19. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISC Türkiye 2026) "Yeni Dünya Düzeninde Siber Savaşlar" ana temasıyla, 20-21 Ekim 2026 tarihlerinde Ankara'da gerçekleştirildi.



2.000'in üzerinde katılımcıyı bir araya getiren ISC Türkiye 2026, Türkiye'nin siber güvenlik geleceğini, dijital egemenliği ve küresel güç mücadelesinin siber boyutunu gündeme taşıdı. 22 Ekim 2026, ANKARA.

Bilgi Güvenliği Derneği tarafından bu yıl 19'uncusu düzenlenen Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISC Türkiye 2026), 20-21 Ekim 2026 tarihlerinde Bilgi Teknolojileri ve İletişim Kurumunun (BTK) ev sahipliğinde gerçekleştirildi. Cumhurbaşkanlığı Siber Güvenlik Başkanlığının katkı ve desteğiyle düzenlenen konferans, **"Yeni Dünya Düzeninde Siber Savaşlar"** ana temasıyla kamu, askerî kurumlar, akademi ve özel sektörden üst düzey temsilcileri, uzmanları ve araştırmacıları bir araya getirdi. İki gün boyunca 2.000'in üzerinde katılımcının yer aldığı konferans, siber güvenliğin ulusal güvenlik, savunma, teknoloji ve uluslararası rekabet açısından taşıdığı stratejik önemi ortaya koydu.

Konferansın açılışında **Ulaştırma ve Altyapı Bakanımız Abdulkadir Uraloğlu, Cumhurbaşkanlığı Siber Güvenlik Başkanı Ümit Önal, BTK Başkanı Mehmet Koçyiğit, Bilgi Güvenliği Derneği Yönetim Kurulu Başkanı Prof. Dr. Mustafa Alkan ve Konferans Başkanı M. Tuncay Gençoğlu** başta olmak üzere kamu ve güvenlik kurumlarının üst düzey temsilcileri, üniversite yöneticileri, akademisyenler ve sektör temsilcileri yer aldı. Açılış programına ayrıca, Orta Doğu Teknik Üniversitesi Rektörü Prof. Dr. Ahmet Yozgatlıgil de katıldı.

Konferansın, 20 Ekim 2026 tarihli ilk gününe ait tüm konuşmacıların konuşmalarının ait metinlere buradan erişilebilir.

BGD YK Başkanı Sayın Alkan konuşmasında, derneğin 19 yıllık faaliyetini üç misyon üzerinden özetledi: Toplumda siber güvenlik farkındalığını yükseltmek, ülkenin ihtiyaç duyduğu uzman insan kaynağının yetişmesine eğitimler ve yaz-kış kamplarıyla katkı vermek, yerli ve milli çözümler üreten sektörün güçlenmesini desteklemek. Derneğin yıllardır her platformda savunduğu

“siber güvenlikte tek bir düzenleyici otorite” talebinin Siber Güvenlik Başkanlığının kurulmasıyla karşılık bulduğunu, bundan sonra derneğin kamu, üniversite ve sektör arasında bir arayüz olarak çalışmaya devam edeceğini söyledi. 2007’den beri konferansa ev sahipliği yapan BTK’ya teşekkür ederek bu yılın BTK’daki son etkinlik olduğunu, 20. konferansın ODTÜ ev sahipliğinde yapılacağını duyurdu.

(Sayın Alkan’ın konuşmasına ilişkin videoya buradan erişilebilir.)

Konferans Başkanı Sayın Gençoğlu konuşmasında, 19 yıldır bilgi güvenliğini konuşan konferansın bu yıl “bilginin ve güvenin istiklal ve istikbalini” müzakere ettiğini söyledi. Siber savaş temasını çağın köklü dönüşümünün bir tezahürü olarak nitelendirdi; siber güvenliği ulusal egemenliğin, stratejik bağımsızlığın ve geleceği tayin etme kudretinin asli unsuru olarak tanımladı. Yapay zekâ ve kuantum teknolojilerinin dönüştürdüğü dünyada güvenliğin, tehditlere yalnızca mukabele edenlerin değil “güvenin yeni mimarisini ilim, akıl ve irfanla inşa edenlerin” eseri olacağını, Türkiye’nin bu dönüşümde yön verenler arasında yer alacağına inandığını ifade etti.

(Sayın Gençoğlu’nun konuşmasına ilişkin videoya buradan erişilebilir.)

ODTÜ Rektörü Sayın Yozgatlıgil konuşmasında, siber güvenliği ülkenin milli güvenliğinin, ekonomik gücünün ve teknolojik bağımsızlığının temel unsuru olarak tanımladı ve ODTÜ’nün bu alandaki kapasitesini aktardı: 2002’den beri kriptografi araştırmacısı yetiştiren Uygulamalı Matematik Enstitüsü ve kuantum sonrası kriptografi çalışmaları, Enformatik Enstitüsündeki siber güvenlik yüksek lisans programı, ODTÜ Teknokent’teki siber güvenlik firmaları ve hızlandırma programları. Kuzey Kıbrıs Kampüsünde açılan siber güvenlik mühendisliği lisans programını “adaların siber güvenlik çalışmaları için uygun yerler” olduğu düşüncesiyle gerekçelendirdi; kampüsten öğrencilerin konferansa getirildiğini belirtti. Üniversitenin birikimini kamu ve sanayiyle ortak araştırmalara ve uygulanabilir çözümlere dönüştürmeyi önemsediklerini söyleyerek 20. konferansa ev sahipliği yapmaktan onur duyacaklarını ifade etti.

(Sayın Yozgatlıgil’in konuşmasına ilişkin videoya buradan erişilebilir.)

BTK Başkanı Sayın Koçyiğit konuşmasında, siber savaşın bir yazılım açığıyla da bir sinyal karıştırıcıyla da görünmez biçimde sürdüğünü, ENISA’nın Eylül raporuna göre AB’yi etkileyen olayların yarısından fazlasının hizmet dışı bırakma saldırısı olduğunu ve en çok hedef alınan sektörün kamu olduğunu aktardı.

(Sayın Koçyiğit’in konuşmasına ilişkin videoya buradan erişilebilir.)

SGB Başkanı Sayın Önal konuşmasını üç soru etrafında kurdu: Dünya nereye evriliyor, tehdit nerede duruyor, biz ne yapmalıyız? 21. yüzyılda gücün veri, algoritma ve hesaplama kapasitesiyle ölçüldüğünü; jeopolitik gerilimlerin olduğu her yerde bir siber cephenin açıldığını, 2024 yazındaki hatalı yazılım güncellemesinin saldırgan olmadan da milyonlarca cihazı çökertmesinin “bağımlılıklarımız düşmanlarımızdan daha büyük bir zafiyet olabilir” dersini verdiğini söyledi. Fransa’da market zincirlerinin soğutma sistemlerine yapılan uzaktan müdahaleyi, Eylül ayında kripto varlık saldırılarında kaybedilen yaklaşık 768 milyon doları örnek verdi. Tehdidi dijital, fiziksel ve bilişsel olmak üzere üç boyutta tanımladı; bilişsel boyutu “en az konuşulan ama en tehlikeli” boyut olarak nitelendirdi ve bu üç alanın ayrı kurumlar, ayrı bütçeler ve ayrı dillerle yönetilmesi hâlinde saldırganın hep bir adım önde olacağını vurguladı. Konuşmasının merkezine

koyduğu dijital egemenliği veri egemenliği, siber dayanıklılık ve caydırıcılık, teknoloji egemenliği, bilişsel egemenlik ve normatif egemenlik olmak üzere beş ayak üzerinde tanımladı. Somut gelişmeler olarak 5 Mayıs 2026'da toplanan ilk Siber Güvenlik Kurulunu, dijital devlet ve kamuda yapay zekâ yetkilerinin Başkanlık çatısı altında toplanmasını ve 47 görev alanında uzman alımını aktardı. Çağrıları: siber güvenliği üst yönetim meselesi yapmak, kamu-akademi-özel sektör arasında tehdit istihbaratı paylaşımı ve ortak tatbikat, dayanıklılık odaklı düşünmek, insanı merkeze almak, küresel iş birliği. "Savaşı en çok teknolojiye sahip olan değil, en iyi birlikte hareket edebilen kazanacak" sözüyle bitirdi.

(Sayın Önal'ın konuşmasına ilişkin videoya buradan erişilebilir.)

Ulaştırma ve Altyapı Bakanı Sayın Uraloğlu, veriyi yeni çağın en stratejik kaynağı olarak tanımladı ve bir ülkenin gücünün veriyi üretme, kendi topraklarında tutma, işleme, koruma ve değere dönüştürme kabiliyetiyle ölçüldüğünü söyledi. Veri merkezlerini "Türkiye'nin yeni dijital kaleleri" olarak konumlandırdı: Temmuz'da Gölbaşı'nda temeli atılan 35.300 metrekarelik Türksat Veri Merkezi (mevcut kapasiteyi ilk fazda 3, ikinci fazda 8 katın üzerine çıkaracak) ve Eylül'de hizmete giren Vodafone İzmir Veri Merkezi. Ulusal Siber Güvenlik Strateji ve Eylem Planı 2024-2028 kapsamında 6 stratejik amaç, 18 hedef ve 61 eylem belirlendiğini, bir sonraki planı Siber Güvenlik Başkanlığının hazırlayacağını belirtti. 7545 sayılı Siber Güvenlik Kanunu ile politikaların tek elden belirlenmesinin sağlandığını, Türkiye'nin ITU 2024 Küresel Siber Güvenlik Endeksi'nde tam puanla Seviye 1 "rol model ülke" kategorisinde yer aldığını hatırlattı. Çocukların dijital ortamda korunmasını siber güvenlik çabalarının en öncelikli boyutu olarak sundu: 15 yaşını doldurmamış çocuklara sosyal ağ hizmetinin sınırlandırılması, e-Devlet üzerinden yaş doğrulaması, 15-18 yaş grubu için özel tedbirler ve zorunlu ebeveyn kontrol araçları.

(Sayın Uraloğlu'nun konuşmasına ilişkin videoya buradan erişilebilir.)

Kamu ve askerî kurumların üst düzey temsilcileriyle akademi ve özel sektörü aynı platformda buluşturan konferans, Türkiye'nin siber güvenlik kapasitesinin geliştirilmesi, kritik altyapıların korunması ve kurumlar arası iş birliğinin güçlendirilmesi açısından önemli bir buluşma niteliği taşıdı.

Yeni dünya düzeninde siber güç ve stratejik bağımsızlık

Dijital teknolojilerin ülkelerin ekonomik, siyasi ve askerî gücünde belirleyici hâle gelmesiyle birlikte siber uzay, küresel güç mücadelesinin en kritik alanlarından biri olarak öne çıkıyor. Kritik altyapılara yönelik siber saldırılar, dijital casusluk faaliyetleri, veri güvenliği ihlalleri ve gelişmiş teknolojilerin savunma alanındaki kullanımı, ülkelerin ulusal güvenlik stratejilerini doğrudan etkiliyor.

ISC Türkiye 2026'nın ana teması olan "Yeni Dünya Düzeninde Siber Savaşlar", bu dönüşümü teknik, stratejik ve jeopolitik boyutlarıyla ele aldı. Konferansta siber tehditlerin değişen niteliği, ulusal siber güvenlik stratejileri, kritik altyapıların korunması, kriptolojinin stratejik önemi ve Türkiye'nin siber güvenlik kapasitesinin geliştirilmesi gibi konular öne çıktı.

Konferans, siber güvenliğin yalnızca teknik bir savunma alanı olmadığını; ulusal egemenlik, ekonomik güvenlik, savunma, diplomasi ve teknolojik bağımsızlıkla doğrudan ilişkili stratejik bir mesele olduğunu bir kez daha ortaya koydu.

Üç temel başlıkta siber güvenlik gündemi

Konferans programı, değişen küresel güvenlik ortamında siber tehditlere karşı geliştirilecek yaklaşımları üç temel başlık altında ele aldı ve 3 oturumda konuşmacılar şunlardı:

1. Oturum: Siber Dayanıklılık ve Caydırıcılık: Siber saldırılara karşı hazırlıklı olma, tehditleri tespit etme, saldırılara etkin biçimde müdahale etme ve kritik sistemlerin sürekliliğini sağlama.

Konuşmacılar:

- Yusuf TANCAN, Siber Güvenlik Başkanlığı, Başkan Yardımcısı
- Tuğgeneral Metin DURMAZ, TSK Siber Savunma Komutanı
- Cem AKOYMAK, Vodafone İcra Kurulu Başkan Yardımcısı (Hukuk ve Kurumsal Güvenlik)
- Serhat SARI, Türk Telekom Siber Güvenlik Direktörü
  Abdurrahman Şakar, Turkcell Siber Savunma Merkezi Direktör Yardımcısı

2. Oturum: Platform Siber Güvenliği: Dijital platformların, iletişim sistemlerinin ve stratejik teknoloji altyapılarının güvenliğinin güçlendirilmesi.

Konuşmacılar:

- Taha YÜCEL, Aselsan Genel Müdür Yardımcısı
- Murat ÇİZGEL, SSB Siber Güvenlik ve Bilişim Sistemleri Daire Başkanı
- Orhan KOCA, Türksat Genel Müdür Yardımcısı
- Salih TALAY, Havelsan Siber Güvenlik Direktörü

3.Oturum: Küresel Rekabette Teknoloji Savaşları ve Siber Casusluk: Teknolojik üstünlük mücadelesi, siber istihbarat, bilgi güvenliği ve dijital egemenlik konularının değerlendirilmesi.

Konuşmacılar:

- Mahmut KÜÇÜK, SGB Ekosistem Geliştirme Genel Müdürü
- Oğuz YILMAZ, BGD Genel Sekreteri/Labris Networks Kurucu Ortağı
- Murad BALAYEV, Azerbaycan Cumhuriyeti Özel İletişim ve Bilgi Güvenliği Devlet Servisi SOME Müdürü
- Hüseyin KURU, J. Mu. Yb, Jandarma Genel Komutanlığı MEBS ve Siber Güvenlik Komutanlığı
- Hasan YAMAN, EGM Siber Suçlarla Mücadele Daire Başkanlığı, Bilgi Teknolojileri Şube Müdürü – Emniyet Amiri

Bu başlıklar kapsamında kamu kurumlarının, güvenlik birimlerinin, savunma sanayisinin, üniversitelerin ve özel sektörün siber güvenlik alanındaki sorumlulukları ve iş birliği imkânları gündeme geldi.

Kamu, savunma sanayisi ve özel sektör aynı platformda buluştu

Konferansın oturumları, siber güvenliğin farklı sektörler açısından taşıdığı önemi ortaya koydu.

Farklı sektörlerden uzmanların katılımıyla gerçekleştirilen oturumlar, siber güvenlikte etkili sonuçlara ulaşmanın yalnızca teknolojik çözümlerle değil, güçlü koordinasyon ve ortak bir güvenlik yaklaşımıyla mümkün olduğunu gösterdi.

"Siber Dayanıklılık ve Caydırıcılık" başlıklı oturumda kamu yönetimi, güvenlik birimleri ve telekomünikasyon sektörünün siber tehditlerle mücadeledeki rolleri ele alındı. Siber saldırılara karşı hazırlıklı olma, operasyonel sürekliliği sağlama ve kurumlar arası koordinasyonun güçlendirilmesi, ulusal siber dayanıklılığın temel unsurları olarak öne çıktı.

Bu oturumda yer alan konuşmacılar ve konuşma özetlerine aşağıda yer verilmektedir.

Yusuf TANCAN – Siber Güvenlik Başkanlığı Başkan Yardımcısı

Yusuf Tancan dayanıklılık ve caydırıcılığı bir madalyonun iki yüzü olarak tanımladı: biri içeriye bakar ("vurulursam ne olur"), diğeri dışarıya ("bana vurmak ne kadar pahalı"). Güvenliğin başarısının kapıdan kimin girmediğiyle değil, kapı aşıldığında içerideki hayatın devam edebilmesiyle ölçüleceğini söyledi. Dayanıklılığı bağışıklık sistemine ve deprem yönetmeliğine benzetti; bağışıklık hücrelerinin birbiriyle konuştuğunu, bir kurumda görülen saldırının ertesi gün başka bir kurumda boşa çıkabilmesi gerektiğini, "sessiz kalan hücrenin hasta hücre" olduğunu vurguladı. Dayanıklılığın dört aşamasını (hazırlanmak, direnmek, toparlanmak, öğrenmek) açıkladı; "hiç açılmamış paraşüt paraşüt değildir, yedeğini hiç geri yüklememiş kurumun yedeği yoktur" dedi. Caydırıcılığı saldırganın hesabını değiştirmek olarak tanımladı; kabiliyet, inandırıcılık ve iletişim unsurlarına dayandığını, mutlaka misilleme anlamına gelmediğini, saldırganın beklediği faydayı engellemenin de caydırıcılık olduğunu belirtti. Atıf zorluğu nedeniyle caydırıcılığın yalnızca saldırganı tespit beklentisine dayandırılmaması, karşılık seçeneklerinde hukuka uygunluk, ölçülülük ve tırmanma riskinin gözetilmesi gerektiğini söyledi. Salondan ayrılırken herkese üç soru bıraktı: En kritik hizmetimiz hangisi, çökerse kaç saatte ayağa kalkarız? En son tatbikatı ve yedekten geri dönüşü ne zaman yaptık? Saldırıya uğradığımız gün kimi arayacağız?

(Sayın Tancan'ın konuşmasına ilişkin videoya buradan erişilebilir.)

Tuğgeneral Metin DURMAZ – TSK Siber Savunma Komutanı

Metin Durmaz, konuya asker gözüyle baktı: siber dayanıklılık TSK için hareket serbestisinin muhafazası, komuta kontrolün korunması, durumsal farkındalığın sürdürülmesi ve görev için kritik sistemlerin işler tutulması demektir; hiçbir saldırı görevin ifasına engel olmamalıdır. Dayanıklılığın savunmaya dayalı caydırıcılığa katkı verdiğini ama tek başına yeterli olmadığını belirterek caydırıcılığın hasmın kazanç-maliyet muhasebesini hedeflediğini, karşılığın yalnızca siber yöntemlerle sınırlı olmayıp kinetik ve kinetik olmayan her vasıtayı, diplomatik ve ekonomik tedbirleri içerebileceğini söyledi. Siber alanda mutlak caydırıcılığın önündeki engelleri sıraladı: atıf ve isnat sürecinin zor, uzun ve siyasi bir karar süreci olması; mesajın karşı tarafta farklı algılanması ihtimali; hangi eylemin silahlı saldırı sayılacağına dair ortak anlayışın bulunmaması. Silahlı saldırı eşiğinin altında sürekli hâle gelen saldırılara karşı klasik caydırıcılığın sonuç vermediğini, caydırıcılığın yetenek ile o yeteneği kullanma kararlılığının bileşimi olduğunu vurguladı. Siber alanın kara, deniz, hava ve uzaydan sonra beşinci harekât alanı olarak TSK konsept ve doktrinlerine yansıtıldığını, Siber Savunma Komutanlığının ulusal ve uluslararası tatbikatlarla bu alanda caydırıcı bir güç olma hedefiyle çalıştığını aktardı.

(Sayın Durmaz'ın konuşmasına ilişkin videoya buradan erişilebilir.)

Cem AKOYMAK – Vodafone İcra Kurulu Başkan Yardımcısı

Cem Akoymak telekomdaki gelişmenin artık yalnızca hız ve kapasite üzerinden okunmaması gerektiğini; yapay zekâ ve otomasyonun şebekelere entegre olduğu yeni dönemde güvenlik ve dayanıklılığın dönüşümün parçası olduğunu söyledi. Bir şirketin operasyonunu durdurmak için fabrikasına girmenin gerekmediğini, tek bir kullanıcı hesabının, internete açık bir uygulamanın ya da bir tedarikçinin saldırı başlangıç noktası olabileceğini belirtti. Vodafone'un küresel siber güvenlik ağını (Birleşik Krallık, Almanya, Romanya, Hindistan, Portekiz) anlattı; bir pazarda ilk kez görülen saldırı tekniğinin diğer pazarlarda önceden alınmış önleme dönüştüğünü, bu bilgiyi yerel güce çeviren unsurun Türk mühendisleri olduğunu vurguladı. Ankara'daki 7/24 siber güvenlik operasyon merkezini, Türkiye'ye yapılan 600 milyar TL'yi aşan yatırımı, son 5 yıldaki 100 milyar TL'lik şebeke yatırımını ve ilk fazı 100 milyon dolara tamamlanan, Tier 3 standardında, 4 MW ile başlayıp 20 MW'ın üzerine çıkacak İzmir Veri Merkezini aktardı. Grubun şebeke test ve inovasyon ortamının İspanya'dan İstanbul'a taşındığını ve yeni nesil şebeke testlerinin artık Türkiye'de yapılacağını açıkladı. İkincil düzenlemelerin sektörle istişare içinde, yatırım ve inovasyon ortamını destekleyecek biçimde şekillenmesini beklediklerini söyledi.

(Sayın Akoymak'ın konuşmasına ilişkin videoya buradan erişilebilir.)

Serhat SARI – Türk Telekom Siber Güvenlik Direktörü

Serhat Sarı, siber dayanıklılığı önleyici tedbirlerin gücü, erken tespit kapasitesi ve hızlı müdahale yetkinliğiyle ilişkilendirerek bunu yalnızca bir bilgi teknolojileri meselesi olarak değil, kurumsal sürdürülebilirliğin ve milli güvenliğin unsuru olarak ele almak gerektiğini söyledi. Caydırıcılığın temeline güçlü teknolojik altyapıyla desteklenen proaktif güvenlik yaklaşımını koydu ve bunun iki boyutunu açıkladı: sıfır güven mimarileri, ağ segmentasyonu, gelişmiş erişim kontrolleri ve çok katmanlı savunmayla saldırının başarı olasılığını azaltmak; tehdit istihbaratı, izleme, analiz ve olay müdahale yetkinlikleriyle güvenlik kapasitesini sürekli güçlendirmek. Türk Telekom'un ülkenin iletişim altyapısına yönelik sorumluluğunun yanında kurumların dijital varlıklarını

korumalarına katkı sunduğunu belirterek "dijital geleceğin gücü yalnızca teknolojik kapasiteyle değil, o teknolojiye duyulan güvenle ölçülecek" dedi. Güvenli dijital geleceğin dayanağı olarak ortak akıl, güçlü altyapı, yerli yetkinlikler ve etkin iş birliğini saydı.

(Sayın Sarı'nın konuşmasına ilişkin videoya buradan erişilebilir.)

Abdurrahman ŞAKAR – Turkcell Siber Savunma Merkezi Direktör Yardımcısı

Abdurrahman Şakar "sahanın sesi" olmak istediğini söyleyerek tek bir rakamla başladı: 2026 küresel tehdit raporuna göre saldırganların ilk erişimden sonra diğer sistemlere geçiş süresi ortalama 29 dakika, en hızlı vaka 27 saniye; bu süre birkaç yıl önce aylar mertebesindeydi. Yapay zekânın saldırgan olmanın maliyetini düşürdüğünü, 100 dolara etkin bir siber saldırgan kiralanabildiğini, sıfırıncı gün açıklıklarını keşfetmenin ve sömürü kodu yazmanın kolaylaştığını, atak yüzeyinin kontrol edilemeyecek biçimde genişlediğini ve bugün saldırganların savunmaya göre önde olduğunu belirtti. Dayanıklılığı "mukavim olmak, esnemek ama kırılmamak" diye tanımladı; tespit ve müdahale sürelerinin ölçülmesini ve simülasyonunu gündem maddesi yaptı. Kurumların itibarının saldırı olmadan da, dark web ve sosyal medyadaki doğrulanmamış "hacklendi" iddialarıyla zedelenebildiğini, bu iddiaları ortaya atanların cezai yaptırıma uğraması gerektiğini söyledi. Siber suç ekosisteminde erişim satıcısından hizmet olarak fidye yazılımına uzanan bir iş bölümü ve dayanışma varken savunma tarafının aynı saldırıyı kurum kurum ayrı analiz ettiğini belirterek IOC paylaşımının ötesinde taktik ve teknik düzeyde bilgi paylaşımına dayalı bir "ulusal bağışıklık sistemi" önerdi. Çözümün daha fazla ürün ve alarm değil, riske göre önceliklendirilmiş, yapay zekâ ve otomasyonla desteklenen bütünleşik bir yapı olduğunu; güvenliğin yalnızca güvenlik ekiplerine bırakılamayacağını, sistem yöneticilerinin yama geçmeyi ve geliştiricilerin zafiyet gidermeyi kendi görevi saymasının gerektiğini söyledi.

(Sayın Şakar'ın konuşmasına ilişkin videoya buradan erişilebilir.)

"Platform Siber Güvenliği" oturumu, savunma sanayisi ve stratejik bilişim altyapılarının korunmasına odaklandı. Aselsan, Cumhurbaşkanlığı Savunma Sanayii Başkanlığı, Türksat ve Havelsan gibi kurum ve kuruluşların temsil edildiği program, kritik teknolojilerin güvenliği ve Türkiye'nin stratejik sistemlerinin korunması konularını gündeme taşıdı.

Bu oturumda yer alan konuşmacılar ve konuşma özetlerine aşağıda yer verilmektedir.

Taha YÜCEL – ASELSAN Genel Müdür Yardımcısı

Taha Yücel, Ukrayna ve İran örnekleri üzerinden savaşın doğasındaki değişimi anlattı: harekât başlamadan önce siber saldırının başladığını, bazen hiç mermi atılmadan siber savaş yaşandığını; pahalı platformların ucuz ve asimetrik teknolojilerle etkisiz kılınabildiğini, milyar dolarlık bir radarın basit sistemlerle üst üste vurularak devre dışı bırakıldığını aktardı. Yakın zamanda bir girişimci arkadaşının şirketinin fidye yazılımıyla kilitlendiğini, yedeğin de sisteme bağlı olduğu için kilitlendiğini anlatarak "en büyük hata" dersini paylaştı. Siber güvenlik yatırımının bir masraf değil stratejik yatırım olduğunu, en değerli varlığın güvenilir insan olduğunu; çalışanlara şirket verisini satmaları için ödeme teklif edildiği yeni bir tehdit boyutuna dikkat çekti. Platform siber güvenliğini dört ilkeyle özetledi: tasarım aşamasından itibaren güvenlik, katmanlı savunma (yedeğin fiziksel olarak ayrılması, birden çok yedek), tedarik zinciri güvenliği (gerekirse tedarikçinin güvenliğine yatırım yapmak) ve kriptografik egemenlik. "Şimdi topla, sonra çöz"

tehdidine karşı post-kuantum kriptografiye bugünden geçilmesi gerektiğini, ASELSAN'ın TOBB Üniversitesi'yle kuantum kriptoloji laboratuvarı yürüttüğünü söyledi; yapay zekâyı hem saldırı hem savunmada olmazsa olmaz olarak tanımladı.

(Sayın Yücel'in konuşmasına ilişkin videoya buradan erişilebilir.)

Murat ÇİZGEL – Savunma Sanayii Başkanlığı Siber Güvenlik ve Bilişim Sistemleri Daire Başkanı

Murat Çizgel, "kaynaklarını iyi kullanan savaşı yönetir" ilkesinin meydan savaşlarından siber ve hibrit savaşlara kadar değişmediğini söyledi; 11 yaşındaki kızının bir kaleyi gezerken söylediği "artık top tüfeğe gerek yok, hacklemek var" sözünü yeni neslin doğal kavrayışına örnek verdi. Devletin politikasını dört somut başlıkla açıkladı. Birincisi siber güvenlik planı: SSB tarafından yürütülecek tüm projelerde yüklenici, kalite planı gibi, tasarımdan lojistiğe kadar aldığı tedbirleri içeren bir siber güvenlik planı hazırlayıp onaya sunmak zorunda. İkincisi tedarik zinciri: bir füzenin alt sistem üreticisindeki zafiyetin görev gününde füzeyi işlevsiz bırakabileceğini anlatarak TR Test ile yürütülen Siber Hijyen ve Siber Hijyen KOBİ programını ve bunun zorunlu hâle getirileceğini aktardı. Üçüncüsü yerlilik: siber güvenlik ürünlerinin ve savunma alt sistemlerinin siber dayanıklılığının sürekli ölçülüp ispatlanacağı SAYGEP (Siber Alan Yetkinlik Geliştirme ve Entegrasyon Platformu) merkezini duyurdu. Dördüncüsü yapay zekâ: uçta çalışan yapay zekânın savunma platformlarının vazgeçilmezi olacağını, ancak içeriği bilinmeyen açık kaynak modellerin belirli bir koordinat veya tarihte "halüsinasyon" görecek şekilde tetiklenmesi riskini vurgulayarak milli modeller için veri kütüphanesi ve altyapı sağlayacak EVREN projesini ("savunma sanayiinin yapay zekâ evreni") tanıttı; verinin yurt dışına gitmeyeceğini ve devletin bunun için ücret almayacağını söyledi.

(Sayın Çizgel'in konuşmasına ilişkin videoya buradan erişilebilir.)

Orhan KOCA – Türksat Genel Müdür Yardımcısı

Orhan Koca, dijitalleşmenin tek bir servisten çok bankacılık, ödeme, kargo gibi birçok sistemin entegre olduğu platformlara dönüştüğünü ve platform güvenliğinin zincirin en zayıf halkası kadar olduğunu söyledi. Son yıllardan somut siber savaş örnekleri verdi: 2016 Kiev elektrik altyapısına Industroyer saldırısı, Şubat 2022'de Rus harekâtının başladığı gün Viasat uydu ağına saldırı, 2023'te İran akaryakıt dağıtım şebekesine saldırı, İran'da IoT ve kamera izlerinden beslenen nokta operasyonları, Lübnan'da çağrı cihazlarına tedarik zinciri aşamasında yerleştirilen patlayıcılar, Suriye'de cevap veremeyen radarlar ve Venezuela operasyonunda kör edilen elektrik ve radar sistemleri. Bu örneklerin güvenliğin teknoloji, fiziksel tedbir, tedarikçi ve lojistiği kapsayan bir bütün olduğunu gösterdiğini belirtti. Yüzde 100 güvenliğin mümkün olmadığını, iddianın "ne kadar dayanıklıyız, ne kadar sürede ayağa kalkarız, felaket kurtarma ve yedeklilik simülasyonları yapıldı mı" olması gerektiğini söyledi. Kullanılan yabancı ekipmanın "belki de zafiyetin ta kendisi" olabileceğini belirterek Milli Teknoloji Hamlesi kapsamında bağımsız altyapıların şart olduğunu vurguladı. Türksat'ın işlettiği platformların ölçeğini paylaştı: 68-69 milyon kullanıcılı e-Devlet'te 9.000'den fazla servis, 1.000'in üzerinde entegre kurum ve yılda 12 milyarı aşan işlem; 6 uydu, bunlardan Türksat 6A'nın ASELSAN, TUSAŞ, CTech ve TÜBİTAK ile yüzde 85 yerlilikle üretilmesi; 5,5 milyon kapasiteli kablo TV altyapısı ve Ulusal Coğrafi Bilgi Sistemi. Yapay zekâyı "güvenlik için yapay zekâ, yapay zekâ için güvenlik" biçiminde iki yönlü ele aldı

ve Türksat'ın kendi dil modelleri üzerinde çalıştığını, 5 yıllık yerlileştirme hedefi koyduğunu açıkladı.

(Sayın Koca'nın konuşmasına ilişkin videoya buradan erişilebilir.)

Salih TALAY – HAVELSAN Siber Güvenlik Direktörü

Salih Talay, siber alanı çelik, barut ve motor teknolojisinden sonra insanlığın savaşa eklediği yeni alan olarak tanımladı ve bu alanın kara, deniz, hava ve uzay platformlarının tamamını yönettiğini, platformların veri üretip otonom karar sistemlerini beslediğini söyledi. Askeri platformlarda tehdidin orantısızlığını "40 milyon dolarlık uçak, 40 dolarlık bir alt bileşen yüzünden görev kaybı yaşayabilir" örneğiyle anlattı; etkinin veri kaybıyla sınırlı kalmayıp görev kaybı, komuta merkeziyle bağlantının kopması ve dost-düşman ayrımının bozulması olabileceğini, siber saldırının fiziksel saldırıyla eş zamanlı gelmesi hâlinde müşterek harekâtı riske atabileceğini belirtti. Otonomi ve sensör füzyonunun karar hızını artırırken yanıltıcı girdilerle sürünün tamamını riske atabileceğini, bu nedenle karar sürecinde insanın bulunduğu mekanizmaların ve uluslararası savaş hukukunun gözetilmesi gerektiğini, askeri platformlarda "üç kere değerlendirip bir kere uyguladıklarını" söyledi. Yapılması gerekenleri sıraladı: tasarımdan itibaren tehdit modellemesi, görev ağlarında katmanlı mimari ve bakım/yükleme süreçlerinde veri aktarım kontrolü, tedarik zinciri güvenliği, operasyonel sürekliliğe yatırım, insan kaynağı ve ortak standartlar. 5 Mayıs 2026'daki Siber Güvenlik Kurulu toplantısında savunma sanayiinin kritik altyapı olarak kabul edilmesini önemli bir adım olarak andı. Havacılıkta DO-326/DO-356, kara araçlarında ISO/SAE 21434 ve BM R155/R156, denizcilikte IACS UR E26/E27 gibi uluslararası standartlar varken yerli standart ve rehber dokümanların çok kısıtlı olduğunu, ivedilikle geliştirilmesi gerektiğini söyledi. Bir platformun 20-50 yıl envanterde kalacağını hatırlatarak yerli üretimin tek başına güvenliği garanti etmeyeceğini, bağımsız ve yerli test-değerlendirme süreçlerinin şart olduğunu belirtti; HAVELSAN'da müstakil bir Platform Siber Güvenliği Grup Liderliği ve tüm projelere uygulanan bir sistem siber güvenliği prosedürü oluşturduklarını aktardı.

(Sayın Talay'ın konuşmasına ilişkin videoya buradan erişilebilir.)

"Küresel Rekabette Teknoloji Savaşları ve Siber Casusluk" başlıklı oturumda ise teknolojik üstünlük mücadelesinin siber boyutu, dijital istihbarat faaliyetleri ve küresel rekabet ortamında bilginin korunmasının önemi ele alındı.

Bu oturumda yer alan konuşmacılar ve konuşma özetlerine aşağıda yer verilmektedir.

Mahmut KÜÇÜK – Siber Güvenlik Başkanlığı Ekosistem Geliştirme Genel Müdürü

Mahmut Küçük, siber casusluğu yalnızca zafiyetlerin istismarıyla verinin ele geçirilmesi olarak değil, kullanılan ürünlerin kendisinin casusluk aracı olabilmesi boyutuyla ele aldı. Teknolojiyi geliştiren tarafın bilgiyi elde etmede avantajlı olduğunu, bu nedenle kritik verilerin, altyapıların ve işlemlerin teslim edildiği noktaya dikkat edilmesi gerektiğini söyledi. Veri egemenliğinin kendi veri merkezinde kendi personeliyle çalışmakla tek başına sağlanamayacağını, güvenlik yönetim sistemi ve denetimin şart olduğunu belirtti. Ekonomik gerekçelerle buluta yönelimin ve "yapay zekâ oyuncağıyla oynama" heyecanının, verinin nereye gittiği değerlendirilmeden küresel sağlayıcıların ücretsiz veya düşük ücretli modellerine aktarılmasına yol açtığını; bu sorumluluğun

yalnızca siber güvenlik birimlerinde değil bireylerde, kurumlarda ve düzenleyici kuruluşlarda olduğunu vurguladı. Verinin nerede ve nasıl saklanacağına ilişkin ikincil mevzuatın yakın zamanda sektörün görüşüne açılarak yayımlanacağını duyurdu.

Tehdidin yalnızca yabancı devletlerin APT gruplarından gelmediğini, kişi güvenlik belgesi gerektiren pozisyonlarda içeriden sızdıran kişilerin, etki ajanlarının ve başka servislerin elemanlarının da kullanıldığını hatırlattı. Güvenliği kurum ağıyla sınırlı görmenin yetmediğini; o ağa erişen uzmanın, subayın veya komutanın evindeki temizlik robotu, akıllı araç ve telefonun da bütünleşik biçimde ele alınması gerektiğini, dijitalleşme arttıkça dijital ayak izinin büyüdüğünü ve bu izlerin büyük yapay zekâ modellerini besleyen "daha üst seviye bir akıl" tarafından toplandığını söyledi. Toplumsal duyarlılığın artırılması ve yalnızca Siber Güvenlik Başkanlığının değil BTK, BDDK, EPDK gibi sektörel düzenleyicilerin de kendi alanlarında müdahale etmesi gerektiğini belirterek "koyduğunuz kural hayata geçmiyorsa o kural konmamış demektir; artık konuşmaktan çok eyleme ve icraata geçme dönemindeyiz" dedi.

(Sayın Küçük'ün konuşmasına ilişkin videoya buradan erişilebilir.)

Oğuz YILMAZ – Bilgi Güvenliği Derneği Genel Sekreteri / Labris Networks Kurucu Ortağı

Oğuz Yılmaz, teknoloji savaşlarını bir senaryo üzerinden ele aldı: Bir pazartesi sabahı elektrik ve internet var, ama dışarıdaki bulut hizmetlerine, lisans doğrulama sunucularına, merkezden yönetilen güvenlik ekranlarına ve güncelleme kaynaklarına erişim yok; müttefik bilinenler servisleri kapatmış olabilir. Kurumların bu durumda en fazla 72 saat idare edebileceğini söyleyerek bunu bir "72 saatlik egemenlik testi" olarak adlandırdı. İlk 6 saatte bağımlılık haritasının çıkarılması gerektiğini (hangi uygulama dışarıya bağlı, hangi lisans yerelde çalışmayı kilitler, kimlik doğrulama ve DNS dışarıya mı bağımlı, loglar nerede), bunun altyapı, kontrol katmanı ve kayıt/izleme sistemleri olmak üzere üç katmanda önceden yazılı olması gerektiğini; sonraki 18 saatte güvenlik politikasını dış ekrana ihtiyaç duymadan değiştirebilme ve şüpheli trafiği kendi ağında analiz edebilme kabiliyetinin, 2. ve 3. günde ise insanın, sürecin ve tedarikin (alternatif haberleşme, yazılı müdahale yetkileri, yedekten dönüş, tedarikçisiz sistemi ayakta tutacak bilgi) sınandığını anlattı. Sıradan bir DDoS saldırısının bile ülke GSYH'sine yüzde 1-3,5 arasında etki ettiği örnekler bulunduğunu, bu nedenle dış servis koptuğunda temel koruma işlevini yerinde sürdürebilen sistemlerin önem kazandığını belirtti; "hazırız" demenin hazır olmak anlamına gelmediğini, dış bağımlılıkları kontrollü ortamda keserek tatbikat yapılması ve tek noktaya bağlı işlevlerin listelenmesi gerektiğini söyledi.

Teknoloji rekabetini satranç ve Civilization gibi sıra tabanlı oyunlara benzetti: bugün en uygun fiyatlı diye seçilen ürün yarın bağımlılığa, bugün yetiştirilmeyen mühendis 5 hamle sonra kurulamayan ekibe, bugün projeye sokulmayan yerli üretici 10 hamle sonra hiç doğmayan alternatife dönüşür. Çip ihracat kısıtlamalarını, yapay zekâ altyapısına erişim şartlarını ve ABD'nin Venezuela, Grönland, İran ve Tayvan hamlelerini enerji, nadir toprak elementleri ve çip üretimi üzerinden teknoloji savaşının hamleleri olarak okudu. Bir platforma bağlanmanın hızlı ve ekonomik görünse de veri taşınabilirliğini, açık standartları, alternatif tedariki ve mühendislik birikimini ihmal ettirdiğini; özgeçmişlere yazılan yabancı ürün sertifikalarının yarın bir ülke güvenliği meselesi olabileceğini söyledi. Sonuç önerileri: kritik altyapılar için 72 saatlik kesinti senaryolarını gerçek tatbikata dönüştürüp her kuruluş için asgari hizmet listesi çıkarmak; kamu

alımlarında fiyat-performansın yanına yerel yönetilebilirliği, dış bağlantı koptuğunda hizmetin sürüp sürmeyeceğini ve alternatif müdahale imkânını zorunlu ölçüt olarak koymak; savunma sanayiinde olduğu gibi devletin ilk müşteri ve stratejik yönlendirici olarak yerli üreticilere saha deneyimi açması (SSB'nin SAYGEP'ini bu yönde bir adım olarak andı); her katmanda yerli olmak şart olmasa da en kötü senaryonun etkisini bilmek ve B planına sahip olmak. Dinleyicilere iki soru bıraktı: Yarın kritik dış teknoloji hizmetleri 72 saat kesilse ayakta kalabilecek miyiz? Bugün imzaladığımız teknoloji alımı 10 hamle sonra elimizi güçlendirecek mi, seçeneklerimizi azaltacak mı?

(Sayın Yılmaz'ın konuşmasına ilişkin videoya buradan erişilebilir.)

Murad BALAYEV – Azerbaycan Özel İletişim ve Bilgi Güvenliği Devlet Servisi SOME Müdürü

Murad Balayev, devletler arası rekabetin yarı iletkenler, yapay zekâ modelleri, bulut ve veri üzerinden yürüdüğünü, siber casusluğun bu savaşın en sessiz ve en ucuz cephesi olduğunu söyledi. BM E-Devlet Endeksi'nde dünya birincisi Danimarka'nın 5 Ekim'de açıkladığı, merkezi nüfus kaydındaki yaklaşık 8,8 milyon kişiye ait verilere yetkisiz erişim olayını anlattı: erişim sorgulama yetkisi olan özel bir şirketin meşru hesabından sağlanmış, olay olağan dışı yüksek bir sorgulama faturasıyla fark edilmiş, zincirin koptuğu halka bir tedarikçinin "123456" parolası olmuş. Dersi: dijitalleşmede birinci olmak dayanıklılıkta birinci olmak demek değil; bir devletin güvenliği güvendiği en zayıf üçüncü tarafın güvenliği kadardır. Azerbaycan devlet SOME'sinin son bir yılda gözlemlediği vakaları paylaştı: enerji sektörüne yönelik Çin bağlantılı APT kampanyası iddiası, Güney Asya kökenli bir grubun diplomatik kurumlara "dahili bilgi notu" görünümlü tuzak belgeyle yürüttüğü casusluk, tarayıcıda açık bırakılan mesajlaşma oturumunun ele geçirilmesi ve Türkiye'yi de hedef listesine alan Rus bağlantılı RedWolf hacktivist grubu. Genişleyen saldırı yüzeyinde üç başlığa dikkat çekti: tedarik zinciri (Klue olayında 2022'den kalma tek bir entegrasyon hesabı üzerinden 20'ye yakın kuruluşun CRM verisinin sızması), "Shadow AI" (kurumlar bilinen yapay zekâ platformlarını yasakladığında çalışanların denetimsiz platformlara yönelmesi; çözüm yasak değil onaylı araç ve eğitim) ve IoT (200.000 cihaza bulaşan botnet, fabrikadan zararlı bileşenle gelen 35 dolarlık projektör). Bir devlet SOME'sinin beş ilkesini sıraladı: görünürlük, yerli analiz kapasitesi (bir üniversitede kurulan zararlı yazılım analizi ve adli bilişim laboratuvarı, agentic SOC ve MDR projesi), tatbikat (enerji sektörü için kriz simülasyonu, siber poligon), insan faktörü ve iş birliği (FIRST, OIC-CERT, Trusted Introducer, APWG üyeliği; müttefik ülke SOME'leri arasında protokol beklemeden paylaşım). "İki devlet, tek millet" anlayışıyla siber alanda da omuz omuza yürüme çağrısıyla bitirdi.

(Sayın Balayev'in konuşmasına ilişkin videoya buradan erişilebilir.)

Hüseyin KURU – Jandarma Muhabere Yarbayı, Jandarma MEBS ve Siber Güvenlik Komutanlığı

Hüseyin Kuru, teknoloji savaşlarını yalnızca yeni ürün geliştirme olarak değil, mevcut teknolojiyi iyileştirme, yerlileştirme, rakibin bilgi birikimine ulaşma ve rakibin erişimini kısıtlama mücadelesi olarak tanımladı; köklü dönüşüm yaratan her teknolojiye (elektrik, internet, bugün yapay zekâ, yarın kuantum) entegrasyonun zorunluluk hâline geldiğini ve teknolojinin ekonomik ve askeri güç üzerinde çarpan etkisi yarattığını söyledi. Teknoloji edinme yollarını (satın alma, transfer, mevcut ürünleri ileri taşıma, tersine mühendislik) anlatırken yerli güvenlik duvarı ve WAF ürünlerinin

yabancı muadillerinin ötesinde yetenekler kazandırdığını örnek verdi. Siber casusluğun fiziksel mesafeyi önemsizleştirdiğini, F-35 programına ilişkin hassas bilgilerin Çin bağlantılı faaliyetlerde hedef alınmasının "teknolojiyi üretmek kadar arkasındaki fikri sermayeyi korumak" dersini verdiğini; 2000-2020 arasındaki 595 Çin bağlantılı casusluk vakasında havacılık, uzay ve bilgi teknolojilerinin öne çıktığını aktardı. Fransa'nın Charles de Gaulle uçak gemisindeki bir personelin spor uygulamasında konum paylaşmasının geminin yerini açığa çıkarmasını, güvenliğin insan, süreç, teknoloji ve operasyonel disiplinle birlikte ele alınması gerektiğinin örneği olarak verdi. Dijital egemenliğin her teknolojiyi sıfırdan geliştirmek anlamına gelmediğini, asıl meselenin kritik bağımlılıkların riskini yönetmek olduğunu; açık standartlar, açık kaynak, veri taşınabilirliği ve mikroservis mimarisinin tedarikçi bağımlılığını azalttığını söyledi. Nitelikli insan kaynağını teknoloji rekabetinin en önemli unsuru olarak öne çıkardı: büyük teknoloji şirketleri arasındaki "yetenek savaşları"nı ve bir yapay zekâ araştırmacısının 200 milyon dolarla transfer edilmesini örnek verdi. ABD ve Çin'in yapay zekâ rekabetini inceleyen 2026 tarihli bir araştırmanın ortak başarı unsurları olarak güçlü devlet yatırımını ve yapay zekânın askeri sistemlerle entegrasyonunu gösterdiğini aktardı. Türkiye için beş öncelik sıraladı: ulusal güvenlik riski yaratan kritik bağımlılıkları belirlemek, tedarik zincirini sürdürülebilirlik ve alternatif kaynak açısından değerlendirmek, tehdit istihbaratını kurumlar arasında hızla paylaşmak, henüz ticarileşmemiş Ar-Ge bilgisini ve fikri mülkiyeti korumak, nitelikli insanı yetiştirip elde tutmak. Konuşmasını üç kelimeyle özetledi: "Üret, koru, kontrol et."

(Sayın Kuru'nun konuşmasına ilişkin videoya buradan erişilebilir.)

Hasan YAMAN – EGM Siber Suçlarla Mücadele Daire Başkanlığı Bilgi Teknolojileri Şube Müdürü

Hasan Yaman konuyu kolluk gözüyle, suç ve delil boyutuyla ele aldı. Siber casuslukta amacın görünür hasar değil uzun süre fark edilmeden erişimi sürdürmek olduğunu, olayın büyüklüğünün sistemin ne kadar kapalı kaldığıyla değil hangi bilginin kimin eline geçtiğiyle ölçüldüğünü söyledi. Mart 2024'te bir Microsoft mühendisinin yarım saniyelik gecikmeyi araştırarak XZ Utils kütüphanesine iki yıldır gönüllü katkı veren biri tarafından yerleştirilen arka kapıyı ortaya çıkarmasını "yıllara yayılan sabır, güvene dayalı ilişki ve küresel bağımlılık" örneği olarak anlattı; keşfin bir güvenlik ürününe değil bir mühendisin dikkatine bağlı olduğunu vurguladı. Teknoloji savaşlarının sahadaki yüzünün bağımlılıklar olduğunu, saldırganın çoğu zaman kurumun kendisine değil güvendiği tedarikçiye saldırdığını belirtti. Salt Typhoon grubunun ABD'de 9 büyük telekom operatörüne sızarak yasal dinleme sistemlerini hedef almasından "yasal yetkiyle kurduğumuz her erişim kapısı saldırganın da ilgisini çeker" dersini çıkardı. Devlet faaliyetleriyle suç yapılarının örtüşmesini iki örnekle açıkladı: Çin'de devlet kurumlarına sözleşmeyle siber saldırı hizmeti satan i-Soon şirketinin belgelerinin sızması ve Şubat 2025'te Kuzey Kore bağlantılı Lazarus grubunun cüzdan yazılımı geliştiricisinin bilgisayarı üzerinden Bybit borsasından yaklaşık 1,5 milyar dolar çalması. Bu nedenle sıradan bir dolandırıcılık soruşturmasında çıkan bir sunucunun çok daha büyük bir faaliyetin parçası olabileceğini, siber suçla mücadelenin casusluğun tespitine de katkı verdiğini söyledi. Yapay zekânın iki yüzünü Hong Kong'da deepfake video görüşmesiyle 25 milyon dolar transfer ettirilen çalışan örneğiyle anlattı; herkese açık yapay zekâ hizmetlerine yüklenen ihale dosyası ve şartnamelerin casusluğun aylarca uğraştığı bilgiyi "kendi ellerimizle vermek" olduğunu belirtti. EGM'nin 2018'den beri yapay zekâya yatırım yaptığını, kurum verisinin tek satırının dışarı çıkmadığı kendi dil modellerini ve erişim destekli üretim mimarilerini geliştirdiğini, bu birikimi diğer kamu kurumlarıyla paylaşmaya hazır olduklarını

açıkladı. Caydırıcılığın delilin korunması ve adli sürecin işletilmesiyle tamamlandığını; 2018 PyeongChang Olimpiyatları saldırısında kasıtlı sahte izler bırakıldığını hatırlatarak teknik iz ile fail arasında otomatik eşitlik kurulamayacağını, soruşturmaların birden fazla ülkeye yayılması nedeniyle uluslararası adli iş birliğinin şart olduğunu söyledi.

(Sayın Yaman'ın konuşmasına ilişkin videoya buradan erişilebilir.)

Yapay zekâ çağında siber güvenlik: Yeni tehditler, yeni savunma yaklaşımları

Konferansın ikinci gününde gerçekleştirilen **"Süper Zekâ Çağında Siber Güvenlik Çalıştayı"**, yapay zekâ teknolojilerinin siber güvenlik alanında oluşturduğu fırsatları ve riskleri gündeme taşıdı.

Yapay zekâ destekli saldırılar, yeni nesil tehdit tespit mekanizmaları, etmen yapay zekâ sistemlerinin güvenliği ve 6G çağında ortaya çıkabilecek riskler, çalıştayın öne çıkan konuları arasında yer aldı. Yapay zekânın hem saldırı hem de savunma kapasitesini dönüştürdüğü günümüzde, güvenli teknoloji geliştirme süreçlerinin ve proaktif savunma yaklaşımlarının önemi değerlendirildi.

Konferansın eğitim programında bilgi güvenliği yönetimi, DevSecOps ve veri sızdırma vakalarının adli bilişim perspektifiyle incelenmesi gibi uygulamaya dönük başlıklara da yer verildi. Böylece stratejik değerlendirmelerin yanı sıra teknik uzmanlık ve uygulama becerilerinin geliştirilmesi de desteklendi.

Akademik araştırmalar ve kriptolojinin geleceği

ISC Türkiye 2026, bilimsel araştırmaların ve teknolojik yeniliklerin paylaşılmasına imkân sağlayan akademik programıyla da dikkat çekti.

Akademik oturumlarda kriptografi, kuantum sonrası kriptografi, blokzincir, yapay zekâ destekli siber güvenlik, ağ güvenliği, kimlik doğrulama ve güvenli sistem tasarımı gibi alanlardaki çalışmalar ele alındı.

Kuantum bilgisayarların mevcut kriptografik sistemler üzerindeki olası etkileri ve kuantum sonrası kriptografik yöntemlerin geliştirilmesi, geleceğin güvenli iletişim altyapıları açısından önem taşıyan konular arasında yer aldı. Yapay zekâ destekli tehdit tespiti, güvenli dijital kimlik mekanizmaları ve yeni nesil haberleşme altyapılarının korunması da bilimsel ve teknolojik gündemin önemli başlıklarını oluşturdu.

Oturum başkanlığını Prof. Dr. Şeref Sağıroğlu'nun yaptığı davetli konuşmacı oturumunda, Finlandiya'daki LUT Üniversitesinden Prof. Dr. Najmul Islam "Blockchain Tabanlı Sistemlerin Sorumlu, Güvenilir ve Yasal Tasarımı ve Kullanımı" başlıklı sunumunda, blokzincir tabanlı sistemlerin sorumlu, güvenilir ve hukuka uygun tasarımı ve kullanımı üzerine değerlendirmelerde bulundu.

(Davetli konuşmacı oturumuna ilişkin videoya buradan erişilebilir.)

Akademik program, üniversitelerde üretilen bilimsel bilginin kamu kurumları ve sektörün uygulama deneyimiyle buluşmasına katkı sağlarken araştırmacılar, uzmanlar ve teknoloji geliştiricileri arasındaki bilgi alışverişini destekledi.

Siber güvenliğe katkı sunan çalışmalar ödüllendirildi

Konferans kapsamında gerçekleştirilen **Siber Güvenlik Üstün Hizmet Ödülleri ve plaket töreni**, siber güvenlik alanına katkı sunan kişi ve kurumların çalışmalarının takdir edilmesi açısından programın önemli bölümlerinden biri oldu.

7 daldaki ödüller;

Kurumsal dalda,

T.C. MSB Kara Kuvvetleri Komutanı Orgeneral Metin TOKEL,

ODTÜ Rektörü Prof. Dr. Ahmet YOZGATLIGİL ve

EGM Siber Suçlarla Mücadele Daire Başkanı Oykun İLGÜN'e;

Bireysel dalda,

Prof. Dr. Ersan AKYILDIZ ve

Prof. Dr. Ali Aydın SELÇUK'a;

Medya dalında,

Murat GÖÇE BTHaber'e,

Özel firma dalında,

CberWise Genel Müdürü Aret KILLIOĞLU'na verildi.

Bilgi güvenliği alanında bilgi birikiminin geliştirilmesi, uzmanlığın yaygınlaştırılması ve Türkiye'nin siber güvenlik kapasitesine katkı sağlayan çalışmaların görünür kılınması, sektörün gelişimi açısından önem taşıyor.

Ödül ve plaket töreni, siber güvenlik alanında emek veren uzmanların ve kurumların katkılarının takdir edilmesine ve mesleki farkındalığın güçlendirilmesine yönelik anlamlı bir buluşma niteliği taşıdı.

(Siber Güvenlik Üstün Hizmet Ödülleri ve plaket törenine ilişkin videoya buradan, erişilebilir)

Ayrıca, ISC Türkiye 2026 Konferansına sponsor olarak destek veren firmalar şu şekildedir;

Platin Sponsorlar: Türksat, Türkcell, TürkTelekom, Türknet, Vodafone;

Altın Sponsor: Labris Networks,

Gümüş Sponsorlar: Anayurt Teknoloji, Aselsan, CberWise,

Yaka Kartı Sponsoru: Picus,

Eğitim Sponsoru: Türktrust,

Stant Alanı Sponsorları: Ankara Üniversitesi Teknokent, Beyes, Difose, Kuantum Siber Güvenlik, Nanova Teknoloji Sistemleri, Nesil Teknoloji, Niltek

Medya ve İletişim Sponsorları: Anadolu Ajansı, Bookmark, Ict Media, Dijital Gündem (DG), BTHaber, Maramiro.

(Sponsorluk Plaket Törenine ilişkin videoya buradan, erişilebilir.)

Türkiye'nin siber güvenlik ekosistemine katkı

2007 yılından bu yana düzenlenen Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Türkiye'de bilgi güvenliği ve kriptoloji alanlarında bilimsel çalışmaların paylaşılmasına, sektörün gelişimine ve farklı paydaşlar arasında iş birliğinin kurulmasına katkı sağlıyor.

Bilgi Güvenliği Derneği öncülüğünde düzenlenen konferans; üniversiteleri, kamu kurumlarını, savunma ve güvenlik alanındaki paydaşları, araştırmacıları ve özel sektör temsilcilerini ortak bir platformda buluşturuyor.

Bu yıl 19'uncusu düzenlenen ve 2.000'in üzerinde katılımcıyı bir araya getiren ISC Türkiye 2026, siber tehditlerin giderek karmaşıklaştığı bir dönemde Türkiye'nin bilimsel ve teknolojik kapasitesinin geliştirilmesi, nitelikli insan kaynağının desteklenmesi ve üniversite-kamu-sanayi iş birliğinin güçlendirilmesi yönündeki ihtiyacı bir kez daha ortaya koydu.

Konferansın ortaya koyduğu temel yaklaşım, dijital geleceğin güvenliğinin güçlü kurumsal iş birliği, bilimsel araştırma, nitelikli insan kaynağı ve sürdürülebilir güvenlik politikalarıyla mümkün olacağı yönünde şekillendi.

Bilgi Güvenliği Derneği, bilgi güvenliği ve kriptoloji alanlarında farkındalığın artırılması, bilimsel bilgi birikiminin geliştirilmesi ve Türkiye'nin siber güvenlik ekosisteminin güçlendirilmesine yönelik çalışmalarını sürdürmektedir.


TÜRKİYE 2026
19.ULUSLARARASI BİLGİ GÜVENLİĞİ
VE KRİPTOLOJİ KONFERANSI
19th International Conference on Information Security and Cryptology
"Yeni Dünya Düzeninde Siber Savaş
"Cyber Wars in the New World Order"


TÜRKİYE 2026
19.ULUSLARARASI BİLGİ GÜVENLİĞİ
VE KRİPTOLOJİ KONFERANSI
19th International Conference on Information Security and Cryptology
"Yeni Dünya Düzeninde Siber
"Cyber Wars in the New World Or


TÜRKİYE 2026
GÜVENLİK
TÜRKİYE 2025
iscturkiye


19.ULUSLARARASI BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI
19th International Conference on Information Security and Cryptology
TÜRKİYE 2026
Altın Sponsor
Yaka Kartı Sponsor
PICUS




Cİ GÜVENLİĞİ
NFERANSI


TÜRKİYE 2026
19.ULUSLARARASI BİLGİ GÜVENLİĞİ
VE KRİPTOLOJİ KONFERANSI
19th International Conference on Information Security and Cryptology
"Yeni Dünya Düzeninde Siber Savaşlar"
"Cyber Wars in the New World Order"


TÜRKİYE 2026
19.ULUSLARARASI BİLGİ GÜVENLİĞİ
VE KRİPTOLOJİ KONFERANSI
19th International Conference on Information Security and Cryptology


TÜRKİYE 2026
19.ULUSLARARASI BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI
19th International Conference on Information Security and Cryptology


BLOCKCHAIN TABANLI SİSTEMLERİN
RESPONSIBLE, TRUSTWORTHY, AND LAWFUL
Oturum Başkanı / Session Chair
Prof. Dr. Şeref SAĞIROĞLU
Chair of IEEE, Blockchain Türkiye
BİLGİ TEKNOLO
VE İLETİŞ
KURUMU
Prof. Dr. Şeref SAĞIROĞLU
Gazi University
Computer Engineering Department /
Chair of IEEE, Blockchain Türkiye WG


ODTÜ


TÜRKİYE 202
IEEE


uWiPeR
Güvenilir Veri Silme Cihazı


Olay Yeri İçin



