ISC Türkiye 2026 Sonuç Raporu

19. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISC Türkiye 2026) , "Yeni Dünya Düzeninde Siber Savaşlar" 20-21 Ekim 2026, BTK Konferans Salonu, Ankara

Konferans hakkında

Bilgi Güvenliği Derneğinin, 2007'den bu yana her yıl düzenlediği Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 19. yılında Cumhurbaşkanlığı Siber Güvenlik Başkanlığının paydaşlığı ve Bilgi Teknolojileri ve İletişim Kurumunun ev sahipliğiyle gerçekleştirilmiştir. Ana tema "Yeni Dünya Düzeninde Siber Savaşlar"; alt başlıklar "Siber Dayanıklılık ve Caydırıcılık", "Platform Siber Güvenliği" ve "Küresel Rekabette Teknoloji Savaşları ve Siber Casusluk" olarak belirlenmiştir. Konferansın açılışını, Ulaştırma ve Altyapı Bakanı Sayın Abdulkadir Uraloğlu yapmış; Siber Güvenlik Başkanlığı Başkanı Ümit Önal, BTK Başkanı Mehmet Koçyiğit ve ODTÜ Rektörü Prof. Dr. Ahmet Yozgatlıgil açılış konuşmalarında yer almıştır. İlk gün 3 oturumda 16 konuşmacı söz almış; Finlandiya LUT Üniversitesinden Prof. Dr. Najmul Islam davetli konuşmacı olarak Blokzincir sistemlerinin sorumlu ve yasal tasarımını ele almıştır. İkinci gün, akademik oturumlar, "Süper Zekâ Çağında Siber Güvenlik" ve "Blokzincir Türkiye" çalıştaylarıyla devam etmiştir. Geleneksel olarak BGD tarafından her yıl 7 dalda verilen Siber Güvenlik Üstün Hizmet Ödülleri kamu, üniversite, kişi, sektör ve medya kategorilerinde sahiplerini bulmuştur.

Konferans iki bakımdan bir dönüm noktası olmuştur. 2007'den beri ev sahipliği yapan BTK'daki son buluşma olmuş; 2027 yılında yapılacak olan 20. Konferansın ODTÜ'de yapılacağı açıklanmıştır. Daha önemlisi, Bilgi Güvenliği Derneği'nin kurulduğu günden beri savunduğu, "Siber güvenlikte tek bir düzenleyici otorite" talebi, 7545 sayılı Siber Güvenlik Kanunu ve Siber Güvenlik Başkanlığıyla karşılık bulmuş olarak ilk kez bu konferansta konuşulmuştur. Konuşmacıların büyük bölümü bu kurumsal yapıyı bir başlangıç olarak değerlendirmiş; asıl işin bu çerçeveyi kamu, akademi ve sektörle birlikte çalışan bir ekosisteme dönüştürmek olduğu üzerinde durmuştur.

Siber savaş bir ihtimal olmaktan çıkmıştır

Konferansın ilk ortak tespiti, siber savaşın artık bugünün gerçeği olduğudur. SGB Başkanı Ümit Önal'ın ifadesiyle, jeopolitik gerilimin olduğu her yerde bir siber cephe açılmakta; Doğu Avrupa'da ilk kurşundan önce kritik sistemlere operasyonlar başlamış bulunmaktadır. Türksat Genel Müdür Yardımcısı Orhan Koca, 2016 Kiev elektrik altyapısı saldırısından, Şubat 2022'deki Viasat uydu ağı saldırısına, Lübnan'daki çağrı cihazlarından Venezuela operasyonunda kör edilen radarlara uzanan bir dizi örnekle, aynı noktayı desteklemiştir. Aselsan Genel Müdür Yardımcısı Taha Yücel, Ukrayna ve İran'dan hareketle pahalı platformların ucuz ve asimetrik araçlarla etkisiz kılındığını, mermiler atılmadan önce siber savaşın başladığını anlatmıştır.

Sayın Önal tehdidi 3 boyutta tanımlamıştır: Dijital, fiziksel ve bilişsel. Fransa'da market zincirlerinin soğutma sistemlerine uzaktan müdahale edilmesi, siber saldırının artık sofranın güvenliğine dokunduğunu göstermektedir. Bilişsel boyutu "en az konuşulan ama en tehlikeli" alan olarak işaretlemiş; güvenini kaybeden bir toplumun en iyi güvenlik duvarına sahip olsa bile içeriden çökeceğini söylemiştir. Bu 3 alanın ayrı kurumlar, ayrı bütçeler ve ayrı dillerle yönetilmesi hâlinde saldırganın hep bir adım önde olacağı tespiti, konferansın sonraki oturumlarında da yankı bulmuştur.

Dayanıklılık, caydırıcılığın altyapısıdır

Birinci oturumun omurgasını, SGB Başkan Yardımcısı Yusuf Tancan'ın "madalyonun iki yüzü" çerçevesi oluşturmuştur. Dayanıklılık içeriye bakar: vurulursam ne olur? Caydırıcılık dışarıya: bana vurmak ne kadar pahalı? Güvenliğin başarısı, kapı aşıldığında içerideki hayatın devam edebilmesiyle ölçülmektedir. Sayın Tancan dayanıklılığı bağışıklık sistemine benzetmiş ve bir ayrıntının altını çizmiştir: bağışıklık hücreleri birbiriyle konuşur, bir kurumda görülen saldırının ertesi gün başka bir kurumda boşa çıkması gerekir. Sessiz kalan hücre hasta hücredir.

TSK Siber Savunma Komutanı Tuğgeneral Metin Durmaz, caydırıcılığın sınırlarını asker gözüyle çizmiştir. Siber alanda atıf ve isnat uzun, zor ve siyasi bir süreçtir; hangi eylemin silahlı saldırı sayılacağına dair ortak bir anlayış yoktur; silahlı saldırı eşiğinin altında süreklilik kazanan saldırılara karşı klasik caydırıcılık sonuç vermemektedir. Bu nedenle caydırıcılık, yetenekle birlikte o yeteneği kullanma kararlılığı olarak düşünülmeli; karşılık da siber araçlarla sınırlı kalmayıp diplomatik, ekonomik ve hukuki araçları kapsamalıdır. Sayın Tancan buna hukuka uygunluk, ölçülülük ve tırmanma riski kaydını eklemiştir.

Sahadan gelen rakamlar tabloyu somutlaştırmıştır. Turkcell Siber Savunma Merkezi Direktör Yardımcısı Abdurrahman Şakar'ın aktardığı 2026 küresel tehdit raporuna göre, saldırganın ilk erişimden sonra diğer sistemlere geçiş süresi ortalama 29 dakikadır; birkaç yıl önce bu süre aylarla ölçülmekteydi. Yapay zekâ saldırgan olmanın maliyetini 100 dolara indirmiş, sıfırıncı gün açıklıklarını keşfetmek kolaylaşmıştır. Sayın Şakar'ın teşhisi açıktır: saldırgan tarafta erişim satıcısından hizmet olarak fidye yazılımına uzanan bir iş bölümü ve dayanışma varken, savunma tarafında aynı saldırıyı her kurum kendi başına analiz etmektedir. Önerisi, gösterge paylaşımının ötesine geçen, taktik ve teknik düzeyde bilgi paylaşımına dayalı bir "ulusal bağışıklık sistemi" kurulmasıdır. Vodafone İcra Kurulu Başkan Yardımcısı Cem Akoymak, küresel ağda bir pazarda görülen tekniğin diğer pazarlarda önceden alınmış önleme dönüştüğünü anlatarak aynı mekanizmanın şirket ölçeğindeki karşılığını göstermiştir.

Bağımlılık, düşmandan büyük zafiyet olabilir

Konferans boyunca en sık tekrarlanan ders bu olmuş ve örnekleri çarpıcı biçimde sıralanmıştır. 2024 yazında tek bir hatalı yazılım güncellemesi ortada saldırgan yokken havalimanlarını, hastaneleri ve bankaları aynı anda felç etmiştir. Azerbaycan Cumhuriyeti Özel İletişim ve Bilgi Güvenliği Devlet Servisi SOME Müdürü Murad Balayev'in aktardığına göre, BM E-Devlet Endeksi'nde dünya birincisi Danimarka, 5 Ekim 2026'da merkezi nüfus kaydındaki yaklaşık 8,8 milyon kişiye ait verilere yetkisiz erişimi açıklamıştır; erişim bir tedarikçinin meşru hesabından sağlanmış, olay yüksek bir sorgulama faturasıyla fark edilmiş,

zincirin koptuğu halka “123456” parolası olmuştur. EGM Siber Suçlarla Mücadele Daire Başkanlığı, Bilgi Teknolojileri Şube Müdürü Hasan Yaman’ın anlattığı XZ Utils vakasında arka kapıyı yerleştiren kişi, projeye 2 yıldır gönüllü katkı vermekteydi ve olayı yarım saniyelik gecikmeyi araştıran bir mühendisin dikkati ortaya çıkarmıştır. Salt Typhoon’un ABD’de 9 telekom operatörünün yasal dinleme sistemlerine sızması, Bybit’ten 1,5 milyar doların cüzdan yazılımı geliştiricisinin bilgisayarı üzerinden çalınması, Klue olayında 2022’den kalma tek bir entegrasyon hesabıyla 20’ye yakın kuruluşun verisinin sızması, aynı kalıbı göstermektedir: saldırgan doğruca kurumun güvendiği tarafa yönelmektedir.

BGD Genel Sekreteri/Labris Networks Kurucu Ortağı Oğuz Yılmaz bu dersi bir senaryoya dönüştürmüştür. Bir pazartesi sabahı elektrik ve internet vardır; ama bulut hizmetlerine, lisans doğrulama sunucularına, merkezden yönetilen güvenlik ekranlarına ve güncelleme kaynaklarına erişim yoktur. Kurumlar bu durumda en fazla 72 saat idare edebilmektedir. Oğuz Yılmaz’ın “72 saatlik egemenlik testi” olarak adlandırdığı bu senaryoda ilk 6 saat bağımlılık haritasının çıkarılmasına, sonraki 18 saat kurumun kendi ağında karar alıp alamadığına, 2. ve 3. gün ise insanın, sürecin ve tedarikin sınanmasına ayrılmaktadır. Kurumlarda “hazırız” demenin hazır olmak anlamına gelmediğini, dış bağımlılıkların kontrollü ortamda kesilerek tatbikat yapılması ve tek noktaya bağlı işlevlerin listelenmesi gerektiğini söylemiştir. Jandarma Genel Komutanlığı MEBS ve Siber Güvenlik Komutanlığı’ndan J. Mu. Yb. Hüseyin Kuru ise dengeyi hatırlatmıştır: dijital egemenlik her teknolojiyi sıfırdan geliştirmek anlamına gelmemektedir; mesele kritik bağımlılıkların riskini yönetebilmek, açık standartlar ve veri taşınabilirliğiyle tedarikçi kilidini gevşetmektir.

Platformlar: 40 dolarlık bileşen, 40 milyon dolarlık uçak

İkinci oturum savunma sanayiinin bakışını yansıtmış ve en somut kurumsal adımların duyurulduğu bölüm olmuştur. Havelsan Siber Güvenlik Direktörü Salih Talay’ın örneği konuyu özetlemektedir: 40 milyon dolarlık bir uçak, 40 dolarlık bir alt bileşen yüzünden görev kaybı yaşayabilir. Askeri platformlarda etki, veri kaybıyla sınırlı kalmamakta; komuta merkeziyle bağlantının kopması, dost-düşman ayrımının bozulması, fiziksel saldırıyla eş zamanlı bir siber saldırının müşterek harekâtı riske atması söz konusu olmaktadır. Bir platformun 20 ila 50 yıl envanterde kalacağı düşünüldüğünde, yerli üretim tek başına güvenliği garanti etmemekte; bağımsız ve yerli test-değerlendirme süreçleri şart olmaktadır.

SSB Siber Güvenlik ve Bilişim Sistemleri Daire Başkanı Murat Çizgel, Savunma Sanayii Başkanlığının 4 adımını isimleriyle sıralamıştır. Başkanlık tarafından yürütülecek tüm projelerde yüklenici artık kalite planı gibi bir siber güvenlik planı hazırlayıp onaya sunmak zorundadır. TR Test ile yürütülen Siber Hijyen ve Siber Hijyen KOBİ programı, savunma sanayiine ürün veren en küçük firmanın bile asgari bir siber güvenlik olgunluğuna ulaşmasını hedeflemekte ve zorunlu hâle getirilecektir. SAYGEP (Siber Alan Yetkinlik Geliştirme ve Entegrasyon Platformu), yerli siber güvenlik ürünlerinin ve savunma alt sistemlerinin dayanıklılığının sürekli ölçülüp ispatlanacağı bir merkez olarak kurulmaktadır. EVREN projesi ise milli yapay zekâ modelleri için verinin yurt dışına çıkmadığı, devletin ücret almadığı bir veri kütüphanesi ve altyapı vadetmektedir. Sayın Çizgel’in uyarısı dikkat çekicidir: içeriği bilinmeyen bir açık kaynak modelin, belirli bir koordinat veya tarihte yanlış görmeye başlayacak biçimde tetiklenmesi, milyar dolarlık bir platformu anlamsız kılabilir.

Sayın Yücel ve Talay'ın tasarımdan itibaren güvenlik, katmanlı savunma, tedarik zinciri ve post-kuantum kriptografi başlıkları birbirini tamamlamıştır. Sayın Yücel'in anlattığı fidye yazılımı vakası, yedeğin sisteme bağlı tutulmasının bütün yatırımı boşa çıkardığını göstermiştir. Sayın Talay'ın dikkat çektiği bir boşluk ise rapora alınmayı hak etmektedir: havacılık, kara araçları ve denizcilik için uluslararası siber güvenlik standartları varken platform güvenliği alanında yerli standart ve rehber doküman çalışması çok kısıtlıdır.

Siber casusluk ve yapay zekânın iki yüzü

Üçüncü oturum, casusluğun değişen biçimini ele almıştır. SGB Ekosistem Geliştirme Genel Müdürü Mahmut Küçük, tehdidin yalnızca zafiyetlerin istismarından gelmediğini, kullanılan ürünün kendisinin casusluk aracı olabildiğini; kurum ağını korumanın yetmediğini, o ağa erişen uzmanın evindeki robottan arabasına kadar dijital ayak izinin bütünleşik ele alınması gerektiğini söylemiştir. Ekonomik gerekçelerle buluta yönelimin ve "yapay zekâ oyuncağıyla oynama" heyecanının kurumsal verinin değerlendirilmeden küresel sağlayıcılara aktarılmasına yol açtığını belirtmiştir; Sayın Balayev aynı olguyu "Shadow AI" adıyla tanımlamış ve çözümün yasak değil, onaylı araç sunmak ve hangi verinin asla girilemeyeceğini tanımlamak olduğunu söylemiştir. Sayın Yaman'ın ifadesi bu noktayı tamamlamaktadır: bir ihale dosyasını veya teknik şartnameyi özetlenmek üzere herkese açık bir yapay zekâ hizmetine vermek, casusluğun aylarca uğraşarak elde etmeye çalıştığı bilgiyi kendi elimizle teslim etmektir.

Sayın Kuru, teknoloji savaşının insan boyutunu öne çıkarmıştır. F-35 programına ilişkin bilgilerin hedef alınması, bir platformu asıl değerli kılanın yıllara yayılan test sonuçları, tasarım tercihleri ve mühendislik deneyimi olduğunu hatırlatmaktadır. Büyük teknoloji şirketleri arasındaki yetenek savaşlarında tek bir araştırmacının 200 milyon dolara transfer edilmesi, insan kaynağının finansal sermaye kadar stratejik hâle geldiğini göstermektedir. Sayın Önal'ın aktardığı, 47 görev alanında uzman alımı ve Orta Doğu Teknik Üniversitesi Rektörü Prof. Dr. Ahmet Yozgatlıgil'in anlattığı ODTÜ programları, bu ihtiyacın Türkiye'deki karşılığını oluşturmaktadır.

Sayın Yaman'ın bir başka katkısı caydırıcılık tartışmasına kolluk perspektifi eklemesi olmuştur: saldırının tespiti, izlerin korunması ve adli sürecin işletilmesi caydırıcılığın parçasıdır; PyeongChang 2018'de kasıtlı sahte izler bırakılması, teknik iz ile fail arasında otomatik eşitlik kurulamayacağını göstermektedir. EGM'nin 2018'den beri geliştirdiği, kurum verisinin tek satırının dışarı çıkmadığı dil modellerini, diğer kamu kurumlarıyla paylaşmaya hazır olması, kamu içinde yerli yapay zekâ kapasitesinin nasıl büyütülebileceğine dair somut bir teklif olarak kayda geçmiştir.

Düzenleyici cephe

Konferans, düzenleyici adımların yoğunlaştığı bir döneme denk gelmiştir. Ulaştırma ve Altyapı Bakanı Abdulkadir Uraloğlu, Ulusal Siber Güvenlik Strateji ve Eylem Planı 2024-2028 kapsamında 6 amaç, 18 hedef ve 61 eylem belirlendiğini, bir sonraki planı Siber Güvenlik Başkanlığının hazırlayacağını; 15 yaşını doldurmamış çocuklara sosyal ağ hizmetinin sınırlandırıldığını ve yaş doğrulamasının e-Devlet üzerinden yapılacağını açıklamıştır. Bilgi Teknolojileri ve İletişim Kurumu Başkanı Mehmet Koçyiğit, BTK'nın ilave güvenlik tedbirlerini ciro sınırı olmaksızın tüm işletmecilere zorunlu kıldığını, 5G'de yerli malı oranının

kademeli olarak yüzde 60'a ve milli haberleşme ürünü oranının yüzde 15'e çıkarıldığını, nüfusu 5.000'in altındaki yerleşimlerde ve otoyol, hızlı tren, tünel güzergâhlarında yeni baz istasyonlarının milli ürünlerden temin edileceğini aktarmıştır. Sayın Önal, 5 Mayıs 2026'da toplanan ilk Siber Güvenlik Kurulunun kritik altyapıların korunmasını ve veri egemenliğini, öncelikli gündem yaptığını; Sayın Talay aynı toplantıda savunma sanayiinin kritik altyapı olarak kabul edildiğini belirtmiştir. Sayın Küçük, verinin nerede ve nasıl saklanacağına ilişkin ikincil mevzuatın yakında sektörün görüşüne açılacağını duyurmuştur. Sektör temsilcileri bu düzenlemelerin yatırım ve inovasyon ortamını destekleyecek biçimde, istişareyle şekillenmesi beklentisini dile getirmiştir.

Konferansın ortaya koyduğu öncelikler

Konuşmaların kesişim kümesinden şu başlıklar çıkmaktadır:

1. **Tatbikat ve asgari hizmet listesi.** Her kurum "en kritik hizmetimiz hangisi, çökerse kaç saatte ayağa kalkarız, yedekten en son ne zaman gerçekten döndük, saldırı günü kimi arayacağız" sorularını cevaplamalı; kritik altyapılar için 72 saatlik dış hizmet kesintisi senaryoları gerçek tatbikata dönüştürülmelidir.
2. **Kurumlar arası bilgi paylaşımı.** Gösterge paylaşımının ötesine geçen, saldırıya karşı geliştirilen taktik ve teknikleri kapsayan bir ulusal paylaşım mekanizması kurulmalı; bir kurumun öğrendiği tehdit diğerinin savunmasına dönüşmelidir.
3. **Tedarik zinciri ve bağımlılık envanteri.** Kamu alımlarında fiyat-performansın yanına yerel yönetilebilirlik, dış bağlantı koptuğunda hizmetin sürüp sürmeyeceği ve alternatif müdahale imkânı zorunlu ölçüt olarak eklenmeli; en küçük tedarikçi dahil asgari siber hijyen şartı aranmalıdır.
4. **Tasarımdan itibaren güvenlik ve yerli standartlar.** Platform ve sistem projelerinde siber güvenlik planı kalite planı gibi zorunlu olmalı; platform güvenliği için yerli standart ve rehber dokümanlar ivedilikle hazırlanmalıdır.
5. **Yapay zekâ ve veri egemenliği.** Kurumsal verinin denetimsiz yapay zekâ hizmetlerine aktarılması politika ve onaylı araçlarla yönetilmeli; milli model geliştirme için EVREN benzeri veri ve altyapı girişimleri desteklenmeli; post-kuantum kriptografiye geçiş bugünden planlanmalıdır.
6. **Yerli üreticiye saha açılması.** Savunma sanayiindeki modelde olduğu gibi devlet ilk müşteri ve stratejik yönlendirici olarak yerli siber güvenlik ürünlerini zorlu testlerden geçirip sahada ispat imkânı vermelidir; SAYGEP bu yönde bir adımdır.
7. **İnsan.** Siber güvenlik üst yönetiminin gündemi olmalı; nitelikli insan kaynağının yetiştirilmesi, elde tutulması ve içeriden tehdide karşı güvenilirliğinin sağlanması, teknoloji yatırımıyla eşdeğer önemde ele alınmalıdır.

Kapanış

Konferansın bütününe bakıldığında konuşmacılar farklı kurumlardan, farklı dillerle aynı yere varmıştır. Sayın Önal'ın cümlesi bunu özetlemektedir: savaşı en çok teknolojiye sahip olan değil, en iyi birlikte

hareket edebilen kazanacaktır. Sayın Tancan'ın 3 sorusu, Sayın Yılmaz'ın 72 saati, Sayın Şakar'ın 29 dakikası ve Sayın Kuru'nun "üret, koru, kontrol et" üçlemesi, konferansın katılımcılara bıraktığı somut ev ödevleridir. Bilgi Güvenliği Derneği, Siber Güvenlik Başkanlığının kuruluşuyla birlikte kamu, üniversite ve sektör arasındaki arayüz rolünü sürdürecek; bu raporda derlenen önceliklerin takibini 20. konferansa taşıyacaktır.

Dijital Egemenlik Stratejisi'ne Doğru

Konferansın 3 oturumu ve açılış konuşmaları birlikte okunduğunda, farklı kurumlardan gelen tespitlerin tek bir kavram etrafında toplandığı görülmektedir: dijital egemenlik. Bu kavram, konferansta kapıları kapatmak ya da her teknolojiyi sıfırdan üretmek anlamında kullanılmamıştır. Ortak tanım, bir ülkenin kendi verisi, altyapısı, teknolojisi ve kararları üzerinde söz sahibi olabilmesi; kriz anında kendi ağında karar alabilmesi, hizmetini sürdürebilmesi ve 10 hamle sonra da hamle yapacak alanının kalmış olmasıdır. Aşağıdaki başlıklar, bu tanımın bir strateji belgesine dönüşmesi için konferansın ortaya koyduğu yapı taşlarını sıralamaktadır.

1. Tehdit tanımı: üç boyut, tek cephe

Siber savaş artık harekâtın öncüsü, çoğu zaman da kendisidir. Enerji şebekelerinden uydu haberleşmesine, akaryakıt dağıtımından soğuk zincire kadar fiziksel dünyaya dokunan saldırılar son 10 yılın sıradan olayları hâline gelmiştir. Konferansta tehdit dijital, fiziksel ve bilişsel olmak üzere 3 boyutta tanımlanmış; bilişsel boyut, yani toplumun neye inanacağını bilememesini, en az konuşulan ve en tehlikeli alan olarak işaretlemiştir. Strateji açısından bunun anlamı açıktır: bu 3 alan ayrı kurumlar, ayrı bütçeler ve ayrı dillerle yönetildiği sürece, saldırgan bir adım önde kalmaktadır. Siber güvenlik, dijital devlet ve yapay zekâ yetkilerinin tek çatı altında toplanması, bu yönde atılmış bir adımdır; aynı bütünleşik bakışın bilişsel güvenliği ve kritik altyapıların fiziksel katmanını da kapsaması gerekmektedir.

2. Bağımlılık, tehdit haritasının merkezindedir

Konferansın en sık tekrarlanan dersi, bağımlılıkların düşmandan daha büyük bir zafiyet olabileceğidir. Ortada saldırgan yokken tek bir hatalı güncellemenin havalimanlarını, hastaneleri ve bankaları aynı anda durdurması; e-devlette dünya birincisi bir ülkenin nüfus kaydının bir tedarikçinin "123456" parolasıyla açılması; 2 yıl sabırla kazanılan güvenin bir açık kaynak kütüphanesine arka kapı olarak dönmesi; yasal dinleme sistemlerinin casusluk hedefi olması; 1,5 milyar dolarlık bir hırsızlığın borsaya değil borsanın yazılım tedarikçisinin bilgisayarına girilerek yapılması aynı kalıbı göstermektedir. Saldırgan, hedefin kendisinden önce hedefin güvendiği tarafa yönelmektedir.

Bu nedenle, stratejinin ilk somut işi bir bağımlılık envanteridir. Her kurum hangi uygulamasının dışarıdaki hangi hizmete bağlı olduğunu, hangi lisansın yerelde çalışmayı kilitleyebileceğini, kimlik doğrulama ve DNS hizmetlerinin nereye bağımlı olduğunu, loglarının nerede durduğunu yazılı olarak bilmelidir. Bu envanter altyapı, kontrol katmanı ve kayıt-izleme sistemleri olmak üzere 3 katmanda tutulmalı; teknoloji zincirinin hangi halkasında karar yetkisinin kime bırakıldığı açıkça belirlenmelidir.

3. Dayanıklılık, caydırıcılığın ön şartıdır

Hiçbir sistem yüzde 100 güvenli olmadığına göre güvenliğin ölçüsü, eşik aşıldığında içerideki hayatın devam edebilmesidir. Dayanıklılık 4 aşamada kurulmaktadır: hazırlanmak, direnmek, toparlanmak ve öğrenmek. Bu aşamaların sahadaki karşılığı tatbikattır. Hiç geri yüklenmemiş yedek, yedek sayılmamakta; krizde ilk kez tanışan ekipler kaybetmektedir. Konferansın önerdiği 72 saatlik dış hizmet kesintisi tatbikatı, kritik altyapılar için bir egemenlik testi işlevi görmektedir: ilk 6 saatte bağımlılık haritası, sonraki 18 saatte kurumun kendi ağında karar alma kabiliyeti, 2. ve 3. günde insan, süreç ve tedarik sınanmaktadır. Her tatbikatın çıktısı, kesintiden etkilenmeyen sistemlerin yanında tek noktaya bağlı işlevlerin listesi ve bir asgari hizmet listesi olmalıdır.

Caydırıcılık bu zeminin üzerine kurulmaktadır. Siber alanda atıf ve isnat, uzun ve siyasi bir süreç olduğundan, hangi eylemin silahlı saldırı sayılacağına dair ortak anlayış bulunmadığından ve saldırıların büyük bölümü silahlı saldırı eşiğinin altında kaldığından, caydırıcılığın yalnızca misillemeye ve saldırganı tespit etmeye dayandırılması mümkün görünmemektedir. Saldırganın beklediği faydayı elde edememesi, yani dayanıklılık, caydırıcılığın en güvenilir biçimidir. Buna yetenek, inandırıcılık ve iletişim; gerektiğinde diplomatik, ekonomik ve hukuki araçlar; her durumda da hukuka uygunluk, ölçülülük ve tırmanma riskinin gözetilmesi eklenmelidir. Delilin korunması ve adli sürecin işletilmesi de caydırıcılığın bir parçasıdır.

4. Ulusal bağışıklık: bilgi paylaşımı

Saldırgan tarafta erişim satıcısından hizmet olarak fidye yazılımına uzanan bir iş bölümü ve dayanışma varken, savunma tarafı aynı saldırıyı kurum kurum ayrı analiz etmektedir. Saldırganın ilk erişimden sonra diğer sistemlere geçiş süresinin ortalama 29 dakikaya indiği bir ortamda bu lüks sürdürülebilir görünmemektedir. Konferansın önerisi, gösterge (IP, hash, alan adı) paylaşımının ötesine geçen, bir kurumun saldırıya karşı geliştirdiği taktik ve tekniklerin, diğer kurumların savunmasına dönüştüğü bir ulusal paylaşım mekanizmasıdır. Bir kurumda görülen saldırı ertesi gün başka bir kurumda boşa çıkmalıdır. Bu mekanizmanın kurulması, düzenleyici otoritenin sorumluluğunda olsa da işlemesi kurumların haber vermesine bağlıdır; sessiz kalan kurum zinciri zayıflatmaktadır. Aynı mantık müttefik ülkelerin ulusal SOME'leri arasında protokol beklemeyen paylaşımı da kapsamalıdır.

5. Tedarik zinciri ve alım politikası

40 milyon dolarlık bir platform, 40 dolarlık bir bileşen yüzünden görev kaybı yaşayabilmektedir. Bu orantısızlık, güvenliğin ana yüklenicide bitmediğini; yüzlerce alt sistem üreticisinin, en küçük tedarikçinin ve bakım-yükleme süreçlerindeki taşınabilir ortamların da, zincirin parçası olduğunu göstermektedir.

Savunma sanayiinde başlatılan uygulama, stratejinin geneline yayılabilecek bir model sunmaktadır: her projede kalite planı gibi zorunlu bir siber güvenlik planı, tedarikçiler için asgari siber hijyen şartı ve ürünlerin dayanıklılığının sürekli ölçülüp ispatlandığı bir test-entegrasyon platformu.

Kamu alımlarında ölçüt de buna göre genişlemelidir. Fiyat-performansın yanına yerel yönetilebilirlik, dış bağlantı koptuğunda hizmetin sürüp sürmeyeceği ve alternatif müdahale imkânı, zorunlu şart olarak eklenmelidir. Bugün en uygun fiyatlı görünen ürün yarın bağımlılığa, bugün yetiştirilmeyen mühendis, 5 hamle sonra kurulamayan ekibe, bugün projeye sokulmayan yerli üretici, 10 hamle sonra hiç doğmayan alternatife dönüşmektedir. Her katmanda yerli olmak şart olmasa bile en kötü senaryonun etki zincirinin bilinmesi ve bir B planının bulunması gerekmektedir.

6. Yerli teknoloji: üretimden ispata

Milli teknoloji hamlesi savunma sanayiinde sonuç vermiştir ve bunun yöntemi yerli üreticilere alan açılması olmuştur. Siber güvenlikte de devletin ilk müşteri ve stratejik yönlendirici olarak uzun vadeli sipariş vermesi, ürünleri zorlu testlerden geçirmesi ve sahada ispat imkânı tanıması beklenmektedir. Ancak yerli üretim tek başına güvenliği garanti etmemektedir. 20 ila 50 yıl envanterde kalacak platformlar için bağımsız ve yerli test-değerlendirme süreçleri, yaşam döngüsü boyunca sürekli iyileştirme ve yerli standart ile rehber dokümanlar gerekmektedir; platform güvenliği alanında bu dokümanların yokluğu konferansta açıkça tespit edilmiş bir boşluktur. Haberleşme tarafında 5G'de yerli malı ve milli ürün oranlarının şart koşulması, frekansın milli sistemle izlenmesi ve milli konumlama uydularının fırlatılması, şebekede hangi cihazın çalıştığının bir egemenlik meselesi hâline geldiğini göstermektedir.

7. Veri ve yapay zekâ egemenliği

Veri, yeni çağın en stratejik kaynağı olarak tanımlanmış; nerede barındırıldığı, hangi hukuka tabi olduğu ve kimin erişebildiği bir devlet politikası konusu olarak değerlendirilmiştir. Konferansın bu alandaki en somut uyarısı, yapay zekâ kullanımına ilişkindir. Ekonomik gerekçelerle buluta yönelim ve denetimsiz yapay zekâ araçlarına kurumsal veri aktarımı, casusların aylarca uğraşarak elde etmeye çalıştığı bilgiyi, gönüllü olarak teslim etmek anlamına gelmektedir. Çözüm, yasaklamak yerine onaylı araçlar sunmak, hangi verinin asla girilemeyeceğini tanımlamak ve çalışanları eğitmektir. Kamu içinde kurum verisinin dışarı çıkmadığı yerli dil modellerinin geliştirilebildiği, bu birikimin kurumlar arasında paylaşılabileceği de konferansta ortaya konmuştur.

İkinci uyarı, içeriği bilinmeyen açık kaynak modellerin kritik platformlara entegre edilmesine ilişkindir. Belirli bir koordinat veya tarihte yanlış görmeye başlayacak biçimde tetiklenebilen bir model, milyar dolarlık bir sistemi anlamsız kılabilmektedir. Milli modeller için verinin yurt içinde toplandığı ve yurt dışına çıkmadığı bir veri kütüphanesi ve hesaplama altyapısı bu riskin cevabıdır. Üçüncü başlık kriptografik egemenliktir: "şimdi topla, sonra çöz" tehdidine karşı post-kuantum kriptografiye geçiş, kuantum hesaplamanın yaygınlaşması beklenmeden bugünden planlanmalıdır.

8. İnsan

Konferansta anlatılan olayların hemen hepsi tek bir tıklamayla, açık bırakılan bir oturumla, bir spor uygulamasında paylaşılan konumla ya da sisteme bağlı tutulan bir yedekle başlamıştır; en önemli keşif ise yarım saniyelik bir gecikmeyi araştıran bir mühendisin dikkatiyle yapılmıştır. İnsan hem en zayıf halka, hem de en güçlü savunmadır. Büyük teknoloji şirketleri arasında tek bir araştırmacı için 200 milyon dolara varan transfer bedellerinin konuşulduğu bir dönemde, nitelikli insan kaynağı finansal sermaye kadar stratejik bir varlıktır. Strateji, insan kaynağını yetiştirmeyi, elde tutmayı, hata yapmaktan korkmadan deneyebileceği ortamlar sunmayı ve içeriden tehdide karşı güvenilirliğini sağlamayı teknoloji yatırımıyla eşdeğer bir başlık olarak ele almalıdır. Siber güvenlik ayrıca bilgi işlem biriminin köşesinden çıkarılıp yönetim kurullarının, bakanlıkların ve rektörlüklerin gündeminin ilk sıralarına taşınmalıdır; bu bir liderlik sorumluluğudur.

Sonuç

Kurumsal çerçeve kurulmuş, kanun çıkmış, ilk kurul toplanmış, strateji ve eylem planı yürürlüktedir. Konferansın bütünü bu çerçevenin bir başlangıç olduğunu ve asıl işin kamu, akademi ve sektörün birlikte çalıştığı bir ekosisteme dönüşmek olduğunu söylemektedir. Konulan kural hayata geçmiyorsa ,konulmamış sayılmaktadır. Dijital egemenlik, ancak bir pazartesi sabahı dış hizmetler kesildiğinde ayakta kalabilen kurumlarla, bugün verilen alım kararlarının 10 hamle sonrasını hesaplayan bir politikayla ve bir kurumun öğrendiğini diğerine aktaran bir paylaşım kültürüyle, ölçülebilir bir hedef hâline gelecektir.