Siber Güvenlik ve Savunma: Problemler ve Çözümler

Editörler
Prof. Dr. Şeref SAĞIROĞLU
Mustafa ŞENOL

Yazarlar
Prof. Dr. Şeref SAĞIROĞLU
Prof. Dr. Ramazan BAYINDIR
Prof. Dr. Yaşar BİLGE
Prof. Dr. Türksel KAYA BENSGHIR
Doç. Dr. Sedat AKLEYLEK
Doç. Dr. Muharrem Tolga SAKALLI
Doç. Dr. Murat CENK
Dr. Öğr. Üyesi İbrahim Alper DOĞRU
Dr. Murat DÖRTERLER
Dr. Ahmet EFE
Dr. Yılmaz VURAL
Dr. Mehmet Rıda TÜR
Dr. Mehmet Bedii KAYA
Dr. Adem TEKEREK
Öğr. Gör. Seyfettin VADİ
Öğr. Gör. Murat AKIN
Arş. Gör. Kübra SEYHAN
Arş. Gör. Meryem SOYSALDI
Gürol CANBEK
Hatice TOMBUL
Mehmet TUNÇKANAT

ISBN: 978-605-2233-50-4

1. Baskı
Mayıs, 2019 / Ankara
1500 Adet

Grafiker Yayınları
Yayın No: 315
Web: grafikeryayin.com

Kapak, Sayfa Tasarımı, Baskı ve Cilt
Grafiker
Grafik-Ofset Matbaacılık Reklamcılık San. ve Tic. Ltd. Şti.
1. Cadde 1396. Sokak No: 6
06520 (Oğuzlar Mahallesi) Balgat-ANKARA
Tel : 0 312. 284 16 39 Pbx - Faks : 0 312. 284 37 27
E-posta : grafiker@grafiker.com.tr
Web : grafiker.com.tr

HAVELSAN Bu kitap HAVELSAN'ın katkılarıyla basılmıştır.

İÇİNDEKİLER

EDİTÖRLERDEN **13**
BİLGİ GÜVENLİĞİ DERNEĞİ'NDEN **17**
ÖN SÖZ **21**

1. BÖLÜM
SİBER GÜVENLİK VE ÖTESİ

1.1. Giriş 25
1.2. Farkındalığı Arttırma 32
1.3. Ekosistem Oluşturma 34
1.4. Veri Koruma ve Mahremiyet 35
1.5. Tatbikatlar 37
1.6. Açık ve Büyük Veri Yaklaşımları 39
1.7. Geleceği Etkileyen Teknolojiler 43
1.7.1. Yapay Zekâ ve Derin Öğrenme 43
1.7.2. Nesnelerin İnterneti (Endüstri 4.0) 47
1.7.3. Sanal Para ve Blok Zinciri 47
1.7.4. Sosyal Medya 49
1.7.5. Bulut Ortamlar 51
1.7.6. Dijital İkiz (Digital Twin) 53
1.7.7. Kuantum Çözümler 55
1.7.8. Beyin Korsanlığı 56
1.8. Değerlendirmeler 58

2. BÖLÜM
SİBER GÜVENLİKTE KRİPTOGRAFİ

2.1. Giriş 63
2.2. Saldırı Örnekleri ve Güvenlik Kavramları 64
2.3. Kriptoloji Bilimi 64
2.3.1. Kriptografi 65

2.3.1.1. Simetrik Kriptografi 66
2.3.1.2. Asimetrik Kriptografi 66
2.3.1.3. Kriptografik Protokoller 67
2.3.2. Kriptoanaliz 67
2.3.2.1. Matematiksel Kriptoanaliz 68
2.3.2.2. Yan Kanal Atakları 68
2.3.2.3. Protokol Atakları 69
2.3.3. Özetleme Fonksiyonları 70
2.4. Kriptografi Temelli Siber Güvenlik 71
2.4.1. İnternet Güvenliği 71
2.4.2. Kablosuz Ağ Güvenliği 73
2.4.3. Bulut Güvenliği 73
2.4.4. Nesnelerin İnterneti Güvenliği 74
2.4.5. Parola Güvenliği 74
2.5. Kuantum Kriptografi 76
2.5.1. Teorisi 76
2.5.2. Uygulamalar 77
2.5.3. Kuantum Bilgisayarlar 78
2.5.4. Kriptografiye Etkisi ve Kuantum Sonrası Kriptografi 80
2.6. Değerlendirmeler 82

3. BÖLÜM
KRİPTOGRAFİK TEST YÖNTEMLERİ VE KRİPTOANALİZ

3.1. Giriş 87
3.2. Boole Fonksiyonları İçin Kriptografik Test Yöntemleri 90
3.3. Blok Şifrelerde Kullanılan Kriptografik Bileşenler 98
3.3.1. Yer Değiştirme Kutuları (S-Kutuları) İçin KriptografikTest Yöntemleri 100
3.3.2. Doğrusal Dönüşümler için Kriptografik Test Yöntemleri 115
3.3.3. Anahtar Planlama Algoritmaları İçin Kriptografik Test Yöntemleri 120
3.4. Kriptoanaliz 121
3.4.1. Doğrusal Kriptoanaliz 124
3.4.2. Diferansiyel Kriptoanaliz 127
3.5. Değerlendirmeler 129

4. BÖLÜM
KUANTUM BİLGİSAYARLAR İLE KRİPTOANALİZ VE KUANTUM SONRASI GÜVENİLİR KRİPTO SİSTEMLERİ

4.1. Giriş 138
4.1.1. Motivasyon 142
4.1.2. Organizasyon 142
4.2. Kuantum Bilgisayarlar ile Kriptoanaliz Algoritmaları 143
4.2.1. Shor Algoritması 143
4.2.2. Grover Algoritması 149
4.3. Matematiksel Altyapı 151
4.4. Kuantum Sonrası Kriptosistem Sınıfları 154
4.4.1. Kafes Tabanlı Kriptografi (Lattice-Based Cryptography) 156
4.4.2. Kod Tabanlı Kriptografi (Code-Based Cryptography) 158
4.4.3. Özet Tabanlı Kriptografi (Hash-Based Cryptography) 159
4.4.4. İzojeni Tabanlı Kriptografi (Isogeny-Based Cryptography) 160
4.4.5. Çok Değişkenli Polinomlar Tabanlı Kriptografi (Multivariate-Based Cryptography) 160
4.5. Değerlendirmeler 164

5. BÖLÜM
KUANTUM BİLGİSAYARLAR SONRASI GÜVENİLİR KAFES TABANLI KRİPTOSİSTEM TEMELLERİ

5.1. Giriş 171
5.1.1. Motivasyon 174
5.1.2. Organizasyon 175
5.2. Matematiksel Altyapı 175
5.2.1. Kafes Tabanlı Kriptografide Temel Tanımlar 177
5.2.2. Kafeslerde Zor Problemler 184
5.2.3. Kafes Tabanlı Kriptosistemlerde Kullanılan Temel Zor Problemler Arası İlişkiler 200
5.3. Kuantum Sonrası Kriptografi İçin Standartlaşma Projesi 202
5.4. Değerlendirmeler 206

6. BÖLÜM
HUKUKİ AÇIDAN BİLİŞİM SUÇLARI, SİBER GÜVENLİK, ADLİ BİLİŞİM VE GÜNCEL TEKNOLOJİLER

6.1. Giriş 213
6.2. Bilişim Suçları 214
6.2.1. Avrupa Konseyi Siber Suç Sözleşmesi 215
6.2.2. Bilişim Sistemine Girme veya Sistemde Kalma Suçu 217
6.2.2.1. Korunan Hukuki Değer 218
6.2.2.2. Tipikliğin Maddi Unsurları 220
6.2.2.3. Tipikliğin Manevi Unsuru 229
6.2.2.4. Hukuka Aykırılık Unsuru 230
6.2.2.5. Suçun Özel Görünüş Halleri 237
6.2.2.6. Yaptırım, Soruşturma ve Kovuşturma Usulü 241
6.2.3. Veri Nakillerini Sisteme Girmeksizin Teknik Araçla İzleme Suçu 242
6.2.3.1. Korunan Hukuki Değer 242
6.2.3.2. Tipikliğin Maddi Unsurları 242
6.2.3.3. Tipikliğin Manevi Unsuru 243
6.2.3.4. Hukuka Aykırılık Unsuru 244
6.2.3.5. Suçun Özel Görünüş Halleri 244
6.2.4. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu 245
6.2.4.1. Korunan Hukuki Değer 246
6.2.4.2. Tipikliğin Maddi Unsurları 246
6.2.4.3. Tipikliğin Manevi Unsuru 248
6.2.4.4. Hukuka Aykırılık Unsuru 248
6.2.4.5. Suçun Özel Görünüş Halleri 248
6.2.5. Yasak Cihaz Veya Programlarla İlgili Suçlar 249
6.2.5.1. Korunan Hukuki Değer 250
6.2.5.2. Tipikliğin Maddi Unsurları 250
6.2.5.3. Tipikliğin Manevi Unsuru 251
6.2.5.4. Hukuka Aykırılık Unsuru 252
6.2.5.5. Suçun Özel Görünüş Halleri 253
6.2.6. Tüzel Kişiler Hakkında Güvenlik Tedbirleri 254

6.2.7. Terörle Mücadele Kanunu 254
6.3. Siber Güvenlik: Politika, Strateji ve Hukuk 255
6.4. Adli Bilişim 258
6.4.1. Adli Bilişimin Temel Safhaları 259
6.4.2. Adli Bilişim İncelemelerinde Güncel Sorunlar 261
6.4.3. Türk Hukukunda Adli Bilişim 264
6.4.3.1. Ceza Muhakemesi Kanununu 134. Maddesi 264
6.4.3.2. Adli Tıp Kurumu Adli Bilişim İhtisas Dairesi 265
6.4.4. Reform Önerileri 266
6.5. Değerlendirmeler 269

7. BÖLÜM
BİLİŞİM SUÇLARINDA ADLİ TIP BİLİRKİŞİLİĞİ

7.1. Giriş 283
7.2. Bilirkişilikte Hukuki Yön 284
7.2.1. Bilirkişi Görevleri 284
7.2.2. Kabul Edilebilirlik 285
7.2.3. Bilirkişi Raporuna Yapılan İtiraz Sebepleri 286
7.2.4. Bilirkişilikle İlgili Sorunların Çözümleri 286
7.2.4.1. Bilirkişiyi Sorumlu Kılma 286
7.2.4.2. Sorulan Soru 287
7.2.4.3. Dosya Düzenlemesi 287
7.2.4.4. Delil 287
7.3. Bilişim Suçlarında İnceleme Yöntemleri 288
7.4. Tarihçe 288
7.5. Veri Madenciliği 289
7.6. Sıklık ve Önem 290
7.7. Siber Suçlar 290
7.8. Ülkemizde İnternet Üzerinden En Çok İşlenen Suç Tipleri 292
7.9. Kişinin Bilişim Aracılığı İle Bağımlı Olduğu, Kumar Oynadığı, Nefret Suçu İşlediği, Saplantılı Durum Geliştirdiği Durumlar 294
7.10. Değerlendirmeler 297

8. BÖLÜM
SİBER GÜVENLİKTE SİGORTALAMA

8.1. Giriş 305
8.2. Öz (Siber) Savunma 306
8.3. Siber Sigortanın Ortaya Çıkışı: Öz Savunmada Mükemmel Siber Güvenlik Yanılgısı 306
8.4. Siber Sigorta Teminatları 308
8.4.1. Siber Sigortada Birinci Taraf Teminat, Yükümlülük Teminatı ve Diğer Kapsanan Konular 308
8.4.2. Birinci Taraf Teminat ve Maliyetleri 308
8.4.3. Siber Sigortanın Gerçekçi Faydaları 309
8.4.4. Temel Faydalar 310
8.4.5. Siber Risklerin Adil Dağılımı: Risk - Prim 311
8.5. Siber Sigorta Ne Değildir? 311
8.6. Dünyada Siber Sigorta Pazarının Gelişim Tarihçesi 312
8.7. Türkiye'de Siber Sigorta İçin Yasal Dayanaklar 314
8.8. Değerlendirmeler 322

9. BÖLÜM
SİBER GÜVENLİK İÇİN SİBER YÖNETİŞİM

9.1. Giriş 328
9.2. Siber Alanda "Yönetişim" Eksikliği 331
9.3. Küresel Siber Teröre Karşı "Siber Güvenlik Yönetişimi" 333
9.4. Siber Yönetişimde Devletin, Kurumların ve Kişilerin Sorumluluğu 336
9.5. Ulusal Siber Güvenlik Stratejisi ve Eylem Planında Yönetişim 341
9.5.1. Siber Güvenlik İlkeleri 342
9.5.2. Siber Güvenlik Riskleri 343
9.5.3. Stratejik Siber Güvenlik Amaçları ve Eylemleri 345
9.6. Ulusal Siber Güvenlik Stratejisi ve Eylem Planının BT Yönetişimi Değerlendirmesi 347
9.7. Yönetişim İle Yönetimin Ayrışması 356
9.8. Siber Yönetişimde Uygulanabilir Ölçeklendirme 360

9.9. Siber Güvenlik Yönetişimi Çerçevesine Olan İhtiyaç 366
9.9.1. Organizasyon Yapısı 367
9.9.2. İş Kültürü 367
9.9.3. Güvenlik Bilinci 368
9.9.4. Siber Güvenlik Yönetişimi 368
9.10. Yöneticilerin Dikkate Almaları Gereken Siber Yönetişim Temel Soruları 368
9.11. Değerlendirmeler 370
9.11.1. Siber Alanı Kimler Yönetmelidir? 372
9.11.2. Siber Alan Yasal (Formel) ve Yasadışı (İnformel) Alanda Nasıl Yönetilmelidir? 372

10. BÖLÜM
SİBER SAVAŞ VE SİBER SİLAHLAR

10.1. Giriş 381
10.2. Siber Güvenlik 382
10.3. Siber Tehdit Seviyeleri 383
10.4. Siber Savaş 385
10.5. Siber Silah 388
10.5.1. Siber Silahların Kavramsal Tasarım Modeli 391
10.5.1.1. Devlet Aktörleri 391
10.5.1.2. Devlet Dışı Aktörler 392
10.5.1.3. Karma Aktörler 392
10.5.2. Siber Silahların Yaşam Döngüsü 393
10.5.3. Yüksek Etkili Siber Silahlar 397
10.6. Siber Silah Pazarı 400
10.7. Siber Risklere Karşı Savunma 402
10.8. Siber Güvenlik Harcamaları 403
10.9. Değerlendirmeler 404

11. BÖLÜM
SİBER TEHDİTLERDE SON NOKTA:
İLERİ DÜZEY KALICI TEHDİTLER

11.1. Giriş 413
11.2. İleri Düzey Sürekli / Kalıcı Tehditler 415

11.3. Zafiyetlerin / Saldırıların / Açıklıkların Boyutunu Anlama 417
11.4. İleri Düzey Kalıcı / Sürekli Saldırı Anatomisi 419
11.4.1. Tanımlar ve APT Özellikleri 420
11.4.2. APT Genel Yapısı ve Aşamaları 421
11.4.3. Siber Saldırılarda APT Rolü 423
11.4.4. APT Saldırı Kronolojisi 423
11.5. APT'lere Karşı Savunma Yaklaşımları 428
11.5.1. Kullanıcıları Kontrol Etmek ve Farkındalığı Arttırmak 428
11.5.2. İsim Oylama Yöntemini Ağ Davranışlarında Yürütmek 429
11.5.3. Değişen Saldırıları Anlamak 429
11.5.4. Son Noktayı Yönetmek 430
11.5.5. Ağın Tüm Trafiğine Odaklanmak 430
11.6. Değerlendirmeler 431

12. BÖLÜM
SIZMA TESTLERİ

12.1. Giriş 439
12.2. Sızma Testi Türleri 442
12.2.1. Kara Kutu Sızma Testi 443
12.2.2. Beyaz Kutu Sızma Testi 443
12.2.3. Gri Kutu Sızma Testi 444
12.2.4. Sızma Testine Karar Verme 444
12.3. Sızma Testine Karşı Zafiyet Değerlendirmesi 445
12.4. Güvenlik Testi Metodolojileri 446
12.5. Sızma Testi Aşamaları 447
12.5.1. Hedefin Kapsamını Belirleme (Target Scoping) 448
12.5.2. Hedef Hakkında Bilgi Toplama (Information Gathering) 449
12.5.3. Hedefi Keşfetme (Target Discovery) 449
12.5.4. Hedefin Envanterini Belirme (Enumerating Target) 450
12.5.5. Güvenlik Açığı Eşlemesi (Vulnerability Mapping) 450
12.5.6. Sosyal Mühendislik (Social engineering) 450
12.5.7. Hedefi İstismar Etme (Target Exploitation) 451
12.5.8. Yetki Yükseltmek (Privilege Escalation) 451

12.5.9. Erişim Sağlamak (Maintaining Access) 452
12.5.10. Belgeleme ve Raporlama 452
12.6. Güvenlik Testi Etiği 452
12.7. Değerlendirmeler 453

13. BÖLÜM
ELEKTRİK ENERJİSİ SEKTÖRÜNDE
SİBER GÜVENLİK

13.1. Giriş 459
13.2. Gelişen Elektrik Şebekesinde Oluşan Tehditler 460
13.3. Güç Sistemlerinde Sürdürülebilir Enerji ve Arz Güvenirliği 463
13.4. Enerji Sektörü, Güç Sistemleri Bileşenleri ve Siber Güvenlik Riskleri 466
13.5. Güç Sistemlerinde Şebeke Bileşenleri ve Siber Saldırılar 468
13.5.1. Güç Sistemlerinde Üretim Bileşenine Yönelik Siber Saldırılar 472
13.5.2. Güç Sistemlerinde İletim Bileşenine Yönelik Siber Saldırılar 475
13.5.3. Güç Sistemlerinde Dağıtım Bileşenine Yönelik Siber Saldırılar 476
13.6. SCADA Kontrol Sistemlerine Yönelik Siber Saldırılar 477
13.7. Siber Saldırılar ve Alınması Gereken Önlemler 478

14. BÖLÜM
SİBER GÜVENLİK OPERASYON MERKEZİ

14.1. Giriş 491
14.2. Güvenlik Sorunları 492
14.3. Güvenlik Operasyon Merkezi 494
14.4. Mevcut Güvenlik Operasyonlarınızın Değerlendirilmesi 497
14.5. Kurumsal Bir Güvenlik Operasyon Merkezinin Beş Temel İşlevi 498
14.5.1. Birinci İşlev: Güvenlik Tehditlerinin İzlenmesi 499
14.5.1.1. Metodoloji 500

14.5.1.2. Kaynaklar 500
14.5.1.3. Ekip Katılımı 501
14.5.1.4. Takip 501
14.5.2. İkinci İşlev: Güvenlik Olayı Yönetimi 501
14.5.3. Üçüncü İşlev: Personelin İşe Alınması, Elde Tutulması ve Yönetilmesi 503
14.5.4. Dördüncü İşlev: Süreçlerin Geliştirilmesi, Yönetilmesi ve Optimizasyonu 504
14.5.5. Beşinci İşlev: Yükselen Tehdit Stratejisi 506
14.6. Kapasite Yönetimi 507
14.7. Değerlendirmeler 509

15. BÖLÜM
İNSANSIZ HAVA ARAÇLARI VE SİBER GÜVENLİK

15.1. Giriş 517
15.2. İnsansız Hava Araçları Sınıfları 518
15.3. İnsansız Hava Aracı Sistemleri 520
15.3.1. İnsansız Hava Aracı Bileşenleri 521
15.3.2. Yer Kontrol İstasyonu Bileşenleri 521
15.3.3. İHA Haberleşme Ağları 522
15.4. İnsansız Hava Araçları Haberleşme Yöntemleri 523
15.5. İnsansız Hava Araçlarına Yönelik Müdahale Yöntemleri 525
15.6. İnsansız Hava Araçlarında Siber Güvenlik 527
15.7. Değerlendirmeler 531

YAZARLARIN ÖZGEÇMİŞLERİ 537

EDİTÖRLERDEN

Bilgi Güvenliği Derneği (BGD), kuruluşundan bugüne kadar ülkemizin **bilgi ve siber güvenliği ile savunmasının** gelişimine katkı sağlamakta, birikimini çevreye aktarmakta, bilgi güvenliği alanında açık kaynak yaklaşımını benimseyen ve bu kapsamda içerik üretilmesine ve geliştirilmesine destek vermekte, bunları yaymakta, paylaşmakta ve kamuoyunun kullanımına sunmaktadır. Düzenlediği ulusal ve uluslararası etkinliklere ait bildiri kitapları serisi, hazırladığı raporlar, taslak strateji dokümanları, eylem planları vb. bunların başında gelmektedir. **Siber Güvenlik ve Savunma Kitapları Serisi** ise BGD'nin ülkemizin siber güvenliğine önemli bir katkısıdır.

Tehditlerin, saldırıların ve açıklıkların artması, boyut ve yön değiştirmesi, farklılaşması, siber tehdit ekosisteminin gittikçe güçlenmeye başlaması, kritik altyapıların hedef haline gelmesi, bilgi ve kaynak hırsızlıklarının çoğalması, yeraltı yapıların etkinleşmesi, siber saldırıların artık savaşa dönüşmesi, siber suç ve suçlularının çoğalması, siber terörün yaygınlaşması vb. olumsuzlukların hızla artması, yapılacak mücadele, alınacak önlem ve karşı koymak için yaklaşımlara duyulan ihtiyacı artırmıştır. Kapsamlı bir mücadele için; ulusal strateji ve eylem planlarına, araştırma merkezlerine, gelişmiş altyapı ve araçlara, lisans ve lisansüstü programlara, nitelikli insan kaynağına, yerli ve milli ürünlerin geliştirilmesine, siber güvenlik ve savunma ekosisteminin oluşturulmasına, ulusal siber olaylara müdahale ekiplerinin sayısının ve niteliğinin arttırılmasına, Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kapsamının büyütülmesine, Siber Güvenlik ve Savunma Kurumu (Ajansı) gibi yapıların kurulmasına ve siber güvenliğin ulusal güvenlikle bütünleşmesine ihtiyaç vardır. Duyulan bu ihtiyacı bir nebze de olsa karşılamak için bu kitap serisi hazırlanmıştır. Bu kitap serisinde, 100'e yakın konu başlığı irdelenmektedir. Her bölümde, farklı bir konu siber güven-

lik ve savunma kapsamında ele alınmakta, değerlendirilmekte ve alınması gereken önlemlere yer verilmektedir.

Bu kitap serisinde sunulan konu başlıkları, ülkemizde bu alanda çalışan akademisyenler, uzmanlar ve çalışanlar ile paylaşılmış ve bu kitap serisine katkı sağlamaları istenilmiştir. Zamanı uygun olan, katkı vermek isteyen uzman veya akademisyenler belirlenen bir konuda bölüm yazarı olmaları için davet edilmişlerdir. Belirlenen süre içerisinde bölümlerini tamamlayan yazarlarımızın eserleri ise uygun olan ciltlerde basılmaktadır. Bundan sonraki süreçte, belirlenen diğer konular belirli sürelerde tamamlanıp takip eden ciltlerde yayımlanacaktır. Siber güvenlik ve savunmaya çok kapsamlı bir bakış sunmayı amaçlayan ve farklı başlıkları bir araya getiren bu kapsamlı eserin, ülke siber güvenliğimiz ve savunmasına katkı sağlaması beklenmektedir.

Bu kitap serimizin ikinci cildinde, 15 farklı bölüm sunulmuştur. Siber güvenliğin farklı açılardan irdelendiği bu ciltte; siber güvenliğin kapsamı ve boyutu, yapılan saldırıların türleri, alınabilecek önlemler, karşılaşılan yeni riskler ve problemlere yer verilmiş, karşılaşılabilecek risklere dikkat çekilmiş ve sonuçta alınması gereken önlemler ve yapılması gerekenler özetlenmiştir. Her bir bölüm; ülkemizde bu alana katkı sağlayan, bu alanda eğitim almış, tez hazırlamış, çalışmalar yapmış değerli akademisyen, kamu çalışanı ve üst düzey yöneticiler tarafından hazırlanmıştır. Her bir bölüm, birbirinden bağımsız olarak hazırlansa da konu bütünlüğü ve devamlılığının sağlanmasına mümkün olduğunca dikkat edilmiştir. Her bölüm editörler olarak tarafımızdan değerlendirilmiş, yazarlara konu içeriği ve başlıklarla ilgili olarak önerilerde bulunulmuş, düzeltmeler yapılması istenilmiş ve sonuçta yapılan değişiklikler dikkate alınarak bu kitap hazırlanmıştır. Kitapta yazılan bölümler tekrar tekrar kontrol edilmiş, yapılan çalışmalar ise her bölümün sonunda bölüm yazarları tarafından değerlendirilmiştir.

Bu kitabın, siber güvenlik ve savunma konusunda yapılacak çalışmalara ışık tutması, yeni çalışmaların yapılmasına katkı sağlaması, bu konuda yapılacak olan işbirliklerini geliştirmesi, bu konunun boyutunun ve kapsamının daha iyi anlaşılmasına katkı sağlaması ve en önemlisi ise bilgi güvenliği ve siber güvenlik alanında duyulan ihtiyacı bir nebze de olsa karşılaması, açık kaynak olarak sunulması ile de kaynaklara erişimi kolaylaştırıcı **bir başvuru kitabı serisi** olması beklenmektedir**. Bu eser serisi açık kaynak olarak**,

Bilgi Güvenliği Derneği internet sayfasında (www.bilgiguvenligi.org.tr) yayımlanmaktadır.

Kitap bölüm yazarlarımız; alan uzmanlıklarına göre her bir bölümü hazırlamışlar, kişisel bilgi birikimlerini hazırladıkları bölümlerde sunmuşlar, eserlerinin açık kaynak olarak yayımlanmasını kabul etmişler ve bu kitabın basımı ve dağıtımı ile ilgili olarak herhangi bir telif hakkı talep etmemişlerdir. Yazarlarımıza, bu kitap serisinin editörleri olarak çok özel teşekkürlerimizi ve şükranlarımızı sunarız.

Kitabın titizlikle hazırlanmasında, kontrolünde ve basılmasında başta yazarlarımız olmak üzere emeği geçen tüm paydaşlarımıza, kitap serisi fikrimizi hayata geçiren Bilgi Güvenliği Derneği Yönetim Kuruluna teşekkürlerimizi sunarız.

Prof. Dr. Şeref SAĞIROĞLU
BGD Kurucu Üyesi ve II. Başkanı
Gazi Üniversitesi MF Bilgisayar Mühendisliği Bölüm Başkanı
FutureTech Genel Müdürü

Mustafa ŞENOL
BGD Disiplin Kurulu Üyesi
HAVELSAN Yönetim Kurulu Başkan Vekili

BİLGİ GÜVENLİĞİ DERNEĞİ'NDEN

Bilgi Güvenliği Derneği (BGD); 22 Temmuz 2007 tarihinde, Bilgi Güvenliği ve Siber Güvenlik alanında toplumun her kesiminde bilgi ve bilinç düzeyini arttırmak, bu konu ile ilgili teknolojik gelişmeleri izlemek, yerli ve milli teknolojilerin geliştirilmesine katkı sağlamak; bireysel, kurumsal ve ulusal düzeydeki riskler konusunda farkındalık oluşturmak ve kamu-sektör-üniversite işbirliklerini geliştirmek amacı ile kurulmuştur.

BGD'nin vizyonu; "bilgi güvenliği alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olmaktır." BGD vizyonu doğrultusunda; tüm paydaşlarla işbirliği yaparak mevzuatın oluşturulmasında ve geliştirilmesinde aktif rol almakta, gerçekleştirdiği konferans, sempozyum, çalıştay ve eğitimler, yayımladığı rapor ve yazılar ile farkındalığın oluşmasına ve bunun davranışa dönüştürülmesine katkılar sağlamaktadır.

Derneğimiz bu kapsamda; "Ulusal Siber Güvenlik Strateji Belgesi" ve "Ulusal Siber Güvenlik Eylem Planı" hazırlanmasına öncülük etmiş, hazırladığı taslak metinler kabul görmüş ve sonuçta ülkemizin siber güvenlik stratejisi ve eylem planlarının gecikmeden yayımlanasına katkı sağlamıştır. Aynı zamanda; bu alanda nitelikli insan kaynağı yetiştirilmesi, mesleki yeterliliklerin belirlenmesi, kamu-endüstri-üniversite işbirliklerinin geliştirilmesi, kümelenme çalışmalarının başlaması gibi önemli politika ve stratejilerin oluşturulmasında etkin rol üstlenmektedir.

BGD, "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı", "Ulusal Siber Güvenlik Stratejisi Çalıştayı", "Veri Merkezleri ve Siber Güvenlik Çalıştayı", "Siber Güvenlik Hukuku Çalıştayı", "Mobil Dünyada Çocuk ve Gençlerin Güvenliği Sempozyumu", "IPv6 Konferansı", "Kritik Enerji Altyapılarının Korunması Sempozyumu", "Ulusal Siber Terör Konferansı", "Siber Güvenlik Yaz Kampı" gibi

etkinlikleri düzenleyerek ve destekleyerek bilgi güvenliğine ihtiyaç duyulan her alanda çalışmalar yürütmüştür. Cumhurbaşkanlığı, Milli Eğitim Bakanlığı, Ulaştırma ve Altyapı Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Sosyal Güvenlik Kurumu ve Üniversiteler gibi farklı paydaşlar ile çalışmalar yürütmektedir.

BGD, **CyberMag Dergisi** ile toplumun tüm kesimlerine ulaşmaya çalışmaktadır. 2019 yılında 12'ncisini düzenleyeceğimiz "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı" kısaca **ISCTurkey Konferansı** olarak bilinen uluslararası etkinlik ile kurulduğu günden bu yana kamu kurumları, özel sektör ve üniversiteleri bir araya getirmeyi başarmıştır.

Bununla birlikte, bilgi güvenliği ve siber güvenlik alanında **ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olan Bilgi Güvenliği Derneği**, bünyesinde oluşturulan BGD Genç ile; bireysel, kurumsal, ulusal ve evrensel boyutlarda bilgi ve iletişim güvenliği alanında teknik, bilimsel, sosyal ve kültürel faaliyetler yürütmek, orta ve yüksek öğrenim gören genç üyelerimizin mesleki gelişimini artırmak, siber güvenlik alanında farkındalık oluşturmak, ülkemizin siber güvenlik uzman kaynağını oluşturmak için gençlerimizin bu alana ilgisini artırmak için faaliyet göstermektedir.

ISCTurkey etkinlikleri, Gazi Üniversitesi, İstanbul Teknik Üniversitesi ve Ortadoğu Teknik Üniverstesi işbirliği ile düzenlenmekte, Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu tarafından sürekli desteklenmektedir. Bu etkinlik, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından "Avrupa Siber Güvenlik Ayı" platformu etkinliklerine dâhil edilen ilk ve tek etkinliktir. Ayrıca, düzenlendiği ilk yıldan beri ülkemizin siber güvenlik alanındaki bilimsel ve sektörel çalışmaların paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamunun bilgilendirildiği, paydaşların eğitildiği, tüm bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişinin sağlandığı ülkemizde bu alandaki en önemli etkinliktir.

Şubat 2019'da yeni bir yönetim kuruluyla göreve başlayan BGD Yönetimi, yapılan çalışmalara yenilerinin eklenmesi, açık kaynak olarak paylaşılacak olan çalışmaların artması ve ülkemizin bu alanda

ihtiyaç duyduğu Türkçe kaynak ihtiyacına katkılar sağlanmasını desteklemektedir.

Bu kitabın hazırlanmasında katkı sağlayan başta editörlerimize, hiç bir beklenti içerisinde olmadan bölüm yazan ve bunu kamuoyu ile ücretsiz paylaşılması konusunda destek veren saygıdeğer yazarlarımıza, destekleyicimize ve bugüne kadar ülke bilgi güvenliği ve siber güvenliğinin gelişimine katkı sağlayan BGD yöneticilerimize ve üyelerimize bu vesile ile şükranlarımı sunarım.

Bu kitap serisinin ikincisinin, ülkemiz siber güvenlik ve savunma çalışmalarına katkılar sağlaması dileğiyle.

Ahmet Hamdi ATALAY
Bilgi Güvenliği Derneği YK Başkanı

ÖN SÖZ

Günümüzde siber güvenlik, beşinci savaş ortamı olarak kabul edilmenin ötesinde tüm ülkeler için ulusal güvenliğin ayrılmaz ve en önemli bileşeni olarak değerlendirilmektedir.

Yerli, güvenilir, yenilikçi ve yüksek kaliteli Siber Güvenlik çözümleri geliştirerek ülkemizin siber güvenliğinin sağlanmasında ana unsur; uluslararası pazarlarda güçlü ve güvenilir Siber Güvenlik teknoloji ve hizmet sağlayıcısı olmak vizyonu ile çalışmalarını yürüten HAVELSAN, ülkemizin siber uzayda güvenliğini sağlayacak bir mükemmeliyet merkezi olmak, ülkemizin yetenek ve kaynaklarının etkin kullanılmasına öncülük etmek adına var gücüyle çalışmalarını sürdürmektedir.

Bir Türk Silahlı Kuvvetlerini Güçlendirme Vakfı şirketi olan HAVELSAN tarafından hayata geçirilen Siber Savunma Teknoloji Merkezi çatısı altında siber güvenlik operasyon merkezi hizmetleri, kurumsal siber güvenlik danışmanlık ve destek hizmetleri, güvenlik analiz ve test hizmetleri, siber güvenlik eğitimleri ve yerli siber güvenlik ürünleri geliştirme faaliyetleri yürütülmektedir.

Siber güvenlik alanında ülkemizin nitelikli insan kaynağını artırmak için Türkçe kaynak ihtiyacının en az bu alanda verilen eğitimler kadar değerli olduğunun bilincinde olan HAVELSAN, bu ihtiyacı karşılamada katkı sağlayacak değerli bir yayın olarak gördüğü bu kitabı desteklemektedir.

Ahmet Hamdi ATALAY
HAVELSAN Genel Müdürü