determined that the most important issue emphasized for the effective use of information technologies in countering cyber terrorism is to raise awareness in this area. The importance of education, scientific studies, non-governmental organizations and the media were emphasized in creating this awareness. Finally, it has been concluded that studies related to the field of cyber security in Turkey are not effective and studies regarding this area should be developed. In this respect, it is thought that the study can contribute to researchers interested in the field.*

**Keywords:** *Security, Terrorism, Cyber Security, Cyber Terrorism, Cyber Attack.*

## Giriş

Terör ve terörün sonuçlarının bütün dünya toplumları için ağır bedelleri olduğu açık bir şekilde görülmektedir. Terörün ve terör eylemlerinin tarihi çok daha eskilere uzansa bile son dönemde globalleşme ile terör grupları da etkinliklerini hiç olmadığı kadar arttırmıştır. Özellikle gelişmiş teknolojilerin sağladığı imkanlar aracılığıyla, terör grupları uluslararası eylemler ve etkileşimler içerisine girmiş bulunmaktadır. Ne yazık ki ulus devlet yapısının korunuyor olması ve uluslararası iş birliğinin yeterli boyutlarda olmamasını bir fırsat olarak değerlendiren terörist gruplar, uluslararası mecrada çok büyük acılara ve yaralara sebebiyet veren eylemler gerçekleştirebilmektedir. Üstelik bu tür gruplarla mücadele konusunda yeterli adımların atılması da her geçen gün daha da zorlaşmaktadır (Bodur, 2005, s.65-66).

Terörizmin ulusal boyutlarından ziyade uluslararası boyutları çok daha korkutucu ve tehlikeli olabilmektedir. Terör grubu faaliyet alanlarından birisi de siber terörizm olarak karşımıza çıkmaktadır. 1990' dan sonra ortaya çıkmaya başlayan siber terörizm kavramı, özellikle de bilgi ve enformasyonlarda meydana gelen gelişmelerin yanı sıra internet ve bilişim teknolojilerindeki ilerlemelerle hız kazanmıştır. Siber terörizm ile ortaya çıkabilecek potansiyel tehditlerin olumsuz sonuçlarından korunmak için, özellikle de ABD gibi ülkelerde bu konuya yönelik çalışmaların yoğunlaştığı ve siber terörizmin daha sık duyulan bir kavram olduğu söylenebilir (Terzi, 2018, s.73).

90'lı yılların başlarında Amerikan Ulusal Bilim Akademisi'nin yapmış olduğu bir araştırma raporunda, bilgisayarın hayatımızın her alanına girmeye başladığı, özellikle de Amerika'da bilgisayara bağımlılık oranının önemli derecede artmakta olduğu vurgulanmakta olup, gelecekte bir teröristin klavye ile oluşturabileceği zararın, belki de bomba patlaması neticesinde oluşabilecek zarardan daha ciddi sıkıntılar oluşturabileceği belirtilmiştir (Ermiş, 2015, s.69-70).

Eskiden bilişim teknolojilerinin ortaya çıkardığı gelişmelerin insanlık için bir tehdit haline gelmesinin sadece bilim kurgu filmlerinde olduğu düşünülebilirdi. Her ne kadar bu olay direkt siber terörizm şeklinde adlandırılmasa da 11 Eylül saldırısının yankıları dünya çapında bir siber terör tehdidinin varlığını açık bir şekilde gün yüzüne çıkarırken, insanların bu durumda nasıl bir negatif psikolojiye sahip olacaklarını da ortaya koymuştur (Bodur, 2005, s.65).

Siber Terörizm günümüzde uluslararası siyaset arenasında, siyasi amaçların yerine getirilmesi için kullanılan bir araç olarak da kullanılmaktadır. Siber terörizm ile mücadele edebilmek için devletlerin ve uluslararası aktörlerin ciddi girişimlerde bulunması gerekmektedir. Aksi halde siber terörizm eylemleri toplumsal olarak çok daha büyük zararlar vererek devam edecektir. Sonuç olarak küresel sistem düşünüldüğünde, siber terörizmin tüm devletler için bir tehdit ve risk oluşturduğunu söylemek mümkündür.

**Terörizm, Terörizmin Tarihsel Gelişimi ve Siber Terörizm**

Terör ve terörizm kavramları ile ilgili gerek literatürdeki, gerek alan uzmanları tarafından, gerekse de diğer otoriteler tarafından yapılan tanımlara bakıldığında ortak bir tanım üzerinde uzlaşı sağlanamadığı görülmektedir. Bu tanımlamalar üzerinde uzlaşı sağlanamamasının bir sebebinin, devletlerin uluslararası çıkarlarına göre hareket etmesi olduğu söylenebilir. Yani bir devlet için, terör ve terör eylemleri ya da grupları bir başka devlet için terör eylemi ve terör grubu olarak tüm uluslararası tanımlamalar ve kabullere rağmen kabul edilmeyebilmektedir. Ülkemiz açısından düşündüğümüzde yakın coğrafyamızda yaşanan gelişmeler bunu açıkça göstermektedir. Terör ve terörizm kavramları ile ilgili ele alınan bazı tanımlamalara aşağıda değinilmiştir.

**Terör ve Terörizm Kavramları**

Terör kelimesi, ideolojik ya da siyasi amaçlar doğrultusunda, genellikle yönetime karşı yapılan, belli bir plan dahilinde şiddet kullanılarak korku yaratıp, istenilenleri kabule zorlamak ya da cezalandırma amacıyla uygulanan bir eylemler dizisi olarak tanımlanabilir. Terör kelimesi Latince ''terrere'' sözcüğünden türemiş olup, kelime manası korku vermek, vazgeçirmek ve dehşet içerisinde bırakmak olarak tanımlanmaktadır. Fransız İhtilali sonrasında ideolojik bir kavrama dönüşen terörün günümüzde çok önemli iki özelliği vardır. Birincisi siyasi bir amaç üstlenmesi, ikincisi ise insanlara korku ve dehşeti yaşatmasıdır (Güzel, 2002, s.7-8).

Terörizm tanımına hukuki açıdan bakıldığında İngilizlerin Terörizmle Mücadele Kanunu tanımına göre; "siyasal kurumlar karşısında şiddet

eylemleri ya da toplumun belirli kesimlerinin kaygı içerisinde tutulması maksadıyla cebr ve şiddet kullanılma durumudur" şeklinde ifade edildiği görülmektedir (Chomsky, 2000, s.60).

Türkiye'nin 3713 sayılı Terörle Mücadele Kanununa göre ise terör; "Terör; baskı, cebir ve şiddet, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzenini değiştirmek, Devletin ülkesi ve milleti ile bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetinin varlığını tehlikeye düşürmek, devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü eylemlerdir" olarak tanımlanmaktadır (www.resmigazete.gov.tr, 2020).

**Terörizmin Tarihsel Gelişimi**

Terörizmin çıkış zamanı ve çıkış yeri hakkında net bir bilgi bulunmamaktadır. Bununla birlikte, siyasal hedefleri elde etmek amacıyla şiddet kullanılması durumu 2000 yıl öncesinden başlamaktadır (Fearey, 1976, s.25). Dünyanın birçok bölgesinde çok sayıda terörist grup ortaya çıkmıştır. Ancak modern anlamda Fransız Devriminin bir kırılma noktası olduğu söylenebilir. Maximilien Robespierre ve taraftarları Fransız Devrimi gerçekleştikten sonra, yeni kurulan Cumhuriyet Rejimi'ni istemeyen ve direnen grupları bastırmak amacıyla askeri birlikler oluşturarak yeni rejime karşı çıkan ayaklanmaları çok kanlı bir şekilde bastırmışlardır (Nacar, 2010, s.26).

Terörizmin sınıflandırmasının nasıl yapılacağı, başlangıç zamanı ve bunun hangi olayla ilişkilendirileceği konuları üzerinde tam olarak fikir birliği sağlanamamıştır. Çalışılan konu itibari ile modern terörizm ile ilgili bilgilerin daha yararlı olacağı düşünülmüştür. Buna göre modern terörizmin nerede ve nasıl başladığı ile ilgili konulara ışık tutan Rapoport, modern terörizmi 4 aşamada incelemiştir (Rapoport, 2004, s.47-48).

*Birinci Aşama*: Bu aşama, 1880 yılı ile I. Dünya Savaşı arası dönemini kapsamaktadır.

*İkinci aşama*: Antikoloniyal aşama, yani self determinasyon (Self Determinasyon: her milletin kendi kaderini kendisinin tayin etmesi) kavramının

ortaya çıkıp yaygınlaşmaya başladığı ve dekolonizasyon sürecinin geniş ölçüde gerçekleştirildiği 1960 yıllarına kadar olan dönemi kapsamaktadır.

*Üçüncü aşama*: 1960-1980 yılları arasını kapsayan bu dönem, aynı zamanda yeni sol düşüncelerin ortaya çıktığı dekolonizayon dönemi olarak da bilinmektedir. Bu dönemde, bağımsızlıklarını kazanamayan milletlerin Batı bloğunda yer alan ülkelerine karşı girdikleri ayrılıkçı hareketleri komünist sol bloğunun desteklediği bilinmektedir.

*Dördüncü aşama*: 1980 yılından itibaren radikal-dini terör eylemlerinin başladığı dönemi kapsamaktadır. Dini düşüncelerin kullanılarak mevcut sistemlere karşı yapılan eylemlerin başlaması bu döneme denk gelmektedir.

**Siber Terörizm**

Siber terörizm bir terim olarak ilk defa 80'li yıllarda Kaliforniya'da Güvenlik ve İstihbarat Enstitüsünde üst araştırmacı olarak çalışan Barry Collin tarafından adlandırılmıştır (Collin, 1997, s.16-17). Siber terör konusunda Dorothy Denning tarafından detaylı olarak bilgi verildiği görülmektedir. Denning 'e göre; "Siber terörizm kavramı, siber terörizm ve siber boşluğun birleşiminden oluşmaktadır. Bu terimin manası, bireylere ve siyasi-sosyal makamlara baskı oluşturmak ve onlara gözdağı vermek amacıyla resmi kurumların ağ bağlantılarına, bilgisayar sistemlerine, bilgi sistemlerine ve veri tabanlarına yönelik yapılan illegal ve zarar veren saldırılar" şeklinde ifade edilmiştir (Denning, 2003, s.23). Denning, her şeyden önce bir saldırının siber terörizm olarak adlandırılması için insanların içine korku salacak kadar bir hasara yol açması ve insan ya da bir eşyaya karşı şiddet unsuru içermesi gerekliliği üzerinde durmuştur. Bununla birlikte, stratejik olarak hassasiyete sahip önemli saldırıların ortaya çıkardığı etkiye göre siber terörizm şeklinde ifade edilebileceğini belirtmiştir. Ancak, önemli bir etki yaratmayan küçük çaptaki saldırıların siber terörizm olarak adlandırılamayacağı belirtilmiştir (Tasam, 2004, s.5, Denning 2003, s.3). Bununla birlikte, bir saldırının siber terör açısından incelendiğinde doğrudan şiddet içermeyen ancak psikolojik olarak korku salan faaliyetlerinin olabileceği gerçeğinin de unutulmaması gerektiğine vurgu yapmıştır (Denning, 2003, s.27).

Terörizm ve internet kavramları birlikte değerlendirildiğinde, uluslararası platformda, işlenen suçlarla ilgili kapsayıcı yasal bir düzenleme bulunmadığı görülmektedir. Terörizm kavramı ile ilgili uluslararası platformda birçok

düzenleme olsa da internet suçları ile ilgili yeterli düzenlemenin olmadığını söylemek mümkündür. Siber Terörizmin uluslararası yasal düzlemde, düzenlemelere dahil olması için öncelikle tanımının yapılması gerekmektedir. Bu terör türünün kapsamı tam olarak belirlenemediğinden tanımı net bir şekilde yapılamamıştır. Bu boşluktan kaynaklı bir çok eylemin gerçekleştirildiğini söylemek mümkündür. İnternet üzerinden yapılan birçok eylem şiddet boyutuna ulaşabilmektedir. Örneğin siber terörizm ile, su ve elektronik güç kaynakları, navigasyon sistemleri, finansal hizmetler alanı, stratejik öneme sahip savunma sanayi sistemleri vb. sistemlere zarar vererek ve bu sistemleri işlemez hale getirerek toplum ve devletler zarara uğratılabilmektedir (Bostan ve Akman, 2011, s.51-52).

Siber terörizmin, uluslararası bir suç olarak değerlendirilmesi bütün dünya devletlerini ilgilendiren ve üzerinde hassasiyetle durulması gereken önemli bir konudur. Çünkü, siber terörizmden etkilenen yeni suç türlerinin uluslararası hukukta bulunan boşlukları kullanarak küresel çapta ciddi zararlar verebileceği düşünülmektedir. Siber terörizm eylemleri ciddi etkileri olan eylemlerdir ve sonuçları sadece bir ülkeyi değil birçok bu tarz bir eylemde bulunabilir. (Ünver, vd., 2011a, s.10).

Devletlerin yapılan bu tarz saldırılara karşı birleşerek iş birliği yapmaları gerekmektedir. Bu yüzden iş birliğinin ilk adımı bu tehlike karşısında birlikte siber terörizmin tanımlanması ve ortak uygulamalarda bulunabilmektir. Eğer bu eylemler uluslararası suç olarak tanımlanmazsa ülke bazında değerlendirilir. Yani bir devlet için suç olan eylem diğer devlet için suç teşkil etmeyebilir. Böyle bir durum ise devletlerarasi çatışmaya yol açabilir. Bu yüzden, siber terör suçlarının soruşturma ve kovuşturma kapsamına alınması için Roma Statüsü'ne alınıp suç olarak tanımlanması ve daha sonra Uluslararası Ceza Mahkemesi (UCM) yargı yetkisi içerisine alınması gerekmektedir. Uluslararası staütüsü olan tarafsız adil bir UCM'nin acil olarak bunu hayata geçirmesi, adil, etkin ve tarafsız bir biçimde uluslararası terör eylemlerinin yargılanarak cezasız kalmamasını sağlaması açısından hayati bir öneme sahip olduğu düşünülmektedir. (Ünver, vd., 2011b, s.42).

**Yöntem**

Bu çalışma, Türkiye'de siber terörizme karşı bilişim teknolojilerinin kullanımı konusunda yapılması gerekenleri belirlemek amacıyla, görüşme verilerine

dayalı nitel yöntem kullanılarak yürütülmüş bir araştırmadır. Araştırmada katılımcıların siber terörizme ilişkin görüşlerini ifade eden verileri toplamak amacıyla görüşme formu kullanılmıştır. Görüşme formu katılımcıların siber terörizm konusundaki görüşlerini belirlemeye yönelik 13 soru içermektedir.

Nitel araştırma; yapılandırılmamış gözlem, yapılandırılmamış görüşme ve doküman inceleme gibi nitel veri toplama tekniklerinin kullanıldığı, olgu ve olayların kendi doğal ortamları içinde gerçekçi ve bütüncül bir şekilde ortaya konmasına yönelik nitel bir sürecin izlendiği araştırma olarak tanımlanmaktadır (Yıldırım ve Şimşek 2008, s.58). Nitel araştırmanın, bir olguyu bireylerin bakış açısından görebilmek ve bu bakış açılarını edinmelerine neden olan süreç ve ortamı ortaya çıkarmak için etkili bir araştırma yöntemi olduğu söylenebilir (Patton, 2014).

Bu araştırmada, alanında uzman deneyimli yedi akademik ve bir idari katılımcının Türkiye'de siber terörizme karşı bilişim teknolojilerinin kullanımı ile ilgili görüşleri ele alınmıştır. Araştırma, nitel araştırma yöntemlerinden fenomenoloji deseni kullanılarak yürütülmüştür. Fenomenoloji deseni, deneyim üzerine odaklandığından çalışmada bu yöntem tercih edilmiştir (Merriam, 2014). Çalışmada yarı yapılandırılmış görüşme yöntemiyle veriler toplanmıştır. Ekiz'e (2003) göre yarı yapılandırılmış görüşme sırasında görüşme yapılan kişilere kısmi bir esneklik sağlanmakta, sorular gerektiğinde yeniden düzenlenmekte ve tartışılmaktadır. Bu tür bir görüşmede, katılımcılarında araştırma üzerinde kontrolleri olmaktadır (Ekiz, 2003). Yarı yapılandırılmış görüşmenin, yapılandırılmış görüşmeye göre biraz daha esnek olduğu söylenebilir. Bu teknikte, araştırmacı önceden oluşturulan ve katılımcılara sormayı planladığı soruları içeren görüşme formunu hazırlamaktadır. Buna karşın araştırmacı görüşmenin akışına bağlı olarak bu sorulara bağlı kalmayıp, farklı yan ya da alt sorularla görüşmenin akışını etkileyebilmekte ve kişinin yanıtlarını derinleştirmesini ve detaylandırmasını sağlayabilmektedir. Eğer katılımcılar görüşme esnasında sorulan sorulara yönelik verdikleri yanıtları önceden sorulan sorular içerisinde belirtmiş ise, araştırmacı bu sorular için yeniden görüş istemeyebilir. Yarı yapılandırılmış görüşme tekniğinin araştırmacıya sunduğu en önemli kolaylık görüşmenin önceden hazırlanmış görüşme formuna bağlı olarak sürdürülmesi nedeni ile daha sistematik bilgi sunması olduğunu söylemek mümkündür (Yıldırım ve Şimşek 2008, Çalışır, 2015, s.12).

Araştırmanın verileri siber terör konusunda uzman katılımcılarla (ağırlıklı akademik uzmanlar) 04/12/2019 – 20/02/2020 tarihleri arasında yapılan görüşmelerden elde edilmiştir. Toplanan veriler elektronik ortamda kayıt altına alınarak sözel ve sayısal işlemler yapılabilmesi için ön çözümlemeye tabi tutulmuştur. Ön çözümleme sonucunda araştırmanın sözel verileri NVivo 12 istatistiksel çözümleme programında analiz edilmiştir.

Görüşme formu üç aşamada geliştirilmiştir. İlk aşamada, öncelikle ilgili alanyazın detaylı bir biçimde incelenmiş, alan uzmanlarıyla görüşmeler yapılmış ve oluşan deneyimle 32 maddelik görüşme madde havuzu oluşturulmuştur. İkinci aşamada, oluşturulan havuzda yer alan maddeler siber terörizm alan uzmanı dört öğretim üyesi ile Ölçme ve Değerlendirme alan uzmanı üç öğretim üyesinin görüşüne sunulmuştur. Uzmanlardan gelen dönütlere göre taslak form oluşturulmuştur. Taslak form dil bilim uzmanlarının incelemesine sunulmuş, onlardan gelen geri bildirimler ışığında soru kökleri üzerinde düzenlemeler yapılmıştır. Üçüncü aşamada ise, altı kişi ile pilot görüşmeler yapılarak formun maddeleri test edilmiştir. Ön uygulamaların tamamlanmasının ardından alan uzmanlarıyla formun değerlendirilmesi yapılmış ve forma son şekli verilmiştir.

Araştırmada katılımcılara siber terörizm konusunda yöneltilen sorular şunlardır:

- Siber terörizme karşı koymada bilişim teknolojilerinin etkin kullanımı için nasıl çalışmalar yapılmalıdır?
- Günümüzde en tehlikeli terör faaliyetlerinden birisi olan siber terörizmi nasıl tanımlarsınız? Hangi tip saldırıları siber terör saldırısı olarak adlandırabiliriz?
- Ülkemizde siber terörizme karşı bilişim teknolojilerinin farkındalığını arttırmak için nasıl çalışmalar yapılmalıdır?
- Siber terör saldırılarına maruz kalmamak için yapılması gereken çalışmalar nelerdir?
- Günümüzde bilişim teknolojileri kullanımının birçok açıdan kurumlar ve bireyler için bir zorunluluk haline gelmesi siber saldırıları tetikliyor mu?
- Ülkemize ciddi bir siber terör saldırısı gerçekleşse karşı koyabilecek bilişim teknolojilerine ve deneyimine sahip miyiz?
- Sizce dünyada ve ülkemizde yapılan siber terör saldırılarında yöntem farklılığı var mıdır? Varsa bunlar nelerdir?

- Siber terörizme karşı siber güvenlik farkındalığını nasıl oluşturabiliriz? Bilişim teknolojilerinde milli ve yerli ürün üretimi ve kullanımı hakkındaki görüşleriniz nelerdir?
- Siber suç ile siber terör kavramları arasında fark var mıdır? Siber terör saldırılarında saldırganlar hangi yöntemleri kullanmaktadırlar?
- Sizce ülkemizde siber terör saldırılarına karşı toplumsal direncin arttırılması için toplum nasıl bilinçlendirilmeli ve ne gibi eğitim verilmelidir?
- Yüksek lisans düzeyinde eğitim almış adli bilişim uzmanlarının kamu kurumlarınca istihdam edilmesi siber terör saldırılarının önüne geçebilmek içim önemli bir adım olabilir mi?
- Yetenekleri arttırılmış ve insan vücuduna yerleştirilebilen kablosuz internet bağlantısı yeteneğine sahip cihazların (insülin pompası, kalp pili, işitme cihazı vb.) siber terör hedefi haline gelmemesi için ne gibi önlemler alınmalı?
- ABD'de 2010 yılının ocak ayında siber atakları analiz edip hangi saldırgan tarafından saldırı gerçekleştirildiğinin tespit edilmesi ve saldırılara göre savunma ve karşı atak stratejileri geliştirmek için siber genom projesi başlatılmıştır. Türkiye'de buna benzer bir proje çalışması var mıdır? Sizin düşünceleriniz nelerdir?

Araştırmaya katkı sunan katılımcılara ait demografik bilgiler ve katılımcılar hakkında tanıtıcı özelliklere ilişkin bilgiler aşağıda verilmiştir.

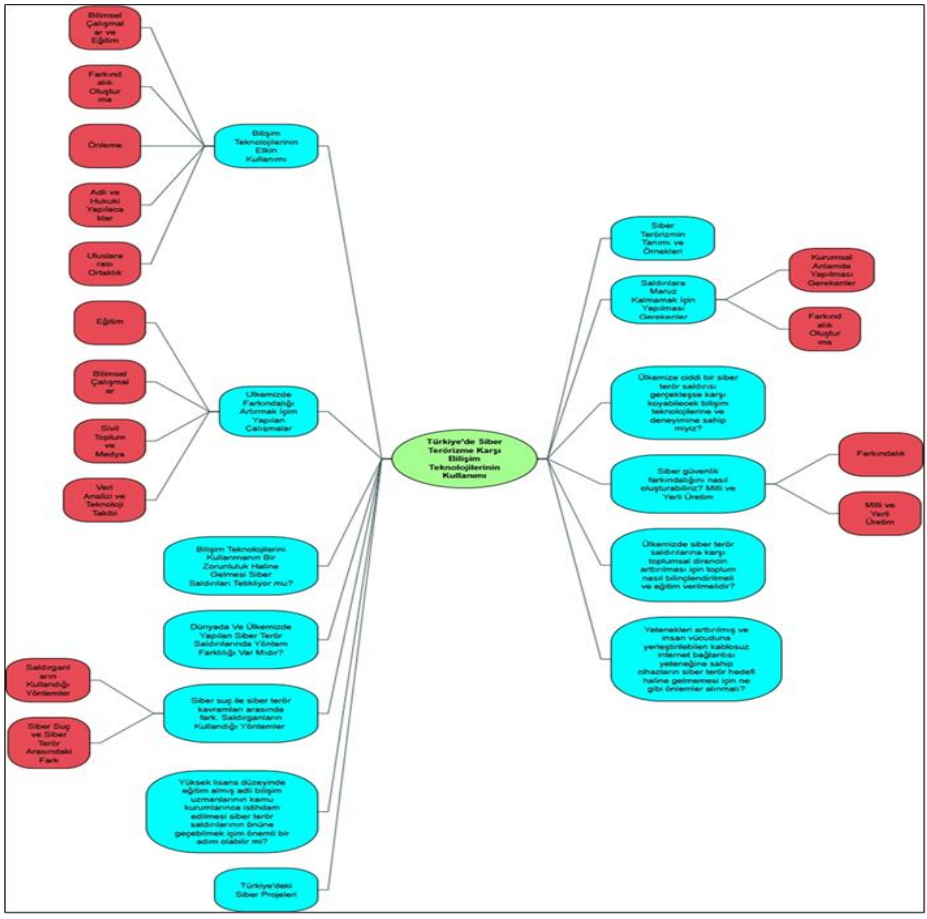
*Tablo 1. Katılımcılar Hakkında Bilgiler*

| Yaşı | Unvanı | Öğrenim Düzeyi | Mesleği | Kurumda Çalışma Süresi | Çalışma Alanı | Bilişim Alanında Çalışma Süresi (Yıl) | Son 5 Yılda Eğitim Verme Durumu |
|---|---|---|---|---|---|---|---|
| 58 | Siber güvelik akademisi kurucusu | Doktora | Akademik personel | 15 | Siber güvenlik, Elektronik imza, Ulusal frekans planı | 20 | Evet |
| 55 | Kişel verileri koruma kurumu danışmanı | Doktora | Akademik personel | 13 | Bilgi güvenliği, Siber güvenlik, | 18 | Evet |
| 57 | Havelsan Yetkilisi | Doktora | İdari personel | 9 | Siber savaş, Siber terörizme karşı siber savunma | 12 | Evet |
| 48 | Daire başkan yardımcısı | Doktora | Akademik personel | 8 | Bilişim suçları, Dijital deliller | 13 | Evet |
| 30 | Bilişim uzmanı | Yüksek lisans | Akademik personel | 6 | Bilgi güvenliği, Siber güvenlik | 10 | Hayır |
| 38 | Bölüm başkanı | Doktora | Akademik personel | 8 | Yapay zekâ, Bilgisayar yazılımı | 10 | Evet |
| 39 | Bilişim sistemleri Uzmanı | Yüksek lisans | Akademik personel | 10 | Network, Bilişim Sistemleri | 10 | Evet |

## Bulgular

Bu çalışma Türkiye'de siber terörizmin daha etkin kullanımı konusunda bu alanla ilgili ne gibi iyileştirmeler yapılması gerektiğini betimlemeye yöneliktir. Elde edilen veriler üzerinde, verilerin çözümlenmesi kısmında değinilen işlemler uygulanmış ve ulaşılan bulgular birinci, ikinci, üçüncü, …., on üçüncü soruya ilişkin bulgular olmak üzere on üç kısımda verilmiştir. Elde edilen bulguların sunulmasında görsel düzenleyiciler kullanılmıştır. Çalışma kapsamında katılımcılar ile yapılan görüşmelerden elde edilen kayıtların dökümleri alınmış ve veriler ayrıntılı olarak düzenlenmiştir. Bu verilerden yararlanılarak kodlar ve temalar oluşturulmuştur.

Araştırmada yapılan görüşmelerden elde edilen verilerin ön incelemesinde, araştırma sorularıyla paralel olacak biçimde on üç temel tema belirlenmiştir. Bu kapsamda, bazı temalara ilişkin kategoriler oluşturulmuştur. Ayırt edici bir kategori oluşmayan temalar kendi içerisinde katılımcı görüşleri doğrultusunda değerlendirilmiştir. Elde edilen bulgulardan oluşturulan tema ve kategoriler aşağıda Şekil 1'de gösterilmiştir.




***Şekil 1. Araştırmanın tema ve kategorileri***

Araştırmaya katılan katılımcılara siber terör konusunda 13 soru yöneltilmiştir. Sorular katılımcıların siber terör konusundaki görüşlerini, bu konuda alınabilecek tedbirleri, yapılması gerekenleri betimlemeye dönüktür.

Siber terörizme karşı koymada bilişim teknolojilerinin etkin kullanımı konusunda katılımcıların kendilerine yöneltilen sorulara verdikleri yanıtların dökümleri alınmış, içerik analizi ile çözümlenmiştir. Katılımcıların oluşturdukları kodlar, bilişim teknolojilerinin etkin kullanımı teması için; bilimsel çalışmalar ve eğitim, farkındalık oluşturma, önleme, adli ve hukuki yapılacaklar ve uluslararası ortaklık alt kategorileriyle ilişkilendirilmiştir. Katılımcıların sorulan sorularla ilgili doğrudan görüşleri verilirken, bu görüşler ifadelerin başlangıcında katılımcılara atanan kodlar ile belirtilmiştir. Örnek: K1, K2, K7 gibi.

***Birinci Araştırma Sorusu: Siber terörizme karşı koymada bilişim teknolojilerinin etkin kullanımı için nasıl çalışmalar yapılmalıdır?*** Katılımcıların siber terörizme karşı koymada bilişim teknolojilerinin etkin kullanımı konusunda verdikleri cevaplar Tablo 2' de verilmiştir:

***Tablo 2. Katılımcıların Siber Terörizme Karşı Koymada Bilişim Teknolojilerinin Etkin Kullanımı Konusunda Verdikleri Cevaplar***

| Kategoriler | Görüşler |
|---|---|
| **Bilimsel Çalışmalar ve Eğitim** | • Bilişim teknolojilerinin etik ve ahlaki kullanımı hakkında eğitim verilmeli<br>• Etkin ve yetkin kullanabilecek yetişmiş insan kaynağı kurumsal ve ülkesel anlamda oluşturululmalı<br>• Açık kaynak geliştirme platformları kurulmalı<br>• Bu konu ile ilgili güvenlik birimleri kurulmalı ve eğitim faaliyetlerinin yürütüleceği enstitüler açılmalı<br>• Bilişim sistemleri vasıtasıyla huzur ortamının sağlanması güvenli iş ortamının ve ekonomik refahın korunması gibi konularda çalışmalar yapılmalı |
| **Farkındalık Oluşturma** | • Bireysel ve kurumsal anlamda bu farkındalığın oluşturulması<br>• Kamuoyu farkındalığı oluşturmak için bilgilendirici ve farkındalık artırıcı kamu spotları hazırlanması<br>• Tüm özel sektör ve kamu kuruluşlarının ve bireylerin internet ve ağ güvenliği konusunda bilinçlendirilmeli ve teknik önlemler alınmalı |
| **Önleme** | • Bilgisayar teknolojisi ürünlerinin herhangi bir açıklık barındırmaması, yetkilendirme düzeylerinde kullanılan kullanıcı adı ve şifrelerin iyi bir şekilde saklanmış olması<br>• "Siber terör ve suçla mücadele ekosistemi" oluşturulmalı<br>• Standartlara uygun olarak sistemlerin kurulması ve işletilmesi, güvenli ortamların oluşturulması, sistemlerin sızma testlerinden geçirilmesi<br>• Kurumlar koordineli çalışmalar yaparak hazırlıklı olmalı ve müdahale edebilme gücü kazanmalı<br>• Bilişim ve iletişim sistemlerinin risk analizlerinin iyi yapılması ve bu risklere karşı sistemlerin yazılımsal ve donanımsal olarak güçlendirilmesi ve ağ sistemlerinin güçlendirilmesi ve yeterli uzman ekibin sağlanması |
| **Adli ve Hukuki Alanda Yapılacaklar** | • Bilişim suçları yasası çıkarılmalı<br>• Siber suçlarla ilgili olarak fail veya faillerin yakalanabilmesi adına bilişim teknolojileri çok etkin bir şekilde kullanılmalı |
| **Uluslarası Ortaklık** | •Uluslararası çözüm bulunması gerekliliği<br>•Ortak yolların geliştirilmesi<br>• İnterpol bünyesinde siber terörizm ile mücadele konusunda birim kurulmalı |

***İkinci Araştırma Sorusu: Günümüzde en tehlikeli terör faaliyetlerinden birisi olan siber terörizmi nasıl tanımlarsınız? Hangi tip saldırıları siber terör***

***saldırısı olarak adlandırabiliriz?*** Katılımcıların verdikleri cevaplara göre kısaca siber terörizmi "terör eylemlerinin bilişim sistemleri araçlarının kullanılarak gerçekleştirilmesi" olarak tanımlayabiliriz. Bu konuda bazı katılımcıların verdikleri cevaplar şu şekildedir:

K2: "*Bilgisayar ve bilgisayar bileşenleri ile bilişim sistemleriyle siber uzayda gerçekleştirilen ve yine politik ya da siyasi bir amaç doğrultusunda insanlara mala cana kamu malına zarar vermeye yönelik amaçlar barındıran her türlü eyleme siber terörizm diyebiliriz.*"

K6: "*Belirli bir sosyopolitik amaca ulaşabilmek için bilgisayar ve bilgisayar teknolojilerinin bireylere veya ürünlere karşı bir toplumu veya hükümeti yıldırma, baskı altına alma amacıyla kullanılması olarak tanımlayabiliriz.*"

Katılımcılar siber terörizmin hukuki bir tanımı olmadığını da belirtmişlerdir. Katılımcılardan K5, "Türk hukuku bakımından siber terörizmin bir kavram olarak tanımlanmadığını ifade etmiştir. 3713 sayılı terörle mücadele kanundaki tanımda sadece terörizmin tanımının yer aldığını siber terörizmin ise bu kapsama girebilmesi için zorlamak gerektiği" şeklinde bu konuya değinmiştir.

Katılımcıların siber terörizme verdikleri örnekler ise şu şekildedir:

"*Siber terörizm ile teröristler; barajlar, ordunun kritik öneme sahip milli sistemleri, trafik ışıkları, telefonlar, elektrik doğalgaz şebekeleri, bilgisayar sistemlerine sızma, ulaşım sistemleri, su sistemleri, bankacılık ve finans, hastane, itfaiye vb. kritik öneme sahip sistemlerin işlevsiz kalmasına neden olabilirler. Bilgisayar sistemlerine ve servislerine yetkisiz erişim, bilgisayar donanım ve sistemlerine zarar vererek sabotajda bulunma , banka ve kredi kartları ile bilgileri ele geçirerek bilgisayar yoluyla dolandırıcılık yapma, tehdit ve şantaj yoluyla siber zorbalık ve çeşitli online platformların terörizm için bir propaganda aracı olarak kullanılması*"; "*kritik alt yapılara saldırılar, havayolu idare sistemlerine yönelik saldırılar veya barajlara , doğalgaz sistemlerine yönelik saldırılar gerçekleştirilebileceği (basınçları değiştirmek suretiyle boruları patlatabilir)*"şeklinde ifade edilmiştir.

***Üçüncü Araştırma Sorusu: Ülkemizde siber terörizme karşı bilişim teknolojilerinin farkındalığını arttırmak için nasıl çalışmalar yapılmalı?*** Ülkemizde siber terörizme karşı bilişim teknolojilerinin farkındalığını arttırmak için yapılacak çalışmalar temasına ilişkin katılımcı görüşleri; eğitim, sivil toplum kuruluşları ve medya ile yapılabilecek faaliyetler, bilimsel

çalışmalar, teknolojilerin takibi ve veri analizi alt kategorileri altında incelenmiştir. Bu konudaki görüşler Tablo 3'te belirtildiği gibidir.

***Tablo 3. Katılımcıların Ülkemizde Bilişim Teknolojilerinin Farkındalığı Arttırmak İçin Yapılabilecekler Konusunda Verdikleri Cevaplar***

| Kategoriler | Görüşler |
|---|---|
| **Eğitim** | • Bilişim teknolojilerinin doğru kullanımına ve bunların sonuçlarında neler olabileceğini gösteren eğitimlerin verilmesi<br>• Bilinçli kişilerin yetiştirilmesi<br>• Bilişim teknolojisi kullanıcısının bilgilendirilmesi<br>• Üniversite müfredatlarına bu alanla ilgili yeni dersler eklenmesi<br>• İlkokuldan başlamak üzere üniversiteye kadar eğitim içeriklerinde müfredatlar da uygulamalarda siber güvenlik, siber saldırı, siber tehdit vb. konularına yer verilmeli<br>• Siber terör faaliyetlerinin hem kurumları hem de bireyleri etkilediği bir gerçektir. Bu kapsamda farkındalığı arttırmak için bireylerinde erken yaşlardan itibaren teknoloji okur yazarlığı konusunda eğitilmeleri gerekmektedir.<br>• Siber terör, siber güvenlik, siber saldırı, siber zorbalık gibi başlıkları da kapsayacak şekilde oluşturulacak bir içeriğin örgün ve yaygın eğitim kurumlarında verilmesi<br>• Okullarda bilişim derslerinin etkin öğretilmesi, siber güvenlik konusunda seminerler verilmesi, lise ve üniversiteler de siber güvenlik ve siber terörizm içerikli derslerin verilmesi, ailelerin mobil cihaz, bilgisayar, sosyal platformların doğru kullanılması için bilinçlendirilmesi, çocuklar için dengeli ve sağlıklı bilgisayar kullanım alışkanlığının kazandırılması ve buna benzer eğitimler verilmesi<br>• Kamu ve özel kurumlarda çalışanların bilişim etiği ve güvenliği konularında bilinçlendirilmesi |
| **Sivil toplum Kuruluşları ve Medya Kullanılmalı** | • Sivil toplum kuruluşları, özel ve kamu kurumlarının birlikte hareket ederek konuya yönelik farkındalığı üst seviyeye çıkarabilecek ortak birtakım etkinlikler; seminerler, konferanslar, çalıştaylar vs. düzenlenmesi, ayrıca medya organlarının (televizyon ve radyo yayıncılığı, sosyal medya vb.) etkin bir şekilde kullanılarak toplumun tüm kesimlerine ulaşılması yoluyla her kesimin bilinçlendirilmesinin sağlanması<br>• Kamu kurum çalışanlarının ilgisi bu yöne çekilmeli sivil toplum kuruluşları aracılığıyla etkinlikler düzenlenmelidir. Medya aracılığıyla kullanıcılar aydınlatılabilir |
| **Bilimsel Çalışmalar** | Üniversitelerde ileri düzey çalışmalar, tezler, projeler ve araştırmalar yapılmalı |
| **Veri Analizi ve Teknoloji Takibi** | • Açıklıklar tehditler ve saldırılar ile kullanılan teknik ve teknolojiler çok yakından takip edilmeli<br>• Saldırganların davranışları iyi bilinmeli ve analiz edilmeli kullandıkları yöntemler teknik ve teknolojiler hakkında bilgi sahibi olunmalı elde edilen birikimler ve deneyimlere göre karşı çözümler geliştirilmeli<br>• Kurumlar arası iş birliği ve veri paylaşımının yapılması ve arttırılması, ortak analiz çalışmalarının yürütülmesi |

Bu soru ile ilgili olarak katılımcılardan K5 farklı bir görüşe sahiptir. K5 "*Siber terörizme karşı bilişim teknolojileri farkındalığının arttırılmasının aynı zamanda teröristlere de bilişim sistemlerinin kullanılması noktasında bir avantaj sağladığı*" şeklinde bu konuda görüşünü ifade etmiştir.

***Dördüncü Araştırma Sorusu: Siber terör saldırılarına maruz kalmamak için yapılması gereken çalışmalar nelerdir?***

Katılımcıların verdikleri cevaplar kurumsal veya devlet olarak yapılması gerekenler ile farkındalığın artırılması alt kategorileriyle ilişkilendirilmiştir. Katılımcıların bu konudaki görüşleri Tablo 4' te verilmiştir.

***Tablo 4. Katılımcıların Siber Terör Saldırılarına Maruz Kalmamak İçin Yapılması Gereken Çalışmalar Konusunda Verdikleri Cevaplar***

| Kategoriler | Görüşler |
|---|---|
| **Kurumsal Anlamda Yapılması Gerekenler** | • Bilişim teknolojilerine hakim olan bir kurum<br>• Sürdürülebilir denetim mekanizması<br>• Siber güvenlik politikası<br>• Bu politikaları hayata geçirecek olan eylem planları<br>• Siber güvenlik alt yapısı<br>• Bilgi seviyesi ve farkındalığı yüksek personeller yetiştirilmesi<br>• Yerli ve milli siber güvenlik çözümleri yazılım ve donanım anlamında geliştirilmeli<br>• Yabancı ürün kullanımı azaltılmalı<br>• Uluslararası işbirlikleri arttırılmalı<br>• En zayıf halkayı tespit edip onun üzerine çalışmalar yapılmalı<br>• Tespit edilen tehditler hızla giderilmeli |
| **Farkındalık Sağlanmalı** | • Kullanıcı şifreleri her hesap için farklı seçilmeli<br>• Şifreler ikinci kişilerle paylaşılmamalı kaynağı bilinmeyen ve şüpheli dosyalara erişim sağlamamalı<br>• Kullanıcıların farkındalık düzeyleri arttırılmalı<br>• Sosyal platformların daha etkin ve bilinçli olarak kullanılması<br>• İlkokul seviyesinden başlanılarak kapsayıcı eğitimlerin verilmesi |

***Beşinci Araştırma Sorusu: Günümüzde bilişim teknolojileri kullanımının birçok açıdan kurumlar ve bireyler için bir zorunluluk haline gelmesi siber saldırıları tetikliyor mu?***

Katılımcıların tamamı bilişim teknolojileri kullanımının zorunlu hale gelmesinin, siber saldırıları tetiklediği şeklinde görüşlerini belirtmişlerdir. Katılımcılar, bu gelişmelerden faydalanmak isteyen kötü niyetli kişilerin her zaman olduğunu ve olmaya da devam edeceğini ifade etmişlerdir. Katılımcılardan bazılarının bu konudaki görüşleri şu şekildedir:

K5: "*Tüm bilgileri merkeze koyduğunuz zaman o bilgilerin yok olması da artık başlı başına bir tehdit haline gelir. Otomatik olarak ne kadar fazla gündelik hayatınızı bilişim sistemlerine yoğunlaştırırsanız o kadar fazla darbe yeme tehlikesi ile karşı karşıya kalırsınız. Tüm devlet kurumları bilişim güvenliği alt yapısı üzerine inşa edilmeli. İnternet üzerinden devlete ödenen fatura belgelerinin veri alt yapısının silinmesi sonucu oluşabilecek bir kaosu düşünün. Kim nerden neyi tahsil etti*

*bilmiyor. Tahsil edilmiş faturaların ikinci kez ödeme yapılması isteniyor, insanlar ödememek için dekontlarını almaya çalışıyor bayağı bir kargaşa ve kaos ortamı oluşur."*

K6: "*TÜİK verilerine göre Türkiye'de 2020 yılı itibariyle internet kullanan bireylerin oranı %79,0, internet erişimi %94,9, olarak gösteriliyor ve gün geçtikçe de artmaya devam ediyor. Bu oranlardaki artışa paralel olarak siber terör faaliyetlerinin de arttığı ve artacağı da çok açıktır. Bu durum siber saldırganların iştahlarını kabartmakta ve siber saldırıları çok ciddi bir şekilde tetiklemektedir."*

***Altıncı Araştırma Sorusu: Ülkemize ciddi bir siber terör saldırısı gerçekleşse karşı koyabilecek bilişim teknolojilerine ve deneyimine sahip miyiz?*** Katılımcıların dördü bu konuda olumsuz cevap verirken sadece biri olumlu cevap vermiştir. Diğer katılımcılardan biri bu konuda tereddütleri olduğunu belirtirken bir diğeri bu konuda elinde somut veriler olmadığı için net konuşamayacağını ifade etmiştir. Bu konuda olumsuz cevap veren katılımcılar ülkemizin kullandığı sistem ve çözümlerin hepsinin yabancı kaynaklı olduğu ve bu kaynakların güvenli olmadığı, kullanılan sistemlerde arka kapıların ve açıklıklarının olabileceği ve güvenliğimizin yabancı devletlere bağımlı olduğunu ifade etmişlerdir. Bu konuda katılımcılardan birinin görüşleri şu şekildedir:

K3: "*Bence bu çok net hayır. Çünkü Türkiye'nin bu konuda kullandığı çözümler yabancı çözümlerdir, zaten bu çözümlerin güvenlikli oldukları ciddi tartışma konusudur. Dolayısıyla mevcut çözüm olarak siber saldırılara karşı önlem olarak almayı düşündüğümüz ya da yapılandırmış olduğumuz alt yapılardaki yazılımsal ve donanımsal alt yapıların bir defa kendi güvenliği tartışmalıdır. Bunların her birinin tersine güvenlik zafiyetleri, güvenlik açıkları, arka kapıları olduğu düşünülebilir. Böyle olduğunda ne yazık ki biz Türkiye olarak bu siber saldırılara önlem alabilecek ne teknolojik imkanlara sahibiz ne de bireysel yetişmiş insan kaynaklarına sahibiz."*

Bu konuda olumlu görüş belirten tek katılımcı, gereken bilgi teknolojilerine ve deneyimine sahip olduğumuzu ancak dünya ölçeğinde yeterli seviyede olmadığımızı ifade etmiştir. Bu katılımcının görüşleri şu şekildedir:

K4: "*Evet ülkemizde terör saldırılarına karşı koyabilecek ve saldırıları önceden tespit edecek bilgi teknolojilerine ve deneyimine sahibiz. Bu alandaki çalışmalarımız her geçen gün artarak devam etmektedir. Ancak dünya siber güvenlik sektörü değerlendirildiğinde sektörümüz belirlenen seviyede değildir. Bunun geliştirilmesi için sektöre verilen teşvikler sürdürülmelidir."*

***Yedinci Araştırma Sorusu: Sizce dünyada ve ülkemizde yapılan siber terör saldırılarında yöntem farklılığı var mıdır? Varsa bunlar nelerdir?*** Katılımcıların konu ile ilgili görüşleri ayrışmaktadır. Bazı katılımcılar bu konuda farklılık yoktur derken bazıları ise fark olduğunu ifade etmektedir. Mesela katılımcılardan K1 ve K2 saldırılar konusunda farklılık olmadığını ifade ederken diğer katılımcılar farklılıklar olduğunu ifade etmektedirler. Katılımcılardan K3 yöntem farklılıklarının çok fazla olduğunu ve ülkelerin yetenekleri ve kabiliyetlerine göre bu saldırı yöntemlerinin ve saldırı tekniklerinin de farklılık gösterebildiğini ifade etmektedir.

Katılımcılardan K6 ise dünyada ve ülkemizde yapılan siber terör saldırılarında yöntem ve amacın aynı olduğunu fakat ülkeye göre saldırılar konusunda farklılıklar olduğunu belirtmiştir. Katılımcılardan K7 ise her ülkedeki insan profiline göre siber saldırı teknikleri geliştirildiğini ifade etmiştir.

***Sekizinci Araştırma Sorusu: Siber terörizme karşı siber güvenlik farkındalığını nasıl oluşturabiliriz? Bilişim teknolojilerinde milli ve yerli ürün üretimi ve kullanımı hakkındaki görüşleriniz nelerdir?*** Siber güvenlik farkındalığını nasıl oluşturabiliriz, milli ve yerli üretim teması; iki kategori şeklinde ele alınmıştır. Birincisi; siber güvenlik farkındalığı kategorisi, ikincisi ise; bilişim teknolojilerinde milli ve yerli üretimin kullanılması kategorisidir. Farkındalık konusunda katılımcıların en fazla üzerinde durdukları konu eğitimdir. Katılımcıların eğitim ve farkındalık ile ilgili görüşleri şu şekildedir:

- Eğitim kurumları ve ilgili bakanlıklar ile iş birliği ile eğitimler verilmeli
- Siber güvenlik uzmanları tarafından çeşitli seminerler, konferanslar verilmeli
- Siber suçların cezalarının normal suçlardan daha ağır olduğu bildirilip, öğretilmeli
- Farkındalık seviyeleri ara ara test edilip eksiklikler giderilmeli
- Her kurum içerisinde farkındalık oluşturulmalı
- Güvenlik güçleri personellerinin mobil cihazları çok dikkatli kullanması özellikle dış kaynaklı olan uygulamalara çok dikkat etmesi sağlanmalı
- Güvenli davranış biçimleri içselleştirilip otomatik tepkiler haline gelmeli

Katılımcılar siber güvenlik konusunda yerli ve milli teknolojinin yeterli olmadığını ifade etmişlerdir. Katılımcılar milli ve yerli teknolojiler konusunda yapılması gerekenleri şu şekilde ifade etmişlerdir:

- Siber güvenlik, milli ve yerli teknolojiler konusunda otoriter bir kuruma ihtiyaç olduğu
- Bu kurumun yerli ve milli teknolojilerle ilgili politika ve stratejiler geliştirmesi gerektiği
- Yerli ve milli teknolojilerin geliştirilmesi noktasında ciddi ar-ge destekleri teşvikleri hayata geçirilmesi gerektiği
- Bunları denetleyecek kurumların da oluşturulması gerektiği
- Yerli ve milli kullanıyorum diye de bir sürü açığı olan programların kullanmaması gerektiği şeklindedir.

***Dokuzuncu Araştırma Sorusu: Siber suç ile siber terör kavramları arasında fark var mıdır? Siber terör saldırılarında saldırganlar hangi yöntemleri kullanmaktadırlar?*** Siber suç ile siber terör kavramları arasında fark ve saldırganların kullandığı yöntemler temasına ilişkin katılımcı görüşleri; saldırganların kullandığı yöntemler ve siber suç ve siber terör arasındaki fark kategorileri altında incelenmiştir. Buna göre katılımcılar, siber suç ve siber terör kavramlarının farklı kavramlar olduğunu ifade etmişlerdir. Katılımcıların genel görüşü siber suçun bireysel amaçlar doğrultusunda gerçekleştirilen genelde maddi kazanç ya da tatmin duygularını yaşamak için belli hedeflere yönelik gerçekleştirilen küçük saldırılar olduğu, siber terörün ise daha çok organize siyasi ya da politik bir amacı olan ve insanlar üzerinde korku yaymayı amaçlayan genelde siber suçta kullanılan yöntemlerden daha geniş kaynaklar ile daha yıkıcı sonuçlar ortaya koyan spesifik ve kritik alt yapılara yönelik gerçekleştiren saldırılar olduğudur. Bu konuda yöntem bakımından fark olmadığı ama amaç olarak farklılık olduğunu ifade eden katılımcılar da vardır. Bu konuda bazı katılımcıların görüşleri şu şekildedir:

K7: "*Siber suç dijital platformlarda hukuksal olmayan tüm eylemleri ifade ediyor. Siber terörü ise fiziksel Dünya'da terör eylemlerinin dijital ortama aktarıldığı bilgisayar ve bilgisayar sistemleri kullanılarak icra edilen eylemler olarak tanımlayabiliriz.*"

K3: "*Siber suç bazen bireysel anlamda kişilerin farkında olmadan işleyebileceği suçlar olabildiği gibi kimliği belirsiz kişilerce bireylerin kendi bilişim alt yapılarını ve sistemlerini kullanarak onun üzerinden suç işlemiş gibi gösterebilecekleri durumlar*

*da mevcuttur. Bu durum maalesef günümüzde sıklıkla karşılaşılan bir durumdur. Biz bunları ayrıştırırken özellikle bireysel anlamda ülkelere, kurum veya kuruluşlara yapılan saldırılara yani siber saldırılara siber terör diyoruz. Ama bu saldırılar bir devlet kuruluş veya örgüt aracılığıyla bilinçli bir şekilde bir başka devlete yapılıyorsa buna da siber savaş diyoruz. Dolayısıyla siber terör veya siber suç dediğimiz unsur birbirinden çok farklı şeylerdir. Bireysel anlamda yapılanlara siber suç, örgütsel ya da ulusal anlamda kurumlara kuruluşlara veya devletlere yönelik yapılan saldırılara ise siber terör diyoruz.''*

Katılımcıların siber terör saldırıları için verdiği bazı örnekler ise şu şekildedir:

APT, DoS, network tabanlı saldırılar sistemlerin devre dışı kalması, enjeksiyon saldırıları (sistemi ele geçirmek ve sistemde kalıcı olarak istedikleri gibi spekülasyonlar yaparak korku ve panik havası yaratmak gibi saldırı gerçekleştirmek), gelişmiş kalıcı tehdit (advanced persistent threat), kötücül yazılım (malware), virüsler-solucanlar, hizmet aksattırma saldırıları (DDoS), fidye-şantaj yazılım (ransomware), oltalama (phishing) saldırıları.

***Onuncu Araştırma Sorusu: Sizce ülkemizde siber terör saldırılarına karşı toplumsal direncin arttırılması için toplum nasıl bilinçlendirilmeli ve eğitim verilmelidir?*** Katılımcıların bu soruya verdikleri yanıtlar incelendiğinde bu konuda yapılması gerekenleri şu şekilde özetlenebilir:

- Bu konuda hem aileleri hem de öğrencileri bilinçlendirici faaliyetler yapılmalı.
- İlkokul, ortaokul, lise ve üniversite seviyesinde dijital okuryazarlık ve bilgisayar teknolojileri dersleri verilmeli.
- Siber güvenlik uzmanların eğitim broşürleri, kamu spotları, bilgilendirici kitaplar hazırlaması.
- Kurumsal bilinci ve yetenekleri de artırmak gerektiği. Siber ordu, siber polis teşkilatı gibi kurumsal yapıları oluşturmak gerektiği.
- İnsanları eğittikten sonra pratik yapmaları için bu konuda tatbikatlar yapılmasının gerekliliği.
- Bilişim teknolojileri sürekli geliştiği için verilen eğitimlerin ve yapılan tatbikatların süreklilik arz etmesi ve güncellenmesi.
- Kişiye özel davranışların güvenli kullanım ve güvenlik farkındalığı kapsamında izlenmesi ve incelenmesi sonucunda elde edilen verilere göre, olumsuzluklar ön plana tutulmamalı, daha çok olumlu, uygun,

yapıcı ve süreklilik arz eden davranış biçimleri teşvik edilerek ödüllendirilmeli.

Bu konuda bazı katılımcıların görüşleri şu şekildedir:

K5: "*Siber terör saldırılarına karşı tatbikatlar yapılmalı. Örneğin belli bir bölgede elektriklerin ve sinyalizasyonun hiç olmadığını düşünelim, belli bir bölgede su akış sisteminde, doğalgaz akış sisteminde bir saldırı üzerine bu hizmetlerin verilemediğini düşünerek bu durumlarda nasıl hareket edileceği noktasında senaryolar üretilmeli ve tatbikatları yapılmalı. İnsanların böyle durumlarda paniğe kapılmamaları için senaryolar hazırlanmalı.*"

K4: "*Öncelikle siber suçların normal suçlardan farklı olduğu öğretilmeli. Bireylerin erken yaşlardan itibaren teknoloji okuryazarlığı konusunda eğitimleri de çok önemlidir. Siber terör, siber güvenlik, siber saldırı, siber zorbalık, siber suç vb. konuları ihtiva edecek şekilde bir içeriğin oluşturularak tüm eğitim kurumlarında müfredata eklenmesi de önem arz etmektedir. Son olarak toplum siber saldırılarının ne olduğunu hakkında bilgi sahibi olmalı böylelikle ileride karşılaşılabilecek saldırılara karşı korunmasız kalmamalı hatta savunma mekanizması oluşturması gerektiği ile ilgili bilgilendirilmelidir.*"

***On birinci Araştırma Sorusu: Lisansüstü seviyesinde eğitim almış adli bilişim uzmanlarının kamu kurumlarınca istihdam edilmesi siber terör saldırılarının önüne geçebilmek içim önemli bir adım olabilir mi?***

Katılımcıların hepsi yüksek lisans düzeyinde eğitim almış adli bilişim uzmanlarının kamu kurumlarınca istihdam edilmesinin çok önemli olduğunu vurgulamışlardır. Katılımcılar ülkemizde bu konuda ciddi bir açık olduğunu ifade etmekle beraber lisans düzeyinde de adli bilişim mühendisliği vb. bölümlerin açılması gerektiğini belirtmişlerdir. Katılımcılardan K5 adli bilişim uzmanı ile siber güvenlik uzmanı arasındaki farklılığa değinmiş ve adli bilişim uzmanının en önemli fonksiyonunun vaka sonrası ilk durum olduğunu dile getirmiştir. Katılımcılardan bazılarının bu konudaki görüşleri şu şekildedir:

K6: "*Kamu ve özel sektörde karşılaşılan ve karşılaşılacak olan siber terör vakalarını teorik, uygulamalı ve hukuki açıdan değerlendirebilecek lisansüstü seviyede eğitim alarak donanımlı hale gelmiş adli bilişim uzmanlarının, kamu kurumlarında öncelikli olarak istihdam edilmesi büyük önem taşımaktadır. Adli bilişim uzmanlığını çok yönlü olarak düşünmek gerekir. Bu uzmanlık deneyimiyle beraber hem bilişim suçlarına karşı alınabilecek önlemler hem de güvenlik politikaları, kurumlarda daha*

*güvenli hale gelebilecektir. Bununla birlikte, adli makamlarca da ortak çalışmalar yürütülerek bilişim suçlarına yönelik bilimsel metotlarında içerisinde yer aldığı bir yol haritası ortaya çıkacaktır".*

K4: "*Siber terörizm ile mücadelede alanında iyi eğitim almış, nitelikli, insan kaynağının önemi çok büyüktür. Personelin siber terör ve saldırı faaliyetlerine karşı eğitilmesi, bu saldırılara karşı uygulanabilecek stratejiler hakkında fikir yürütebilmesi, bilgisayar donanım ve yazılım kaynaklarının gizliliği ve dolayısıyla bu yolla ulaşılabilecek evrakların gizliliği seviyesinde uygun ortamlarda tutulması terör saldırılarının önlenmesi açısından önemli birer adımdır. Bu adım, siber terör saldırılarının önlenmesi, takibi ve aynı zamanda sorumluların tespiti hususunda büyük önem taşımaktadır. Adli bilişim uzmanlarının istihdamı saldırıların önüne geçebilmek için önemli bir adım olacaktır."*

K2: "*Sistemi yöneten kişi ile siber güvenliğini koruyan kişinin aynı kişi olmaması gerekir. Denetim mekanizması açısından bir siber güvenlik uzmanının veya adli bilişim uzmanının istihdam edilmesi siber saldırılar karşısında daha güçlü hale gelmemizi sağlayacaktır.*"

***On ikinci Araştırma Sorusu: Yetenekleri arttırılmış ve insan vücuduna yerleştirilebilen kablosuz internet bağlantısı yeteneğine sahip cihazların (insülin pompası, akıllı saat, kalp pili, işitme cihazı vb.) siber terör hedefi haline gelmemesi için ne gibi önlemler alınmalı?*** Katılımcılar bu cihazların hayati önem taşıdığına ve bu cihazların güvenliğine çok dikkat edilmesi gerektiğine vurgu yapmışlardır. Katılımcıların bu konuda yapılmasını öngördüğü durumları şu şekilde özetleyebiliriz:

- •Bu cihazların güvenliğini sağlayabilecek yazılımlar sürekli denetlenmeli.
- Herhangi bir açığının olup olmadığına dair sertifika istenmesi.
- Hasta doktor ilişkisi gizliliği sağlanmalı.
- Sadece yetkili doktor tarafından erişim sağlanmalı.
- Hasta ve doktor arasındaki veri akışına saldırı olmaması için kriptolama uygulaması, şifreleme teknikleri geliştirilmeli.
- Kullanıcıların bilinçlendirilmesi.
- Antivirüs yazılımları ve kapalı sistemler kullanılmalı.
- Güvenirliliği ve sertifikaları test edilmeden hayati risk taşıyan cihazlar kullanılmamalı.
- Donanımlar dışardan saldırılara kapatılmalı.

- Gömülü sistem programlama, kablolu ve kablosuz iletişim teknolojileri ve özellikle kablosuz ağ bağlantı konusunda gelişmiş güvenlik duvarları tasarlayabilecek ve güvenilir yazılım geliştirebilecek eğitmenlere ihtiyaç olduğu.
- Milli kaynaklarla geliştirilebilecek biyomedikal projelerde yazılım ve donanım test süreçlerinde alfa ve beta testlerinin çok dikkatli yapılması.

Katılımcılar sadece bu cihazların değil, nesnelerin interneti teknolojisinde yaşanan gelişmelerden dolayı internete bağlanabilen bütün sistemleri, internet bağlantılı giyilebilir cihazları (saat, gözlük, vb.) da ele almak gerektiği üzerinde durmuşlardır. Katılımcıların bazılarının bu konudaki görüşleri şu şekildedir:

K6: "*Bunların yanı sıra 2017 yılında satılan 310 milyon internet bağlantılı giyilebilir cihazların (saat, gözlük, vb.) sayısının 2021 yılında yarım milyara ulaşması beklenmektedir. Matematik, fizik, bilgisayar bilimi ile uğraşan araştırmacılarla toplum bilimciler tarafından birlikte hareket edilerek ortaya çıkan ve çıkabilecek sorunların çözümü ve olası siber terör eylemlerinin önlenmesi için çalışmalar yapılmalıdır*."

K3: "*Bu konuyu daha geniş bir perspektiften düşünmek gerekir tüm bilişim alt yapılarıyla yönetilen bütün sistemleri ele almak yani internete bağlanabilen hemen hemen bütün sistemlerden bahsetmek daha gerçekçi olacaktır. Örnek olarak sağlık sistemini ele alalım. Hastanelerde yoğun bakım, hastalara verilecek ilaçlar, tedavi yöntemleri, tahlil sonuçlarını vb. gibi tüm süreçlerin bilgisayar ortamında gerçekleştiği bilinmektedir. Birilerinin bu sistemleri ele geçiriyor olması hem teşhisi hem tedaviyi hem de bütün sağlık uygulamalarında çok ciddi hayati olumsuz sonuçlar doğurabilir. Sağlıkta, enerjide, ulaşımda, suda, elektrikte, doğalgazda bütün kritik alt yapı uygulamalarında da durum farklı değildir. Hemen hemen her alanda bilişim teknolojileriyle yönetilen bütün alt yapılarda bu tehdit ve tehlike vardır. Burada siber güvenliğe yönelik önleyici tedbirlerin alınması son derece önemlidir. 27001 bilgi güvenliği yönetim sistemi başta olmak üzere bilişim sistemleri güvenlik alt yapıları oluşturulması gerekir. Bunlarla ilgili yazılım, donanım, güvenlik çözümleri alt yapıları oluşturulmalıdır. Sadece bunlar yeterli olmamakla birlikte aynı zamanda kullanıcıların ve uygulayıcıların bu konudaki gerekli yasal ve hukuki düzenlemeleri, teknik ve idari süreçleri siber güvenlik alt yapılarıyla uygun hale getirmeleri gerekmektedir. Siber güvenlik, topyekûn mücadeleyi gerektirir. Teknik anlamda çözüm geliştirme, yazılım ve donanım ihtiyaçlarını giderme ve insanla bu işin üstesinden gelmek mümkün*

*değildir. Bu mücadele de, bahsedilen tüm bileşenlerin bir araya getirilerek uçtan uca bir güvenlik çözümü oluşturulması gerekir. Ancak bu şekilde önlem alınabilir*".

***On üçüncü Araştırma Sorusu: ABD'de 2010 yılının ocak ayında siber atakları analiz edip hangi saldırgan tarafından saldırı gerçekleştirildiği ve saldırılara göre savunma ve karşı atak stratejileri geliştirmek için siber genom projesi başlatılmıştır. Türkiye'de buna benzer bir proje çalışması var mıdır? Sizin düşünceleriniz nelerdir?*** Katılımcılar ilk önce siber genom projesini açıklamış Amerika ve daha başka ülkelerde bu tarz birçok projenin olduğunu ifade etmişlerdir.

Katılımcıların verdikleri cevaplara göre siber genom projesi ABD'nin en ileri araştırmalarını yapan ileri araştırmalar birimi olan Savunma Bakanlığına bağlı DARPHA tarafından geliştirilen bir projedir. Projenin amacı, öncelikle saldırganların geçmişteki dijital izlerine ya da dokümanlarına bakarak yapılan saldırı ile bu dijital izler arasında bir ilişki olup olmadığını belirlemektir. Daha sonra, eğer ilişki tespit edilirse kişiye özel bir yapı oluşturup, kişilerin geçmiş kodlardaki verilerini analiz ederek tekrar kullanıldığında saldırganı tespit etmeye yöneliktir.

Katılımcıların Türkiye'de buna benzer çalışmaların olup olmadığı konusunda farklı görüşleri vardır. Bazı katılımcılar Türkiye'de böyle bir çalışma olmadığını ifade etmişlerdir. Bu katılımcılar Türkiye'nin bu çalışmalardan önce kendi siber güvenlik çözümlerimizi kendi yerli kritik alt yapılarımızda kullanabilecek yazılım çözümlerimizi geliştirmemiz gerektiğini, kendi siber güvenlik ve strateji eylem planını hayata geçirmemiz gerektiğini ifade etmişlerdir. Aynı zamanda bu projeleri yönlendirebilecek ve yönetebilecek bir üst kuruluşun olması gerektiğini de vurgulamışlardır. Bazı katılımcılar ise Türkiye'nin bu şekilde çalışmaları olduğunu belirtmişlerdir. Katılımcıların bu konuda verdikleri örnekler aşağıda belirtilmiştir.

K4: "*ASTARUS programı; derinlemesine veri analizi yaparak gizli bağlantıları ortaya çıkarır, tehdit unsurlarının önceden tespitini sağlar. Adli davalar için deliller toplanması ve çözümlenmesi yasa dışı kişi ve örgütlerin tespit ve takibi, sahtecilik tespiti, akıllı şehir uygulamaları, lojistik destek ve kestirimci bakım, acil durum yönetimi bazı kullanım alanlarıdır.*"

K5: "*Türkiye'nin böyle bir çalışması var. Uzun süredir üzerinde çalıştıkları hatta Türkiye ye karşı yapılan saldırıların profillerini çıkarttılar.*"

K6: *"Bizim de BAYRAKTAR, HAVELSAN, ASELSAN, TUBİTAK gibi yerli ve milli üretimler üzerine çalışmalar yapan firmalarımız mevcut olarak çalışmalar yapıp yerli ve milli ürün üretimi yapmaktadır."*

**Tartışma ve Sonuç**

Siber terör ya da siber terörizm tüm dünya ülkeleri için büyük bir tehdit haline gelmiştir. Son yıllarda tüm devletler güçleri ölçüsünde bu tehditlerle mücadeleye yönelik çok önemli tedbirleri uygulamaya koymaya başlamışlardır. Ülkemizde 2015 yılında ".tr" alan adlarından IP adreslerine ulaşılmasını engellemek üzere gerçekleştirilen siber terör saldırısı Türkiye'nin bu tür saldırılara yönelik önemli adımlar atması gerekliliğini ortaya koymuştur. 2020 yılında Emniyet Genel Müdürlüğü bünyesinde siber operasyon merkezinin açılması bu adımların uygulamaya konulmaya başladığını göstermektedir. Ancak ülkemizin henüz yeterli seviyede olmadığını da söylemek gerekir. Nitekim, araştırma bulguları da çalışmanın varsayımıyla paralellik göstermiştir. Bu çalışmada, yedi alan uzmanı ile (ağırlıklı akademik personel) yapılan mülakatlar aracılığıyla, uzmanların Türkiye'de siber terörizme karşı bilişim teknolojilerinin kullanımı ile ilgili görüşleri alınmıştır. Görüşleri alınan uzman katılımcıların bilgileri, nitel araştırma yöntemlerinde kullanılabilen NVivo 12 paket programı ile analiz edilmiş ve bulgular aktarılmıştır. Araştırmada yapılan görüşmelerden elde edilen verilerin ön incelemesinde, araştırma sorularıyla paralel olacak biçimde on üç temel tema oluşturulmuştur. Elde edilen bulgulara göre; bilimsel çalışmalar ve eğitim, farkındalık oluşturma, önleme, adli ve hukuki yapılacaklar, uluslararası ortaklık, eğitim, bilimsel çalışmalar, sivil toplum ve medya, veri analizi ve teknoloji takibi, saldırganların kullandığı yöntemler, siber suç ve siber terör arasındaki fark, kurumsal anlamda yapılması gerekenler, milli ve yerli üretim konusunda alınabilecek tedbirler ile ilgili konuların ön plana çıktığı tespit edilmiştir. Bulgulardan elde edilen bir başka sonuca göre, siber terörizme karşı koymada bilişim teknolojilerinin etkin kullanımı için vurgulanan en önemli konunun bu alana yönelik farkındalığın oluşturulması olduğu tespit edilmiştir. Bu farkındalığın oluşturulmasında ise, eğitim, bilimsel çalışmalar, sivil toplum kuruluşları ve medyanın önemi üzerinde durulmuştur. Elde edilen bu veriler neticesinde araştırmaya ilişkin bazı öneriler aşağıda sunulduğu gibidir:

- Bilişim teknolojilerini konu alan kurum ve kuruluşlarda çalışan uzman kişilerle temas kurulup beklentilerini belirleyerek, devlet ile özel sektör arasındaki uyumun sağlanabilmesi için bir çalışma yapılabilir.
- Türkiyenin farklı devlet kurum ve kuruluşlarında çalışan uzmanlarla yapılan bu çalışma genişletilerek özel kurum ve kuruluşlardaki uzmanlarla da yapılabilir.
- Siber terörizm alanında araştırma yapacak olan araştırmacıların, buna benzer çalışmalarda ülke dinamikleri açısından yerli ve milli konulara ağırlık vermesi gerektiği söylenebilir.
- Bu araştırma, Türkiye'de görev yapan uzmanlarla gerçekleştirildiğinden ulusal düzeyde kalmıştır. Bundan sonraki çalışmalar uluslararası uzmanlarında dahil edilmesi ile genişletilebilir.
- Araştırmada adli bilişim uzmanlığının önemi üzerinde durulmuştur. Bu kapsamda adli bilişim programlarının ön lisans, lisans ve lisansüstü düzeyde hızla artırılması ve bu yolla alan uzmanlarının yetiştirilmesi önerilmektedir. Bu konunun, ülkenin geleceği açısından hayati derecede bir öneme sahip olduğu düşünülmektedir.
- Siber saldırı faaliyetlerinin ve çeşitlerinin gün geçtikçe arttığı görülmektedir. Bu artış hızına paralelel olarak saldırılara karşı koyabilmek için, gelişen teknolojinin hızının değil ivmesinin nasıl yakalanabileceği konusunda çalışmalar yapılması önerilmektedir.
- Araştırmaya katılan uzmanlar, sivil toplum ve medyanın daha aktif bir şekilde bu konulara dikkat çekmesi gerektiği görüşünü belirtmişlerdir. Bu iki önemli ve itici gücün bu alana yönelik çalışmalarda gözardi edilmemesi önerilmektedir.

Sonuç olarak araştırma bulgularına göre, siber terörizme karşı koymada bilişim teknolojilerinin etkin kullanımı için vurgulanan en önemli konunun bu alana yönelik farkındalığın oluşturulması olduğu tespit edilmiştir. Bu farkındalığın oluşturulmasında ise, eğitim, bilimsel çalışmalar, sivil toplum kuruluşları ve medyanın önemi üzerinde durulmuştur. Son olarak, ülkemizde siber güvenlik alanı ile ilgili çalışmaların yeterli düzeyde olmadığı ve bu alana yönelik çalışmalara ağırlık verilmesi gerektiği sonucu elde edilmiştir. Bu açıdan çalışmanın alana ilgi duyan araştırmacılara katkı sağlayabileceği düşünülmektedir.

**EXTENDED ABSTRACT**

# Cyber Terrorism against the Use of Information Technology in Turkey

*

Ahmet Doğan– Furkan Abacı
*Osmaniye Korkut Ata University*

Cyberterrorism has become a major threat to all countries of the world. In recent years, all states have begun to implement crucial measures to combat these threats to the extent of their power. When we look at cyber terrorism from another angle, it is seen that cyber terrorism is also used as a tool for the fulfillment of political goals in the international political arena today. In order to combat cyber terrorism, states and international actors need to take serious initiatives. Otherwise, it is possible to say that the acts of cyberterrorism will continue with much greater social harm all over the world. Regarding the extremely important and popular subject, in the article, in order to determine the effective use of information technologies against cyberterrorism in Turkey and to reveal what improvements should be made in this field, first of all, in order to understand the theoretical part of the subject and to create an infrastructure for practice, conceptual subjects such as terrorism, the historical development of terrorism, cyber terrorism, etc. were included. Then, the application part was started and for this purpose, data were collected by semi-structured interview using phenomenology design, one of the qualitative research methods based on interview data. The data were obtained through interviews with field experts (mainly academicians), by taking the opinions of field experts on the use of information technologies against cyber terrorism in Turkey. The research questions directed to the field experts in the article are as follows:

- What kind of work should be done for the effective use of information technologies in countering cyberterrorism?
- How would you describe cyberterrorism, which is one of the most dangerous terrorist activities today? What types of attacks can be named a cyberterrorist attack?

- What kind of work should be done to increase the awareness of information technologies against cyberterrorism in our country?
- What should be done in order not to be exposed to cyberterrorist attacks?
- Does the use of information technologies become a necessity for institutions and individuals in many ways today, triggering cyber attacks?
- Do we have the information technologies and experience to withstand a serious cyberterrorist attack in our country?
- Do you think there is a method difference in cyberterrorist attacks in the world and in our country? If so, what are these?
- How can we create cyber security awareness against cyberterrorism? What are your views on the production and use of national and domestic products in information technologies?
- Is there a difference between the concepts of cybercrime and cyberterrorism? What methods do the attackers use in cyber terrorist attacks?
- In your opinion, how should society be made conscious and what kind of training should be given in order to increase the social resistance against cyberterrorist attacks in our country?
- Could the employment of forensic experts who have received postgraduate education in public institutions be an important step to prevent cyberterrorist attacks?
- What measures should be taken to prevent devices with enhanced capabilities and capable of wireless internet connection (insulin pump, pacemaker, hearing aid, etc.) that can be implanted in the human body from becoming a target of cyberterrorism?
- In January 2010, the cyber genome project was launched in the USA to analyze cyberattacks, determine which attacker carried out the attack, and develop defense and counter-attack strategies according to the attacks. Is there any similar project work in Turkey? What are your thoughts?

The data collected as a consequence of the answers given as a result of the interviews with the field experts were analyzed with the NVivo 12 package program, which can be used in qualitative research methods, and codes were created on these data by content analysis. The generated codes

were brought together according to their similar characteristics and grouped under categories. In the preliminary analysis of the data obtained, thirteen basic categories were created in parallel with the research questions. Categories are presented in relation to themes. In this context, the theme of information technologies consists of; scientific studies and education, awareness-raising, prevention, forensic and legal actions, international partnership categories; the theme of studies to raise awareness in our country consists of the categories of education, activities that can be done with non-governmental organizations and the media, scientific studies, and technology monitoring; the theme of the difference between the concepts of cybercrime and cyber terrorism and the methods used by attackers consists of; the categories of the methods used by the attackers and the difference between cybercrime and cyberterrorism; the theme of what should be done to avoid being attacked consist of the categories of what needs to be done in the institutional sense and awareness-raising; national and domestic production theme consists of awareness, domestic and national categories.

As a result, according to the research findings, it has been determined that the most important issue emphasized for the effective use of information technologies in countering cyber terrorism is raising awareness for this field. In raising this awareness, the importance of education, scientific studies, non-governmental organizations, and media were emphasized. In addition, it has been concluded that the studies on cyber security in our country are not sufficient and it is necessary to focus on studies in this field. As a result of these inferences, it is thought that the study can contribute to researchers who are interested in the field.

**Kaynakça / References**

Bodur, H. E. (2005). Dini motifli terör fenomeni ve İslam'ın siyasal istismarı. *KSÜ İlahiyat Fakültesi Dergisi, 5*, 65-88.

Bostan, A. ve Akman, İ. (2011). Bilişim güvenliği: Kullanıcı açısından bir durum tespiti. *IV. Ağ ve Bilgi Güvenliği Sempozyumu*, 51-56.

Chomsky, N. (2000). *Terörizm kültürü ABD terörü.* (Çev: Taha Cevdet). İstanbul: Pınar Yayınları.

Collin, B. C. (1997). The future of cyberterrorism: Where the physical and virtual worlds converge. Proceedings of the 11th Annual International Symposium on Criminal Justice Issues, 1 Nisan 2020 tarihinde *http://www.crime-research.org/library/Cyberter.htm* adresinden erişilmiştir.

Çalışır, G. (2015). Müşteri ilişkileri yönetiminin önemi ve etkisi üzerine bir çalışma: Eskişehir Sanayi Odası Atap A.Ş. örneği. *Gümüşhane Üniversitesi Sosyal Bilimler Elektronik Dergisi, 12*, 159-184.

Denning, D. E. (2003). *Information Technology and Security. To appear in Grave New World: Global Dangers in the 21st Century* (Michael Brown ed.). Washington, DC: Georgetown University Press, 1-23.

Ekiz, D. (2003). *Eğitimde Araştırma Yöntem ve Metotlarına giriş: Nitel, nicel ve eleştirel kuram metodolojileri*. Ankara: Anı Yayıncılık.

Ermiş, U. (2015). *Siber caydırıcılık kavramının nükleer caydırıcılık olgusu ile karşılaştırmalı analizi.* (Yayınlanmamış Yüksek Lisans Tezi). Uludağ Üniversitesi, Sosyal Bilimler Enstitüsü, Bursa.

Fearey, R. A. (1976). International terrorism. *Department of State Bulletin, 74*, 394-403.

Güzel, C. (2002). *Korkunun Korkusu: Terörizm, Silinen Yüzler Karşısında Terör.* Içinde, (der.) Cemal GÜZEL, Ankara: Ayraç Yayınevi.

T.C. Resmi Gazete, Yasama Bölümü, 1 Şubat 2020 tarihinde *https://www.resmigazete.gov.tr/arsiv/20843_1.pdf* adresinden erişildi.

Merriam, S. B. and Bierema, L. L. (2014). A*dult learning: Linking theory and practice*. San Francisco: CA: Jossey-Bass.

Nacar, F.B. (2010). *Avrupa Birliği ülkeleri ve Türkiye'de bilişim suçlarının ceza hukukundaki uygulamaları*. (Yayınlanmış Yüksek Lisans Tezi). Atılım Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Patton, W. and Mcmahon M. (2014). *Career development and systems theory: Connecting theory and practice.* Rotterdam: Sense Publishers, 1-463, 3. Basım.

Rapoport, D. C. (2004). The Four Waves of Modern Terrorism. Audrey Kurth Cronin and James M. Ludes (eds.), *Attacking Terrorism: Elements of a Grand Strategy*, Washington DC: Georgetown Uni. Press, 46-73.

Tasam. (2020). Siber terörizm raporu. 15 Mayıs 2020 tarihinde *https://tasam.org/Files/Icerik/File/siber_terorizm_raporu_84be5753-d219-418f-9a68-e6c719b645b1.pdf* adresinden erişildi.

Terzi, M. (2018). Bilgi ve iletişim teknolojilerine dayalı oluşumlar ile bu oluşumların uluslararası ilişkilere güvenlik bağlamındaki etkisi: Siber terörizm. *Kara Harp Okulu Bilim Dergisi, 28*(1), 73-108.

Ünver, M., Canbay, C. ve Mirzaoğlu, A. G. (2011a). Uluslararası kuruluşların siber güvenlin faaliyetleri. *Bilgi Teknolojileri ve İletişim Kurumu*, 1-28.

Ünver, M., Canbay, C. ve Mirzaoğlu, A. G. (2011b). Siber güvenliğin sağlanması: Türkiye'deki mevcut durum ve alınması gereken tedbirler. *Bilgi Teknolojileri ve İletişim Kurumu*, 1-68.

Yıldırım A. ve Şimşek H. (2008). *Sosyal bilimlerde nitel araştırma yöntemleri*. Ankara: Seçkin Yayınları.

**Kaynakça Bilgisi / Citation Information**

Doğan, A. ve Abacı, F. (2021). Türkiye'de siber terörizme karşı bilişim teknolojilerinin kullanımı. *OPUS–Uluslararası Toplum Araştırmaları Dergisi*, *18*(42), 5968-5998. DOI: 10.26466/opus.901520.