SİBER GÜVENLIK VE SAVUNMA: FARKINDALIK VE CAYDIRICILIK

Şeref Sağıroğlu ve Mustafa Alkan.(Ed.).(2018). Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık.Ankara: Grafiker Yayınları.pp.400. ISBN: 978-605-2233-22-1(paperback).

Doğan ARAR[13]

Yirminci yüzyılın ikinci yarısı itibâriyle bilgi ve iletişim teknolojilerinde (BİT) yaşanan gelişmeler, toplumsal ve bireysel kolaylıkların yanında çeşitli güvenlik problemlerini de beraberinde getirmiştir. Özellikle son yıllarda internet altyapısındaki tehditlerin artması, suçluların çoğalması ve terörizmin hız kazanması; bu alanda bireysel ya da kolektif kapsamlı bir mücadelenin yürütülmesi gerekliliğini ortaya çıkarmıştır. Başka bir deyişle, dijital ortamda elzem olan farkındalık ve caydırıcılığın sağlanması meselesi, siber güvenlik ve savunmanın çatısı altında toplanmıştır.

Dünyanın farklı coğrafyalarında farklı birimler tarafından ele alınan bu meseleye, ülkemizde hem teorik hem pratik bakımdan zengin katkılar sunan oluşumların başında, hiç şüphesiz Bilgi Güvenliği Derneği (BGD) bulunmaktadır. BGD siber güvenlik alanında düzenlediği ulusal ve uluslararası çapta etkinlikler, hazırladığı raporlar, eylem planları ve taslak strateji dokümanları vb. ile sorumluluk almaktadır. BGD'nin son yıllarda bu alana sunduğu önemli katkılardan biri de, ilki Aralık 2018'de yayımlanan "BGD Siber Güvenlik ve Savunma Kitap Serisi" olmuştur. Bahse konu seride siber güvenlik alanında uzman akademisyenler, kamu çalışanları ve üst düzey yetkililerin aynı amaç uğruna bir araya gelmesi de hayli merak uyandırmaktadır. Tüm bu noktalardan hareketle bu çalışmada, editörlüğünü Prof. Dr. Şeref Sağıroğlu ve Prof. Dr. Mustafa Alkan'ın üstlendiği, ayrıca serinin ilk kitabı olan "Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık" analize tâbi tutulmuştur.

Kitabın *Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler* başlıklı birinci bölümünde ilk olarak, siber dünyada kullanılan terimler ve kavramlara yer verilerek, bahse konu alana ilişkin terminolojik sınırlar çizilmiştir. Ek olarak bu bölümde siber alanda baş gösteren saldırılar ve türlerine dikkat çekilirken, aynı zamanda saldırılar karşısında alınabilecek önlemler maddeler hâlinde özetlenmiştir.

[13] Yüksek Lisans Öğrencisi, Selçuk Üniversitesi, Uluslararası İlişkiler Bölümü, doganarar1@gmail.com

Siber Güvenliğin Temelleri başlıklı ikinci bölümde, siber güvenlik ve savunma bilimi ya da bilgi güvenliği bilimi kapsamında değerlendirilebilecek şifre bilim (kriptoloji), stenografi, kuantum şifreleme yaklaşımları ile matematiksel fonksiyonlar, şifreleme ve şifre çözme algoritmaları, şifreleme tarihçesi/bilimi/önemi, kullanılan standartlar, özetleme algoritmaları ve elektronik imza gibi hususlar incelenmiştir (49). Kitabın temel inceleme konusunu oluşturan siber güvenlik ile uygulama ortamı olan siber uzay hakkında bilgilerin verildiği üçüncü bölümde (*Siber Güvenlik*); siber savaşlar, tehditler ve dolayısıyla bu alanda güvenliğe duyulan ihtiyaç irdelenmiştir. Ayrıca, siber güvenliğin önemi birtakım istatistiki veriler aracılığıyla da desteklenmiştir.

Siber güvenlik farkındalığı ile buradan hareketle farkındalık ölçüm yöntem ve modellerinin incelendiği dördüncü bölümde, bilgisayar ve internet kullanıcı sayısındaki artış neticesinde saldırganların hedeflerindeki değişimlere/sistematik yaklaşımlara değinilmiştir. Bununla birlikte farkındalık perspektifiyle "siber saldırı yaşam döngüsü", örnek bir olay ile desteklenerek açıklanmıştır (114).

Son olarak siber farkındalığın; bilgi güvenliğinin sağlanmasında etkin bir unsur olduğu gerçeğinden yola çıkarak kavramsal değerlendirilmesi, bileşenlerinin açıklanması ve seviyesinin belirlenmesi/artırılması gibi hususlara yer verilmiştir. Bir önceki bölümle ilintili olarak, siber uzayda makul güvenlik seviyesine erişilmesi ve devamlılığının sağlanması için gerekli olan güvenlik farkındalığı beşinci bölümde de yinelenmiştir. Bu bölümde insan temelli güvenlik farkındalığının yaratılmasında rol oynayan uygulamalar, davranış kalıpları ve yol gösterici prensipler belirtilmiştir.

Kitabın *Siber Güvenlikte Büyük Veri ve Açık Veri Kullanımı* başlıklı altıncı bölümde ise, siber ortamın en önemli bileşenlerinden biri olan "veri" olgusuna temas edilmiştir. Veriye sahip olanlar ve bunları analiz edenlerin, siber alanda karşılaşılabilecek olası tehditlerden daha az etkileneceğine ya da konuyla ilgili üstün muhakeme yetenekleri sayesinde yeni teknolojiler geliştirerek bir anlamda "krizi fırsata çevirebileceklerine" dikkat çekilmiştir. Bölüm, ülkemiz için açık ve büyük veri konusunda yapılabilecekleri, elde edilebilecek kazanımları ve alınması gereken önlemleri içeren tavsiyelerle bitirilmiştir.

Hibrit (karma) savaş kapsamında siber savaş ve siber caydırıcılıktan bahsedilen yedinci bölümde kısaca savaş olgusunun tanımına, çeşitleri ve evrimine değinildikten sonra; hibrit

savaşın tanımı, süreç ve uygulamaları üzerinde durulmuştur. Bunun yanında hibrit savaşın uygulama yöntemlerinden biri olan siber savaş ile taraflarının talep ve amaçlarından vazgeçmesine yönelik siber caydırıcılığın önemi ve uygulamaları vurgulanmıştır. Bölüm sonunda günümüzün savaşları olarak nitelendirilebilecek hibrit savaşlar ile yine bu kapsamda siber savaş ve siber caydırıcılık konularında ülkemiz için yapılabilecekler tartışılmıştır.

Sekizinci bölümde siber güvenliğin tesis edilmesinin önündeki bir başka engel olan kötü amaçlı yazılımlar (truva atları, virüsler, solucanlar, casus yazılımlar vb.) ele alınmıştır. Siber uzayda dinamiklik ve biçimi/hedefleri bakımından zaman zaman değişkenlik arz eden kötü amaçlı yazılımlar, konuyla ilgili analizi de kaçınılmaz kılmıştır. Dolayısıyla bu bölümde bahse konu yazılımların tespit edilmesi, nasıl çalıştığının anlaşılması ve yayılmasını engellemek amacıyla bir analiz yapılmıştır. *Siber Terör, Terörizm ve Mücadele* başlıklı dokuzuncu bölümde ise, son yıllarda günlük hayatın bir parçası hâline gelen ve insanlara kolaylıklar sunan internetin fırsatlarını kötüye kullanmak isteyen saldırganların eylemleri üzerinde durulmuştur. Siber terörizm adı verilen bu eylemler bütününe ait temel kavramlar, yöntemler ve mücadele teknikleri çeşitli örneklere de başvurularak açıklanmıştır.

Genel olarak Dünyada, özel olarak Türkiye'de kişisel verilerin korunmasına (KVK) değinilen onuncu bölümde; bu kapsamda yürütülen çalışmalar, temel düzenlemeler, veri koruma modelleri anlatılmıştır. İlâveten ülkemizde 2016'dan beri yürürlükte olan Kişisel Verilerin Korunması Kanunu ile Kişisel Verileri Koruma Kurulu'nun çalışmalarına da yer verilmiştir. Avrupa ile ülkemizde yürürlükte olan kişisel verileri koruma düzenlemeleri tartışılarak bölüm sonlandırılmıştır. On birinci bölümde, günümüzde iletişimden bankacılığa, alışverişten e-ticarete pek çok işlemin gerçekleştirilebildiği mobil cihazlardaki siber güvenlik konusu ele alınmıştır. Bu bağlamda mobil cihazlara yönelik siber saldırılara ve saldırılar karşısında kullanıcıların alması gereken önlemlere atıfta bulunulmuştur.

Siber Güvenlik Denetimi başlığını taşıyan on ikinci bölümde, bilgi teknolojileri (BT) kontrolleri üzerindeki denetime olan ihtiyaca vurgu yapılmıştır. Bunun yanında siber güvenlik kontrollerinin, BT denetimlerinde ihtiyaç duyulan güvence ve danışmanlık faaliyetleri üzerinde de durulmuştur. Siber alanda güvenlikle ilişkili olan riskler, zafiyetler ve tehditlerin denetimlerde dikkate alınabilmesi adına gerekli olan yaklaşım biçimi ve teknikler sağlanmıştır. Son olarak *COBIT-5* çerçevesinde siber güvenlik denetimlerinin nasıl yapılması gerektiğine dair bilgiler aktarılmıştır. Kitap, *Siber Güvenlik İçin Büyük Veri Yaklaşımları*

başlığını taşıyan on üçüncü bölüm ile noktalanmıştır. Bu bölümde siber alanda yaşanan genişleme sonucunda perçinleşen büyük veri ile siber güvenlik arasındaki ilişki anlatılmıştır. Bu ilişki; siber güvenlik için büyük veri, siber tehdit olarak büyük veri, büyük verinin güvenliği alt başlıklarında detaylı bir şekilde yorumlanmıştır.

Kitap, siber güvenliğin ağırlığını günden güne hissettirdiği ve sıkça tartışıldığı bu dönemde, meselenin kavranması ve geleceğe yönelik düzenlemeler yapılması noktasında zengin bir bakış açısı sunmaktadır. Diğer taraftan hemen hemen her bölümde kullanılan nicel birtakım veriler, yazarların öne sürdükleri görüşleri sağlamlaştırmaktadır. Buna ek olarak, daha önce belirtildiği üzere, bu alanda yetkin çok sayıda ismi bir araya getirerek kitabın ortaya çıkarılmasında emeği olan editörler Sağıroğlu ve Alkan için de ayrı bir parantez açılmalıdır. Tüm bunlar alt alta toplandığında kitabı, siber güvenlik ve savunma alanında "referans kitap" olarak betimlemede hiçbir beis bulunmamaktadır. Siber güvenlik ve savunma alanında Türkçe literatürdeki boşluğu dolduran kitabın, gelecekte yapılacak yeni çalışmaları teşvik etmesi temennisiyle…