

ISCTurkey 2026 – 19. Uluslararası Bilgi Güvenliđi ve Kriptoloji Konferansı

Açılış Günü Konuşma Metinleri (20 Ekim 2026, BTK Konferans Salonu, Ankara)

AÇILIŞ KONUŞMALARI

00:05:35 Prof. Dr. Mustafa ALKAN – Bilgi Güvenliđi Derneđi Yönetim Kurulu Başkanı

Sayın Bakanım, sayın başkanlarım, Sayın Yargıtay Başkanım, saygıdeđer komutanlarım, sayın rektörlerim, kamu kurum ve kuruluşlarımızın ve sektörümüzün çok deđerli yöneticileri, çok kıymetli katılımcılar, sevgili öğrenciler. Bilgi Güvenliđi Derneđi olarak bu yıl 19'uncusunu gerçekleştirdiđimiz Bilgi Güvenliđi ve Kriptoloji Konferansı'na hoş geldiniz diyor, hepinizi saygıyla, hürmetle selamlıyorum.

Bilgi Güvenliđi Derneđi olarak 19 yıldır siber güvenlik alanında faaliyetlerimizi kesintisiz bir şekilde sürdürmeye çalışıyoruz. İlk kurulduğumuzdan bugüne kadar birçok kamu kurum ve kuruluşumuzla, üniversitelerimizle ve sektörümüzle birlikte, öncelikle Türkiye'de siber güvenlik konusundaki farkındalıđı en yüksek seviyeye çıkarabilmek için yoğun faaliyet gösterdik ve çaba sarf ettik. Bu noktada epey bir mesafe katettiđimizi, ülke adına epey bir yol aldığımızı söyleyebiliriz.

İkinci temel amacımız, kuruluşumuzdan bugüne kadar siber güvenlik konusunda ülkemizin ihtiyaç duyduğu insan kaynağının yetiştirilmesine katkı sağlamak idi. Bu konuda da 19 yıldır yapmış olduğumuz eğitimler, yaz kampları, kış kampları, siber güvenlik çalışmalarıyla önemli ölçüde insan kaynağının yetiştirilmesine de katkı sağladığımızı düşünüyorum.

Bir üçüncü misyon olarak kendimize görev edindiğimiz, ülkemizin yine ihtiyacı olan siber güvenlik sektörünün güçlenmesi, büyümesi, özellikle yerli ve milli çözümlerle siber güvenlik alanındaki ulusal güvenliđimizin sağlanması açısından sektörümüzün desteklenmesi, yerli ve milli çözümlerin geliştirilmesi noktasında da yoğun çalışmalarımız, faaliyetlerimiz oldu. Bu konuda da Türkiye olarak çok önemli noktalara, mesafelere gelindi. Bundan dolayı da son derece mutluyuz.

Bir diđer önemli husus: Türkiye'mizde, malum, siber güvenlik konusunda, yetki konusunda kurumlar arasında birtakım problemler vardı. En çok istediğimiz şey, Türkiye'de siber güvenlik özelinde düzenleyici bir otoritenin bulunması ve o otorite sayesinde Türkiye'nin politikalarının, stratejilerinin ve siber güvenlik alanındaki faaliyetlerinin yürütülmesi konusu idi ki bu konuda da her ortamda, her platformda Bilgi Güvenliđi Derneđi olarak yoğun çaba sarf ettik. Günün sonunda Türkiye'de Siber Güvenlik Başkanlığının kurulmuş olması gerçekleşti. Bu, ülkemiz için son derece önemli bir konu. Bu vesileyle Siber Güvenlik Başkanlığımıza hayırlı olmasını diliyoruz. Sayın Bakanımızın, Sayın Başkanımızın nezdinde bu kurumumuzun siber güvenlik alanında

bundan sonraki faaliyetleri etkin bir şekilde, yetkin bir şekilde, yetkili bir şekilde ve geniş imkânlarıyla eksik kalan, yapılması gerekenleri çok ileri seviyede yapacağı konusunda son derece inanıyoruz ve bunun gerçekleşmesinden de büyük mutluluk duyuyoruz.

Bir başka mutluluğumuz, böyle bir başkanlığın kurulmasıyla beraber Bilgi Güvenliği Derneği olarak biz de kendimizi bundan sonra daha rahat hissedeceğiz ve şimdiye kadar bizim kısıtlı imkânlarla, sınırlı imkânlarla gerçekleştirmeye çalıştığımız bu faaliyetleri Siber Güvenlik Başkanlığımız inşallah çok daha etkin, yetkin bir şekilde gerçekleştirecek. Bundan sonra Bilgi Güvenliği Derneği olarak biz inşallah sektör, üniversite ve kamu arasında bir arayüz olma noktasında faaliyetlerimizi sürdürmeye çalışacağız.

2007 yılından beri bize ev sahipliği yapan Bilgi Teknolojileri ve İletişim Kurumuna, geçmiş bütün yöneticilerine ve çalışanlarına bu vesileyle bir kez daha teşekkür etmek istiyorum. Bu, bizim buradaki son etkinliğimiz olacak. İnşallah bundan sonraki etkinliklerimizi Orta Doğu Teknik Üniversitesi ev sahipliğinde yapıyor olacağız. Sayın Rektörümüze buradan, huzurlarınızda teşekkür etmek istiyorum. Bu alanda Rektörümüz çok ciddi faaliyetler, çalışmalar gerçekleştirdi. Hem Türkiye’de hem Kıbrıs’ta siber güvenlik alanında bölümler açılması noktasında çok yoğun çalışmalar yaptı. İnşallah, Allah nasip ederse önümüzdeki yıl ODTÜ ile birlikte, Sayın Rektörümüzün destekleriyle 20’ncisini orada gerçekleştiriyor olacağız.

Ben bu vesileyle 20 yıldır bize destek veren, katkı veren, kuruluşumuzdan bugüne kadar emeğini esirgemeyen bütün dernek yöneticilerimize, başkanlarımıza, çalışanlarımıza, bize destek veren sektörümüzün çok değerli kurumsal üyelerine, tüm temsilcilerine, başta Ulaştırma Bakanlığıımız olmak üzere Sayın Bakanımıza bir kez daha şükranlarımı arz etmek istiyorum. Yıllardır bizi hiç yalnız bırakmadı, bize her türlü alanda destek verdi, güç verdi. Aynı şekilde kurum ve kuruluşlarımız, bakanlıklarımız, yedi tane üniversitemiz sürekli bizimle birlikte bu çalışmalar içerisinde yer aldı. Herkese çok teşekkür ediyorum.

Sayın Bakanım, zamanınızın sınırlı olduğunu biliyorum ama konferansımızın ana temasının siber güvenlik ve siber savaşlar olduğu noktasından hareketle birkaç cümleyle de sözlerimi bitirmek istiyorum. Sayın Bakanım, değerli konuklar; hepimiz biliyoruz ki dünya, siber savaşların yoğun bir şekilde gerçekleştiği yeni bir dünya düzenine girdi.

Siber savaş dediğimizde bizim aklımıza en büyük siber savaş olarak WikiLeaks gelir. WikiLeaks, ABD’nin en büyük siber savaş denemesidir. ABD, WikiLeaks’te şu üç noktayı denedi. Birincisi: bilgi ve iletişim teknolojilerini kullanarak, interneti kullanarak, sosyal medyayı kullanarak ülkeler üzerinde nasıl bir savaş elde ederim, ülkeleri nasıl çökertirim ve ülkeleri nasıl ele geçiririm, bunu test etmek istedi. İkincisi: WikiLeaks’le, eğer ABD’ye yönelik böyle bir siber savaş ve siber saldırı olursa, internet ve sosyal medya kullanılarak ABD’ye yönelik bir saldırı gerçekleşirse ABD olarak ulusal güvenliğini nasıl sağlarım, bunu test etti. Üçüncüsü de iletişim teknolojilerini, internet teknolojilerini, sosyal medya teknolojilerini kullanma yeteneğim nedir, bunu test etti.

Ve nitekim ilk uygulamayı biliyorsunuz: Tunus’ta başlayan bir olayla birlikte, Tunus’ta ortaya çıkan iç kargaşa ve iç savaşlar sonucu bütün Orta Doğu’ya yayılan, 14 İslam ülkesini yerle bir eden, ekonomik anlamda ve siyasi anlamda çökerten bir sonuç ortaya

çıktı. Buna da Arap Baharı dendi. Şimdi aynısı Avrupa'da uygulanmaya başladı. İkinci fazı, İsrail'e en çok karşı olan, geçen günlerde İspanya ile başlayan, sonra Fransa'yla devam eden, sonra İtalya'ya geçen ve beklentimiz odur ki bütün Avrupa'ya, Orta Doğu'da Arap Baharı'nda olduğu gibi yayılmak suretiyle Avrupa'yı kasıp kavuran bir savaşa, siber savaşa doğru gidiliyor olmasıdır ki bu, son derece önemli bir sonucun ve sürecin başlangıcıdır.

Asıl önemli olan konu ise yakın gelecekte aynı savaşla, aynı tehditle Türkiye olarak bizlerin de karşı karşıya kalacak olmasıdır. Avrupa beş yıl önce bu tehdidi gördü ve ciddi bir proje başlattı; "Böyle bir savaş karşısında siber egemenliğimizi, siber direncimizi, dijital dayanıklılığımızı nasıl sağlarız?" diye beş yıldır çalışmasını yapıyordu. Demek ki yetmemiş ki başarılı olamadı ve Avrupa şimdi kaynamaya başladı. O yüzden bizim de böyle muhtemel saldırılara, savaşlara karşı dijital egemenliğimizi, siber bağımsızlığımızı, siber dayanıklılığımızı, dijital direncimizi nasıl artırmamız gerektiği noktasında bugünden tezi yok, bütün kurum ve kuruluşlarımızla birlikte ciddi bir proje, ciddi bir çalışma başlatmamız ülkemizin ulusal güvenliği açısından son derece önem arz ediyor.

Bu açıdan, hazır bütün kurum ve kuruluşlarımız ve yöneticilerimiz, başta Sayın Bakanımız burada olmak üzere, bizim ivedilikle önümüzdeki süreç içerisinde muhtemel böyle bir tehdit karşısında ulusal güvenliğimizi sağlayabilmek için dijital direncimizi, dijital dayanıklılığımızı, siber dayanıklılığımızı ve siber egemenliğimizi sağlayacak çalışmalara başlamamız gerekiyor. Biz Bilgi Güvenliği Derneği olarak 20 yıldır yaptığımız gibi bu konunun sürekli gündemde olması, canlı tutulması, ulusal güvenliğimiz, milli güvenliğimiz açısından siber güvenliğin önemini ve önemini her ortamda, her platformda gündeme getirme, dile getirme çabası ve gayreti içerisinde olacağız.

Ben bu vesileyle bu etkinliğimize katkı veren, destek veren başta Sayın Bakanımız, Bakanlığımız ve tüm kurum ve kuruluşlarımız olmak üzere teşekkürlerimi, şükranlarımı arz ediyorum. Etkinliğimizin sağlıklı, başarılı bir şekilde tamamlanmasını diliyorum, hepinizi en derin saygılarımla selamlıyorum.

00:15:32 Prof. Dr. M. Tuncay GENÇOĞLU – Konferans Başkanı

Kıymetli protokol üyeleri, muhterem bilim insanları, saygıdeğer konuklar, çok sevgili öğrencilerim; Fransa'dan, Finlandiya'dan ve İspanya'dan aramızda bulunan kıymetli proje ortaklarımız; gönül coğrafyamızdan aramızda bulunan kıymetli dostlar. 19'uncusunu icra edeceğimiz Bilgi Güvenliği ve Kriptoloji Konferansı'na teşriflerinizden dolayı şükranlarımı sunuyorum. Hoş geldiniz, şeref verdiniz.

Kıymetli hazırun, 19 yıldır bilgi güvenliğini konuşuyoruz. Bugün ise bilginin, güvenin istiklal ve istikbalini müzakere etmek üzere bir aradayız. Bu müzakerelerimizi yarınki akademik sunumlarımızla inşallah daha da öteye götüreceğiz.

Konferansımızın bu yılki teması, bilindiği üzere, siber savaş. Bu temamız çağımızın geçirdiği köklü dönüşümün bir tezahürüdür. Zira siber güvenlik; ulusal egemenliğin, stratejik bağımsızlığın ve geleceği tayin etme kudretinin asli unsurlarından biridir. Yapay zekâ ve kuantum teknolojilerinin dönüştürdüğü bu yeni dünyada biz inanıyoruz ki

istikbalin güvenliği, yalnızca tehditlere mukabele edenlerin değil, güvenin yeni mimarisini ilim, akıl ve irfanla inşa edenlerin eseri olacaktır. Ülkemizin bu dönüşümde yalnızca takip eden değil, yön verenler arasında yer alacağına inancım tamdır.

Bu duygu ve düşüncelerimle, teşrifleriyle bizleri onurlandıran siz kıymetli konuklarımıza, kıymetli bilim insanlarımıza, katkı sunan tüm paydaşlarımıza ve hassaten özveriyle, arka planda büyük emeklerle buraya gelmemizi sağlayan değerli çalışma arkadaşlarımıza şükranlarımı arz ediyorum. 19. Bilgi Güvenliği ve Kriptoloji Konferansımızın ülkemiz, bilim dünyamız ve insanlığın müşterek istikbali için hayırlara vesile olmasını Cenab-ı Hak'tan niyaz ediyor, hepinizi hürmet ve muhabbetle selamlıyorum.

00:18:55 Prof. Dr. Ahmet YOZGATLIGİL – Orta Doğu Teknik Üniversitesi Rektörü

Çok kıymetli Bakanım, kıymetli Bakan Yardımcım, Siber Güvenlik Başkanım, Bilgi Teknolojileri ve İletişim Kurumumuzun Sayın Başkanı, kıymetli rektörüm, rektörlerim, Bilgi Güvenliği Derneğimizin kıymetli başkanı, değerli konuklar, kıymetli meslektaşlarım, sevgili öğrenciler; hepiniz hoş geldiniz.

Siber güvenlik, Başkanımız da söyledi, zaten ülkemizin milli güvenliğinin, ekonomik gücünün ve teknolojik bağımsızlığının en önemli unsurlarından biri. Bilimsel birikimimizi, kritik altyapılarımızı ve savunma sistemlerimizi korumak, Türkiye'nin üretme ve kendi geleceği hakkında karar verme gücünü korumaktır. Bu alanda güçlü olmamız çok kritik. Biz bilimsel yetkinlik, nitelikli insan kaynağı ve kendi teknolojilerimizi geliştirme kapasitemizi bu alanda mutlaka kullanmalıyız.

Biz Orta Doğu Teknik Üniversitesi olarak çalışmalarımızı bu sorumlulukla yürütüyoruz. Uygulamalı Matematik Enstitümüz 2002'den bu yana kriptografi alanında araştırmacılar yetiştiriyor. Kuantum sonrası kriptografi çok kritik bir konu; bu konudaki çalışmalarımızla geleceğin güvenlik ihtiyaçlarına şimdiden hazırlanıyoruz. Enformatik Enstitümüzde, Ankara'da siber güvenlik yüksek lisans programımız var. Çok sayıda mezunumuz ve laboratuvarlarımızla ülkemizin ihtiyaç duyduğu uzmanları yetiştiriyoruz. Ağ ve donanım güvenliğinden veri mahremiyetine kadar uzanan alanlarda araştırmalar yürütüyoruz. Tabii ODTÜ Teknokent, kıymetli Bakanım, çok önemli bir ekosistem. Burada siber güvenlik alanında firmalarımız ve hızlandırma programlarımız aracılığıyla bu birikimin ürüne dönüşmesini, kamu ve sanayinin ihtiyaçlarıyla buluşmasını destekliyoruz.

Sayın Bakanım, biz bu kapasiteyi Kuzey Kıbrıs Kampüsümüzde de geliştiriyoruz. Adalar, özellikle siber güvenlik alanındaki çalışmalar için çok uygun yerlerdir. Biz burada siber güvenlik mühendisliği lisans programını hayata geçirdik. Burada öğrencilerimizi kriptografi, ağ güvenliği, güvenli yazılım geliştirme ve sayısal adli inceleme alanlarında yetiştiriyoruz. Yine bilgisayar ve yazılım mühendisliği programlarımızla ve yapay zeka mühendisliği yüksek lisans programımızla bu eğitim ve araştırma ortamını güçlendiriyoruz. Tabii bugün aslında Kuzey Kıbrıs Kampüsümüzden öğrencilerimiz de aramızda; onları da bu önemli toplantıya katılmaları için adadan getirdik. Biz hem Ankara'daki hem de Kuzey Kıbrıs'taki birikimimizi kamu kurumlarımız ve sanayimizle ortak araştırmalara ve uygulanabilir çözümlere dönüştürmeyi çok önemsiyoruz.

Türkiye'nin güvenli dijital geleceğine yetiştirdiğimiz insanlarla ve geliştirdiğimiz teknolojilerle katkı sunmaya inşallah devam edeceğiz. Ben 19. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nı düzenleyen Bilgi Güvenliği Derneği'ne, kıymetli başkanına ve Siber Güvenlik Başkanlığımıza, ev sahipliği için de yine Bilgi Teknolojileri ve İletişim Kurumumuza teşekkür ediyorum. İnşallah, Başkanımız da açıkladı, gelecek sene, kıymetli Bakanım, sizleri ODTÜ'de ağırlamaktan büyük onur duyacağız. Hepinize saygı ve hürmetlerimi sunuyorum.

00:22:10 Mehmet KOÇYİĞİT – Bilgi Teknolojileri ve İletişim Kurumu Başkanı

Sayın Bakanım, Sayın Bakan Yardımcım, Bilgi Güvenliği Derneği'nin değerli yöneticileri, Sayın Siber Güvenlik Başkanım, kıymetli misafirler, sevgili gençler. Sizleri kurumumuzda ağırlamaktan memnuniyet duyuyor, hepinizi şahsım ve kurumum adına saygıyla selamlıyorum.

Teşrifleriyle bizleri onurlandıran Sayın Bakanımıza, Bilgi Güvenliği Derneği'ne ve konferansın bu yılki paydaşı Siber Güvenlik Başkanlığımıza şükranlarımı sunuyorum.

Bu yılın teması “Yeni Dünya Düzeninde Siber Savaşlar”. Bugün bu savaşlar bir yazılım açığıyla da, bir sinyal karıştırıcıyla da son derece hızlı ve görünmez biçimde sürüyor. Bir sabah okulunuzun sitesine girmeye çalıştığınızı düşünün: sayfa açılmıyor. Belediyenin sitesi de açılmıyor. Hastanenin randevu sistemi de; bir yerlerden binlerce bilgisayar aynı anda aynı kapıya yüklenmiş ve kapı kilitlenmiş. Avrupa Birliği Siber Güvenlik Ajansı'nın Eylül ayında yayınladığı rapora göre geçen yıl Avrupa Birliği'ni etkileyen siber olayların yarısından fazlası tam olarak buydu. En çok hedef alınan sektör de kamu sektörüydü.

Sayın Bakanım, haberleşme altyapımızı güvenle büyütmek için Mart ayında aldığımız kurul kararıyla ilave güvenlik tedbirlerini, net satış tutarlarına bakılmaksızın tüm işletmecilerimiz için zorunlu hale getirdik. 6 Şubat depremlerinin tecrübesinden hareketle 5G yetkilendirmesinde işletmecilerimize, afet anında sahaya hızla ulaşılabilecek bir haberleşme gücünü hazır tutma yükümlülüğü getirdik. Bunun yanı sıra olağanüstü durumlar için de işletmecilerimiz beş yılın sonunda uydu bağlantısıyla çalışabilen 450 mobil baz istasyonunu hazır tutmakla yükümlüdür.

Değerli katılımcılar, geçtiğimiz hafta Washington'da katıldığımız MILCOM 2026'da yeni dünya düzeninin haberleşme cephesini yakından gördük. Elektronik karıştırmanın yapay zeka ile tespiti, GPS sinyallerinin karıştırıldığı ortamlarda yakın yörünge uydularıyla konumlama ve kuantum bilgisayarlara dayanıklı şifreleme, konferansın en konuşulan başlıklarıydı. Ülkemiz bu yarışın seyircisi değil. Bugün gururla ifade etmeliyim ki ASELSAN ile birlikte geliştirdiğimiz Milli Monitör Sistemi frekanslarımızı gece gündüz izliyor ve izinsiz yayınları ihbara gerek kalmadan tespit ediyor. Enterferans konum tespit teknolojimiz dünyanın en gelişmiş sistemlerinden biri.

Fergani Uzay, ULUBEY Küresel Konumlama Sistemi için milli uydularımızı ardı ardına uzaya gönderiyor. Çünkü artık biliyoruz ki LEO olarak da bilinen yakın dünya yörüngesi, yeni nesil yüksek hassasiyetli navigasyon teknolojilerinde yeni bir dönemin küresel oyun sahasıdır. Türkiye'yi bu büyük yarışa dahil eden, bu muazzam vizyonu ortaya koyan

başta Sayın Selçuk Bayraktar olmak üzere tüm Fergani ekibini yürekten tebrik ediyorum.

Şebekemizde hangi cihazın çalıştığı da artık bir egemenlik meselesi. Bu nedenle 5G'de yerli malı oranının kademeli olarak yüzde 60'a, milli haberleşme ürünü oranının yüzde 15'e çıkmasını şart koştuk. Eylül ayında aldığımız kurul kararıyla da nüfusu 5.000'in altındaki yerleşim yerleri, otoyol, hızlı tren hattı ve tünel gibi güzergâhlarda yeni kurulacak baz istasyonlarının milli haberleşme ürünü tanımına uygun ürünlerden temin edilmesine karar verdik.

Kıymetli misafirler, Sayın Cumhurbaşkanımızın liderliğinde yürütülen Milli Teknoloji Hamlesi ile savunma sanayiinde kazandığımız bağımsızlığı haberleşmede de kazanmakta kararlıyız. Kendi şebekesini kendi ürünüyle kuran, kendi frekansını kendi gözüyle izleyen ve kendi uydusuyla yolunu bulan bir Türkiye, Türkiye Yüzyılı'nın en sağlam teminatı olacaktır. Bu anlayışla Siber Güvenlik Başkanlığımız ve tüm paydaşlarımızla omuz omuza çalışmaya devam edeceğiz.

Konferansın düzenlenmesinde emeği geçen herkese teşekkür ediyor, iki gün sürecektir oturumların ülkemiz için hayırlı sonuçlar doğurmasını temenni ediyor, hepinizi saygıyla selamlıyorum.

00:26:47 Ümit ÖNAL – Cumhurbaşkanlığı Siber Güvenlik Başkanlığı Başkanı

Sayın Bakanım, Bakan Yardımcım, Bilgi Teknolojileri Kurumu Başkanım, çok değerli başkanlarım, kıymetli komutanlarım, kamu kurumlarımızın çok değerli yöneticileri, kıymetli akademisyenler, sektörümüzün öncüleri, sevgili gençler, hanımefendiler, beyefendiler; hepinizi saygıyla, muhabbetle selamlıyorum. Böylesine kıymetli bir toplulukla bir arada olmanın memnuniyetini yaşadığımı ifade ederek sözlerime başlamak istiyorum.

Dünya, güvenlik kavramının yeniden tanımlandığı tarihsel bir eşikten geçiyor. Yeni dünyanın güvenlik denklemi dijital alanı, fiziksel dünyayı ve bilişsel alanı birlikte anlamayı gerektiriyor. Bu denklem gelecekte yaşanabilecek bir ihtimal değil; bugünün jeopolitik güç mücadelesinin aslında yeni bir formu. Artık geleceğe ait bir öngörü değil, bugünün gerçekliğini konuşuyoruz. Çünkü siber savaş artık bir senaryo değil, bir haber başlığı da değil; sabah uyandığımızda kullandığımız telefonda akşam yatarken kapattığımız ışığa kadar günlük hayatımızın içinde.

Bu yüzden bugün, bu konferans vesilesiyle, sizinle aslında üç soru etrafında düşüncelerimi paylaşmak istiyorum. Birinci soru: Dünya nasıl bir yöne evriliyor? İkincisi: Bu yeni düzende tehdit tam olarak nerede duruyor? Üçüncüsü ve en önemlisi de: Biz ne yapmalıyız? Bu üç soru etrafında biraz konuşmak istiyorum.

20. yüzyılda güç toprakla, çelikle, petrole ölçülüyordu. 21. yüzyılda güç veriyle, algoritmayla, hesaplama kapasitesiyle ve en önemlisi bunlara kimin hükmettiğiyle ölçülüyor. Son birkaç yılda hep birlikte izledik: Jeopolitik gerilimlerin olduğu her yerde bir siber cephe de açıldı. Doğu Avrupa'daki savaşta ilk kurşun atılmadan önce kritik sistemlere yönelik siber operasyonlar çoktan başlamıştı. Orta Doğu'daki çatışmalarda

bankalar, kamu hizmetleri ve haberleşme altyapısı hedef alındı. Küresel telekomünikasyon ağlarına sızan, yıllarca fark edilmeden kalan operasyonlar gördük. Denizin altındaki iletişim kablolarında yaşanan şüpheli olaylar, uydu ve konum sistemlerine yönelik karıştırma ve aldatma faaliyetleri artık sıradan olaylar. Ve 2024 yazında tek bir hatalı yazılım güncellemesinin milyonlarca cihazı nasıl çökerttiğini; havalimanlarını, hastaneleri, bankaları aynı anda nasıl felç ettiğini hep birlikte gördük. Ortada bir saldırgan bile yoktu. Bu bize çok önemli bir şeyi söyledi: Bağımlılıklarımız, düşmanlarımızdan daha büyük bir zafiyet olabilir.

Bu konuşmayı hazırlarken gündeme gelen, henüz soğmamış bir olay var hepimizin zihinlerinde; hâlâ artçıları da medyadan okuyoruz. Onu da paylaşmadan geçmiş olmak istemiyorum. Fransa'da bir market zincirine, hatta bir değil birkaç market zincirine ait yüzlerce soğutma sistemine sızan saldırganlar, biliyorsunuz, buzdolaplarının sıcaklık derecelerini uzaktan değiştirdi. Soğuk zinciri bozulan dondurulmuş ürünler imha oldu, doğal olarak kullanılamaz hale geldi. Ortada kilitlenmiş bir ekran yok, fidye ya da fidye yazılımı yok, fidye notu yok. Sadece bir ülkenin gıda tedarik zincirine uzaktan yapılan sessiz bir müdahale var. Bu artık bir bilgisayarın değil, aslında sofranın güvenliği meselesi haline geldi.

Dijital cephede de tablo çok farklı değil. Eylül ayında kripto varlık saldırılarında yaklaşık 768 milyon dolar çalındı ve Eylül, 2026'nın en kötü ayı oldu. Kayıpların büyük bir kısmı iki olaydan geldi; bunlardan birinde izlerin bir devlete çıktığını hep beraber gördük. Yani siber suçla jeopolitik güç mücadelesi artık iç içe geçmiş durumda. Bunun adı siber olay da değil artık; stratejik bir gerçeklik.

Siber uzay; kara, deniz, hava ve uzaydan, bildiğimiz uzaydan sonra beşinci harekât alanı olarak artık tanımlanıyor. Ben bu tanıma bir adım daha öteye götürüyorum ve siber uzayı diğer dört alanın hepsinin sinir sistemi olarak tanımlıyorum. Onu kaybeden, aslında diğerlerinin hepsini kaybetmeye açık hale gelir.

Şimdi ikinci soru: Tehdit nerede? Geleneksel bakış açımız siber güvenliği sunucuların, ağların ve yazılımların güvenliği olarak görüyordu. Bu bakış bugün artık yetersiz. Ben tehdidi üç boyutta görüyorum.

Birinci boyut dijital boyut. Evet, bildiğimiz alan: kötü amaçlı yazılımlar, fidye saldırıları, veri sızıntıları, tedarik zinciri saldırıları. Burada oyunun kurallarını değiştiren şey ne? Yapay zeka. Saldırganlar artık yapay zekayı keşif yapmak, kod yazmak, ikna edici sahte içerikler üretmek ve hatta saldırıları otonom bir şekilde yönetmek için kullanıyor. Elbette savunmada da aynı teknoloji bizim en büyük müttefikimiz; bu tartışmasız. Ama şunu unutmayalım: Bu yarışta hız artık insan hızı değil, makine hızı. Bir yandan da kuantum bilgisayarların bugün güvendiğimiz şifreleme sistemlerini gelecekte tehdit edeceği gerçeğiyle yaşıyoruz. Bugün çalınan şifreli bir veri, yarın çözülmek üzere bir yerde bekletiliyor olabilir. Buna "şimdi topla, sonra çöz" yaklaşımı deniyor. Bildiğiniz gibi, hazırlığımızı bugünden yapmak zorundayız.

Dijital boyuttan sonra ikinci boyut fiziksel boyut. Artık bir bit bir atomu devirebiliyor. Enerji şebekeleri, su arıtma tesisleri, ulaşım sistemleri, sağlık cihazları, liman ve havayollarının otomasyonları, akıllı şehirler; hepsi birbirine bağlı, hepsi hedef. Bir hastanede ameliyat robotunun, bir barajda kapakların, bir rafineride vananın arkasında

artık bir yazılım var. Az önce anlattığım Fransa örneği tam da bu. Siber saldırı bugün fiziksel hasar, hatta can kaybı üretebilecek bir araç. Denizaltı kabloları, veri merkezleri, baz istasyonları gibi fiziksel altyapılar da artık siber stratejimizin ayrılmaz bir parçası. Biraz evvel Başkanımız ifade etti: Siber güvenlik bilgisayar odasının, sistem odalarının dışına çıktı; ülkenin bütün coğrafyasında.

Üçüncü boyut bilişsel boyut. Bence en az konuşulan ama en tehlikeli boyut, bilişsel boyut. Burada hedef makineler değil; insan zihni ve toplum algısı. Dezenformasyon kampanyaları, algı operasyonları, yapay zeka ile üretilmiş sahte ses ve görüntüler, sosyal medya algoritmalarıyla yönlendirilen toplumsal öfke. Bir sahte videonun bir ülkenin borsasını sarsabildiği, bir seçim dönemini zehirleyebildiği, bir kriz anında toplumu paniğe sürükleyebildiği bir çağdayız. Bir toplumun neye inanacağını bilmemesi en büyük güvenlik açığı. Çünkü güveni kaybeden toplum, en iyi firewall'a sahip olsa bile içeriden çöker.

Değerli konuklar, bu üç boyut birbirinden ayrı değil, iç içe. Bir saldırgan dijital bir saldırıyla fiziksel bir sistemi durdurur, ardından bilişsel bir kampanyayla toplumda panik yaratır. Biz bu üç alanı hâlâ ayrı ayrı kurumlarla, ayrı bütçelerle, ayrı dillerle yönetiyorsak saldırgan her zaman bizden bir adım önde.

Şimdi konuşmamın merkezine geliyorum. Sayın Bakanım, biraz uzattığımı da farkındayım; ama böylesine müstesna bir topluluğu bulmuşken ben de fırsatı değerlendirmek istiyorum. Dijital egemenlik, konuşmamın merkezi. Kimi zaman bu kavram yanlış anlaşılabilir. Dijital egemenlik kendimizi dünyadan soyutlamak değil; kapılarımızı kapatmak hiç değil. Küresel bir çağın içindeyiz, ağın içindeyiz ve öyle kalacağız. Dijital egemenlik; kendi verimiz, kendi altyapımız, kendi teknolojimiz ve kendi kararlarımız üzerinde söz sahibi olabilmek.

Kendimize şu soruları soralım. Bu soruları sadece Türkiye için sormayalım; bunlar genel, jenerik sorular. Ülkenin en hassas verisi kimin sunucusunda duruyor? Kritik sistemlerimizin yazılımı kim tarafından güncelleniyor, kim durdurabiliyor? Bir kriz anında hangi hizmetlere erişimimizin kesilmeyeceğinden emin olabiliyoruz? Yapay zeka modellerimiz hangi veriyle, kimin kuralıyla eğitiliyor? Bu soruların cevabı bize ait değilse, o zaman elimizdeki şey, evet, konfor; ama egemenlik hiç değil.

Dijital egemenliğin beş ayağı olduğuna inanıyorum. Altı, yedi, sekiz de olabilir; ben beş olduğuna inanıyorum. Birincisi veri egemenliği. Verinin nerede durduğu, kimin hukukuna tabi olduğu, kimin erişimine açık olduğu stratejik bir karar; veri egemenliği, dijital egemenliğin en önemli ayaklarından biri. İkincisi, siber dayanıklılık ve caydırıcılık. Dijital altyapılarımızı yıkıcı etkilere karşı korumak, akıllı savunma; ama savunma yetmez, akıllı taarruz yetenekleriyle caydırıcılık sağlamak da yine en kritik bileşen. Üçüncüsü, teknoloji egemenliği. Yerli ve milli çözümler sadece yazılım ve donanım üretmek değil; çip tasarımı, işletim sistemine, kriptografiden bulut altyapısına kadar kritik teknolojileri kendi kabiliyetlerimizle geliştirmek demektir. Dördüncüsü, bilişsel egemenlik. Dijital platformlar, algoritmik sistemler ve organize etki faaliyetlerinin bilişsel, psikolojik ve sosyolojik etkilerine karşı bireylerin ve toplumun bağımsız düşünme, bağımsız karar verme ve irade oluşturma kapasitesini de korumak zorundayız. Beşincisi, normatif egemenlik. Yani uluslararası siber normların, standartların ve

kuralların şekillendirildiği masada yer almak, bunlara etki edebilmek. Kuralları başkaları yazarsa biz onları sadece uyguluyoruz.

Türkiye bu yolda önemli adımlar atıyor ve bu adımların bir kısmı daha yakın zamanda atıldı. 5 Mayıs 2026'da, Siber Güvenlik Başkanlığı kurulduktan sonraki ilk Siber Güvenlik Kurulu toplandı; önümüzdeki günlerde de ikincisi yapılacak. Siber Güvenlik Kurulu, kritik altyapıların korunmasını ve yerli ve milli teknolojilerde kapasite geliştirmeyi öncelikli olarak ele aldı. Aynı toplantıda veri egemenliği ayrı bir başlık olarak masaya yatırıldı; verinin yalnızca teknik bir unsur değil, stratejik bir değer olduğu da vurgulandı. Yani artık konuşulan şey bir teknoloji tercihi değil, bir devlet politikası haline geldi.

Siber Güvenlik Başkanlığının görev tanımına dijital devlet alanı da eklendi. Kamuda yapay zeka uygulamalarına yönelik yetkiler de yine Siber Güvenlik Başkanlığı çatısı altında toplandı. Bu şu demek: Siber güvenlik, dijital dönüşüm ve yapay zeka ayrı ayrı masalarda değil, aynı masada konuşuluyor. Konuşmamın başında üç boyutun iç içe olduğunu söylemiştim; kurumsal yapı da bu gerçeğe göre şekillendi. Üstelik bu çerçeve insana yatırımla da besleniyor. Başkanlığımız siber tehdit istihbaratından adli bilişime, yapay zekadan kritik altyapı güvenliğine tam 47 farklı görev alanında uzman personel alımı yapmakta. Bu, dijital egemenliğin üçüncü ayağıyla, yani insan kaynağıyla ilgili çok somut bir işaret. Ancak bir kanun, bir kurum, bir alım süreci yolun sadece başlangıcı. Asıl mesele, bu çerçeveyi kamu, akademi ve özel sektörle gerçekten çalışan bir ekosisteme dönüştürmek; buna ihtiyacımız var.

Şimdi üçüncü soruya ve nihayet konuşmamın sonlarına doğru geliyorum: Ne yapmalıyız? Yine birkaç çağrıda bulunmak istiyorum.

Birinci çağrım: Siber güvenliği üst yönetim meselesi yapalım. Siber güvenlik, bilgi işlem departmanının köşesinde kalan bir konu değil. Yönetim kurullarının, bakanlıkların, rektörlüklerin gündeminde ilk sıralarda olmalı. Bunu şirketimizde de, kurumumuzda da, bugün burada yüksek sesle söylüyorum: Bunun bir liderlik sorumluluğu olduğunu asla unutmayalım.

İkinci çağrım: Kamu, akademi ve özel sektör siber güvenlikte aynı geminin yolcuları. Kamu regülasyon ve vizyon sağlar, akademi bilgi ve yetenek üretir, özel sektör çeviklik ve inovasyon getirir. Bu üçü birbiriyle konuşmazsa saldırgan, inanın, hepsiyle ayrı ayrı baş edebilir. Tehdit istihbaratını paylaşmalıyız, ortak tatbikatlar yapmalıyız, güven temelli hızlı bir bilgi akışı da kurmalıyız. Unutmayalım, saldırganlar birbiriyle çok iyi paylaşıyor. Biz neden paylaşmayalım, paslaşmayalım?

Üçüncü çağrım: Dayanıklılık odaklı düşünelim. Hiçbir sistem yüzde yüz güvenli değil; bunu biliyoruz. Soru "Saldırıya uğrayacak mıyız?" değil; kesinlikle uğrayacağız. "Saldırıya uğradığımızda ne kadar çabuk toparlanacağız?" Asıl soru bu olmalı. Bu yüzden önleme kadar tespit, müdahale ve toparlanma kabiliyetlerimize de yatırım yapmalıyız. Yedeklilik, kriz tatbikatları, sıfır güven mimarisi ve kuantum sonrası şifreleme planları artık lüks değil, bir zorunluluk.

Diğer bir çağrım: İnsanı merkeze alalım. Siber farkındalık, ilkokuldan başlayan ve yönetim kurulu odasına kadar giden bir kültür olmalı. Dijital okuryazarlık mutlaka bilişsel

dayanıklılıkla birleşmeli. Bir toplum olarak gördüğümüz her şeye değil, doğrulayabildiğimiz şeylere inanmayı öğrenmeliyiz.

Son olarak küresel iş birliği: Siber tehditler sınır tanımıyor. Hiçbir ülke, hiçbir kurum bu tehditle tek başına baş edemez. Bugün bu salonda ve önümüzdeki oturumlarda farklı kültürlerden, farklı ülkelerden dostlarımız olacak; bu aslında en güzel gösterge. Siber uzayın sorumlu, öngörülebilir ve adil kurallarla yönetilmesi için ortak akıl geliştirmek zorundayız.

Değerli katılımcılar, konuşmamın başında siber savaşların bugünün gerçeği olduğunu söyledim. Son bir ekleme: Bir savaş kazanacak olan, en çok teknolojiye sahip olan değil, en iyi şekilde birlikte hareket edebilen olacak. Önümüzdeki günlerde burada, kendi alanlarında en önemli isimlerden oluşan bir kadro oturumlarda, panellerde, koridor sohbetlerinde fikirlerini paylaşıyor olacak. Sizden bir ricam var: Sadece dinlemeyin; tanışın, tartışın, iş birliği kurun. Bu konferansın en önemli çıktısı sunumlar değil, burada kurulan bağlantılar olacak.

Yeni dünya düzeninde egemenlik, yalnızca fiziksel sınırları koruyabilmekle mümkün değil. Aynı zamanda dijital varlıklara sahip çıkabilmek, kritik altyapıları ayakta tutabilmek ve toplumun karar alma süreçlerini sağlıklı bir şekilde yürütebilmesiyle ölçülecek. Geleceğin güçlü devletleri yalnızca teknoloji üretenler değil; teknolojiyi kendi iradesiyle yönetebilen, krizler karşısında ayakta durabilen ve dijital dünyada kararlarını kendi başına verebilen devletler olacak.

Bu konferansın, yeni dünya düzeninde siber savaşlar gerçeğini sadece tarif eden değil, bu düzende bizim nasıl bir yer edineceğimize dair ortak bir vizyon çizen bir buluşma olmasını diliyorum. Bu önemli buluşmayı mümkün kılan Bilgi Güvenliği Derneğine, tüm destekçilerimize, konuşmacılarımıza, organizasyon ekibimize ve elbette katılımlarıyla bizleri onurlandıran Sayın Bakanımıza şahsım ve kurumum adına yürekten teşekkür ediyorum. Konferansımızın hayırlı, verimli ve ilham verici olmasını diliyorum. Beni sabırla dinlediğiniz için hepinize saygılarımı, sevgilerimi arz ediyorum.

00:46:47 Abdulkadir URALOĞLU – Ulaştırma ve Altyapı Bakanı

Salon bayağı doluymuş ha, maşallah. Yukarıda biz onları görmemiştik. Epey ilgi alaka var. Güzel, memnun oldum.

Değerli Siber Güvenlik Başkanımız, BTK Başkanımız, Bilgi Güvenliği Derneği Başkanımız ve onun değerli yöneticileri, Bakan Yardımcımız, değerli rektör hocalarımız, sektörümüzün değerli temsilcileri, bilişim sektörünün yine temsilcileri, hanımefendiler, beyefendiler, sevgili gençler; Kıbrıs'tan yine gelen kardeşlerimiz var. Bugün ve yarın farklı ülkelerden de katılımcılarımızın olacağı bilgisini almış oldum.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nın 19.'su vesilesiyle sizlerle birlikte olmaktan büyük memnuniyet duyuyorum. Bu anlamlı buluşmanın ülkemizin siber güvenlik vizyonuna ve dijital dönüşüm yolculuğuna güçlü bir katkı sağlamasını da temenni ediyorum. Bu vesileyle uzaktan yakından gelen herkese hoş geldiniz, sefalar getirdiniz diyorum.

Değerli misafirler, bilgi çağımızın en değerli hazinesidir. Siber güvenlik, yazılım ve teknolojileri ise bu hazineyi koruyan en kritik kalkan olmaya devam ediyor. Yeni çağın en stratejik kaynağı veridir, yani bilgidir. Veri artık yalnızca arşivlenen bir yığın değil; üretimin hammaddesi, güvenliğin kalkanı, ekonominin motoru ve egemenliğin de temelidir. Yapay zeka, bulut bilişim, nesnelerin interneti ve yüksek performanslı hesaplama çağında bir ülkenin gücü, veriyi üretebilme, kendi topraklarında tutabilme, işleyebilme, koruyabilme ve değere dönüştürebilme kabiliyetiyle ölçülmektedir. Bu verinin nerede barındırıldığı, hangi standartlarda işlendiği ve kimlerin kontrolünde olduğu meselesi artık yalnızca teknolojik değil, aynı zamanda stratejik, ekonomik ve milli bir meseledir. Ve şüphesiz verinin egemenliğini tesis eden ülkeler, yarının da potansiyel kazananlarıdır.

Saygıdeğer misafirler, değerli gençler; bu yılki konferansımızın ana teması olan “Yeni Dünya Düzeninde Siber Savaşlar”, küresel ölçekte yaşanan gelişmeleri isabetli biçimde yansıtmaktadır. Siber dayanıklılık ve caydırıcılık, platform siber güvenliği ile küresel rekabette teknoloji savaşları ve siber casusluk başlıkları hem ülkemiz hem de uluslararası toplum açısından kritik önem taşımaktadır.

İşte bu anlayışla kamu ve özel sektör eliyle yükselttiğimiz veri merkezlerini Türkiye’nin yeni dijital kaleleri olarak konumlandırıyoruz, şekillendiriyoruz ve görüyoruz. Temmuz ayında Ankara Gölbaşı’nda temelini attığımız Türksat Veri Merkezi, 35.300 metrekarelik dev alanıyla Türkiye’nin en büyük veri merkezlerinden birisi oluyor. Mevcut kapasitemizi ilk fazda 3 kat, ikinci fazda 8 katın üzerine çıkaracak bu tesis, e-Devlet başta olmak üzere kritik kamu verilerini yerli yazılımlarla, uluslararası standartlarda ve en üst düzeyde güvenlikle inşallah koruyacaktır.

Bir yandan kamunun kritik dijital yükünü taşıyacak bu dev kale yükselirken, diğer yanda özel sektörün gücüyle bölgesel ve uluslararası kapasiteyi büyötmeye de devam ediyoruz. Eylül ayında hizmete aldığımız Vodafone İzmir Veri Merkezi de Ege Bölgesi’nin en büyük veri merkezi olarak bu dijital kaleler zincirine önemli bir halka olarak eklenmiştir. Böylece Türkiye’nin dijital güvenlik haritasını adım adım genişletiyoruz.

Kriptoloji açısından veri merkezleri, dijital varlıklarımızın uzun vadeli güvenliğinin de aynı zamanda teminatıdır. Kritik verilerin şifrlenmesi, anahtar yönetimi, erişim kontrolleri, tedarik zinciri güvenliği ve gelecekteki kuantum tehditlerine karşı dayanıklı altyapıların kurulması bu merkezlerin en temel işlevlerindendir. Veriyi kendi topraklarımızda tutmak, işlemek ve korumak; siber güvenliğimizin, siber bağımsızlığımızın ve teknolojik egemenliğimizin en somut ifadesidir. Bu projeler sayesinde Türkiye, artan veri üretimi, bulut bilişim ve yapay zeka ihtiyaçlarına cevap verecek ölçeklenebilir altyapı kazanırken, bölgesel bir dijital altyapı ve veri merkezi üssü olma hedefini de güçlendirmektedir.

Değerli katılımcılar, ülkemizde siber güvenlik kapasitesinin geliştirilmesine yönelik çalışmalarımızı kararlılıkla sürdürüyoruz. Bakanlığımız koordinasyonunda hazırlanan Ulusal Siber Güvenlik Strateji ve Eylem Planı 2024-2028 kapsamında çalışıyoruz; inşallah bir sonrasını Siber Güvenlik Başkanlığımız hazırlayacak. Elbette eksikler varsa onu da yenileyeceğiz. Değerli Başkanım, bu kapsamda siber dayanıklılık, proaktif siber

savunma ve caydırıcılık, insan odaklı yaklaşım, teknolojinin güvenli kullanımı, yerli ve milli teknolojilerin geliştirilmesi, uluslararası iş birliği alanlarında 4 yıllık süre boyunca 6 stratejik amaç, 18 hedef ve 61 eylem belirledik.

Bu stratejik yaklaşımın kurumsal karşılığını ise Cumhurbaşkanlığımıza bağlı olarak kurulan Siber Güvenlik Başkanlığımız oluşturmaktadır. Biraz önce bahsettiğim gibi 7545 sayılı Siber Güvenlik Kanunu ile güçlendirilen bu altyapı; ulusal siber güvenlik politikalarının tek elden belirlenmesini, kritik altyapıların korunmasını, siber tehditlere karşı koordineli mücadeleyi, müdahaleyi ve kamu-özel sektör-akademi iş birliğini daha etkin hale de getirecektir. Siber Güvenlik Başkanlığı'nın kuruluşu, ülkemizin siber dünyadaki milli çıkarlarını koruma iradesinin somut bir tezahürüdür.

Uluslararası Telekomünikasyon Birliği'nin 2024 Küresel Siber Güvenlik Endeksi'nde Türkiye'nin tüm alanlarda tam puan alarak Seviye 1 "rol model ülke" kategorisinde yer alması, bu alandaki kurumsal kapasitemizin uluslararası düzeyde tescilli anlamına da aynı zamanda gelmektedir.

Bilgi Teknolojileri ve İletişim Kurumumuz da elektronik haberleşme, posta ve elektronik güven hizmetleri sektöründe düzenleme, gözetim ve denetim faaliyetlerini titizlikle sürdürmektedir, sürdürmeye devam edecektir. Bu yıl alınan kurul kararıyla yetkilendirilen tüm işletmecilerin, ekonomik büyüklüklerine bakılmaksızın ilave güvenlik tedbirlerini almakla yükümlü kılınması; sektörel güvenlik seviyesinin yükseltilmesi ve altyapılarımızın siber dayanıklılığının artırılması açısından çok önemli bir adımdır.

Değerli misafirler, bu kapsamlı siber güvenlik çabalarımızın ve kurumsal yapılanmamızın en hassas, en öncelikli boyutunu ise hiç şüphesiz geleceğimizin teminatı olan çocuklarımızın dijital dünyada korunması oluşturmaktadır. Dijital dünyada en çok korumamız gerekenler, olmazsa olmaz, gençlerimiz ve çocuklarımızdır. Bildiğimiz üzere Siber Güvenlik Başkanlığımızca hazırlanan ve Resmî Gazete'de de yayınlanan yönetmelikle 15 yaşını doldurmamış çocuklara sosyal ağ hizmeti sunulması sınırlandırılmıştır. Yaş doğrulamasının e-Devlet üzerinden yapılması, 15-18 yaş grubu için özel koruma tedbirleri uygulanması ve ebeveyn kontrol araçlarının zorunlu kılınması, çocuklarımızın dijital ortamın risklerinden korunması yönünde kararlılığımızın çok açık bir göstergesidir. Çocuklarımızın sağlıklı gelişimini ön planda tutmak, ailelerimizin yanında olmak ve platformların daha fazla sorumluluk üstlenmesini sağlamak, milli güvenlik anlayışımızın ayrılmaz bir parçasıdır.

Geleceğin dünyasında veri; hızlı olana, güvenli olana ve egemen olana ait olacaktır. 5G ve ilerleyen dönemde 6G teknolojileri, yazılım tabanlı şebekeler ve yapay zeka uygulamalarının yaygınlaşması; çekirdek ağ güvenliği, tedarik zinciri güvenliği ve kriptografik altyapıların güçlendirilmesi gibi alanlarda yeni ihtiyaçları da beraberinde doğurmaktadır. Siber güvenlik yalnızca teknolojiyle değil, insan odaklı bir yaklaşımla ve kamu, özel sektör ile akademi arasındaki güçlü bir iş birliği ile güçlenir.

Bu konferansın küresel siber tehditlerin değerlendirilmesi, kritik altyapılarımızın güvenliğinin daha da güçlendirilmesi ve kurumlar arası iş birliğinin derinleştirilmesi bakımından önemli katkılar sağlayacağına ben canı gönülden inanıyorum. Konferansımız iki gün sürecek, değerli Başkanım, öyle bilgi aldım. Gerçekten çok geniş bir katılım var. Burada sadece sunumları dinlemek değil, yine Siber Güvenlik

Başkanımızın da söylediği gibi soruları sormak, etkileşim kurmak ve gerçekten sorgulamak; sadece öğrenmek değil, sorgulamak. O anlamda da yeterince gencimiz ve burada kamu ve özel sektörden yeterince paydaşımız bir arada. Ben kıymetli buluyorum.

19. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nın siber güvenlik farkındalığını artıran, yenilikçi çözümler üreten ve ülkemizin dijital geleceğini güçlendiren kararlara vesile olacağına ben canı gönülden inanıyorum. Bizim için yol gösterici olacaktır, bilgilendirici olacaktır. Bizlerin alacağı kararlarda bize ışık tutacak bir süreç olacağına inanıyorum. Bu vesileyle emeği geçenlere huzurlarınızda teşekkür ediyorum. Sizleri saygıyla selamlıyorum. Kalın sağlıklıyla.

1. OTURUM: SİBER DAYANIKLILIK VE CAYDIRICILIK

01:30:39 Yusuf TANCAN – Siber Güvenlik Başkanlığı Başkan Yardımcısı

Kamu kurumlarımızın ve sektörümüzün değerli temsilcileri, değerli akademisyenler, saygıdeğer komutanlarım, değerli gençler, hepinizi saygıyla selamlıyorum.

Konferansın ülkemizin siber dayanıklılığına ve caydırıcılığına önemli katkılar sunmasını temenni ediyorum.

Siber güvenliğin belki de en stratejik iki kavramı üzerinde konuşuyor olacağız: dayanıklılık ve caydırıcılık. Bir madalyonun iki yüzü gibi. Birisi içeriye bakar: Vurulursam ne olur? Diğeri dışarıya bakar: Bana vurmak ne kadar pahalı?

Günümüzün karmaşık tehdit ortamında yalnızca saldırıları önleyeceğimiz varsayımı üzerine bir güvenlik mimarisi inşa etmek biraz yanlış olur. Çünkü güvenliğin başarısını sadece kapıdan içeri kimin girmediğiyle ölçemeyiz. Asıl başarı, kapı aşıldığında dahi içerideki hayatın devam edebilmesidir. İşte siber dayanıklılık tam olarak bu anlayışın ifadesidir.

Siber caydırıcılık ise bundan bir adım daha ileri gider. Yalnızca saldırı karşısında ne yapacağımızla değil, potansiyel saldırganın o saldırıyı gerçekleştirmeye değmeyeceğini düşünmesini nasıl sağlayacağımızla ilgilenir. Dayanıklılık saldırının sonuçlarını sınırlar. Caydırıcılık ise saldırı kararının verilmesini zorlaştırır. Biri saldırı gerçekleştiğinde ayakta kalmamızı sağlar, diğeri saldırının hiç gerçekleşmemesine katkıda bulunur. Güçlü bir ulusal siber güvenlik mimarisi, bu iki kapasiteyi birbirinden ayırmadan birlikte geliştirebilme yeteneğidir.

Ben dayanıklılık kavramını vücudumuzdaki bağışıklık sistemi üzerinden düşünmeyi oldukça isabetli buluyorum. Bedenimiz her gün binlerce mikropla karşılaşır. Cilt bir bariyerdir; ama asıl iş, içeri giren tehdidi tanıyan, öğrenen ve hatırlayan hücrelerin

elindedir. Güçlü bağışıklığı olan insan, hiç hastalanmayan değil, hastalandığında toparlanabilen insandır.

Burada önemli bir noktaya dikkatinizi çekmek istiyorum. Bağışıklık hücreleri yalnız çalışmaz, tek çalışmaz; birbirleriyle konuşur. Bir yerde tehdit görülünce vücudun her yerine haber gider. Buradan siber güvenliğe, hatta ülke ölçeğine gelelim: Bir kurumda görülen bir saldırı, ertesi gün başka bir kurumda boşa çıkabilmelidir. Bu haber akışını örgütlenme sorumluluğu bizde; ama akışın çalışması kurumların haber vermesine bağlı. Bağışıklık sisteminde sessiz kalan hücre, hasta hücredir.

Konuya bir de deprem üzerinden bakalım. Biz bu coğrafyada depremin ne demek olduğunu acı bir hafızayla biliyoruz. O hafıza bize şunu öğretti: Dayanıklı bina, sarsıntıyı hiç hissetmeyen bina değil; sallanan ama yıkılmayan binadır. Deprem yönetmeliği bir bina için öneri değil, şarttır. Çünkü o binanın çökmesi yalnızca içindekilerin değil, yanındakilerin de sorunudur. Mesele, gelişine engel olunamayan bir sarsıntının yıkıcı etkilerinden uzak kalabilmektir.

Kritik sistemlerimizi belirlemek, yetkileri sınırlamak, alternatif altyapılar oluşturmak, yedeklerimizi güvence altına almak, olay müdahale ekiplerimizi hazır tutmak ve kriz anında kimin hangi kararı vereceğini önceden belirlemek zorundayız. Çünkü saldırı anı, ilk defa plan yapacağımız zaman değildir. Kriz anında hangi sistemin öncelikli olduğunu tartışıyorsak, sorumlulukların kimde olduğunu araştırıyorsak veya alternatif iletişim kanalımızın bulunmadığını fark ediyorsak, sorun yalnızca saldırganın kabiliyetinde değil, bizim hazırlık düzeyimizdedir. Kritik hizmetlerimizin tek bir tedarikçiye, tek bir iletişim kanalına, tek bir veri merkezine veya tek bir teknik çözüme bağlı olması en büyük risklerden biridir.

Bu noktada siber dayanıklılığın dört temel aşamasından bahsetmek istiyorum: hazırlanmak, direnmek, toparlanmak ve öğrenmek.

Hazırlanmak; riskleri önceden belirlemek, kritik varlıkları tanımak, sorumluları ve sorumlulukları netleştirmek ve gerçekçi senaryolar üzerinden tatbikat yapmaktır. Yedeklerinize hiçbir zaman tam olarak güvenmeyin; yedeği deneyin. Hiç açılmamış bir paraşüt, paraşüt değildir. Yedeğini hiç geri yüklememiş bir kurumun yedeği yok demektir.

Direnme; saldırının yayılmasını sınırlamak, kritik hizmetleri korumak ve etkilerin büyümesini önlemektir.

Toparlanma aşaması; sistemleri güvenli biçimde yeniden devreye almak, vatandaşlara ve hizmet kullanıcılarına kesintisiz bilgi vermek ve temel işlevleri mümkün olan en kısa sürede yeniden ayağa kaldırmak, hizmete sunmaktır.

Öğrenmek ise yaşanan olaydan sonra hangi yapısal eksikliklerin giderilmesi gerektiğini ortaya koymaktır. Az önceki ödül töreninde kırdığımız ödüllerde olduğu gibi; sonradan şeyi kaldırdılar değil mi? Onu kaldırıncı yapısal problem çözülmüş oldu.

Şimdi madalyonun diğer yüzüne, yani caydırıcılık kavramına bakalım. İyi bir satranç oyuncusu yalnızca rakibinin yaptığı hamlelere cevap vermez; rakibin hangi hamleleri yapabileceğini, hangi seçeneklerden vazgeçmek zorunda kalacağını ve kendi

hamlesinin karşı tarafta nasıl bir sonuç doğuracağını da hesaplar. Siber caydırıcılık da yalnızca saldırı gerçekleştikten sonra verilecek karşılıkla ilgili değildir; saldırganın hesabını, planını değiştirmekle ilgilidir.

Saldırganın bir sistemi hedef almadan önce şu sorularla karşılaşmasını bekleriz ve isteriz: Bu saldırıdan beklediğim faydayı elde edebilecek miyim? Hedefin savunmasını aşabilecek miyim? Elde ettiğim erişimi, istediğim sonucu üretmek için kullanabilecek miyim? Saldırının kaynağı ve sorumluları ortaya çıkarılabilecek mi? Ve daha önemlisi, bu eylemin siyasi, ekonomik, hukuki sonuçları olacak mı? Olacaksa ne olacak? İşte caydırıcılık, bu hesapları etkileme kapasitesidir. Bu da üç unsurla mümkündür: kabiliyet, inandırıcılık ve iletişim.

Burada önemli bir noktayı da vurgulamak istiyorum. Caydırıcılık mutlaka misilleme anlamına gelmez. Saldırganın hedefinden beklediği faydayı elde etmesini engellemek de temel yollardan biridir. Eğer bir saldırgan bir ülkenin kritik hizmetlerini durdurmayı hedefliyor, fakat o ülke alternatif sistemleri sayesinde hizmetlerini sürdürebiliyorsa, saldırının beklenen getirisi azalır. Eğer çalınan veriler, güvenli tasarımlar ve doğru erişim politikaları sayesinde saldırgana beklediği imkânı sağlamıyorsa, saldırının etkisi sınırlanmış olur. Eğer kurumlar hızlı biçimde tespit, müdahale ve toparlanma sağlayabiliyorsa, saldırganın zaman ve kaynak avantajı daralmış olur. Dolayısıyla dayanıklılık, caydırıcılığın altyapısını oluşturur. Saldırganın kazanımını azaltmak, saldırının maliyetini artırmak ve başarı ihtimalini düşürmek, caydırıcılığın birbirini tamamlayan boyutlarıdır.

Hepimizin bildiği üzere siber uzayda bir saldırının kaynağını kesin biçimde belirlemek her zaman ne kolaydır ne de mümkündür. Saldırganlar farklı sistemleri kullanabilir, faaliyetlerini gizleyebilir veya sorumluluğu başka aktörlere yönlendirmeye çalışabilir. Bu nedenle caydırıcılık, yalnızca saldırganın kim olduğunu tespit edebilme beklentisine dayandırılmamalıdır. Güvenli altyapılar, güçlü savunma, etkili uluslararası iş birliği, hukuki mekanizmalar, olaylara müdahale kapasitesi ve gerektiğinde diplomatik araçların kullanılması hep birlikte değerlendirilmelidir.

Ayrıca karşılık verme seçenekleri belirlenirken hukuka uygunluk, ölçülülük, kanıtların güvenilirliği ve tırmanma riskleri göz önünde bulundurulmalıdır. Çünkü amaç yalnızca güçlü görünmek değildir. Amaç, güvenliği gerçekten artırmak ve krizlerin daha büyük çatışmalara dönüşmesini önlemektir. Güç, yalnızca karşılık verebilmek değil; doğru zamanda, doğru araçlarla ve doğru sınırlar içerisinde hareket edebilmektir.

Türkiye'nin siber güvenlik alanındaki hedefini yalnızca saldırılara karşı savunma yapmak olarak tanımlayamayız. Bizim hedefimiz; dijital altyapıları ve kritik hizmetleri dayanıklı, teknolojiye alternatiflerini üretmiş, insan kaynağı güçlü ve uluslararası iş birliğinde etkin bir ülke olmak. Bu hedef esasen dijital egemenlik anlayışımızla da doğrudan ilişkili. Dijital egemenlik ile siber dayanıklılık ve caydırıcılık arasında çok önemli bir ilişki var. Dolayısıyla bunları birbirinden kopuk politikalar olarak değerlendirmiyoruz.

Dijital çağda güvenlik yalnızca sistemleri korumak değil; devletin işleyişini, ekonominin sürekliliğini, vatandaşın güvenini ve ülkenin geleceğini korumaktır. Geleceğin güvenlik mimarisini birlikte kurmak kamu, akademi ve özel sektör olarak hepimizin ortak

sorumluluğu. Bu sorumluluğu ancak bilgiyle, iş birliğiyle, kararlılıkla ve ortak bir gelecek vizyonuyla yerine getirebileceğimize inanıyorum.

Salondan çıkarken yanınızda üç soru götürmenizi rica ediyorum, istirham ediyorum. Yarın sabah kurumlarınıza, şirketlerinize gittiğinizde bu üç soruyu gerek yönetim kademesindeki gerek çeşitli kademelerdeki çalışanlarınıza sormanızın önemli olduğunu düşünüyorum.

Birinci soru: En kritik hizmetlerimiz hangisi ve çökerse kaç saatte ayağa kalkarsınız? Bu soruyu masaya yatırmanın önemli olduğunu düşünüyorum.

İkinci soru: En son tatbikatı ne zaman yaptık? Yedeğimizi en son ne zaman gerçekten tekrar yükledik? En son yedekten geri dönüşümüzü ne zaman yaptık?

Üçüncü soru: Saldırıya uğradığımız gün kimi arayacağız? Hangi konuda kim yetkili, kim sorumlu?

Bunları kurumlarımızda, şirketlerimizde, kuruluşlarımızda üzerinde ciddi bir şekilde tartışacak şekilde masaya yatırmalı ve en temel sorular olarak sormalıyız.

Konferansın yeni iş birliklerine, güçlü fikirlere ve ülkemizin siber dayanıklılığına katkı sağlayacak somut adımlara, somut çıktılara vesile olmasını diliyorum. Beni sabırla dinlediğiniz için hepinize teşekkür ediyor, hepinizi saygıyla selamlıyorum.

01:45:05 Tuğgeneral Metin DURMAZ – TSK Siber Savunma Komutanı

Konuşmama başlamadan önce; kamu kurum ve kuruluşlarının çok kıymetli, değerli yöneticileri, özel sektörün ve firmalarımızın değerli temsilcileri, akademik camiamızın değerli, kıymetli temsilcileri ve hocalarımız, Silahlı Kuvvetler personelimiz, gençler, tüm katılımcılar; hepinizi saygıyla selamlıyorum.

Sayın Başkanımın konuyla ilgili ifade ettiği ve altını çizdiği hususlar bir açıdan beni çok memnun etti, çok mutlu etti. Çünkü neredeyse yüzde yüz bir mutabakat ve anlayış birliği içerisinde olduğumuzu anladım, gördüm. Zaten Sayın Başkanım ile beraber birçok fırsatta, gerek yurt içinde gerek yurt dışında, düşüncelerimizi ve değerlendirmelerimizi paylaşma imkânını, fırsatını bulmuştuk. Diğer taraftan da biraz üzıldüm; çünkü neredeyse söylemek istediğim her konuyu belki benden çok daha güzel şekilde ifade etti. Sağ olun Başkanım. Evet, doğru, haklısınız.

Ulusal siber güvenlik stratejisi ve eylem planları yıllardan beri yayınlanır. Bunların içinde de özellikle altı çizilen ve belirtilen bir husus, siber güvenliğin ulusal güvenliğimizin ayrılmaz bir parçası olmasıdır. Ulusal kurum ve kuruluşlarımızın görev ve sorumlulukları da bu anlayış çerçevesinde belirlenmiştir. Malumlarınız, siber dayanıklılığın sağlanması ve siber alanda caydırıcılığın tesisi, bu ulusal siber güvenliğin tesis edilmesinde odak alanlarından biridir.

Ben bir asker olarak siber dayanıklılık ve siber caydırıcılık konularına bakış açımı sizlerle paylaşmak istiyorum.

Siber dayanıklılık; bir siber saldırıya karşı koyabilme, temel işlevleri sürdürebilme ve sonrasında süratle toparlanarak etkileri atlatabilme kapasitemizle ilgilidir. Diğer bir deyişle siber dayanıklılık, siber saldırıları engelleme ve caydırmada önleyici tedbirler başarısız olduğunda dahi görevimize devam edebilme kabiliyetidir. Gerçek hayatta elde edilen tecrübeler, siber saldırıların tamamen önlenmesinin mümkün olmadığını göstermiştir, göstermektedir. Bununla birlikte siber dayanıklılık; tehditleri öngörmeyi, görev için kritik sistemler arasındaki bağımlılıkları anlamayı, siber saldırılara karşı koymayı ve etkilerini sınırlamayı, kritik temel hizmetleri sürdürmek için alternatif yol ve yöntemleri önceden belirlemeyi ve gerçekçi tatbikatlarla bu gibi durumlara hazırlıklı olmayı gerektirmektedir.

Askeri açıdan ise siber dayanıklılık bizim için hareket serbestisinin muhafazasını, komuta kontrolün korunmasını, durumsal farkındalığın sürdürülmesini ve görevimiz için kritik sistemlerin işler hâlde tutulmasını ifade etmektedir. Her türlü siber tehdide karşı yüksek hazırlık seviyesine sahip olan Silahlı Kuvvetler, hiçbir saldırının görevinin ifasına engel olmasına fırsat vermemelidir.

İnsan eliyle yaratılmış siber alanın kendine has özellikleri, bu alanı savunmada ve korumada daha kapsamlı yaklaşımları gerekli kılmaktadır. Bu nedenle ulusal siber alanın savunulması ve korunması; kamu, özel, sivil ya da asker, tüm milli güç unsurlarının ve kuruluşlarının rol alacağı bütüncül bir anlayışı gerektirmektedir.

Dayanıklılık, başarılı bir siber saldırının sağlayacağı avantajı azaltabilir. Ayrıca saldırganın hedeflediği sonuca ulaşacağına ilişkin beklentiyi zayıflatarak caydırıcılığa, özellikle de savunmaya dayalı caydırıcılığa katkıda bulunabilir. Ancak dayanıklılık tek başına caydırıcılık sağlamak için yeterli değildir. Bu ifade bizi siber alanda caydırıcılık kavramına ulaştırıyor.

Caydırıcılık, hasmın karar alma süreçlerini hedefler. Hasmın saldırmakla elde etmeyi umduğu kazançla karşılaşacağı maliyet ve zarar arasında yapacağı muhasebeyi lehimize etkilemeyi amaçlar. Klasik caydırıcılık anlayışı, engellemeye ve savunmaya dayalı caydırıcılık, bunun yanında cezalandırmaya dayalı caydırıcılık olarak iki yaklaşımı benimsemektedir. Malumunuz, savunmaya dayalı caydırıcılıkta saldıran tarafın güçlü savunma ve dayanıklılık sayesinde istediği sonucu elde edemeyeceğini; cezalandırmaya dayalı caydırıcılıkta ise düşmanca faaliyetinin daha şiddetli karşılık göreceğini bilmesi ve anlaması hedeflenmektedir.

Burada siber saldırılara mutlaka ve sadece siber yöntemlerle karşılık verilir şeklinde bir sınırlama bulunmadığının altını çizmek istiyorum. Karşılık, en etkili sonucu verecek her türlü kinetik ve kinetik olmayan vasıtalarla, diplomatik tedbirlerle, ekonomik yaptırımlarla ya da hukuki süreçlerle verilecek karşılıkları içerebilir.

Bununla birlikte siber alanda mutlak caydırıcılığın sağlanmasının önünde bazı engeller bulunduğunu bilmemiz gerekiyor. Bu engeller klasik anlayışın hayata geçirilmesini zorlaştırıyor. Bunlardan birincisi, siber saldırıyı gerçekleştiren kim olduğunu bulmanın zorluğu. Isnat, atıf olarak ifade ettiğimiz bu süreçler zor, karmaşık ve uzun sürelidir; teknik bulgularla desteklenen politik bir karar sürecidir atıf ve isnat süreci. İkincisi, verilen mesajın karşı tarafta aynı şekilde algılanmaması olasılığıdır. Bir diğeri ise hangi eylemin karşılık gerektiren bir saldırı olduğuna dair ortak anlayışın eksikliğidir. Her

lkenin hangi fiilin silahlı bir siber saldırı olduđuna dair tanımını farklılık arz etmektedir. rneđin bazı lkeler siber casusluđu silahlı bir saldırı olarak kabul ederken bazıları etmemektedir. Hangi durumda siber saldırıların silahlı bir saldırı olarak kabul edileceđi, saldırı eřiđinin ne olduđu konusu gri, muđlak bir alan olarak karřımıza çıkmaktadır.

Açık savař hâleri haricinde silahlı saldırı sayılabilecek bir siber saldırıdan lkelerin kaçındıđını göryoruz. Fakat her gn silahlı saldırı eřiđinin altında gerçekteřen ve srekli hâle gelen siber saldırılara karřı caydırıcılık yaklařımlarının sonu vermediđi ařıkârdır. Dolayısıyla savunma ve saldırı yeteneklerine sahip olmak, tek başına caydırıcılık etkisini oluřturmak iin yeterli deđildir. Caydırıcılık, sahip olduđumuz yeteneklerin ve bu yetenekleri kullanacađımıza dair kararlılıđımızın bir bileřimidir. Caydırıcılıđın; yksek teknoloji ve operasyonel yetenekler, kararlılık, uluslararası iř birliđi, ortaklıklar, stratejik iletiřim ve hukuksal normları da kapsayacak řekilde, milli g unsurlarının tam bir uyum ierisinde hareket ettiđi btncl bir yaklařımla tesis edilmesi gerekmektedir.

Bu noktada lkemizin siber alanda en nemli g unsurlarından biri Trk Silahlı Kuvvetleridir. Gerçekte muharebe ortamında elde edilen tecrbeler, siber yeteneklerin muharebe sahasında harekâtin kaderini tayin edecek bir olgu hâline geldiđini gstermiřtir, ispatlamıřtır. Bunun sonucunda siber alan; kara, deniz, hava ve uzaydan sonra yeni bir askeri harekât alanı olarak kabul edilmiřtir. Bu anlayıř hepimizi, siberin siber gvenlik yaklařımlarının tesinde muharebe sahasını řekillendiren bir yetenek olduđu noktasına ulařtırmak zorundadır. Trk Silahlı Kuvvetleri de bu yaklařımı benimsemiřtir, konsept ve doktrinlerine yansıtmiřtir; bu konuda alıřmalarını gayretle srdrmektedir.

Bu anlayıř ve bilinle, mensubu olduđum Trk Silahlı Kuvvetleri Siber Savunma Komutanlıđımız; siber alanda dnyadaki geliřmeleri ve diđer lke silahlı kuvvetlerinin edindiđi tecrbeleri yakından takip etmekte; gerçekteřtirdiđi kapsamlı eđitimler, katıldıđı ve ev sahipliđi yaptıđı ulusal ve uluslararası tatbikatlar ve yrtlen projelerle hem personelinin yetkinliđini hem de imkân ve kabiliyetlerini her geen gn daha ileri seviyelere ulařtırmakta ve kara, deniz, hava ve uzayda olduđu gibi siber alanda da etkin, caydırıcı ve saygın bir g olma hedefi dođrultusunda alıřmalarını azim ve kararlılıkla srdrmektedir.

Beni sabırla dinlediđiniz iin teřekkr ederim. Oturumdan hemen nce koridorda ve fuaye alanında karřılařtıđımız ve bize ok ilgi gsteren geen arkadařlarımız oldu. İlk fırsatta kendilerini tekrar dinlemeye ve sorularını cevaplamaya alıřacađımı da ifade etmek istiyorum. Teřekkr ederim.

01:56:59 Cem AKOYMAK – Vodafone İcra Kurulu Başkan Yardımcısı (Hukuk ve Kurumsal Gvenlik)

Sayın başkanlarım, sayın rektrlerim, sayın komutanlarım, Bilgi Gvenliđi Derneđi’nin deđerli yneticileri ve sevgili geenler. Sayın Başkanım konuřmasını yaparken bir yandan kendi notlarımı kafamda gzden geiriyordum. nmde deđildi ama řimdi evirdike greceđim ki, neredeyse hemen hemen Sayın Komutanımın da sylediđi

gibi, birebir karşılığı var benim notlarımda. O yüzden, eğer şu anda bir siber saldırı altında değilsek, bunları mümkün olduğu kadar atlayarak geçmeye çalışacağım.

Bu yıl 19'uncusu düzenlenen ve hem ülkemiz hem de dünya açısından büyük önem taşıyan siber güvenlik temalı bu konferansta Vodafone'u temsil etmekten büyük gurur duyuyorum. Bu yıl biz de Vodafone olarak 20. yılımızı kutluyoruz. Geçtiğimiz 20 yılda teknolojinin çok değiştiğini, ihtiyaçların yeniden şekillendiğini, dijital dünyanın ekonomideki ve günlük hayatımızdaki yerinin çok daha farklı bir noktaya geldiğini hep birlikte müşahade ediyoruz. Bu dönüşümün temel unsurlarından bir tanesi de teknolojik altyapılar oldu; bugün daha modern bir deyişle "gigabit altyapılar" diyoruz. Hızlı ve kesintisiz geniş bant ağları ekonomik gelişimin temel yapı taşlarından biri haline gelmiş durumda. Telekom teknolojileri geliştikçe, bağlantının hızı ve kapasitesi artmanın dışında, kullanım alanlarının da belki bundan sadece 3 yıl önce bile öngöremeyeceğimiz kadar geliştiğini, eksponansiyel bir biçimde arttığını gözlemliyoruz.

Ancak bugün böyle bir alışkanlık var: Telekomdaki gelişmeyi hız ve kapasite üzerinden okuyoruz. Ama artık bunun daha fazla böyle olmaması gerektiğine inanıyoruz. Yapay zekânın ve otomasyonun şebekelere giderek daha fazla entegre olduğu, yeni kullanım alanlarının yavaş yavaş ortaya çıkmaya başladığı ve güvenlik ile dayanıklılığın, Başkanımın belirttiği gibi, çok daha fazla önem kazandığı yeni bir teknolojik dönemin, yeni bir eranın içine giriyoruz aslında. Bu nedenle siber güvenliği bu teknolojik dönüşümün de en önemli parçalarından biri olarak değerlendiriyoruz.

Şu an siber güvenlik, tüm dünyayı ve devletleri ilgilendirdiği gibi, bir şirketin de tüm operasyonlarını temelden etkileyen bir gündem. Bugün bir şirketin operasyonunu durdurmak için, bu sabahki, az önceki örnekte olduğu gibi, artık fabrikasına girmeniz gerekmiyor ya da veri merkezinde fiziksel bir saldırıda bulunmanız gerekmiyor; hatta oraya ulaşmanız da gerekmiyor. Tek bir kullanıcı hesabıyla bile, internete açık herhangi bir uygulamayla, bir yazılım ya da birlikte çalıştığınız bir tedarikçi üzerinden de bir atak başlangıç noktası söz konusu olabiliyor ve bunlardan herhangi biri, işimizin tamamını etkileyebilecek bir saldırının başlangıç noktası olma potansiyeline sahip. Dolayısıyla siber güvenliği de artık ulaşıp bırakılan sabit bir durum olarak değerlendirmemek gerekiyor.

İşte bu kısımlar, örneğin Başkanımın söylediği gibi aynı: tehdidi öngörme, saldırıya dayanma, hızla toparlanma ve her olaydan öğrenme. Bunlar birebir bizim de kendi notlarımıza aldığımız ve caydırıcılık bakımından en önemli gördüğümüz hususlar. Caydırıcılık aslında bu dört yetkinliğin temel ve doğal bir sonucu. Saldırıyı erken öngören, kolay aşılamayan ve hızla ayağa kalkan bir altyapı, saldırının maliyetini artırdığı gibi başarı ihtimalini de düşürüyor. Dolayısıyla bugün en etkili caydırıcılığın da dayanıklılık olduğunu bu vesileyle ben de vurgulamak istiyorum.

Yine aynen Başkanımın da ifade ettiği gibi, böyle bir tehdidi öngörebilmek için geniş bir görüş alanına ve haber ağına ihtiyaç var. Bu bağlamda Vodafone olarak biz de en önemli gücümüzü, küresel ölçekte edindiğimiz bilgi birikimi ve bu bilgi birikimini Türk mühendislerinin uzmanlığıyla birleştirebilmemiz olarak görüyoruz. Grubumuz siber güvenlik hizmetlerini Birleşik Krallık, Almanya, Romanya, Hindistan ve son olarak Portekiz'deki merkezlerden oluşan küresel bir ağ ile koordineli şekilde yönetiyor; Türkiye

de buna dahil. Lizbon'daki yeni merkezimiz yapay zekâ ve kuantum güvenliği gibi geleceğin tehdit alanları üzerinde halen çalışmalarını sürdürüyor. Faaliyet gösterdiğimiz pazarlardan gelen telemetriyi ortak bir güvenlik modeli altında değerlendiriyor, milyarlarca olay ve logu Vodafone sistemleri içerisinde işliyoruz.

Bu ağın, bu haberleşme ağının ülkemiz için anlamını ise şöyle değerlendiriyoruz: Bir pazarda ilk kez görülen bir saldırı tekniği, diğer pazarlarda önceden alınmış bir önleme dönüşebiliyor. Farklı ülkelerde, farklı düzenleyici ortamlarda, farklı tehdit aktörlerine karşı, farklı ölçeklerde edinilmiş olan tecrübe Türkiye'deki savunmamızı daha olgun hale getiriyor. Bir olay müdahale planının ya da bir güvenlik mimarisinin değeri, gerçek koşullarda sınanmış olmasından gelmekte. Biz de Türkiye'de tam olarak, başka pazarlarda bu sınavlardan geçmiş yöntemleri uygulamaya elimizden geldiğince gayret ediyoruz. Tabiatıyla bu kendiliğinden yerel bir güce dönüşmüyor. Onu dönüştüren, bu bilgiyi alıp Türkiye'nin koşullarına uyarlayan, geliştiren ve sahada uygulayan bizim mühendislerimiz, hukukçularımız, çalışma arkadaşlarımız.

Vodafone olarak siber güvenliğe attığımız bu önem doğrultusunda Ankara'da 7/24 çalışan bir siber güvenlik operasyon merkezi kurduk. Müşterilerimize öncesinde zafiyet taraması yapıp danışmanlık veriyor, sonra sistemlerini profesyonel bir şekilde koruyor; işletmelerin değişen tehdit ortamlarına karşı daha dayanıklı hale gelmelerine destek oluyoruz. Ağ güvenliğinden e-posta güvenliğine, zafiyet yönetiminden antivirüs, erişim yönetimi ve risk analizine kadar uzanan geniş bir çözüm portföyüyle kurumların dijital varlıklarını korumaya ve iş sürekliliklerini güçlendirmeye yardımcı oluyoruz.

Dayanıklılık, siber savunmanın yanında altyapının kendisiyle de ilgili tabiatıyla. Bugüne kadar Türkiye'ye yaptığımız yatırımın reel değeri 600 milyar TL'yi aşmış vaziyette. Yalnızca son 5 yılda şebekemize 100 milyar TL'nin üzerinde bir yatırım yaptık ve kapasitemizi de bundan 3 sene öncesine göre 3 kat artırmış durumdayız. Sayın Bakanın sabahki konuşmasında bahsettiği İzmir Veri Merkezimiz de bunun en önemli örneklerinden biri. İlk fazı 100 milyon dolarlık yatırımla tamamlanan tesis, toplamda 7.500 metrekarelik alan üzerinde, bugün itibarıyla 650'den fazla kabinet ile faaliyet gösterecek şekilde hazırlandı. Uluslararası Tier 3 standartlarına uygun yüksek güvenlikli altyapıya ve yapay zekâ iş yüklerini destekleyen ölçeklenebilir bir mimariye sahip olan bu veri merkezi başlangıçta 4 MW kapasiteyle hizmet verecek. Bu konuda iş birliği yaptığımız DAMAC Digital isimli şirketle protokollerimiz kapsamında bu yatırımın toplam değerinin 300 milyon doların da üzerine çıkmasını ve kapasitenin de 20 megavatın üzerine çıkmasını bekliyoruz.

Dayanıklılığın dördüncü ayağı öğrenmek demişti Sayın Başkan. Bu alanda açık konuşmak gerekirse, bilgi şu an bizim açımızdan tüm dünyadan Türkiye'ye akıyor vaziyette. Vodafone Grubu, şebeke altyapısına yönelik test ve inovasyon ortamını yakın zaman önce İspanya'dan İstanbul'a taşıdı. Grubumuzun yeni nesil şebeke testleri bundan sonra tamamen Türkiye'de yapılacak. Bu, gelecekteki şebekelerin güvenliğini daha ilk tasarım aşamasından itibaren Türk mühendisleriyle birlikte düşünme fırsatı anlamına geliyor. Bizim açımızdan Türkiye'deki ekiplerimiz artık tüm pazarlardaki bilgileri görerek burada bilgi üretmeye başladılar ve bunu ilk kez 5G sürecinde deneme imkânı bulduk. Grubumuzun 5 kıtadaki 5G deneyiminden yararlandık; ama bu bilgiyi, 81

ilde 922 ilçede ilk 5G sinyalinin verildiği anda tüm şebekeyi ayağa kaldırarak bir nevi tatbik etmiş olduk.

Vodafone olarak amacımız Türkiye’de kalıcı teknik kapasite ve katma değer üretmek. Bugün Türkiye’de 50 milyar TL’lik bir satın alma hacmine, 1.200’ün üzerinde tedarikçiye ve yaklaşık 6.000 satış noktasına ulaşan büyük bir ekosisteme sahip vaziyetteyiz ve bu ekosistemle yaklaşık 40.000 kişilik doğrudan ve dolaylı istihdam yaratıyoruz. Bu ekosistemin her bir halkası aynı zamanda siber dayanıklılığın da bir halkası; bunu böyle görüyoruz. Tedarik zincirindeki her güçlü halka bütün yapıyı daha dayanıklı kılıyor. Bu nedenle Türkiye’de teknolojiye yaptığımız yatırımları yalnızca kendi altyapımızın gelişmesi açısından değil, daha geniş bir teknolojik kapasitenin oluşması ve ekonomik değere dönüşmesi açısından da ele alıyoruz.

Uluslararası deneyimimizden gelen risk yönetimi, uyum ve güvenlik kültürü, mevzuata ve düzenleyici beklentilere uymamızı aslında bir nevi sağlamlaştırıyor, ona zemin hazırlıyor. Uluslararası standartlar hukukumuzun gereklerini karşılamamız için bize sağlam bir zemin sunuyor ve temelde her ikisi birbirini tamamlıyor. Bu çerçevede önümüzdeki dönemde ikincil düzenlemelerin, ilgili sektörlerle istişare içerisinde, mevcut yetkinlikler ve sektör gerçekleri dikkate alınarak şekillenmesini arzu ediyoruz. Bu yönde zaten çalışmalar olduğunu biliyoruz. Bizim Vodafone olarak yaptığımız yatırımlar çerçevesinde bundan sonrası için de beklentimiz şu: Bu, tek başına yönetilen bir sistem değil. Kamu kurumları da, devlet kurumları da, üniversiteler de, şirketler de, Başkanım sizin söylediğiniz gibi, bu işin, bu ekosistemin hepsi birer parçası. Bu ortak sorumluluk bilinci dahilinde, yatırım ve inovasyon ortamını tehdit etmeyen, aynı zamanda onu destekleyen ve sektör beklentilerine de uygun bir düzenleyici ortamın ortaya çıkabilmesi için gereken katkıyı vermekten büyük mutluluk duyacağız.

Çok teşekkür ediyorum. Saygılar sunuyorum. Daha fazla uzatmayayım, çok fazla tekrara girmek istemiyorum. Sağ olun.

02:07:50 Serhat SARI – Türk Telekom Siber Güvenlik Direktörü

Sayın başkanlarım, sayın komutanlarım, sektörümüzün değerli temsilcileri, değerli konuklar. 19. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı’nda Türk Telekom adına sizleri saygıyla selamlıyorum.

Bu yıl “Yeni Dünya Düzeninde Siber Savaşlar” temasıyla bir araya geliyoruz. Dijital teknolojilerin ekonomik, toplumsal ve stratejik dengeleri yeniden şekillendirdiği bir dönemde siber güvenlik her zamankinden daha kritik bir önem taşıyor. Türk Telekom olarak siber güvenliğin geleceğine ışık tutan bu değerli platformun platin sponsoru olmaktan büyük memnuniyet duyuyoruz. Bugün burada yalnızca teknolojiyi değil; kurumlarımızın, ekonomimizin ve ülkemizin dijital geleceğini konuşuyoruz. Bu çerçevede yeni dünya düzenini iki önemli kavram üzerinde odaklanarak ele almak istiyorum: siber dayanıklılık ve caydırıcılık.

Değerli konuklar, dijitalleşmenin hayatımızın her alanına yayıldığı günümüzde siber güvenlik de sürekli gelişen ve dönüşen bir alan haline geldi. Artık güçlü güvenlik altyapılarını oluşturmanın yanı sıra değişen tehditleri öngörebilmek, riskleri erken aşamada tespit edebilmek ve gerektiğinde hızlı ve etkin aksiyon alabilmek büyük önem

taşıyor. Siber dayanıklılık, bu bütüncül güvenlik yaklaşımının temelini oluşturuyor. Kritik altyapılardan finans sistemlerine, telekomünikasyondan kamu hizmetlerine kadar uzanan dijital ekosistemde güvenliğin sürdürülebilirliği; önleyici tedbirlerin gücü, erken tespit kapasitesi ve hızlı müdahale yetkinliği ile doğrudan ilişkili.

Siber dayanıklılık; sistemlerin güvenliğini sürekli güçlendirmeyi, olası tehditlerin etkisini sınırlandırmayı, veri bütünlüğünü korumayı ve hizmet sürekliliğini destekleyen mekanizmaları etkin biçimde yönetmeyi gerektiriyor. Çünkü günümüzde siber güvenlik yalnızca teknolojik sistemlerin korunmasıyla sınırlı değil; kurumlara duyulan güvenin, ekonomik istikrarın ve kritik hizmetlerin sürekliliğinin de önemli bir bileşeni. Bu nedenle siber dayanıklılığı yalnızca bir bilgi teknolojileri meselesi olarak değil, kurumsal sürdürülebilirliğin ve milli güvenliğin stratejik unsurlarından biri olarak değerlendirmeliyiz.

Değerli katılımcılar, siber güvenliğin bir diğer önemli boyutu ise caydırıcılık. Geleneksel güvenlik anlayışında caydırıcılık büyük ölçüde fiziksel savunma kapasitesi üzerinden değerlendirilirken dijital dünyada çok daha farklı dinamikler söz konusu. Siber tehditlerin sınır tanımayan yapısı, gelişen saldırı yöntemleri ve giderek karmaşılaşan dijital ekosistem, caydırıcılık anlayışının da sürekli geliştirilmesini gerektiriyor.

Siber alanda caydırıcılığın temelinde, güçlü teknolojik altyapılarla desteklenen proaktif güvenlik yaklaşımı bulunuyor. Bu yaklaşımın iki önemli boyutu var. İlki, güçlü savunma mimarileriyle tehditlerin başarıya ulaşma olasılığını azaltmak. Sıfır güven mimarileri, ağ segmentasyonu, gelişmiş erişim kontrolleri ve çok katmanlı güvenlik çözümleri sistemlerimizin korunmasında ve olası risklerin etkisinin sınırlandırılmasında önemli rol oynuyor. İkinci boyut ise gelişmiş tehdit istihbaratı, izleme, analiz ve olay müdahale yetkinlikleri ile güvenlik kapasitesini sürekli güçlendirmek. Tehditleri erken aşamada belirleyebilmek, güvenlik olaylarını doğru analiz edebilmek ve ilgili paydaşlarla koordinasyon içinde hızlı aksiyon alabilmek, etkin bir siber güvenlik yaklaşımının vazgeçilmez unsurları arasında yer alıyor. Bu iki yetkinliği bir araya getirdiğimizde yalnızca savunma kapasitemizi değil, siber alandaki caydırıcılığımızı da güçlendirmiş oluyoruz.

Saygıdeğer konuklar, Türk Telekom olarak Türkiye'nin dijital dönüşümüne liderlik ederken siber güvenliği bu dönüşümün ayrılmaz bir parçası olarak görüyoruz. Ülkemizin iletişim altyapısına yönelik sorumluluğumuzun yanı sıra kurumların dijital varlıklarını korumalarına ve güvenlik yetkinliklerini geliştirmelerine katkı sunuyoruz. Siber güvenlik alanındaki teknolojik birikimimiz, uzmanlığımız ve sunduğumuz çözümlerle dijital ekosistemin güvenliğini güçlendirmek için çalışıyoruz. Bizim için siber güvenlik yalnızca mevcut sistemleri korumak değil, geleceğin dijital dünyasını güvenle inşa edebilmektir. Bu anlayışla proaktif güvenlik yaklaşımını, gelişmiş teknolojileri, nitelikli insan kaynağını ve güçlü iş birliklerini önceliklendiriyoruz. Çünkü biliyoruz ki dijital geleceğin gücü yalnızca teknolojik kapasiteyle değil, o teknolojiye duyulan güvenle de ölçülecek.

Geleceğin dijital dünyasında fark yaratacak kurumlar; riskleri öngörebilen, güçlü önleyici mekanizmalar geliştiren, değişen tehditlere hızla uyum sağlayabilen ve güvenlik yetkinliklerini sürekli ileriye taşıyan kurumlar olacaktır. Türk Telekom olarak ülkemizin siber güvenlik ve dayanıklılık vizyonuna katkı sunmayı stratejik sorumluluklarımızdan

biri olarak görüyoruz. İnaniyoruz ki güvenli bir dijital geleceğin en güçlü dayanağı ortak akıl, güçlü teknolojik altyapı, yerli yetkinlikler ve etkin iş birliğidir.

ISCTurkey 2026'nın bu ortak vizyonun gelişmesine önemli katkılar sağlayacağına inanıyorum. Etkinliğin düzenlenmesinde emeği geçen, başta Bilgi Güvenliği Derneği ve Siber Güvenlik Başkanlığı olmak üzere tüm kurumlarımıza, değerli akademisyenlerimize ve sektör temsilcilerimize teşekkür ediyorum. Hep birlikte daha güvenli, daha güçlü ve daha dayanıklı bir dijital gelecek inşa etmek dileğiyle sizleri saygıyla selamlıyorum.

02:14:11 Abdurrahman ŞAKAR – Turkcell Siber Savunma Merkezi Direktör Yardımcısı

Sayın başkanlarım, sayın komutanlar, değerli katılımcılar, sevgili gençler ve bu güzel etkinliği düzenleyen Bilgi Güvenliği Derneği'ni saygıyla selamlıyorum.

Başkanımız ve diğer katılımcılar genel çerçeveyi çok güzel çizdiler. Ben biraz sahadan bahsetmek istiyorum; sahanın sesi olmak istiyorum.

Konuşmama tek bir rakamla başlamak istiyorum: 29 dakika. 29 dakika ne demek? 2026 yılında yayınlanan küresel tehdit raporuna göre saldırganların ilk erişimi sağladıktan sonra içerideki diğer sistemlere erişim süresi ortalama 29 dakika. Gözlemlenen en hızlı vaka ise 27 saniye. Peki bizim kurumumuzda bir saldırının fark edilmesi, değerlendirilmesi ve müdahale edilmesi ne kadar sürüyor? Dakikalar mı, saatler mi? Bu 29 dakika aslında birkaç sene önce aylar mertebesindeydi. Sonra günler mertebesine düştü. Şu an dakikaları konuşuyoruz. Bu sürenin giderek kısalması aslında yaklaşan tehlikenin ne kadar ciddi olduğunu bizlere gösteriyor.

Yapay zekâyı konuşurken genelde ne kadar akıllı modeller geliştirildiğini tartışıyoruz. Piyasadaki birçok bulut tabanlı veya on-prem büyük dil modeli kıyaslanıyor. Fakat burada siber güvenlik açısından çok daha farklı bir konu var: Yapay zekâ, saldırgan olmanın maliyetini düşürüyor. Yani siz bugün 100 dolar harcayarak çok etkin, akıllı, bilgili bir siber saldırganı kullanabiliyorsunuz ve bunun maliyeti sadece 100 dolar.

Bugün kurumlarda siber güvenliği yönetenlerin, yöneticilerin en büyük korktuğu sayı sıfır: zero-day'ler, sıfırıncı gün açıklıkları. Geçmişte sıfırıncı gün zafiyetlerini bulmak çok ciddi emek, profesyonellik ve teknik bilgi birikimi gerektirirdi. Bugün geldiğimiz nokta itibarıyla sıfırıncı günleri keşfetmek ve bunları sömürecek kodları yazmak çok kolaylaştı. Sıfırıncı günlerle beraber artık sistemleri baypas etmek ve içeriye girmek çok daha kolaylaştı.

Siber güvenlik ekiplerinin karşılaştığı diğer en büyük problem ise dijital dünyanın sürekli büyümesi ve karmaşıklaşması. Yazılım geliştirme hızı artıyor. Her gün yeni yazılımlar geliştiriliyor. Bununla beraber yeni uygulamalar, tedarikçiler, bulut servisleri, IoT cihazları hayatımıza giriyor. Çok hızlı gelişen ve büyüyen bir ekosistemden bahsediyoruz. Bu, siber güvenlikçiler için atak yüzeyinin gittikçe genişlemesi ve kontrol edilemeyecek bir noktaya ulaşması anlamına geliyor.

Toparlayacak olursak, içinde bulunduğumuz zaman diliminde yapay zekânın da katkılarıyla beraber saldırganlar lehine bir fark var. Günümüzdeki durumu

değerlendirdiğimizde saldırganlar defansif tarafa göre biraz daha öndeler. Tabii zamanla bu avantaj dengelenecek, ama o vakte kadar hiç olmadığı kadar tehdit altındayız diyebiliriz.

Şimdi burada siber dayanıklılık kavramı öne çıkıyor. Çünkü siber dayanıklılık hiç saldırıya uğramamak değil; saldırı karşısında mukavemet gösterebilmek, kritik hizmetleri sürdürebilmek ve değişen koşullara hızla uyum sağlayabilmek demek. Aslında eskiler buna “mukavim olma” derdi, bilirsiniz. Yani esnemek ama kırılmamak. Çünkü kırıldığınız anda olay biter. Yaşanacak bütün durumlara karşı vereceğimiz tepkilerin çalışmasını önceden yapmak demek. Saldırıya uğradığımızda tespit edebilecek miyiz? Ne kadar ayakta kalabiliriz? Ne kadar hızlı karşılık verebiliriz? Time to detect, time to respond türevlerini ne kadar iyileştirebiliyoruz? Her duruma hazır mıyız? Bunların simülasyonunu yaptık mı? Bu önemli bir gündem maddesi.

Tabii hiçbir yatırım bizi tek başına koruyamaz; doğru şekilde kurgulanması gerekiyor. Doğru şekilde kurgulanmış teknoloji yatırımları bize hız, esneklik ve adaptasyon sağlayacak. Bu nedenle yaptığımız her yatırımda, her bir organizasyonda cyber resilience, yani dayanıklılık kavramını ön planda tutarak hareket etmemiz gerekiyor.

Bahsetmek istediğim bir başka konu daha var. Kurumların itibarı artık bir siber saldırı olmadan da etkilenebiliyor. Mesela bir sabah kalktığımızda herhangi bir kurumla ilgili sosyal medyada veya dark web forumlarında bir veri sızıntısı haberini çok sık görüyoruz: “Kurum hacklendi, milyonlarca veri sızdırıldı.” Bu haberler çok hızlı bir şekilde yayılıyor, çünkü yalanın alıcısı çok oluyor. Ama ortada henüz doğrulanmış bir veri yok. Bunun doğrulanması yapılmadan, o kurumun hacklendiğiyle, verilerin sızdırıldığıyla ilgili birçok haber bir anda basına yansıyor. Belki o veriler yıllar öncesine ait olabiliyor veya zaten public olan veriler bir şekilde derlenip toparlanıp sunulabiliyor. Bu tarz durumlarda kurumun itibarı zedelenabiliyor. Son dönemde aslında bununla sıklıkla karşılaşyoruz; belki birçoğunuza tanıdık da gelmiş olabilir. Şimdi burada bu iddiaların çok ciddi bir şekilde araştırılması gerekiyor. Bu iddiaları ortaya atanların da ciddi bir şekilde sorgulanarak cezai yaptırımlara maruz kalmalarının bizler için elzem olduğunu düşünüyoruz. Bu sebeple kriz anlarında doğru bilgiyi, doğru iletişimi sağlamak ve gerekli birimleri bilgilendirmek çok önemli.

Diğer bir konu ise, başkanım da bahsetti aslında, çok da mutlu oldum, çok da güzel bir örnekti: bağlılık sisteminden bahsetti. Şimdi siber suç ekosisteminde her alanda ciddi bir uzmanlaşma var. Mesela bir grup ilk erişimi sağlıyor, bu erişimi satıyor. Diğer grup fidye yazılımı geliştiriyor, bu fidye yazılımını “as a service” olarak sunuyor. Baktığınız zaman komuta kontrol merkezi hizmetini veren var. Burada aslında biraz para harcayıp çok güzel bir saldırı altyapısı oluşturabilirsiniz ve saldırganlar arasında böyle bir dayanışma var. Diğer tarafa, savunma tarafına baktığımız zaman biz ne yapıyoruz? Çoğu zaman aynı saldırıyı ayrı ayrı kurumlar analiz ediyor. Aynı tekniklere karşı farklı yöntemler geliştiriyoruz. Saldırganlar bu yöntemi avantaja çevirirken biz bu bilgiyi çoğu zaman kurum sınırları içerisinde tutuyoruz. Tabii bunun birçok sebebi var. Buradaki bilgiyi paylaşmaktan kastım şu değil: IOC’den bahsetmiyorum; bir hash, IP veya domain bilgisinden bahsetmiyorum. Bir kurum bir saldırıyla karşılaştığı zaman bu saldırıya karşı hangi teknik ve taktikleri geliştirdi? İçeride bunun analizini nasıl yaptı? Bu bilgi aslında çok değerli. Çünkü o kurumun karşılaştığı durumu henüz yaşamayan birçok kurum var.

Bu bilgi paylaşımı sağlıklı bir şekilde yapıldığı zaman diğer kurumları da biz aslında savunmuş oluyoruz. Buna belki ulusal bağışıklık sistemi diyebiliriz. Burada bir çalışma ihtiyacımız var gibi duruyor.

Değerli katılımcılar, yapay zekâ saldırganlara hız ve ölçek kazandırıyor. Ama aynı teknoloji savunma tarafında da önemli fırsatlar sunuyor. Peki burada çözüm daha fazla güvenlik ürünü satın almak mı? Daha fazla zafiyet taramak, daha fazla alarm üretmek mi? Bunlara elbette ihtiyacımız var. Ancak asıl ihtiyacımız siber güvenliği daha akıllı ve bütünleşik bir yapıya dönüştürmek. Artık ne kadar çok şey tespit ettiğimiz değil, tespit ettiğimiz bütün bu verileri risk anlamında değerlendirerek en riskli olanları önceliklendirip kapatmak önemli.

Bununla beraber yapay zekâ ve otomasyonu da bir fırsat olarak görmemiz gerekiyor. Çünkü ekiplerin sayısı sınırlı, atak yüzeyi genişliyor. Yapay zekâ ve otomasyonla ekiplere nefes aldırarak buradaki emeği farklı işlere kanalize edebiliriz.

Tabii son olarak şunu da söylemek gerekiyor: Güvenliği yalnızca güvenlik ekiplerinin sorumluluğuna bırakmamamız gerekiyor. Yani siber güvenlik bir ekibin tek başına sağlayacağı bir konu değil; bütün kurumun beraber hareket ederek ele alabileceği bir konu. Örneğin işletim sistemi ve veri tabanı yöneticilerinin buradaki yamaları geçmeyi kendine bir sorumluluk olarak alması gerekiyor. Yazılım geliştiricilerin bir yazılımı geliştirdikleri zaman buradaki zafiyetleri gidermeyi kendilerine bir görev olarak atfetmeleri gerekiyor.

Son olarak sözlerimi toparlayacak olursam: Saldırı gerçekleştiğinde ayakta kalabilmek, hızlı toparlanabilmek ve öğrendiklerimizi ortak savunma gücüne dönüştürebilmek yeni düzenin ayakta kalma prensipleridir diyerek konuşmamı tamamlıyorum. Herkese teşekkürler, saygılar.

DAVETLİ KONUŞMACI OTURUMU

02:23:07 Prof. Dr. Şeref SAĞIROĞLU – Gazi Üniversitesi Öğretim Üyesi

Evet, değerli katılımcılar, 19. Bilgi Güvenliği ve Kriptoloji Konferansı'nın öğleden sonraki ilk oturumuna hepiniz hoş geldiniz. Bu oturum davetli konuşmacı oturumumuz, keynote speaker oturumu. Size Prof. Dr. Najmul Islam'ı kısaca tanıtacağım, daha sonra kendisini buraya davet edeceğim. Bu oturum İngilizce olacak, çeviri yok; sizlerin de bildiğini düşünüyoruz, programda ilan edildiği gibi. Hızlıca kendisinin özgeçmişini okuyayım.

Kendisi öncelikle Finlandiya LUT Üniversitesi Yazılım Mühendisliği Bölüm Başkanı. 2022 yılında Finlandiya Yılın Bilgi Sistemleri Bilim İnsanı Ödülü'nü almış, 2024 yılında LUT Vakfı Ödülü'nü kazanmış bir konuşmacımız. Horizon Europe, Finlandiya Araştırma Konseyi, Business Finland ve Avrupa Birliği CHIST-ERA gibi kuruluşlar tarafından finanse edilen milyonlarca euroluk araştırma projelerine liderlik eden bir bilim insanı. Yüksek lisans derecesini Finlandiya'daki Tampere Teknoloji Üniversitesi'nden, doktora derecesini de Finlandiya Turku Üniversitesi'nden almıştır. Çalışma konuları stratejik bilgi

sistemleri, bilgi sistemleri ve karar destek sistemleri. Katkıda bulunduğu, editörlüğünü yaptığı dergiler var; bu arada pek çok alanda saygın dergilerde yayınları ve saygın konferanslarda konuşmaları olduğunu da ifade edeyim.

Okay. Thank you very much for your attention. I invite Professor Najmul Islam for his presentation. Thank you.

02:25:14 Prof. Dr. Najmul ISLAM – LUT Üniversitesi Yazılım Mühendisliği Bölüm Başkanı

Thank you, everyone. Thank you for the wonderful introduction of me. My name is Najmul, and I would like to thank Professor Tuncay for inviting me for this keynote. I am very glad to be here today.

Today I am going to speak about responsible, trustworthy, and lawful design and use of blockchain-based systems. But before I really go into the topic of today, I would like to introduce myself a little bit better, because I know that there are many academics here and maybe you would like to have more collaboration with European universities. So that is why I would like to tell a little bit more about me and my university, so that you could contact me later for more collaboration.

So, this is me. This photo was taken some 14 years ago; I hope that I look the same. I am originally from Bangladesh, but I have lived in Finland for the last 20 years. I did my master's and PhD in Finland, and I am now a full professor and head of the Department of Software Engineering at LUT University in Finland. The department is quite big: we are around 120 people, and I have been leading that 120-person department for the last one and a half years or so. I am also an adjunct professor at Tampere University, another Finnish university in Tampere.

My research is all about responsibility, the responsible use of software systems. When I talk about responsibility, I try to capture a very broad scope. It is not just sustainability and things like that; security, lawful design, everything comes under the umbrella of responsibility. I have been very active in Horizon projects and local national projects. In one of the projects we were working with Professor Tuncay; the project name is DI4SPDS, and the project is about the security and privacy of decentralized systems. From there I got connected to Turkey, and then I am here, and once again, thank you for that. The project is an initiative by the European Union. Other than that, I have been very active in other projects, like GDPR compliance of blockchain-based systems, and then AI governance and auditing AI, and there are a couple more projects and so on.

I have been extremely successful in terms of publishing in high-quality journals and conferences, and I am an editor of several journals. I have a couple of awards; for instance, I was the Finnish Information Systems Scientist of the Year in 2022, and I was also the winner of the LUT Foundation award in 2024. We have a very interesting lab called the Blockchain Lab, where we do all blockchain-related and security-related work. There is a website for that; you could take a look, and if you find anything interesting, then just contact me or one of the people from there.

But now let us go to today's topic. Today I am going to give you a very holistic view. I will not just talk about, let us say, very technical things, but try to give you a very holistic view of blockchain-based systems. I will cover topics from the sociotechnical perspective, which means that I will talk about things related to the users, the developers, and also policymakers or the regulatory bodies and so on. So not just about technical things, so that all of you can somehow connect with this. I will try to raise a few critical questions about blockchain in general. But I will not answer those questions; it will give you some kind of critical thinking. So at the end of the keynote you will leave this place with more questions, most likely, when you are going to use blockchain. The content of this keynote is based on the research that my team and I have been doing for the last several years, 5 to 10 years or so.

All right. So, as I was telling you about the critical questions, the most critical question I would like to raise is: does blockchain really matter? Can anyone comment? Is blockchain really useful? Yes? Okay. We will see. But why am I saying this? Blockchain has been here for quite some time, but maybe so far the only application you have heard of is cryptocurrency, the big application. Have you heard of any big business, any very big application that generated hundreds of millions or so, other than cryptocurrency? All we see is that some small-scale pilots were there in the supply chain context, some very small-scale pilots, but there is nothing big so far except cryptocurrency. So this is why I was trying to raise the question: does blockchain really matter?

We were looking into this very broad question from different perspectives. The first perspective is the user or consumer perspective. Let us take a look from the consumer side: what do consumers and users think about blockchain? We did some research looking especially into blockchain's transparency feature, because that is one of the most important features, as we all know. We wanted to look into whether this transparency feature really improves trust or, let us say, the satisfaction of the consumer. Then we found that yes, indeed, transparency increases trust, and then maybe it increases consumer satisfaction. However, when we tried to look a little bit further, what we found was that yes, transparency really matters, transparency as a feature really matters, but it does not matter if you are getting the transparency from a blockchain-based system or from a non-blockchain-based system. So what the user really wants is transparency, nothing about the technology. Then we looked into the same thing in different contexts, the supply chain context, the smart grid context. I have several PhD students looking at these things from different perspectives and different contexts, and we find that this is really the case: from the user perspective it does not really matter. They want transparency, they want security, they want those features, but it does not matter if it is coming from blockchain or some other system.

Okay, so that is the thing from the user perspective. But now let us take a look from the regulatory perspective. I come from the European Union, so there we practice this regulation, and I hope that all of you have heard of it: GDPR, the General Data Protection Regulation. As you know, in the European Union all services should follow this law. GDPR stands for General Data Protection Regulation, and it is considered the toughest privacy and security law in the world. This is not my statement; if you go to the official website, they wrote that sentence, that it is the toughest privacy and security law,

and it imposes obligations onto organizations anywhere, as long as you collect data from European subjects. There have been many GDPR violations, and the penalties for violations are really big: 20 million euros or 4% of global revenue, whichever is higher, plus compensation to the data subjects. Amazon, Google, H&M, they were all fined. Public organizations also received this kind of penalty, in Norway and many other countries. This is a very important regulation in Europe.

We now try to look into blockchain and GDPR to understand the regulatory perspective. Of course we could bring in other regulations, but I prefer this one, as it is the most used one and the most known one, so I just picked this one. In GDPR there are some concepts, concepts like personal data. What is personal data? Personal data is any information that relates to an individual who can be directly or indirectly identified. Data processing means any action performed on the data. Data subject means the citizens, or the people whose data you are collecting. Data controller means that each organization needs to have at least one person responsible for saying how the personal data has been processed in the organization. And data processor means some third party that processes personal data.

So these are some basic concepts, but now let us take a look at the GDPR principles and how blockchain works with these principles if you compare them side by side. The first GDPR principle is called lawfulness, fairness and transparency. This means that processing must be lawful, fair and transparent to the data subject. Now just think of blockchain. Blockchain provides you traceability. Blockchain provides you transparency. So the data subject can really see how his or her data has been used or shared. If you think about the first principle of GDPR, then it seems that blockchain is quite aligned with this, and blockchain in fact provides this. So if you need something lawful, fair and transparent, maybe blockchain could be used.

Then the next one is purpose limitation. It is about processing data for the legitimate purposes specified explicitly to the data subject when you collected it. I think this one is also somehow okay with blockchain. Data minimization means that you need to collect as little data as possible, just to provide the subject the service; do not collect too much data. But then the next one is about accuracy, and accuracy is about keeping personal data accurate and up to date. This basically means that your data should be editable, but blockchain does not allow you to edit your information. So if the GDPR principle of accuracy has to be followed, then there is a paradox here. Then the next one, even more interesting, is storage limitation: you may only store personally identifying data as long as necessary for the specified purpose. This means that the data needs to be removed at some point, but blockchain is just growing and growing and growing from the very beginning, and deleting is not possible. So again you see there is a discrepancy between blockchain and GDPR. Then the next one is integrity and confidentiality. We know that blockchain provides integrity and confidentiality with different techniques, very solid techniques, so there should not be any issue; this is quite aligned with blockchain. And then accountability. Accountability is about the data controller. As I was telling you, there should be a data controller who is responsible for showing that GDPR compliance has been achieved. But now, if you think about a decentralized system, who is the data controller? There are many miners; who could be

the controller, how do you define the controller, whose responsibility is it if something happens? So that is also a little bit challenging in the case of blockchain.

Then this is basically the same thing: these are the rights of the citizen under GDPR that must be given if you develop some systems. Among these, the third one is called the right to rectification. This means your data should be editable; when your address changes, you should be able to change it, but blockchain does not allow editing. And then the right to erasure means the data should be removed if a citizen wants, but blockchain does not allow that. So this is basically the same thing that I just explained. Continuing with this, as I have explained, there is some kind of paradox, there are some incompatibilities between blockchain and GDPR, and this has also been acknowledged by the European Parliamentary Research Service. When we tried to look into the use cases that have been tried in the context of supply chain or anywhere else, we really saw that GDPR was not really taken into consideration when they developed those systems.

So this is just the same thing in a very summarized manner: GDPR recommends data minimization, purpose limitation, modification and deletion of data when necessary. But blockchain is an append-only database that continuously grows when new data is added; modification and deletion are not allowed, or not recommended. And then again, according to GDPR there should be one data controller, but blockchain is a decentralized system, which means that there could be many data controllers, and then some kind of coordination needs to be done, and this makes the allocation of responsibility very difficult.

Then, when looking into the solution for this, we saw that some business cases have used this: what they did was just store personal data in another database, off-chain, and make a link between the off-chain side and the chain. Then if somebody asks to delete something, they just cut the link. But the question is then: how important was the blockchain really, if you just need to maintain another side database? There are some other solutions which are found in the literature, but they have not really been implemented in any of the use cases that we have studied so far. About the controller, some literature says that miners could be the controller, data providers could be the controller, some designated nodes could act as the controller, and things like that. And then in GDPR there is this territorial scope, which says that European citizens' data should be stored in Europe. So in that case, this kind of worldwide big blockchain is not really the solution; some kind of small-scale blockchain is really the solution. But as I was telling you, blockchain also provides this lawfulness, and it shows that your data has been fairly shared. So in some aspects blockchain and GDPR are very much aligned.

Okay. So now we know what kind of discrepancies there are between blockchain and GDPR. Let us now take a look at the developers' perspective. From the developer perspective, I would say that if someone develops a system, it has to be GDPR by design, or regulatory compliant by design. So blockchain architects need to be aware of these kinds of challenges from the very beginning, and when they develop the system they should remember that they should follow the regulation, whichever it is: if it is European, then European regulation; if it is somewhere else, then that regulation. What

we are really suggesting here is regulatory compliance by design. From the very beginning, you as a developer try to bring the design principles into the system. Not later, after you have developed the system and now you need to somehow comply with the regulation; that should not be the approach. From the very beginning, proactively, you should put all these regulatory design principles into the system rather than reacting later. And if you really want to do that, this kind of development cannot be done by a lonely developer who just uses his technical skill to do it. I mean, there should be interaction between developers, end users, policymakers, legal experts and so on. Only then could you find the right design requirements and design principles to build your system. Then also the takeaways for the developers are: collect as little personal information as possible, because GDPR also says that; and then the off-chain solution looks like the only solution available. We did not see any other solution that has been used in the current business cases.

And then this is one use case that we tried at our university, with my team. The product is called SafeRecord. Our idea was: when, let us say, experts from India apply to Finland or Europe for a job, how do we verify their credentials? How can we verify that their certificates are not fake? The same thing can be applied, for instance, in the educational context, when students from the subcontinent or from Brazil or somewhere else are applying to us: how do we verify that their bachelor's degree and master's degree certificates are not fake? For that kind of thing we developed a system, a blockchain-based credential verification system. What we really did, as I was telling you, is that before developing such a system you need to speak with different stakeholders; it is not just a developer or designer or architect developing it from his technical skills. What we did is we talked with recruitment agencies, employers, universities and so on, and then we tried to understand what kind of challenges they are facing. We also looked into the GDPR documents and so on, and based on that we really approached it. Then we developed the proof of concept, and it was working.

But then the bigger problem comes, and the bigger problem is how to make money then. So okay, we have a solution, we have a software solution, but it is a blockchain-based system, and it brings new questions, questions like: who runs the nodes? What is the incentive mechanism? And we could not really answer those. Although those questions sound not so difficult to hear, when you think of these questions from the business point of view, it is not that easy to answer. Are the universities interested in running the nodes? If they want to, why do they do that? So we could not really figure out who pays for it and how to make money out of it. So then we just had it as a proof of concept, just like other cases. There are tens of such cases in the supply chain context and in other contexts where they just tried, and then they could not make money out of it, and our situation was the same.

So again, I started with "does blockchain matter?" I do not know if you have an answer, or if you have more questions. I have more questions, but you can think about whether it matters or not. But one thing is that blockchain helps to develop responsible systems, because it provides traceability; it shows how your data has been shared and things like that. So yes, it helps to develop responsible systems, but we do not have a solid case yet other than cryptocurrency. But maybe in the future some use case will come, especially now with AI and automated decisions; perhaps everything could be stored in

blockchain to check. We did not really see the actual use case yet, so maybe more cases, or more relevant use cases, will come, and we, the researchers, need to find it out; business people need to find it out. With that, I would like to thank everyone. Thank you.

Soru: In your presentation, could interacting blockchain with artificial intelligence and multi-agent systems fundamentally change its role in future cybersecurity architecture, for instance as an adaptive trust architecture?

Cevap: Adaptive trust architecture, yes. I think you are absolutely right. Scalability is one problem, and as I said, probably we do not really have the right use cases yet, so maybe more use cases will be coming in the future. But yes, currently scalability is obviously one reason. Thank you very much.

Soru (Prof. Dr. Şeref Sağiroğlu): Professor, let me ask you one question. When we consider systems from the security perspective, we have privacy by design, security by design, governance by design, and also recently resilience by design, and more recently AI by design. How do you see this from the blockchain perspective?

Cevap: I do not really have a right answer, but I think in Europe it is not just about blockchain; in general, people are trying to be lawful by design, and there has already been some research. They are talking about this. So I started with this term “GDPR by design”, and then suddenly I started to look at that, and some people started to think a little bit further: it is not just about GDPR, it is regulatory compliance by design or lawful by design. So I think we will have more design perspectives in the future than what I understand now.

Soru: I am a PhD student; my topic is blockchain adoption in agricultural finance. Initially I wanted to work on practical data, but I could not find any real application, like you talked about. Is GDPR, or regulatory compliance, a driver or a barrier for blockchain?

Cevap: Yes. This regulation is definitely a kind of barrier, in the sense that it slows down the technology, and this is a very debated topic at this moment in Europe, especially in AI. When you talk about AI, then you see that the US and China are leading, and Europe is doing regulations. This is something often told as a joke, but it is really the fact. If you also look at how many European innovations there are so far in the AI domain or some other domains, there are not many, or maybe none. So yes, you are absolutely right, regulation kind of delays the process. But on the other hand, you cannot really do anything with the technology; there should be some kind of regulation, some kind of barrier, otherwise we need to follow rules. So yes, it somehow delays, but still I see it as a good thing.

But then, about your PhD research, I have more comments. One of the things that you could do, for instance: you could design some scenarios. There is no blockchain-based application, most likely, as you are saying, but you could design some kind of scenario and then send it to, let us say, 200 or 300 people, and then you get quantitative data through the scenario. Also, you can make some user interfaces; you can design them by yourself and then show that this is the blockchain-based system, and then you could

show another, non-blockchain-based system, and then you could ask their perception about adoption and make a comparison. That kind of research we have also been doing, so if you go to my Google Scholar profile, you will find those kinds of papers as well; that might help you. Okay, I know you have more questions. Thank you. Thank you.

Prof. Dr. Şeref SAĞIROĞLU: Peki. Evet, Profesör Doktor, buyurun hocam. Biz oturumu burada kapatıyoruz; gündemi biraz uzattık ama. Evet, buyurun. Estağfurullah. Teşekkürler.

2. OTURUM: PLATFORM SİBER GÜVENLİĞİ

03:01:55 Taha YÜCEL – ASELSAN Genel Müdür Yardımcısı

Hocalarım, değerli konuklar, değerli misafirler, hepiniz hoş geldiniz. Tabii bu 19. Siber Güvenlik ve Kriptoloji Konferansı; konu başlığı özenle seçilmiş. “Yeni dünya düzeninde siber savaşlar” çok anlamlı. Gerçekten çok emek verilmiş. Tabii 19 kere bu TÜBİTAK destekli konferansı yapabilmek önemli bir başarı. Bundan dolayı hem konferans başkanı Tuncay Gençoğlu hocamıza, hem Mustafa Alkan hocamıza, hem de değerli Bilgi Güvenliği Derneği yöneticilerimizin hepsine teşekkür ediyoruz.

Değerli arkadaşlar, geçmişe baktığımızda, yani bu savaş düzeniyle ilgili bir yönüyle kısaca Dünya Savaşı’na kadar, biraz geriye baktığımızda şunu görüyoruz: Geçmişte çeliği güçlü olan, motoru güçlü olan, hızlı tank yapabilen, çok sayıda tank yapabilen, çok sayıda uçak yapabilen ve bir yönüyle aslında ekonomik gücüyle de bu tür pahalı, görece pahalı ürünleri üretilip hızlıca sahaya sürüp bu avantajla harekât alanında avantaj elde eden ülkeler ve ordular gördük. Ve bu tabii hâlâ da, bugün itibarıyla tank, uçak vesaire savaş silahlarının bir parçası; ama hepsinde bir değişikliği son savaşlar bize gösterdi. Bundan neyi kastediyorum? Hemen yanı başımızda Ukrayna Savaşı’na baktığımızda, savaşın ilk başından itibaren -ki yıllar oldu, yıllardır süren bir savaş- teknoloji kullanımının ve asimetrik teknoloji kullanımının çok fazla olduğunu görüyoruz. Aslında bu tür savaşların öncü habercisinin de siber güvenlik saldırıları olduğunu görüyoruz. Yani bir yere bir harekât olmadan önce, önce bir siber savaş başlıyor, önce bir siber saldırı başlıyor, siber savunma başlıyor; ondan sonra, ardından asıl mermiler ateşleniyor. Yani mermiler atılmadan önce aslında siber savaşın başladığını görüyoruz. Siber ortam bunda da aslında bir savaşın habercisi gibi oluyor. Bazen hiç mermi atılmadan siber savaş oluyor. Pek çok ülke bunlarla muhatap oluyor. Türkiye de hedef ülkedir veya bir şekilde bu anlamda güçlü olması gerekir, caydırıcı olması gerekir.

Ukrayna’ya yine baktığımızda, aslında bu çok karışık bir olgu da değil: Asimetrik olanın avantajlı olduğunu görüyoruz. Bundan kastımız ne? Az önce bahsettim ya, pahalı sistemler, pahalı platformlar ve bunların bir şekilde savaş alanında harekâtı yönlendirmesi... İşte bunlara ucuz teknolojilerle, ucuz belki yöntemlerle karşı koyduğunuz veya karşı tarafa bunlarla saldırdığınız zaman, işte Ukrayna’da bunu gördük. Yani koskoca Rus ordusu belli bir yerde tabii ki belli kazanımlar elde etti ama daha sonrasında Batı’nın da verdiği destekle belli bir alana sıkıştı ve savaş oradan ilerlemiyor; orada bir şekilde ciddi bir mücadele sürüyor. O ne mücadelesi? Dronlarla

yapılan mücadele, yapay zekâlı sistemlerle yapılan mücadele. İlk başta biraz daha görece akılsız dronlarla saldırı yapılıyordu; belli kamikaze dronlar ve benzeri silahları gördük. Sonrasında bunlar kolay vurulmaya başladı. Bunlar yapay zekâyla manevra yapmaya başladılar. Bu sefer bunu önleyen sistemler yapay zekâ ve üstün yazılım teknolojileriyle karşı koymaya başladı. Ama sonuç olarak sürü saldırıları ve benzeri saldırılar, bunları gördük.

Diğerini de yine İran Savaşı'nda gördük. Aslında İran, karşılarındaki güçler karşısında gemi, tank, uçak vesaire birçok anlamda görece çok zayıftı. Çok rahat bir savaş olacağını öngörüyorlardı. Yani savaşın başlangıcında, biliyorsunuz, "Biz 8 günde, 9 günde bitiririz bu işi; 10 gün bile olmaz" gibi bir öngörü vardı. Bu açıklamalar, resmî açıklamalar internet sayfalarında duruyor: "Bunu 8 günde bitiririz, 7 günden sonra iş biter" vesaire. Böyle açıklamalarla başlayan süreç ne kadar oldu? Hâlâ dün itibarıyla yine belli saldırılar oluyordu, belli savunmalar oluyordu. Peki İran'ı burada güçlü yapan ne oldu? Karşıdaki ülkelere karşı aslında teknolojiyi kullanmak oldu. Yani o tankla, uçakla savaşmadı. İran'ın bir tane uçak kaldırdığını ben hatırlamıyorum. Hepsini bir yerlere sakladılar, bir yerlere park ettiler; bir kısmı vuruldu zaten. Ama hava sahasında vesaire herhangi bir mücadelesi yoktu. Yerin altına girmiş ve aslında baştan buna güzel bir şekilde hazırlanmış. Belli ki buradan öğrenecek çok ders var.

Kendisini bir kere güvenli bir ortama, en azından belli üretim ve saldırı imkânlarıyla saklamış. Bu önemli. Yani güçlü bir direniş yapısı var. Karşısında da geliştirdiği belli sistemler var; aldığı belli destekler var tabii ama kendi teknolojisi de var. Karşısındaki güçlü sistemleri ucuz sistemlerle vurabiliyor. Örnek vermek gerekirse, çok değerli -ne kadar değerli? Milyar dolar değerinde- büyük bir radarı basit sistemlerle birkaç kere vurdu, en sonunda artık kullanılamaz hale getirdi. Tam yerini ve ayrıntısını söylemeyeyim, zaten açık bilgi kaynaklarında var bunlar. Üst üste vurdu: Önce ilk hasarı verdi, tamir ettiler; bir daha hasar verdi; en sonunda artık geri dönmez şekilde vurdu ve o radar işlevini kaybetti. Milyar dolar seviyesinde, çok güçlü bir radardı o. Aslında iyi de korunuyordu bu arada. Bu tür sistemleri yapanlar bunun koruma sistemlerini de yapıyorlar. Aramızda Sami Duman Bey var, bizim eski hava savunma direktörümüz; sağ olsun, ASELSAN'ın bunlarla ilgili hava savunma ve benzeri sistemleri o ülkelerde fazlasıyla var. Buna rağmen mani olamadılar. Niye? Çünkü aslında her sistemin zafiyeti var, her sistemin açığı var. Buradan siber güvenlik alanına geleceğim.

Değerli arkadaşlar, tabii değişen tehditler, yani yeni savaş ortamında, siber güvenlik alanında ve bu tür asimetric tehditlerle, evinden hiç çıkmayan, iyi yetişmiş bir bilgisayar kullanıcısının görece ucuz bir bilgisayarla oluşturduğu bir tehditten bahsediyoruz. Yani bu aslında çok fazla bir ölçek gerektirmiyor, çok fazla bir yatırım gerektirmiyor, çok fazla bir organizasyon gerektirmiyor; ama çok büyük bir hasar verebiliyor, çok büyük bir imkân oluşturabiliyor. Daha yakın zamanda, birkaç gün önce değerli bir arkadaşımın, bir girişimci arkadaşımın önemli bir şirketi siber saldırıya uğramış. Sabahın köründe aradı. Zaten anladım; sabahın köründe, ben de toplantıya tam girdiğim bir dönemdi, üst üste aradığını görünce ciddi bir sıkıntı olduğunu anladım. Kendisine döndüm, "Ne oldu?" dedim. Dedi ki "Bütün sistemlerimiz kilitlendi; bizden ciddi bir miktar istiyorlar." Ransomware ile tamamen kilitlemişler. "Yedeğin yok muydu?" dedim. "Yedek de sisteme bağlıydı" dedi. Eyvah! En büyük hata işte. Yani aslında yedeğe yatırım yapmış, yedek sistem oluşturmuş, altyapısını güçlü bir şekilde kurmuş, belki firewall'a vesaireye

yatırım yapmış; ama yedeği sistemden fiziki olarak ayırıp bir yerde saklaması gerekirken yedeği de sistemle entegre tutunca ve saldırıya maruz kalınca yedekler de tabii kilitlenmiş. Yani yedeği de elinde değil. Yapacak çok fazla bir şey yok. Tabii mutlaka belli çalışmalar yapılıyor ama şunu demek istiyorum: Görece basit bir saldırıyla çok büyük bir yapıya -ki bu dediğim arkadaşımın grubu içinde hastaneler falan olan bir grup, yani onda oldukça sıkıntılı- verilen hasar çok fazla iz bırakıyor.

Peki ne yapmak lazım değerli arkadaşlar? Bir kere burada siber güvenlik dediğimiz olgu ve yeni savaş düzeninde en önem vermemiz gereken konu, tabii ki birazdan bahsedeceğim pek çok önlemi almak lazım ama her şeyin ötesinde insan unsuruna çok çok dikkat etmek. Bir kere yetişmiş siber güvenlik çalışanlarına emanet ettiğiniz sistemler var; siber güvenliği bir masraf olarak veya basit bir gider kalemi olarak görmemek lazım. Siber güvenlik yatırımı bir şirket için stratejik bir yatırımdır. Bunu çok net bir şekilde zihninizde olgunlaştırmamız lazım. Siber güvenliğe yapılan yatırım bir masraf, bir finansal yük veya bir israf değil; tam tersine, stratejik, olmazsa olmaz, olmadığı zaman çok fazla zarar göreceğiniz bir yatırımdır. Ondan dolayı bu noktada tabii insana yapılan yatırım da böyle. Birçok kuruluşun birçok pahalı ekipmanı var; ama o kuruluşlara “En değerli varlık nedir?” diye sorduğunuz zaman -benim çalıştığım kurum da öyle- en değerli varlık insan. Hem de güvenilir insan. Tabii burada işin güvenlik boyutu da önemli. Yine aramızda olan yönetim kurulu üyelerimizden değerli bir siber güvenlik yöneticimiz var. Onunla bugün konuşurken dedi ki: “Artık iş öyle bir boyuta geldi ki çalışanlara, şirketin verisini satmaları veya bir şekilde çalmaları için belli bir ödeme teklif ediliyor. Başka bir şirkette de yine tanıdık birisini bulursa, orada komisyon teklif ediliyor.” Bu şimdi ahlaki bir soruna ve aynı zamanda insanla ilgili ciddi bir endişeye sevk eden bir durum ortaya çıkarıyor.

Ne yapmak lazım? Aslında daha önce de vurgulandı: Zero trust (sıfır güven) politikasıyla, yani hiçbir şeye güvenmeden, hiçbir eksik bırakmadan sistemi bir kere iyi tasarlamak lazım. Ve sistemden veri çıkışını, verinin nereye gittiğini sürekli takip etmek lazım. Çok değerli varlığınız olan verinizin, kendi kullanıcılarınız tarafından bile acaba gerçekten ihtiyaç için mi kullanıldığını, yoksa kendi yetkisi olmayan veya ihtiyacı olmayan verileri de alacak şekilde fazlaca bir veri transferi mi yapıldığını sürekli takip edip, yapay zekâ ve benzeri sistemlerle de destekleyerek izlemek lazım. Yani sistemi sürekli tarayıp takip etmek ve en ufak bir anomalide bunun önlemini almak lazım.

Bunun için platform siber güvenliğini -konu başlığımız- ben dört temel ilke olarak özetledim. Aslında daha fazla da özetlenebilir ama bunlardan birincisi: daha tasarım aşamasında siber güvenlik. Tasarım çok önemli. Ürün tasarlarken, birçok üründe daha tasarım aşamasında belli parametreler, kriterler oluşuyor ve tasarımı doğru yaparsanız ondan sonra ürün başarılı oluyor. Yoksa tasarımı düzeltmek çok zor; onu üretim sırasında tekrar olgunlaştırmak, tekrar düzeltmek çok zor. Tasarımı baştan sağlama yapmak lazım. İşte tasarım yaparken siber güvenliği de tasarımın içinde bir parametre haline getirmek lazım. Bir sistem tasarlıyorsunuz; bu herhangi bir ürün olabilir, bir muhasebe yazılımı olabilir, siber güvenlik alanında yine başka bir konu olabilir. Bir yazılım yapıyorsunuz; bunun daha tasarım aşamasında siber güvenliğini, yani platformun siber güvenliğini nasıl sağlayacağınızı da bir parametre olarak tanımlayıp, tasarım parametreleri arasında siber güvenlik unsuruyla birlikte, yani baştan güvenli tasarlanması önemli. Sistemi bu şekilde tasarlamak lazım.

İkincisi, katmanlı savunma. Yani tek bir güvenlik duvarı değil, birkaç katman. Bunda tabii bütün yumurtaları aynı sepete koymamak; az önce bahsettiğim arkadaşımın yaptığı hatayı yapmamak, yani yedeği sisteme entegre etmemek, yedeği fiziki olarak ayırmak, gerektiği zaman entegre edip tekrar önlemini almak, birden çok yedek tutmak bu anlamda önemli; ve birkaç katman.

Üçüncüsü, tedarik zinciri. Aslında hiçbir şirket, belli bir ölçeğe ulaşmışsa, kendi başına her şeyi üretmiyor. Yurt içinden ve yurt dışından çeşitli tedarikçilere belli tasarımlarını ürettiriyor, belli kısımları topluyor ve bir ürün haline getiriyor. Hepimiz öyle yapıyoruz, büyük şirketlerin hepsi. Burada tedarik zincirindeki siber güvenlikle ilgili açık da sizin açığınız olabilir. Çünkü ona bağlantı kuruyorsunuz, onunla mutlaka veri alışverişinde bulunuyorsunuz, o sizin bir parçanız oluyor. Belli bir aşamada onun verisini sizin takip ediyor olmanız lazım: Üretiyor mu, üretmiyor mu, ne aşamada vesaire. Onun güvenli olması, sisteminin hacklenmemesi, sisteminin çökmemesi; aksi halde sizin üretiminizi aksatıyor. O eğer hacklenirse ve onun sistemi donarsa sizin üretiminiz kalır. O yönüyle de size veri olarak hiç zarar vermese bile, o zarar gördüğü zaman siz de zarar görüyorsunuz; çünkü stratejik ortakınız, müttefiksiniz. Ondan dolayı tedarik zincirinizdeki yapıların da siber güvenliğine önem vermek lazım. Bunun, daha işin başında size tedarikçi olacak yapılarla planlanması lazım ve onların siber güvenliğine gerekirse sizin yatırım yapmanız veya destek olmanız lazım ki yarın ondan dolayı belli bir ölçekte bir sıkıntı yaşamayasınız.

Dördüncüsü de kriptografik egemenlik. Bundan kastım şu: Tuncay hocam da kuantum kriptoloji ve benzeri konuları, sağ olsun, ülkemize kazandırmaya çok çalışıyor. ASELSAN'ın TOBB Üniversitesi ile yürüttüğü bir kuantum kriptoloji çalışması var; üniversitede bir laboratuvarımız var. Orada aslında yapılması gereken şey şu: Sabah da bahsedildi ya, “şimdi veriyi al, sonra çöz”. Şimdi çözemediğiniz kriptoları da yarın kuantum hesaplama sayesinde çözebilir imkâna gelebilirsiniz. İşte bunu da öngörerek post-kuantum kriptografi, yani kuantum sonrasında sistemlerinizin kriptosunun kırılmasına karşı şimdiden önlem almak lazım. Siz belki ürünlerinizde ve birçok şeyde kuantum hesaplamayı kullanamıyorsunuz ama en azından kriptoloji, şifreleme alanında post-kuantum kriptoloji ile ilgili önlemleri almak, buna göre bazı şifrelerle sisteminizi korumanız yarın kuantum sonrasında sizi güvenli hale getirir. Ama bunu şimdiden yapmak lazım. “Bekleyelim, kuantum hesaplama daha fazla yaygınlaşsın” dersiniz çok geç kalabilirsiniz, çok büyük bir tehditle karşı karşıya kalırsınız.

En sonuncusu da yapay zekâ. Zaten en önemli konu yapay zekâ; olmazsa olmaz. Yapay zekâyla saldırılıyor, yapay zekâyla karşılanıyor. Biliyorsunuz siber güvenlikte de yapay zekâ, hem saldırı hem savunma anlamında çok önemli bir konu. Bunun için bu alanda da şirketlerin, siber güvenlik başta olmak üzere birçok alanda yapay zekâyı doğru bir şekilde kendi amaçları için kurgulaması, buna göre doğru yapay zekâ ürünleriyle siber güvenlik önlemlerini desteklemesi, insan unsurundan arı olarak yapay zekâyı bazı görevleri vererek sistemleri daha güvenli hale getirmesi çok çok kritik.

Hepimizin ortak sorumluluğu: Ülkenin siber güvenliği hepimizin sorumluluğu. Bu platform da, Bilgi Güvenliği Derneği de bunu yapıyor, bunun için çaba gösteriyor. Çok zor oluyor arkadaşlar bu konferansın hazırlanması. Ben kısa bir dönem, biraz hocalarımın da zorlamasıyla 3 sene buraya başkanlık yaptım. Tam pandemi dönemiydi;

oradan da biliyorum. Daha sonrasında yeterince katkı sağlayamıyorum ama böyle arada geliyorum, hocalarıma misafir oluyorum. Ama şunu biliyorum: Hem Tuncay hocamı hem Mustafa hocamı hem de tüm ekibi çok tebrik ediyorum. Konuşmacıları organize etmek, konuları bulmak, konu başlığını bulmak, yer planlamak, gençlerle, öğrencilerle doğru bir şekilde eğitim programları yapmak çok zor; bunlar çok çok zor şeyler. Ciddi bir emek gerekiyor. Bunların karşılığında da herhangi bir ücret almıyorlar, herhangi bir para da kazanmıyorlar. Bunlar bir fedakârlıkla yürüyor; muhtemelen sunucu arkadaşımız da böyle. Ondan dolayı bunu çok takdir etmek lazım, hepsini tebrik etmek lazım, aynı zamanda da destek olmak lazım. Bu tür dernek ve benzeri çalışmalara, mümkün olduğu kadar imkânı olan gençlerimizin destek olmasını ben tavsiye ediyorum. Hepinize saygılar sunuyorum efendim. Sağ olun.

03:19:11 Murat ÇİZGEL – Savunma Sanayii Başkanlığı Siber Güvenlik ve Bilişim Sistemleri Daire Başkanı

Başkanım, koordinatörlerim, genel müdürlerim, kamudan, Türk Silahlı Kuvvetlerinden ve sanayicimizden gelen değerli katılımcılar; ben öncelikle hepinize merhaba diyor ve sizlerle birlikte olduğum için hakikaten burada duyduğum keyfiyeti belirtmek isterim. Ben Murat Çizgel. Savunma Sanayii Başkanlığında siber güvenlik ve bilişim sistemlerinden sorumlu daire başkanı olarak görev yapıyorum; ama savunma sanayiinde de 26 yıllık bir tecrübem var. Bizim konuşmalarımız Taha Bey’le ikimiz de savunma sanayiinden olduğumuz için birbirini tekrar eden hususlar olacak; o yüzden izniniz olursa hafif hikâyeleştirerek konuşacağım.

Şimdi, çoğumuz bu kitabı okumuşuzdur diye düşünüyorum: 50 sayfa olduğu ve klasikler içerisinde de yer aldığı için, Savaş Sanatı. Biz savunma sanayiinde bunu çok kere karşılıyoruz; ama herkesin de bildiği bir konu var: Savaşı nasıl kazanırsınız? Bir, ya zengin olacaksınız ya da kaynaklarınızı çok iyi kullanacaksınız. Her ikisini de başarırsanız galip olan sizsiniz. Kaynakları verimli kullanmak her zaman geçerli oldu. Zamanında meydan savaşları vardı ve o meydan savaşlarında insan sayınız ne kadar fazlaysa ya da taktiklerinizle daha az insanla meydanda güçlü olmayı becerebiliyorsanız kazanıyordunuz. Sonrasında konvansiyonel bir süreç geldi. Konvansiyonel dünyada da topunuzu, tankınızı, füzenizi ne kadar fazla yapar ve saldırırsanız o kadar iyi oluyordu. Günümüzde de yavaş yavaş siber savaşlar ve hibrit savaşlar gelmeye başladı. Kaynakları iyi kullanan, önümüzdeki dönemde savaşı yönetir; bu her zaman geçerli olacak. Bu kitabın yazıldığı binlerce yıl öncesindeki gerçeklik hiçbir zaman değişmedi, değişmeyecek.

Bir buçuk ay önce ailecek tatile çıktık. Bir yeri geziyoruz; bir kale, hakikaten çok da yıkılmamış, güzel de bir kale. Kızım 11 yaşında, şu soruyu sordu: “Baba, bu kale niçin vardı?” Dedim ki, “Burada tüfekler vardı. Denizin kenarında zaten; gemiler geçerse onları savunuyor, onların geçmesini engelliyor, koruyor.” Yani bu bir savunma tarafı. “Şimdi niye yok?” dedi. “Niye hiçbir top, tüfek veya bir şey yok?” “Günümüzde ihtiyaç yok,” dedik; çünkü bu aşamada artık buraya sizin bir top tüfek koymanızla bir savunmayı gerçekleştirme şansınız kalmadı. Çünkü adam füzeyle atıyor, başka konvansiyonel ve yeni yöntemler kullanıyor. 11 yaşındaki kızım şunu söyledi: “Tabii, artık günümüzde bunlara da ihtiyaç yok. Hacklemek var.” Bu kendi ifadesi. 11 yaşındaki

çocuk, zaten bu siber dünyaya native olarak doğdukları için, bu işi çok ciddi anlamda kavramış durumda: “Ne gerek var ki zaten top tüfek yapmaya? Hacklemek var zaten.” O kadar doğru söyledi ki. 11 yaşındaki çocuğun vizyonu arkadaşında da var, sizin çocuklarınızda da aynı vizyon var. Biz şu anda karar vericiler olarak aslında bu vizyonu çok daha fazla kabullenip buna yönelik politikalar üretmemiz gerekiyor.

Rahmetli Erbakan’ın videosu çok dolaşıyor bu sıralarda. Bundan 15-20 yıl önce mi çekilmiş, tam da bilmiyorum: “Günü gelecek, size atılan bir füzeyi siz onu havadayken ele geçireceksiniz ve yönlendireceksiniz; böylelikle adamın milyarlarca dolar harcayarak yaptığı füzeyi siz çok daha düşük bir maliyetle onun kendisi için kullanacaksınız.” Bunu hepimiz izlemiştir diye düşünüyorum. Bu çok güzel bir platform siber güvenliği örneği. Bu örnekte “günü gelecek” dediği ifade var cümlesinde; günü geldi ve şu an itibarıyla milyar milyar dolarlar harcayıp bir kullanımında yüzlerce milyon dolar heba edeceğiniz bir platformu bir kodla çok rahat bir şekilde manipüle edebilir, saptırabilir ve işlevsiz hale getirebilir noktaya geliyorsunuz.

Şimdi bunun artık hepimizin farkında olması nedeniyle, Taha Bey’in dediği gibi, o adımların hemen hemen hepsini ben de aynı ifadelerle kullanacağım; ama devlet olarak üzerimde bir sorumluluk var. “Söylüyorsun da arkadaşım, onun yerine devlet olarak bir politikanız var mı? Bir yönteminiz var mı?” Bu da bana bir mecburiyet; ben de onun karşılığında bir şey söylemem gerekecek.

Birincisi: Tasarım aşamasından itibaren platform ve sistemlerinizde, kalite güvence planları gibi, risk yönetim planları gibi başından itibaren dikkat etmeniz gerekiyorsa, siber güvenlik kapsamında ne yapmamız gerekiyor? Devlet olarak şöyle bir şey yapıyoruz. Savunma Sanayii Başkanlığını bilenler bilir: Biz Türk Silahlı Kuvvetlerimiz ve emniyet ve güvenlik kuvvetlerimiz için projeler yürütüyoruz, onların tasarımlarını yaptırıyoruz ve onları kullanıcılarına teslim ediyoruz. Artık Savunma Sanayii Başkanlığı tarafından tasarımı ve üretimi gerçekleştirilecek tüm projelerde siber güvenlik planı, kalite planları gibi bir mecburiyet. Yüklenici onu hazırlamak zorunda, bizlere onaya sunmak zorunda. Sunduğu planın içerisinde tasarım sürecinden lojistik sürecine kadarki süreçte aldığı tedbirleri ve tedarik yönetimi içinde ne tür tedbirler alacağını, ne yapacağını bize belirtmek zorunda; biz de ona bağlı olarak “şunu düzeltin, şunu yapın” diyerek, en azından şimdiden tasarım sürecinde, kendi yaptığımız özgün ürünlerimizin içerisinde siber güvenliği de bir başlık olarak ele alıp tasarım sürecine dahil etmeye başlamış durumdayız.

İkinci bir ifade geldi: tedarik zinciri. O kadar kıymetli ki, ben bunu şöyle bir örnekle vereyim. Siz ne kadar dikkat ederseniz edin, füze yapıyorsunuz, en kıymetli bir platform. Bunun içerisinde o kadar çok alt sistem ve bileşen var ki, bunlar hep bir şekilde onun görev sistemi, görev bilgisayar sistemi içerisinde birbiriyle çalışıyor. Tedarik zincirindeki bir firmamız aslında bu siber güvenlik konularına çok fazla değinmiyor, ehemmiyet vermiyor ve kendisinin yaptığı alt sistemle alakalı tasarımları bir şekilde birisi tarafından hacklenmiş, ona yönelik bir bilgi oluşmuş ve yaptığı alt sisteme de, içerisinde eğer bir kodlama varsa, belki bir şekilde bir şey dahil edilmiş; hiç farkında bile değil. Ve günü geldiğinde, lazım olacağı gün o alt sistem o füzeyle beraber işini yapmaya çalışırken füzenin de gerçek anlamda işini yapmamasına sebebiyet verebiliyor. Bu anlamda sadece ana yüklenicilerimizin ve projelerimizin siber güvenlik planı çerçevesinde

tasarım süreçlerini düzgün yürütmesi uygun olmayacak. Sizin birlikte çalıştığınız yüzlerce, binlerce alt sistem üreticisinin de bu anlamda siber güvenlik seviyesinde bir dirençlerinin ve farkındalıklarının olması sağlanacak. Bunu sağlamak için de bizim TR Test firmamızla beraber yürüttüğümüz bir program var: Siber Hijyen ve Siber Hijyen KOBİ diye. Bunun temel amacı, savunma sanayiine ürün verecek en küçük firmanın dahi siber güvenlik açısından belirli bir bilince, bilgi birikimine ve altyapıya sahip olması; ki teslim edeceği ürün ve hizmetlerde böyle bir zafiyet ortadan kalksın. Bu programımızı ayrıca inşallah bütünüyle daha zorunlu hale getirerek devam edeceğiz.

Bu anlamda üçüncü bir başlık açacağım. Ne olursa olsun, savunma sanayii ürünlerimizi nasıl kendimiz yaparsak onu daha iyi yönetebiliyorsak, siber güvenlik alanında da ürünlerimizin yerli olması olmazsa olmaz, önemli bir husus. Bu zamana kadar Siber Güvenlik Kümelenmesi diye 10 yıldır bir ekosistem yönetildi. İnşallah Siber Güvenlik Başkanlığımız bu ekosistemi çok daha etkin ve verimli bir şekilde yönetmeye devam edecek ve daha da etkinleştirecek. Biz de Savunma Sanayii Başkanlığı olarak siber güvenlik ürünlerimizin, hatta aslında biraz da savunma sanayiinde üretilen alt sistemlerin siber dayanıklılığının ölçülebileceği bir altyapı oluşturmayı kararlaştırdık. Bunun adına da SAYGEP diye bir merkez koyduk: Siber Alan Yetkinlik Geliştirme ve Entegrasyon Platformu. Bunun temel amacı, artık ekosistemimizdeki firmalarımızın ürünlerinin bu entegrasyon altyapısında sürekli çalışırılığını göstererek, kamu kurumları da dahil olmak üzere güvenilirliğinin sürekli ispat edildiği, oradaki geri bildirimlerin verilerek siber güvenlik ürünü üreten firmaların da ürünlerini çok daha iyi hale getirdiği bir mekanizma oluşturmak. Bu oluşturduğumuz mekanizmayı da inşallah Siber Güvenlik Başkanlığımızla birlikte yürütmeye devam edeceğiz. Temel olarak yapılmış olan siber güvenlik ürünlerinin başka kurumlar tarafından kullanılması açısından garantör olmak ve “bakın ne kadar güzel çalışıyor” diyebileceğimiz bir altyapı oluşturmak. Oluşturduğumuz bu altyapı, savunma sanayiindeki alt sistem ve bileşenlerin üretimi sonrasında onların da siber dayanıklılığını ölçebilecek bir altyapıya sahip olacağı için ayrıca böyle bir destek hizmeti de verecek.

Son başlık olarak ben de yapay zekâya gireceğim. Biz bütün alt sistemlerimizi, tüm tasarım süreçlerimizi, hepsini siber dayanıklılığa uygun bir şekilde yürüttük, ürettik. Ama artık yapay zekânın girmediği hiçbir alan yok. Bu uçta çalışan yapay zekâ unsuru, savunma sanayii için önümüzdeki dönemde olmazsa olmaz başlıklardan bir tanesi. İster arayıcı başlığı kuvvetlendirsın, arayıcı başlığınızın etkinliğini çok daha verimli şekilde artırsın; ister görev fonksiyonlarını daha kıymetli hale getirsın; uçta, platform üzerinde çalışan yapay zekâ, savunma sanayiinin olmazsa olmaz unsuru olarak önümüzdeki dönemde bizi bekleyen bir yapı.

Gördüğüm kadarıyla yapay zekâda şöyle bir bağımlılık oluyor genelde: Son 10 yılda geliştiği ve çok büyük GPU altyapıları kullanılarak geliştirildiği için büyük modeller açık kaynak olarak servis ediliyor. Gerek görüntü modelleri olsun gerek dil modelleri olsun, bu büyük açık kaynak modeller üzerine yapay zekâ çalışmalarımızı ekleyelim, bunu da o çok kıymetli olan arayıcı başlığımızla beraber çalıştırayım diyoruz. Ve şundan eminiz: Uçtan uca savunma sanayii siber güvenliğini sağladı; ama açık kaynakta bilmediğimiz attention algoritmalarından tutun transformer algoritmalarına kadar, bilmediğimiz, gizli ve hiçbir zaman öğrenemeyeceğimiz bir yapay zekâyı oraya “bakın, ben de yapay zekâ ekledim” diye koyacağız. En önemli unsur da şu: Şöyle bir tetiklenme ihtimali olabilir mi?

Normalde çok daha iyi görsün diye koyduğum yapay zekâ, o koordinatta ya da o tarih geldiğinde halüsinasyon görmesine sebebiyet verirse, milyar milyar dolarlar harcayarak ürettiğim füze veya koruyucu mekanizma hiçbir anlam ifade etmeyecek.

Şimdi savunma sanayii açısından eğer siber güvenlik diyorsak ve önümüzdeki dönemde yapay zekâ bizim artık vazgeçilmez bir unsurumuz diyorsak, millîleşme konusunda biraz daha fazla birliktelik olması ihtiyacı olan bir alan oldu yapay zekâ. Biz burada bunun artık yavaş yavaş üniversitede de derslerini vermeye başladık. Devlet olarak, Savunma Sanayii Başkanlığı olarak, özellikle açık kaynakta verinin dışarıya gitmemesi, verinin çok daha fazla burada toplanması ve o veri sayesinde millî modellerimizin geliştirilebileceği hem büyük altyapının hem de veri kütüphanesinin oluşması açısından bir proje başlattık. Bu projeyi teker teker herkese anlatıyoruz, üniversitelerimize anlatıyoruz. Burası bizim açık kaynak kütüphanelerimizin olacağı yer olacak. Adını EVREN koyduk; “savunma sanayiinin yapay zekâ evreni” sloganıyla çıktık. Bunun şu teminatını verebilirim: O altyapı, lazım olduğu sürece büyüyecek. O veri sizler için, sizin kullanımınız için, modelinizin gelişmesi için orada duracak; yurt dışına göndermeyeceksiniz ve bu devlet bunun için sizden para almayacak. Bunu bir görev olarak aldık. Amacı da şu: Biz mümkün olduğunca açık kaynağımızı dahi kendimiz kontrol edebilir olalım ki, o zaman yapay zekâ dahil platformumuzun en ucundan sonuna kadar her tarafında kendimizden emin olarak devam edelim istiyoruz.

Sürelerimiz de çok olmadığı için ben de sıkılmak istemiyorum. Taha Bey’le aynı başlıkları söylüyoruz; zaten bunlar hepimizin yol haritasında. Ben devlet olarak her bir başlığın yanına bir isim söyledim: siber güvenlik planı, SAYGEP, Siber Hijyen ve EVREN. Saygılarımı sunuyorum.

03:33:45 Orhan KOCA – Türksat Genel Müdür Yardımcısı

Sayın Başkanım, Sayın Genel Müdürlerim, değerli akademisyen hocalarım, siber güvenlik alanında çalışan kıymetli uzman arkadaşlar, değerli misafirler; hepinizi şirketim Türksat adına ve şahsım adına saygıyla selamlıyorum. 19’uncusu düzenlenen Bilgi Güvenliği ve Kriptoloji Konferansı’nın hepimiz için faydalı olmasını diliyorum. Bu yılki konferans konumuzun başlığı “Yeni Dünya Düzeninde Siber Savaşlar”. Bizlerin burada olmasının sebebi, Türksat olarak aslında işlettiğimiz platformlarda buna yönelik ne tarz çalışmalar yapıyoruz ve ne tarz tecrübelerimiz var, bunları sizlerle paylaşmak istiyorum.

Kıymetli katılımcılar, dijitalleşme artık hayatımızın her yerini kapsıyor. Bundan 10 yıl önce, 20 yıl önce yüz yüze yaptığımız pek çok işlemi artık dijital ekranlar üzerinden yapıyoruz. Bankacılık hizmetleri, alışveriş, e-Devlet üzerinden pek çok kurumla yapılan işlemler; bunları artık dijital bir âlemde yapıyoruz. Hatta bunun bir adım ötesine de giderek dijitalleşme aslında entegrasyonla, bir servisle de değil, birden fazla sistemle birlikte bir platforma dönüşmüş durumda. Yani siz bir işlemi yaparken aynı zamanda arka tarafta bir bankacılık hizmetiyle entegre olarak çalışıyorsunuz, bir ödeme platformunu kullanıyorsunuz, bir satın alma yapıyorsunuz, aynı zamanda bir kargo şirketi ile birliktesiniz. Dolayısıyla bütün bunlar bir platform oluşturuyor ve bugünkü oturumumuzun başlığı da platform güvenliği.

Bu platformların güvenliğınden söz ederken öncelikle vurgulamamız gereken şey, platformu oluşturan unsurların güvenliğı. Yani biz bir ekosistemden bahsediyoruz. Bu platformun güvenliğini oluşturan her bir unsur; bazen bir yazılım olabilir, bazen bir donanım olabilir veya bir uygulama olabilir, başka bir kurumla entegrasyon olabilir, ara bağlantılar olabilir, aradaki bir kriptolama işlemi olabilir, bir protokol olabilir. Dolayısıyla bütün bunların uçtan uca güvenliğini sağlayabiliyorsak şayet, o zaman bir ekosistem ve platform güvenliğınden bahsedebiliriz diye düşünüyorum. Çünkü netice itibariyle “bir zincirin en zayıf halkası kadar güçlüyüz” diye bir söz var, malumunuz. Herhangi bir platformun herhangi bir unsurunda yaşanabilecek siber bir zafiyet, bir sorun, aslında bütün ekosistemin ve platformun da zafiyete düşmesine yol açıyor.

Şimdi konu başlığımız siber savaşlar. Buradan ben de aslında somut olarak, çok uzun olmayan son 3-5 yıl içerisinde karşılaştığımız, maruz kaldığımız siber savaşlardan bazı örnekler vermek istiyorum. Çünkü savaşlar artık arkadaşlar sadece cephelerde değil; kıymetli konuşmacılar benden önce bunu çok güzel ifade ettiler. Veri merkezlerinde oluyor, haberleşme ağlarında oluyor, dijital platformlarda yaşanıyor. Savaşlar genellikle, konvansiyonel bir savaşın ön cephesi olarak öncelikle siber savaş olarak başlıyor; biz bunu görüyoruz.

2016 yılında Ukrayna’da, Kiev’de elektrik işletim altyapısına yönelik bir saldırı gerçekleşti. Industroyer diye bir zararlı, şehrin büyük oranda endüstriyel elektrik altyapısına zarar verdi ve elektriksiz bıraktı. Bunun hemen yanında, Şubat 2022’de Rusya’nın askeri harekâtı başlattığı gün, eş zamanlı olarak Ukrayna’ya hizmet veren Viasat diye bir uydu var; bu Viasat uydusunun internet ağına yönelik bir siber saldırı gerçekleşti ve bütün ülke genelinde haberleşme sistemleri, uydu sistemleri bundan zarar gördü. Malumunuz askeri iletişimde, normal iletişim ağlarınızın yanında uydu haberleşmesi de çok yaygın olarak kullanılıyor. Bunun ne kadar sistematik olarak yapıldığını ve buradaki bir platformun sadece uduya zarar vermekle ilgili olmadığını, onun bileşenlerinde olan herhangi bir sistem de hedef alındığında nasıl zarar verdiğini gösteren bir örnek olarak karşımıza çıktı.

Diğer bir örnek İran. İran’da 2023’te akaryakıt dağıtım şebekelerine yönelik bir saldırı düzenlendi. Şehirde hiçbir akaryakıt sistemi bir müddet çalışamaz hale geldi, insanlar kuyruklar oluşturdu. Savaş hemen başlamadan önce bunlar tabii toplumda korku ve belirsizlik ortamı oluşturmak için kullanılan, aslında asimetrik savaş taktikleri olarak kullanılıyor. Bunun dışında İran’da hedefi çok belli nokta operasyonlarına biz şahit olduk. Yani bir apartman binasının belli bir katının belli bir noktasına düzenlenen operasyonları gördük. Bu operasyonlarda elde edilen veriler ve konum bilgileri, hem dijital hem fiziksel, aslında hibrit bir savaş modelinin örneklerini bize gösterdi. Kullanıcıların kendi dijital ekipmanları, telefonları belki yoktu; ama şoförünün, arabasının, korumasının veya kamera kayıtlarının, aslında bir IoT platformunun geçtiği her yerdeki iz bırakan, IP alan her bir varlığın güvenliğınin; toplanan verilerle ve tabii ki belki yerinde olan istihbaratla da bu tarz saldırıları, hibrit saldırıları gördük. Çok gözümüzün önünde bunlar yaşandı.

Diğer çarpıcı bir örnek yakın zamanda Lübnan’da gerçekleşti. Hizbullah lider kadrosu, dijital önlem almak için aslında telefonu bırakmışlar, telefon kullanmıyorlar; kendilerince tedbirlerini almışlar. Fakat kullandıkları çağrı cihazları içerisinde yerleştirilen patlayıcılarla

ve bunların bir zamanda dışarıdan tetiklenmesiyle (ki burada elektronik haberleşme sistemleri kullanılıyor) üst düzey komutanların dâhil olduğu, çok sayıda yaralının ve ölünün olduğu bir olay yaşandı. Bu bize çok net bir şekilde olayın sadece teknolojik boyutunun olmadığını; teknolojiyle alakalı önlemlerle birlikte fiziksel önlemlerin, güvenlik önlemlerinin, ekosistemin, tedarikçinin, lojistiğin tamamını kapsayan bir bütün olduğunu gösterdi. Çünkü cihazların dağıtılmadan önce ele geçirilerek içlerine o patlayıcıların yerleştirilmiş olduğunu açık kaynaklardan yaptığımız araştırmalarda gördük.

Diğer bir çarpıcı örnek Suriye’de. Suriye’de de İsrail’in yaptığı saldırılarda radar sistemlerinin cevap veremediğini ve hava saldırılarının gerçekleştirildiğini gördük. Ve son bir örnek, malumunuz, Maduro’nun yakalanması sırasında; bunların hepsi açık kaynaklarda da olduğu için ben dikkatinizi çekmek üzere söylüyorum, Venezuela’da operasyonun olduğu gün hem elektrik şebekesinde hem radar sistemlerinde birtakım problemler, sorunlar yaşandı. Tabiri caizse sistemler kör edildi ve gerekli operasyonlar yapıldı.

Dolayısıyla kıymetli katılımcılar, karşı karşıya olduğumuz durum milli güvenliğimiz için, ülke güvenliğimiz için çok önemli, bizim için dikkate değer bir durum. Burada yapmaya çalıştığımız şey aslında sadece bir unsur değil; uçtan uca bütün sistemlerimizin güvenliğini alma hususunda bizlere önemli görevler düşüyor. Bunları nasıl yapacağız diye baktığımız zaman, ilk olarak siber dayanıklılığımızı (gün boyu bunlar konuşuldu) güçlendirmemiz gerekiyor. Siber dayanıklılık, zafiyete maruz olmamak demek değil. Yani bütün güvenlik sistemleri ne zaman sızılabilir? Yeterince zaman ve yeterince para konulursa, odaklanılırsa her şeye; yani yüzde 100 bir güvenlikle asla zaten bahsedemiyoruz. Dolayısıyla mesele, “Biz siber bir atağa maruz kalmayız, yüzde 100 güvenliyiz” iddiası değil. İddiamız bütün sistemlerimiz için şu olmalı: Evet, siber bir müdahale olabilir; fakat ne kadar dayanıklıyız? Ne kadar kısa sürede tekrar ayağa kalkabileceğiz? Hangi kritik sistemlerimiz bundan en az etkilenecek? Geri dönüş senaryolarımız nelerdir? Bir felaket kurtarma merkezimiz var mı? Yedekliliğimiz, bunların simülasyonları yapılmış mı? gibi unsurları mutlaka inceliyor olmamız lazım.

Ve esas buradaki ana konulardan bir tanesi, Sayın Başkanlarım da bahsetti; aslında yerli ekosistem, Milli Teknoloji Hamlesi adıyla bizim adlandırdığımız kendi ekipmanlarımız, kendi cihazlarımız, kendi varlıklarımız olmadan aslında bizim bir milli güvenlikle bahsetmemiz mümkün değil. Çünkü kullandığımız ekipmanlar belki de zafiyetin ta kendisi; bilemiyoruz. Yani zamanı geldiğinde bizi koruyor zannettiğimiz şeyler belki de bir saldırı yüzeyi, atak yüzeyi olacak. Dolayısıyla biz, milli ve ulusal güvenliğimizi kapsayan konularda mutlaka Milli Teknoloji Hamlesi çerçevesinde kendi ürünlerimizi, altyapılarımızı, bağımsız altyapılarımızı geliştirmek durumundayız. Bunlarla alakalı kapasitemizi inşa etmek durumundayız.

Buradaki Milli Teknoloji Hamlesi ve milli, yerli üretimin sağlanabilmesi için tabii ki çok önemli bir adım atıldı; bundan çok mutluluk duyuyoruz. Sayın Başkanımız da bahsetti: Siber güvenlik ekosistemindeki bu düzenleyici, denetleyici görev Siber Güvenlik Başkanlığımıza verildi. İnşallah bu konuda hem ekosistem hem mukavemet hem siber saldırı alanlarında önemli çalışmalar artarak devam edecektir. Geçmişte de bu çalışmalar yapıldı ve inşallah daha da ileriye taşınacaktır. Dolayısıyla bunların koordinasyonu, tek bir elden yönetilmesi ve iş birliği çok kritik bir aşamadır.

Diğer önemli bir konu, bütün konuşmacılarımız değindi: yapay zeka tarafı. Biz yapay zekayı iki bağlamda düşünüyoruz: Güvenlik için yapay zeka, yapay zeka için güvenlik. Yani yapay zekada da diğer ürünler gibi hem kendisi; asimetric olan bu yapay zekayla bize doğru gelen atakları karşılamayı bir insan marifetiyle yapabilmemiz mümkün değil, yapay zekayı kullanmamız gerekiyor. Ama bu yapay zekayı da kullanırken ona karşı da tedbirlerimizi almamız gerekiyor. Bunun birinci yolu tabii kendi dil modellerimizi geliştirmek. Sayın Başkanımızın bahsettiği Evren projesi, TÜBİTAK'ın geliştirdiği projeler; Türksat olarak biz de kendi içimizde dil modelleri üzerine çalışıyoruz. Bunlar çok kritik, hayati.

Türksat olarak 68-69 milyon kullanıcımızın olduğu e-Devlet platformunu yönetiyoruz. Bunun üzerinde 9.000'den fazla servis çalışıyor, 1.000'in üzerinde kurum entegre. Aradaki entegrasyonlarda yıllık 12 milyarın üzerinde işlem oluyor. Uydu haberleşme ağıımız var; mevcutta 6 adet uydumuz var. Bunların sonuncusu, son uydumuz Türksat 6A; çok şükür burada ASELSAN'ımız, TUSAŞ, CTech ve TÜBİTAK'la birlikte yüzde 85 oranında yerlilikle üretildi. Bizim esas istediğimiz şey bu. 5,5 milyon kapasiteye sahip bir kablo TV altyapımız var. Bunun gibi Türkiye Ulusal Coğrafi Bilgi Sistemi'ni yönetiyoruz; bütün ülkedeki coğrafi bilgi sistemlerinin işletildiği platform. Bütün bu platformlarda biz de bahsettiğim konulara, tasarımdan itibaren (by design) güvenliğe ve her unsurunun titizlikle incelenmesine ve esas önemli olarak aslında yerlileştirme stratejisine önem veriyoruz ki şu an 5 yıllık bir yerlileştirme stratejisi hedefi koyduk kendimize ve adım adım inşallah burada ilerliyoruz, çalışıyoruz.

Siber dayanıklılık, dijital egemenlik, milli teknoloji, milli güvenliğimizle doğrudan ilgili; ve bunları yapabilmemiz için regülasyona, düzenleyici-denetleyici kuruma ve ortak iş birliğine ihtiyaç var. Siber güvenlik, sadece bir kurumun, bir başkanlığın cevap veremeyeceği kadar büyük. Dolayısıyla burada bütün kurumlara, kuruluşlara görevler düşüyor. Biz de üzerimize düşen görevleri yapmak için mücadele ediyoruz.

Kıymetli vakitlerinizi ayırdığınız, sabırla dinlediğiniz için hepinize teşekkür ediyorum. Saygı ve selamlarımı iletirim.

03:47:23 Salih TALAY – HAVELSAN Siber Güvenlik Direktörü

Sayın Başkan, başkanlarım, genel müdürlerim, komutanlarım, kamunun, özel sektörün ve akademinin kıymetli temsilcileri ve sevgili öğrenciler.

Günümüz dünyasında, konvansiyonel savaş alanları olan kara, deniz ve havanın aksine insan eliyle oluşturulmuş bir alan olarak siber alan, ülkeler arasında gelişen neredeyse tüm gerilim ve çatışmaların başladığı, hatta bazı gerilim ve çatışmaların tamamen cereyan ettiği, siber alanda başlayıp siber alanda bittiği bir dünyada yaşıyoruz.

Az önce Sayın Genel Müdürümün bahsettiği bir konu var: Bahriyesi ne kadar güçlü olursa ülkeler o kadar güçlüydü; komutanım, yanlışıımı düzeltin. Savaş tarihi, insanlık tarihi kadar eskidir. Geldiğimiz dünyada karşılaştığımız konvansiyonel savaş alanlarında, içinde yaşadığımız kara, deniz ve hava ortamlarında önce çelik vardı. Daha sonra barut, savaşın gidişatını değiştiren bir faktör oldu. Üçüncü olarak bunlara ekleyebileceğim motor teknolojisi, yani savaşan araçlar ve platformlar üretmemizi sağlayan motorlar, konvansiyonel savaş alanlarını değiştirdi. Bunların üzerine insanlık,

kendi eliyle geliřtirdiđi yeni bir savař alanı daha ekledi: siber alan. İřin gzel tarafı, mevcut konvansiyonel savař alanlarının tamamında siber alan artık etkin ve etkili. Çnk geliřtirdiđimiz kara, deniz, hava ya da uzay platformlarının tamamı siber alandan ynetiliyor; burada veri retiyor, bu verileri bađlantılı bir řekilde bir merkezle paylařıyor, hatta bu verileri aktardıđı yapay zeka sistemleriyle otonom karar verme sistemlerini besliyor. Bununla birlikte platformlara otonom zellikler kazandırıyoruz; otonom kararlar verip belli grevleri icra edebiliyorlar.

Konvansiyonel savař alanlarında hangi platformlarımız var? Uçaklarımız var; tanklar, uydular, denizaltılar, savař gemileri, insansız hava araçlarımız var. Ana taşıyıcı niteliđinde olan bu sistemler donanım, yazılım, kritik alt sistemler ve geliřmiř haberleřme altyapıları barındırıyor ve bunları tek bir gvde zerinde entegre ediyor. Bu entegre platformlar, askeri anlamda belli bir grevi icra etmek iin kullanılıyor.

Askeri platformların siber gvenliđini ele alırken tehditlerin deđiřken niteliđini dođru bir řekilde anlamamız gerekiyor. Muharebe sahasının dijitalleřmesiyle birlikte gncel savunma sanayii ekosisteminde yer alan askeri platformlar, az nce bahsedildiđi gibi ok yksek maliyetlere mal olurken ok dřk maliyetlerle zarar grebiliyor. rnek vermek gerekirse 40 milyon dolarlık bir uađınız, 40 dolarlık bir donanım bileřeni, bir alt sistem bileřeni yznden grev kaybı yařayabilir; grevini icra edemeyecek duruma gelebilir ya da savařmaya hazır olma durumunu, greve hazırlık durumunu kaybedebilir.

Bunlarla birlikte, bu platformlara siber gvenliđi bir koruma katmanı olarak sonradan eklemek deđil, az nce de bahsedildiđi gibi platformların tasarım ařamasında; platformun kritik sistem ve alt sistem bileřenlerinin, donanımlarının tedarici ařamasında tedarik zincirine ynelik ktcl yazılımlar ya da kimlik avı saldırıları, hizmet kesintisine neden olabilecek kritik alt bileřenlerin belirlenmesi gibi ařamalarda bu platformların gvenliđini sađlamak gibi bir sorumluluđumuz ortaya ıkıyor. Tabii ki bu saldırıları dzenleyen aktrlere bakacak olursak, yođunluklu olarak devlet destekli aktrler, siber operasyon dzenleyen, casusluk faaliyeti ierisinde olan gruplar ve geliřmiř tehdit unsurları karřımıza ıkıyor. Dolayısıyla tehdidin boyutuyla birlikte almamız gereken nlemlerin kritikliđi de artıyor. Bununla birlikte uydu tabanlı konumlama ve zaman hizmetlerinin yanıtılması ya da engellenmesi, haberleřme bađlantılarının karıřtırılması, grev yerlerinin deđiřtirilmesi ve sistemlere gvenilmeyen, dođrulanmamıř nc parti yazılım bileřenlerinin eklenmesi gibi riskler de platformların karřı karřıya olduđu riskler arasında.

Burada zellikle vurgulamak istediđim husus, siber tehditlerin etkisi. Bu etki, geleneksel sistemlerimizde, geleneksel veri merkezlerimizde iřlettiđimiz sistemlerimizdeki gibi veri kaybıyla sınırlı deđil: grev kaybı, komuta merkeziyle bađlantının kaybedilmesi, dost-dřman ayrımını yapamayıp dost birliklere zarar verebilecek nitelikte saldırılara hedef olması sz konusu. İřin en vurucu tarafı, bu platformlara ynelik siber saldırıların fiziksel bir saldırıyla eř zamanlı olarak ortaya ıkması durumunda mřterek harektı ve btnleřik savunma planlarını riske atabilecek dzeyde risklere sebep olabileceđini deđerlendiriyoruz.

Tabii ki günümüzde, az önce de detaylıca değinildi, yapay zeka ve otonomi teknolojileri ağırlıklı olarak platformlara kazandırılmış durumda. Bu platformlar çevrelerinden sürekli veri toplayan birer sensör haline dönüşüyor ve çoklu sensör füzyonuyla, olumlu taraftan bakacak olursak, karar mekanizmalarını hızlandırırken daha etkin ve verimli askeri kararlar verilmesini sağlıyor. Diğer taraftan bu sensörlerin manipüle edilmesi, hedef alınması, yapay zeka modellerinin yanıltıcı girdilerle karşı karşıya bırakılması ya da görev yazılımlarını etkileyecek birtakım müdahalelerle oluşabilecek zafiyetler, otonom sistemlerin yanlış değerlendirmeler yapmasına ve bir sürü halinde çalışan platformlarda sürünün tamamını riske atmasına sebep olabilecek riskler barındırıyor.

Tabii ki bu teknolojik gelişmeleri askeri platformlara aktarırken, implemente ederken biraz daha temkinli adımlar atmamız gerekiyor. Özellikle otonomi özelliği kazandırılan ya da belli bir görev planlamasında erişim kaybında o görevi nasıl sonuçlandıracağını belirlemesi beklenen bu platformlar için, karar verme sürecinde insanın bulunduğu değişik mekanizmalar mutlaka ortaya koymak gerekiyor. Çünkü uluslararası savaş hukukundan ve adil savaş kuramından bahsetmemiz gerekiyor. Otonom bir sisteminiz, bir siber saldırıyla başka bir ülkede, karşı ülkenin size savaş açmasına sebep olacak bir askeri etki oluşturabilir ki bu, uluslararası hukukun da çok ciddi anlamda tartıştığı ve henüz net bir sonuca ulaşmadığı bir konu olarak karşımıza çıkıyor.

Burada teknolojik gelişmeleri doğrudan askeri platformlara aktaramıyoruz dedim. Buradaki amaç teknolojiyi yavaşlatmak ya da bu platformları en son teknolojiden faydalandırmamak değil; bu teknolojilerin her daim güvenilir kalmasını sağlamak. Dolayısıyla üç kere değerlendirip bir kere uyguluyoruz. Günlük yaşamda kullandığımız tüketici elektroniğinde belki çok daha rahat alıp kullanabildiğimiz birtakım teknolojik bileşenleri bir askeri platforma entegre etme aşamasında, bunun tüm atak yüzeylerini, buna karşı yapılacak bir saldırının tüm olası etkilerini bütünlük olarak ele alıp inceleyip değerlendirdikten sonra bu platformlara entegre etmeye karar verebiliyoruz.

Peki nelerin yapılması gerekiyor? İlk olarak, güvenliği az önce söylediğim gibi tasarım aşamasından itibaren esas alarak, istisnasız bütün askeri platformların geliştirilmesi sürecinde tehdit modellemesi, kritik bileşenlerin belirlenmesi, güvenlik gereksinimlerinin sistem mimarisine yerleştirilmesi, yazılım ve donanım bileşenlerinin düzenli olarak test edilmesi, güvenlik açıklarının sistem hizmete alınmadan önce tespit edilip giderilmeye çalışılması gerekiyor. Bu aslında diğer sistemlerden, gündelik yaşamda kullandığımız tüketici elektroniğinden çok da farklı olmayan bir yapı. Tabii ki tehdit modellemesi her tüketici elektroniğine uygulanacak bir şey değil; ama askeri platformlarda bu süreçlerin detaylı bir şekilde uygulanması gerekiyor ki zaten Savunma Sanayii Başkanlığımız yeni platform projelerinin tamamında bunu bir rehber doküman aracılığıyla bize yönlendirmiş durumda.

Platformlarda görev ağları ile platformlar arasında katmanlı ağ mimarisi ve koruma mekanizmaları kurulması gerekiyor. Bu da bildiğimiz geleneksel ağların ayrıştırılması ilkesinden biraz daha farklı. Çünkü bir şekilde bakım bağlantıları ya da taşınabilir ortamlarla platformlara görev yüklemesi gibi süreçlerde, platformlar gerçek zamanlı olarak bağlantılı olmasa bile bağlantılılık özelliği kazanabiliyor. Ya da bir bağlantı sahibi cihaz üzerine aktarılan zararlı bir yazılımın bu platformun üzerine üçüncü bir taraf tarafından taşınması, aktarılması durumları söz konusu. Buradaki ağ izolasyonu ve

ayrıştırma ile veri aktarım süreçlerindeki güvenlik kontrollerinin de ekstra hassasiyetle yapılması gerekiyor.

Tedarik zinciri güvenliğinden bahsedildi; tekrara düşmemek için çok fazla girmeyeceğim. Ama bu tedarik zincirindeki en ufak bir kırılmanın, az önce verdiğim örnekte olduğu gibi 40 dolarlık bir alt sistem bileşeninin 40 milyon dolarlık bir platformun görev kaybına ya da kaza kırma uğramasına sebep olabileceği durumlarla karşı karşıyayız.

Siber dayanıklılık ve operasyonel sürekliliğe daha çok yatırım yapılmalı konumuz vardı. Siber dayanıklılık bugün zaten çokça konuşuldu; çok fazla değinmeyeceğim. Operasyonel sürekliliğe daha çok yatırım yapılmalı. Aslında sürdürülebilir bir ekosistem geliştirme konusunda siber güvenlik kümelenmemiz bugüne kadar bayrağı belli bir noktaya getirdi. Bundan sonra Siber Güvenlik Başkanlığına da ciddi görevler düşüyor. Ama özellikle şunu vurgulamak istiyorum: 5 Mayıs 2026 tarihinde toplanan Siber Güvenlik Kurulu'nun ilk toplantısında savunma sanayii de kritik altyapı sektörü haline dönüşmüş oldu; daha doğrusu kritik altyapı olarak kabul edilmiş oldu. Dolayısıyla bu alandaki tedarikçi güvenliğinin, tedarik zincirinin güvenliğinin ve ekosistem güvenliğinin bundan sonra çok daha önemli bir başlık altında inceleneceğini umut ediyoruz.

Beşinci başlığımız, insan kaynağı ve kurumsal iş birliğinin güçlenmesi. Burada tarafların birbiriyle iş birliği yaptığı, ihtiyaç makamının gereksinimleri doğru tanımladığı bir ortamda tedarik makamlarının bunları doğru şekilde entegre edebildiği, doğru ekosistemin içerisinde bu platformların geliştirilmesinin sağlandığı geniş çaplı bir koordinasyon ihtiyacı var. Bu, hiçbir kurumun ya da hiçbir sektör paydaşının tek başına yapabileceği bir şey değil. Bir araya gelip aslında ortak standartlar geliştirilmesi gerekiyor ve bu ortak standartlar çerçevesinde güvenilir test ve değerlendirme mekanizmaları oluşturulmalı; bu şekilde bir ekosistem kurgusu genişletilmeli.

Platform siber güvenliği olarak HAVELSAN'da platform siber güvenliği projelerimizde çokça başvurduğumuz birtakım uluslararası standartlar var. Hava tarafında mesela DO-326, havacılıkta uçuşa elverişlilik siber güvenlik süreci spesifikasyonu ve DO-356, uçuşa elverişlilik güvenliği yöntemleri ve değerlendirmeleri gibi standartlar hâlihazırda var. Kara platformlarının güvenliği konusunda ISO/SAE 21434, kara araçlarının elektrikli ve elektronik sistemlerinin güvenliğine ilişkin uluslararası olarak geliştirilmiş, kullandığımız bir mühendislik standardı var. Birleşmiş Milletler'in R155 ve R156 tip onay regülasyonu ile yazılım güvenlik güncellemeleri, kara araçları için güvenliği kurallara bağlayan birtakım uluslararası düzenlemeler mevcut. Denizcilik tarafında Uluslararası Klas Kuruluşları Birliği IACS'ın UR E26 gemilerin siber dayanıklılığı ve UR E27 deniz platformlarındaki sistem ve alt sistem ekipmanlarının siber dayanıklılığına ilişkin kontrol şemaları yer alıyor.

Fakat bu uluslararası çalışmalar bile yeterli değilken yerli kaynağa baktığımız zaman, bu alanlarda, yani platform güvenliği alanında yerli olarak geliştirilmiş standart ve rehber doküman çalışması çok kısıtlı. Bunların ivedi olarak geliştirilmesi ve detaylandırılması gerekiyor.

Sayın Başkan, değerli katılımcılar; askeri platformların siber güvenliği konusunda başarıyı yalnızca tespit edip engellediğimiz güvenlik açıklarıyla ya da saldırı

vektörleriyle ölçemeyiz. Asıl ölçüt, kritik görevlerin güvenilir bir şekilde sürdürülebilmesi, tehditlerin zamanında tespit edilmesi, sistemlerin saldırılara karşı dayanıklılığı ve gerektiğinde güvenli şekilde yeniden faaliyete geçebilmesini sağlamakla mümkündür. Bu hedeflere ulaşabilmek için savunma sanayii, askeri kuruluşlar, akademi ve siber güvenlik ekosistemi arasında kalıcılığı sağlanmış bir iş birliği ortamı oluşturulmalıdır. Yerli ve milli teknolojilerin geliştirilmesi bu çerçevede yalnızca bir üretim hedefi olarak değil, kritik bileşenler üzerindeki kontrolün, teknik bilginin, bakım yeterliliğinin ve uzun vadeli sürdürülebilirliğin güçlendirilmesi açısından ele alınmalıdır. Çünkü buradaki kritik konumuz şu: bir askeri platform 20, 30, belki 50 yıl boyunca envanterde kalacak, görevini yürütmeye devam edecek ve bu süre boyunca üzerindeki dijital sistem ve alt sistemlerin güvenliğini garanti etmemiz gerekiyor. Bahsettiğimiz süreler, günümüzün dijital dönüşüm ekosisteminde, gelişen teknolojiler dünyasında çok da kolay süreler değil.

Bununla birlikte yerli üretim tek başına güvenliği garanti etmeyecektir. Geliştirilen sistemlerin bağımsız bir şekilde test edilmesi, uluslararası iyi uygulama örnekleriyle uyumlu güvenlik süreçlerinin işletilmesi ve yaşam döngüsü boyunca sürekli iyileştirme yapılması gerekiyor. Bu test ve değerlendirme süreçlerinin de, aynı teknolojiyi geliştirme safhasında olduğu gibi, yerli ve milli olarak kurgulanması gerekiyor.

Son olarak, biz platform siber güvenliği konusunda Siber Güvenlik Direktörlüğümüz çatısı altında müstakil bir Platform Siber Güvenliği Grup Liderliği organizasyon birimi oluşturduk ve bu birim çerçevesinde faaliyetlerimizi sürdürüyoruz. Sözleşmesinde bulunsun ya da bulunmasın, HAVELSAN tarafından geliştirilen bütün projelerde, ürün ya da hizmetlerde uygulanmak üzere bir sistem siber güvenliği prosedürü dokümanı oluşturduk; kendi iç süreçlerimize bunu adapte ettik ve tüm iç ve dış projelerde bu prosedürü uygulamaya başlamış durumdayız.

Sözlerimi tamamlarken şu hususun altını özellikle çizmek istiyorum: Geleceğin savunma kabiliyeti yalnızca daha gelişmiş platformlar üretmekle değil, bu platformların güvenliğini her koşulda, her durumda koruyabilmekle şekillenecektir. Siber güvenlik, askeri gücün dışında duran teknik bir faaliyet değil; askeri gücün etkinliğini, sürekliliğini ve caydırıcılığını doğrudan belirleyen, hatta belli durumlarda etki çarpanı haline dönüştüren stratejik bir yetenektir. Bu nedenle hedefimiz yalnızca siber saldırılara karşı korunan sistemler geliştirmek değil, aynı zamanda tehditleri öngörebilen, saldırılar karşısında görevini sürdürebilen, gerektiğinde kendini güvenli bir şekilde yeniden toparlayabilen ve sürekli gelişen bir savunma ekosistemi oluşturmaktır.

Bu düşüncelerle hepinizi saygıyla selamlıyorum.

3. OTURUM: KÜRESEL REKABETTE TEKNOLOJİ SAVAŞLARI VE SİBER CASUSLUK

04:04:29 Mahmut KÜÇÜK – Siber Güvenlik Başkanlığı Ekosistem Geliştirme Genel Müdürü

Değerli katılımcılar, Sayın Başkanlarım, Bilgi Güvenliği Derneği'nin hazirununa ve yönetim kurulu üyelerine, hepsine teşekkür ediyorum. Sizlere de bu kıymetli etkinliğe katıldığınız için hoş geldiniz diyorum.

Konu olarak tabii siber casusluk olunca, konunun kendi cazibesinden diyeyim, konu başlığının katılımının biraz daha yüksek olması beklenirken akşam saatlerine kalmasının getirdiği bir etkinin de göz ardı edilmediğini görüyoruz. Bu konu özellikle siber casusluk başlığı altında ele alındığında, sadece verinin korunması, sızıntısı, yetkisiz ellere geçmesi; devlet destekli aktörler tarafından veya endüstriyel birtakım rekabet koşullarıyla, ekonomik, sosyal, politik gerekçelerle verilerin el değiştirmesi, birtakım espionaj faaliyetleri çerçevesinde elde edilmesi gibi düşünülebilir sadece.

Ama şimdi casusluk dediğimiz kavramla biraz başlamak istiyorum arkadaşlar. Casusluk tabii tarihte çok eski, ilk devirlerden itibaren düşmanın ya da rakibin konumunu, gücünü, düşüncesini, planını, stratejisini ele geçirme ve mümkünse sadece ele geçirme değil, yönlendirme; yönlendirmek için bu verileri toplama, sonrasında da etkisiz hale getirmek için kullanımı söz konusu. Baktığımızda, biz dijital dünyaya geldiğimizde casusluk dediğimizde bir insandan bahsetmiyoruz. Kullandığımız altyapıların aslında zaman içerisinde sadece zafiyetlerin kullanılarak veya yanlış yapılandırmalar kaynaklı verilerin ele geçirilmesi şeklinde değil, kullanılan ürünlerin kendisinin casusluk ürünü olduğunu da görmeye başladık. Zaten bunların uzun zamandır böyle kullanıldığına dair birtakım bilgiler, birtakım tespitler söz konusuydu.

Bu da bize aslında teknolojiyi geliştiren tarafın veriyi, bilgiyi elde etme konusunda avantajlı bir konumda olduğunu ve aslında sizin de teknolojiyi kullanırken bunun bir arka planının olabileceğini düşünmeniz, değerlendirmeniz, buna göre kendinizi konumlandırmanız; kritik verilerinizi, kritik altyapılarınızı, kritik işlemlerinizi, değerli bilgilerinizi teslim ettiğiniz noktaya dikkat etmeniz gerektiğini gösteriyor.

Tabii bu bakış açısıyla değerlendirdiğimizde de başta kamu ve kritik altyapılara da hizmet veren kurum, kuruluş ve özel sektör kuruluşlarının dikkat etmesi gereken birçok husus olduğunu da söyleyebiliriz. Örneğin kullanılan verilerin nerede saklandığı, veri egemenliği konusu. Tabii verilerinizi her zaman kendi veri merkezinizde, kendi lokasyonunuzda, fiziksel olarak kendi personelinizle yönetiyor olmanız da tabii ki her zaman yüzde yüz bu anlamda güvende olduğunuzu göstermiyor. Zaten burada alınması gereken bir güvenlik yönetim sistemi, denetlemesi vesairesi, bütün o siber güvenlik faaliyetlerini, güvenlik için gereken önlemleri almanız lazım.

Ama son dönemde daha fazla ekonomik saiklerle buluta doğru bir yönlendirme; bir de, tırnak içerisinde, tabirimi mazur görün, yapay zeka oyuncağıyla oynama. Bu oyuncakla oynarken bir şeyler geliştirmenin getirdiği heyecanla sürekli bu verilerin bir taraftan

nereye gittiği, kimlerin eline geçtiği, nasıl kullanıldığı değerlendirilmeden, özellikle global servis sağlayıcılarının düşük ücretlerle veya ücretsiz sunduğu modellere bunların aktarımı gibi konular söz konusu günümüzde. Buraları değerlendirirken sadece siber güvenlik personelinin kendisinin ya da siber güvenlikten sorumlu birimlerin, başkanlıkların bir sorumluluğu olduğunu söyleyemeyiz. Burada hem bireylere hem kurumlara hem denetleyici, düzenleyici kurumlara çok ciddi ödevler düşüyor ki zaten bu verilerin nerede, nasıl saklanması gerektiği, kimler tarafından elde edilebileceği risklerine ve risk değerlendirme süreçlerine göre nasıl kullanıma sunulacağı, bundan nasıl faydalanılacağına ilişkin birtakım değerlendirmeleri, birtakım yönlendirmeleri de Başkanlığımız çok yakın bir zamanda ikincil mevzuat düzenlemeleriyle, sektörün görüşlerine açarak yayınlanması sürecini işletiyor olacak.

Şu anda tabii biz bu konuları değerlendirirken, ele alırken sadece karşımızda X, Y, Z devletlerinin devlet destekli saldırı ya da casusluk ekipleri, APT grupları, hedefli saldırı grupları gibi gruplardan bahsetmiyoruz. Kendi içimizde de yakın geçmişte yaşadığımız, kişi güvenlik belgesi gerektiren konuları hatırlayalım. Çalıştırdığımız personelmiş gibi bizim kurumumuza ya da kendi çalıştığınız kurumlara içeriden sızan, içeriden dışarıya bilgileri sunan, sızdıran, bu verilerin bir şekilde yetkisiz ellerce ele geçirilmesine sebep veren, bu amaçla çalışan kişi, şahıs, örgüt, başka servis ajanı, etki ajanı gibi kişilerin de burada kullanılabildiğini görüyoruz.

Yakın zamanda da şunları göreceğiz belki: Evimize aldığımız araçlar, aletler, işte ev temizlik veya yardım robotları, kullandığımız bütün o ekipmanlar verinin toplanıp işlendiği, bir yerlere servis edildiği bir düzlemi bize gösteriyor. Yani sadece kurumunuzdaki, işte bu bir kolluk olabilir, bizim askeriyemiz, ordumuz, ordunun ağında kullanılan bir yapının, bir altyapının, sistemin güvenliğini sağlamak yetmiyor. Oraya erişen uzmanın, subayın, komutanın evinde, evindeki cihazın da aslında güvenliğiyle bütünleşik bakmak lazım. Çünkü birçok şeyi sadece orada değil, arabada, akıllı elektrikli araçların içerisinde konuşuyoruz. Telefon geliyor, telefonda konuşuyoruz. Evimizde konuşuyoruz. Bunları paylaşıyoruz. Birtakım şeyler, ister istemez o veriler toplanıyor. Biyometrik veri dersanız zaten hakeza; her şeyi hızlı bir şekilde kullanabilmek, dijital para cüzdanıyla para taşımadan birçok şeyi halledebilmek için, hayatı kolaylaştırmak adına her şeyi dijitalleştirdikçe de dijital ayak izimiz artıyor. Ve dijital ayak izleri de o ayak izlerinin tutulduğu, saklandığı büyük veri merkezleri, bunların yönetildiği uygulamalar, bütün bunların toparlanıp analiz edildiği büyük yapay zeka modellerinin beslendiği daha üst seviye bir akıl tarafından yönlendiriliyor.

Bütün bu çerçeveyi niye anlatıyorum? Çünkü hayatımızda oluşturduğumuz bu bütün dijital ayak izleri, birilerinin aslında toplamayı hedeflediği ve bunun için yatırım yaptığı, gerektiğinde ücretsiz kullandığı hedefler oluyor, ortamlar oluyor. Bunların kullanımı konusunda hep beraber bir duyarlılık geliştirmemiz lazım. Toplumsal farkındalığı bu noktada artırmamız lazım. Gerektiğinde de ilgili noktada düzenleyici, denetleyici kurum ve kuruluşların, ki bu sadece Siber Güvenlik Başkanlığı değil, ilgili sektörel düzenleyici, denetleyici kurumlar BTK, BDDK, EPDK gibi kuruluşların da bu sektörlerde ilgili müdahaleleri yaptırıyor ve yapıyor olması lazım. Çünkü koyduğunuz kural hayata geçmiyorsa bu kural aslında konmamış demektir. Bunları hayata geçirmemiz için artık konuşmaktan daha çok eyleme ve icraata geçmemiz gerektiği bir dönemdeyiz diyorum.

Hepinize çok teşekkür ediyorum. İnşallah bundan sonra daha çok eylem ve icraatlarımızı sizlerle paylaşacağız demek istiyorum.

04:14:14 Oğuz YILMAZ – Bilgi Güvenliği Derneği Genel Sekreteri / Labris Networks Kurucu Ortağı

Sayın dinleyiciler, öncelikle konferansımıza hoş geldiniz diyorum. Umarım konferans, beklediğiniz şekilde size katkı sağlayan bir konferans olarak devam ediyordur. Konferansın yarınki oturumlarında da oldukça teknik tarafla, akademik makalelerle devam ediliyor olacak. Bugün burada üçüncü oturumumuzda biraz teknoloji savaşları konusuna değinmek istedik. Ben teknoloji savaşları açısından bir konuşma yapmak istiyorum. Gün boyu çok değerli, nitelikli konuşmalar dinledik. Ben size biraz farklı bir açıdan yaklaşacağım.

Şöyle bir durum hayal edelim. Bir pazartesi sabahı işlerimize geldik. Büyük bir banka olabilir, telekom operatörü olabilir, enerji dağıtım şirketi olabilir; bunun başında olduğunuzu düşünün. Elektrik var, internet de var. Ama baktığınızda dışarıdaki bulut hizmetlerine erişim yok. Lisans doğrulama sunucularına, merkezden yönetilen güvenlik ekranlarına erişimleriniz yok. Güncelleme kaynaklarına erişemiyorsunuz. Bunu bir savaş ortamı olarak da düşünebilirsiniz; müttefik bildikleriniz servisleri kapatmış olabilir. Bu tür bir durumda aslında en uç tolerans süresi 72 saat. 72 saate kadar kurumlarda personel, olağan biriken işleriyle idare edebilir belki; ama 72 saatten sonra artık kurumlar ve personel, bugünkü dijitalleşmiş ortamda bir nevi işsiz kalabilir. Kurumun bundan sonra çalışmaya devam edebilmesini biraz sorgulamak istiyorum.

Peki, böyle bir ortamda bir saldırı başladı. Kendi ağınızda kendi kararınızı alabiliyor musunuz? Saatler ilerliyor. Kendi elinizdeki seçenekler artıyor mu, azalıyor mu? Bunu aslında bir “72 saatlik egemenlik testi” gibi de okuyabilirsiniz. Hep diyoruz ya, dijital egemenlik. İşte aslında dijital egemenlik bugün değil; o gün geldiğinde biraz daha anlayacağımız, sahip olup olmadığımızı göreceğimiz bir şey. O yüzden o günü hayal ederek ilerleyelim istiyorum.

İlk 6 saate bakalım. İlk 6 saatte bulmak gereken şey çoğunlukla şu: Neye bağımlıyız? Dışarıda bir hizmet erişilemez hale geldiğinde hangi uygulama etkilenir? Hangi güvenlik cihazının lisansı, yerelde dahi çalışmayı kilitleyebilir? Hangi kimlik doğrulama veya DNS hizmeti dışarıya bağımlı? Bunları bilmek zorundayız. Bir diğer önemli soru da: Loglar nerede? Bunları olay başladıktan sonra öğreniyorsak, krizin en kıymetli saatlerini, o pazartesi sabahının ilk 6 saatini teknoloji envanteri çıkartmakla harcıyoruz demektir. Demek ki ilk hamle aslında bu bağımlılık haritasını, teknoloji envanterini önceden çıkartmak. Her kurum, teknoloji zincirinin hangi halkasında karar yetkisini kime bıraktığını yazılı olarak biliyor olmalı.

Bunları da üç katmanda tanımlayabiliriz. Birincisi, hizmeti çalıştıran altyapılar: sunucu, elektrik, ağ, haberleşme. İkinci katman, sistemi yöneten kontrol katmanı diyebileceğimiz kimlik doğrulama, politika yönetimi, lisanslama, sertifika ve uzaktan erişim katmanı. Üçüncüsü de aslında gözümüz kulağımız olan log sistemleri, izleme sistemleri, monitöring sistemleri. Çünkü sunucular sabah sağlam olabilir ama yönetim paneline, ekranına giremiyorsanız; ağınız çalışıyor olabilir ama bir arıza olduğunda onun

kayıtlarına erişemiyorsanız, o gün aslında yapabileceğiniz çok da bir şey kalmıyor. İşte 72 saatlik egemenlik testi dediğimiz böyle bir test de tam olarak bunların, yani altyapının, kontrolün ve kayıt sistemlerinin birlikte çalışmasına bağlı.

Bir sonraki 18 saatte neler olabilir? Envanter çıktı. Şimdi sıra biraz yönetime gelmeli. Kurumun güvenlik politikasını değiştirmek için dışarıdaki bir ekrana ihtiyaç var mı? Şüpheli bir trafiği kendi ağımızda analiz edebiliyor muyuz? Saldırı anında hangi servise öncelik vereceğiz? Buna bir mühendis anlık karar verebiliyor mu, yoksa bir karar zinciri yürümek zorunda mı? İşte bu sorular, dikkat ederseniz, siber güvenliği sıradan bir bilişim harcaması olmaktan çıkartıyor. Çünkü güvenlik sistemleri dijital altyapılarda giriş noktasında yer alıyor ve hangi bağlantının geçeceğini, hangisinin kalacağına, hangi isteğin engelleneceğine, hangi hizmetin ayakta kalacağına karar veren sistemler.

Mesela DDoS saldırılarını düşünelim. Bir kamu hizmetinin ya da bankacılık uygulamasının ulaşılabilir hale geldiğini düşünün. Bu, birkaç sunucunun yavaşlamasıyla kalmaz; insanların günlük işi aksar; ticarete, finansa, kamuya duyulan güven sarsılır. Daha önce yazdığım bir akademik makalede siber saldırıların ülkelerin gayri safi millî hasıllarına etkisini incelemiştim. Gerçekten alelade bir siber saldırının bile ülke gayri safi millî hasıllarında yüzde 1'lere, hatta yüzde 3,5'a varan etkiler yarattığı örnekler var. Guatemala'da olmuş bir olay: Memurlar 30 gün maaş alamamış ve ülkenin o seneki gayri safi millî hasılları yüzde 3,5 düşmüş. Çok büyük rakamlar bunlar. Demek ki aslında "bir DDoS" deyip geçmemek lazım. Bu dahi işi etkileyebilir, ticareti etkileyebilir, finansı ve kamuya duyulan güveni etkileyebilir. Bu yüzden günümüzün güvenlik konjonktüründe kritik ağlarda çalışan, yerinde, dışarıya bağımlı olmayan, dış servis koptuğunda da temel koruma işlevini yerinde sürdürebilen sistemler gittikçe daha fazla önem kazanıyor.

Şimdi 18 saati biraz irdeledik. Bundan sonraki ikinci ve üçüncü güne bakalım. İlk günü bu tür tedbirlerle geçirdik. İkinci gün ve üçüncü gün artık biraz daha insanın, sürecin, tedarikin sınıandığı bir dönem. Alternatif haberleşme hattı var mı? Müdahale yetkileri yazılı mıydı? Olayı yönetecek yetişmiş mühendis kurumda var mı? Yedekler vardı; yedeklerden geri dönebiliyor mu? Bir tedarikçiye ulaşamadık, olağanüstü bir ortam var; tedarikçiye ulaşamadık diye bir sistemi ayakta tutacak bilgi kurumumuzun içinde var mı, yoksa o tedarikçi olmazsa çalışmıyor muyuz? İşte bunların hepsi bu ikinci ve üçüncü günde yavaş yavaş ortaya çıkıyor. Teknolojik egemenlik dediğimiz şey de tam olarak bu: Krizde karar verebilmek, müdahale edebilmek, hizmeti sürdürebilmek. Aslında bugünün teknoloji savaşlarının ana konusu da belki yıllar sonra olabilecek o pazartesi sabahına bir hazırlık.

Biraz açık konuşmak istiyorum. Bugün kurumlarda yapılan toplantılarda "Efendim, biz hazırız" denilebilir; ama bu, hazır olduğumuz anlamına maalesef gelmiyor. Kritik sistemleri riske atmadan, kontrollü ortamda dış hizmet bağımlılıklarını tek tek irdelemek, keserek tatbikatlar yapmak gerekiyor. Sistem kendini koruyor mu? Mühendis cihazı yerelde yönetebiliyor mu? Cihaz dışarıdan bağımsız çalışabiliyor mu? Hizmet ne kadar sürede geri geliyor? Böyle bir testin, böyle bir tatbikatın sonucunda hazırlanacak bir rapor çok önemli. Bu raporda kesintiden etkilenmeyen sistemler tabii ki liste olarak olmalı; ama kesintiden etkilenen, tek noktaya bağlı, işlev kesintisi yaşayan işlevlerin de

listesi bulunmalı. Çünkü eğer dijital egemen olmayı hedefliyorsak dışarıya bağımlı sistemleri tek tek ikame etmek durumundayız.

Peki bu 72 saatin teknoloji savaşlarıyla ilgisi ne, diye sorabilirsiniz. Ben teknoloji rekabetini sıra tabanlı, yani “turn based” oyunlara benzetiyorum. Daha önce de oynadığınız, mesela Civilization: Bir adım siz atarsınız, bir adım bilgisayar oynar. Ya da satranç düşünün. On adım sonra nerede bulunacağınız, şu anda attığınız hamleyle çok ilişkilidir. Teknoloji rekabeti de aslında biraz böyle. Bugün ilk satın alma maliyetine bakarak seçtiğiniz, “en uygun fiyatlı” dediğiniz ürün yarın sizin için bağımlılık olabilir ve dijital egemenliğinizi bitiren ürün olabilir. “Bugün tüm dünya satın alıyor” dediğiniz bir ürün yarın bağımlılığa dönüşebilir. “Nasıl da yurt dışından firma destek veriyor” deyip bugün yetiştirmedığınız bir mühendis, 5 hamle sonra kuramayacağınız bir ekip demek aslında. Bugün var olan bir projeye sokmadığınız bir yerli üretici, 10 hamle sonra ihtiyaç duyduğunuz alternatifi hiç doğmaması demek. Buna biraz böyle bakmak gerekiyor.

Devletler için de aynısı geçerli. Çipler üzerindeki ihracat kısıtlamalarını duyuyorsunuz, değil mi? Yapay zekâ altyapılarına erişim şartları: Şu erişebilir, bu erişemez; bu modeli bu kullanabilir, bu kullanamaz gibi şartlar. Yazılım ekosistemlerinin kuralları. Bunların hepsi aslında teknoloji savaşında birer hamle. Bunları böyle okuyacağız. Ve her hamle, karşı tarafın bir sonraki adımdaki seçeneklerini daraltmak için var. Bakın, son bir yılı düşünün. Amerika’nın hamlelerini düşünün: Venezuela’yı, Grönland’ı, İran’ı, Tayvan’ı düşünün. Bunlar hepimize alelde, bir delinin hareketleri gibi görünebilir. Ama özünde hepsi birer teknoloji savaşı. Bunu da hissetmeliyiz. Bakın, birisi enerjiyle ilişkili, birisi nadir toprak elementleriyle ilişkili. Nadir toprak elementi demek çip demek, GPU demek, dolayısıyla yapay zekâ demek. Birisi rakibini yavaşlatma, rakibinin ucuz enerji kaynağını kesme demek; İran. Tayvan konusu, Amerika’nın bugün Tayvan’ın yanında olması, üretimi kendi topraklarına taşıyana kadar kendisine ana sağlayıcı olan Tayvan’ı korumak demek. Yani bugün ABD’nin gördüğünüz alakasız bir hamlesi bile aslında 5 yıl sonra Çin’e bağımlı olmamanın birer adımı.

Teknoloji savaşında yapay zekâ devrimi aslında bunu şekillendiriyor. Yapay zekâ devrimiyle beraber tüm dünyada yeni bir ekonomi şekilleniyor. Bu yeni ekonomide güçler değişiyor. Gelecekte potansiyel güç olmak isteyenler de bunları adım adım, bir satranç oyunu gibi, sıra bazlı bir oyun gibi kuruyor. Sıra tabanlı oyunlarda güçlü taşı hemen ileri sürmek cazip gelebilir. Ama bugünün kazanan oyuncularını, bu hamlenin kazancını değil, karşılığında yarın hangi yolların kapanacağını da hesaplayanlardır ve öyle olmalıdır. Kazanan satranç oyuncuları bunu yapabilenlerdir.

Bizim konumuzda da böyle. Bir platforma bağlanmak hızlı ve ekonomik olabilir; tek tuşla devreye alabiliyor olabilirsiniz. Ama bu tür sistemleri kullandıkça veri taşınabilirliğini, açık standartları, alternatif tedariki, kendi mühendislik birikiminizi ihmal edersiniz. Aslında yaptığınız her yeni hamle bugün sizin işinizi kolaylaştırıyor, bugünkü hamleyi cazip hale getiriyor gibi görünse de gelecekte çok daha pahalı; 10 hamle sonra da sizi hamle yapacak yeriniz kalmamış bir pozisyonda bırakacak. Bugün özgeçmişinize yazdığınız, burada kurumlarda çalışan profesyonel bilişim sistemi uzmanları vardır, özgeçmişinize yazdığınız yabancı bir ürünün sertifikasındaki ürün, yarın çocuklarınızın geleceğini etkileyen bir ülke güvenliği meselesi olabilir. Bu konuya artık böyle bakmak

lazım. Günümüzün teknoloji savaşlarında, Türkiye'nin teknoloji politikasında da ben bunun esas alınması gerektiğini düşünüyorum.

Birkaç sonuç başlığı sayayım. Örneğin kritik altyapılar için 72 saatlik kesinti senaryolarını gerçek tatbikatlara dönüştürmeliyiz. Tatbikatın sonucunda her kuruluşun bir asgari hizmet listesi çıkmalı: Ne mutlaka çalışır tutulmalı? Ne gerektiğinde kontrollü olarak durdurulabilmeli? Hangi yetkiyi kim nasıl kullanabilmeli? Kamu alımlarında fiyat-performansın yanında, zorunlu olarak, yani "must" olarak, yerel yönetilebilirliği, hizmetin dış bağlantı koptuğunda sürüp sürmeyeceğini, alternatif müdahale imkânının bulunup bulunmadığını da mutlaka koymak durumundayız. Operatörün, kurumun ve güvenlik üreticisinin arasındaki sorumluluk paylaşımları da ayrıca çok önem taşımakta.

Öte yandan tabii yerli teknoloji üreticilerini saha deneyimine ilerletmeliyiz. Savunma sanayiinde büyük bir başarının sergilendiği zaten herkesçe malum. Bu nasıl oldu? Yerlilere yol açarak, alan açarak oldu. Siber güvenlikte bunu başarmak istiyorsak yapacağımız şey de bundan farklı bir şey değil. Devlet ilk müşteri; stratejik yönlendirici olabilir, uzun vadeli siparişler verebilir, ürünleri zorlu testlerden geçirebilir ve gerisini özel sektör ile üniversite birlikte büyütür. Bir ürünün dayanıklılığını böylece kataloglarda değil sahada görmüş, ispatlamış oluruz. Bu noktada Savunma Sanayii Başkanlığı ilgili Daire Başkanı Murat Çizgel Bey'in konuşmasında bahsettiği SAYGEP buna benzer bir proje. Onun dışında Siber Güvenlik Başkanlığımızın da benzer bir ilerlemesi olduğunu biliyorum. Bunları da bilerek doğru yolda olduğumuzu özellikle belirtmek isterim.

Tabii her katmanda yerli olmak zorunda mıyız? Olmayabilir. Ama etki zincirinde olası en kötü senaryonun neyi nasıl etkileyeceğini bilmeliyiz. Buradaki bir kabullenme, o gün geldiğinde, o pazartesi sabahı geldiğinde bana neye mal olacak; bunu görebiliyor olmak zorundayız. Globalle çalışırken bile kritik kararları verebilecek kapasiteyi elimizde tutmalı ve B planına mutlaka sahip olmak durumundayız.

Konuşmamı tamamlarken size iki tane de soru bırakmak istiyorum. Yarın sabah kritik dış teknoloji hizmetleri 72 saat boyunca kesilse ayakta kalabilecek miyiz? Tamamınız kendinize sorun. Bugün attığınız bir teknoloji hamlesi, imza attığınız bir teknoloji alımı, 10 hamle sonra elimizi güçlendirecek mi, yoksa seçeneklerimizi azaltacak mı? Bu 10 hamleyi 5 yıl olarak da okuyabilirsiniz, 10 yıl olarak da okuyabilirsiniz. Bir dünya savaşı olacaksa, ki herkes bunu söylüyor, yabancı akıllı bilişim sistemleri bizim için hızlandırıcı mı olacak, engelleyici mi olacak? Bu soruyu da lütfen sorun. Böyle bir dünyada kriz anında ayakta kalabilmek, bence 10 hamle sonra da kendi hamlesini yapabilecek durumda olmaya bağlı. İşte bence bunlar artık teknoloji egemenliğinin, teknoloji dayanıklılığının, dijital egemenliğin ana ölçütleri olmalıdır.

Çok teşekkür ediyorum. Arz ederim.

04:28:06 Murad BALAYEV – Azerbaycan Cumhuriyeti Özel İletişim ve Bilgi Güvenliği Devlet Servisi SOME Müdürü

Sayın yönetim kurulu üyeleri, kamu kurumlarının, savunma sanayisinin ve üniversitelerin kıymetli temsilcileri, değerli meslektaşlarım, sevgili öğrenciler, hanımefendiler, beyefendiler. Hepinizi, temsil ettiğim Devlet Servisi, onun Siber Olaylara

Müdahale Merkezi ve şahsım adına en içten duygularımla, saygı ve muhabbetle selamlıyorum.

Sözlerimin hemen başında, bu anlamlı konferansa davet edilmemiz vesilesiyle Türkiye Cumhuriyeti Cumhurbaşkanlığı Siber Güvenlik Başkanlığına nazik davetleri ve sıcak misafirperverlikleri için yürekten teşekkür ediyor; bölgemizin en köklü bilimsel buluşmalarından biri hâline gelen bu konferansı 19. kez büyük bir özveriyle hazırlayan Bilgi Güvenliği Derneğine ve emeği geçen herkese başarılar diliyorum.

Konferansın bu yılki ana temasının siber savaşlar olarak belirlenmesini ve bana bu konuyu ele alan oturumda söz verilmesini son derece anlamlı buluyorum. Çünkü bugün paylaşacaklarım teorik değerlendirmeler değil; son bir yılın, devlet SOME'si olarak bizzat gözlemlediğimiz, araştırdığımız ve kamuoyuyla paylaştığımız olayların bize öğrettikleridir.

Yaşadığımız çağda devletler arasındaki rekabet artık yalnızca topraklar, pazarlar ve enerji kaynakları üzerinden değil; yarı iletkenler, yapay zekâ modelleri, bulut altyapıları ve veri üzerinden yürüyor. Buna teknoloji savaşları diyoruz. Bu savaşın en sessiz, en görünmez ve en ucuz cephesi ise siber casusluktur. Bir devletin yıllarca biriktirdiği bilgi, bugün tek bir ortalama e-postasıyla ya da tek bir güvenilen tedarikçi hesabıyla rakiplerin eline geçebiliyor.

Maalesef bu tehdidin en gelişmiş ülkeleri bile etkilediğini görmek için uzağa bakmamıza gerek yok. Danimarka, bildiğiniz üzere Birleşmiş Milletler E-Devlet Gelişmişlik Endeksi'nde 2024 yılında üst üste dördüncü kez dünya birincisi olmuş bir ülkedir. Ancak sadece iki hafta önce, 5 Ekim'de Danimarka hükümeti, merkezi nüfus kaydındaki yaklaşık 8,8 milyon kişinin isim, adres ve kimlik numarasına yetkisiz erişim sağlandığını açıkladı. Erişim, sorgulama yetkisi bulunan özel bir şirketin meşru hesabı üzerinden sağlanmıştır. Olay bir güvenlik alarmıyla değil, olağan dışı yüksek bir sorgulama faturası sayesinde fark edildi. Basına yansıyan iddialara göre zincirin koptuğu halka ise küçük bir tedarikçinin "123456" gibi bir parola kullanmasıydı.

Ülke tarihinin en büyük veri ihlali bize çok net bir şey söylüyor: Dijitalleşmede dünya birincisi olmak, siber dayanıklılıkta birinci olmak anlamına gelmiyor. Bir devletin güvenliği, güvendiği en zayıf üçüncü tarafın güvenliği kadardır.

Siber savaş, 7 gün 24 saat kesintisiz süren bir savaştır. Kaynağı, hedefi ve menzili belirsizdir. Biz devlet SOME'leri bu belirsizliğin tam ortasında, ilk hatta duruyoruz. Şimdi izninizle son bir yılda gözlemlediklerimizi sizlerle paylaşmak istiyorum.

Değerli meslektaşlarım, son bir yıl teknoloji savaşlarının ve siber casusluğun bizim için soyut bir kavram olmadığını gösterdi. Kamuoyuyla paylaştığımız bazı kullanım senaryolarını, use case'leri teknik ayrıntılarına varmadan aktarmak istiyorum.

Birincisi, enerji sektörümüze yönelik devlet destekli faaliyetlerdir. Bu yılın Mayıs ayında devlet SOME'miz, Çin ile bağlantılı olduğu değerlendirilen bir APT grubunun petrol ve doğal gaz sektörümüzde faaliyet gösteren bir şirkete karşı çok aşamalı bir casusluk kampanyası yürüttüğüne ilişkin iddiaları araştırdı. Threat hunting sonucu devlet ağımızda bu faaliyete ait bir izle rastlanmadı. Ancak tüm göstergeler önleyici olarak

engellendi ve kurumlarımıza geriye dönük tarama tavsiyeleri verildi. Buradan çıkan ders açıktır: Enerji, küresel rekabetin en kıymetli bilgi varlığıdır ve bu alandaki her şirket artık bir devlet hedefidir.

İkincisi, diplomatik ve stratejik kurumlarımıza yönelik hedefli casusluktur. Zararlı yazılım araştırma laboratuvarımız var. Güney Asya kökenli olduğu değerlendirilen ve diplomatik kurumlar ile savunma sektörünü hedef almasıyla tanınan bir APT grubunun kampanyası incelendi. Kamu kurumlarımıza, güncel siyasi gündemi istismar eden, yüksek öncelikli dahili bilgi notu görünümünde bir tuzak belge gönderilmişti. Belgeyi açan kullanıcı, meşru bir yazılımın kurulum mekanizması üzerinden zararlı bir zincire, C2 sunucusuna yönlendirilmişti. Nihai amaç uzun süreli ve sessiz bir istihbarat toplama faaliyetiydi.

Üçüncüsü, insan alışkanlıklarını istismar eden saldırılardır. Laboratuvarımızın yayımladığı bir diğer araştırmada, bir kamu kurumu çalışanının web tarayıcısında açık bıraktığı anlık mesajlaşma oturumunun ele geçirildiğini ve çalışanın gönderdiği resmî belgelerin iş arkadaşına zararlı arşivler olarak ulaştığını tespit ettik. Sisteme yerleştirilen arka kapının fidye yazılımı dahi indirebildiğini laboratuvar ortamında doğruladık. Bu olay bize en sofistike güvenlik duvarının bile açık bırakılmış bir oturumu koruyamayacağını hatırlatıyor.

Dördüncüsü, giderek siyasi bir baskı aracına dönüşen hacktivizmdir. Geçen yıl ekim ayında, Rus kökenli bir hacktivist yapıyla ittifak eden ve NATO ülkeleri başta olmak üzere birçok devleti, aynı zamanda Türkiye'yi de hedef alan RedWolf hacktivist grubunun hedef listesinde ülkemizin de bulunduğunu kamuoyuyla paylaştık ve kurumlarımızı DDoS'a karşı hazırlığa çağırdık. Hacktivizm ucuz, gürültülü ve görünür bir silahtır. Ancak arkasındaki siyasi mesajı ve devlet gölgesini görmezden gelemeyiz.

Devlet destekli aktörler ve hacktivistler tehdidin yalnızca bir yüzüdür. Asıl zorluk, korumakla yükümlü olduğumuz saldırı yüzeyinin her gün genişlemesidir. Bu hususta üç başlığa dikkat çekmek istiyorum.

Birincisi, benden önce de birçok konuşmacının, meslektaşımın ele aldığı tedarik zinciri. Haziran ayındaki Klue olayında saldırganlar, bir pazar istihbaratı platformunun 2022'den kalma tek bir eski entegrasyon hesabını ele geçirdi ve müşterilere ait erişim belirteçleri üzerinden, önde gelen siber güvenlik şirketleri dahil 20'ye yakın kuruluşun CRM verilerini toplu olarak dışarı sızdırdı. Tek bir kuruma dahi sızmaya gerek kalmadı; verilen güven yeterliydi. Danimarka ile aynı ders: Entegrasyon envanteri, belirteç ömrü, en az yetki ve tedarikçi denetimi bugün lüks değil, zorunluluktur.

İkinci konuyu Shadow AI olarak belirtmek istiyorum. Temmuz ayında devlet kurumları için yayımladığımız bir uyarıda vurguladığımız gibi, kurumlar bilinen yapay zekâ platformlarını yasakladığında çalışanlar bilinmeyen, denetimsiz platformlara yöneliyor. İç yazışmalar, sözleşmeler, kişisel veriler kurumun haberi olmadan üçüncü taraflara aktarılabilir. Sorun yapay zekânın kendisi değil, görünmez ve yönetilmeyen kullanımıdır. Çözüm yasaklamak değil; onaylı araçlar sunmak, hangi verinin asla girilemeyeceğini tanımlamak ve çalışanları bu hususta eğitmektir.

Üçüncü konu, nesnelerin interneti. Bu yıl dünya genelinde yaklaşık 200.000 cihaza bulaşan Dispor botnetini ve fabrikada gömülmüş zararlı bileşenlerle, kullanıcı farkında

olmadan onu bir vekil sunucu ağına parçası yapan 35 dolarlık bir projektörü gündeme taşıdık. Ağa bağlı her ucuz cihaz hem bir casusluk sensörü hem de DDoS silahı olabilir. Satın alma standartları, ağ ayırımı vesaire.

SOME perspektifinden yaklaştığımızda, peki bir devlet SOME'si bu tabloya nasıl cevap vermeli? Son bir yılın tecrübesi bize beş ilkeyi öğretti.

Birincisi, görünürlük olmadan savunma olmaz. Her istihbarat göstergesini devlet ağıımız genelinde anlık ve geriye dönük tarıyoruz. Bulgularımızı kurumlarımızla ve kamuoyuyla paylaşıyoruz. Çünkü güven ancak şeffaflıkla kurulur.

İkincisi, yerli ve millî analiz kapasitesi. Eylül ayında ülkemizde ilk kez zararlı yazılım analizi ve dijital adli bilişim laboratuvarını bir üniversitede hizmete verdik. Kendi geliştirdiğimiz adli analiz araçlarıyla incelemelerimizi yapıyor, bulgularımızı uluslararası literatüre kazandırıyoruz. Bunun yanı sıra tehdit istihbaratı ve agentic SOC hizmetlerini bir merkezde toplayıp analiz eden ileri seviye bir MDR projesi üzerinde de çalışıyoruz. Bir saldırıyı başkasının raporundan öğrenen değil, kendi kaynaklarımızla çözebilen bir SOME olmak hedefimiz.

Üçüncüsü, tatbikat mevzusu. Ağustos ayında enerji sektörümüz için üst düzey bir siber kriz simülasyonu yürüttük. Siber poligonumuzda kurumlarımızla düzenli uygulamalı eğitimler yapıyoruz. Kriz anında ilk kez tanışan ekipler haliyle kaybeder.

Dördüncüsü, insan faktörü. Aylık bilgi güvenliği webinarlarımız, üniversitelerdeki ustalık dersleri ve bölgelerdeki farkındalık programlarıyla en zayıf halkayı en güçlü halkaya dönüştürmeyi hedefliyoruz. Çünkü anlattığım olayların hemen hepsi tek bir tıklamayla başlıyor.

Beşincisi ve belki de en önemlisi, iş birliği. Biz uluslararası FIRST, OIC-CERT, Trusted Introducer, APWG gibi toplulukların aktif üyesi olarak göstergelerimizi paylaşıyor; çeşitli ülkelerin ilgili millî ve devlet SOME'leriyle, kuruluşlarıyla iş birliği yapıyoruz. Bu hususta en azından müttefik ülkelerin ulusal SOME'leri arasında protokol beklemeye ihtiyaç duyulmamalı diye düşünüyorum.

Sözlerimi bitirirken şunu vurgulamak isterim: Bugün hiçbir devlet, hiçbir kurum “bize saldırmazlar” deme lüksüne sahip değildir. Gereken soru “saldırı olacak mı?” değil, “saldırı olduğunda ne kadar hazırız?” sorusu olmalı. Danimarka'nın tecrübesi mükemmel sistemlerin değil, dayanıklı ekosistemlerin kazandığını; bizim tecrübemiz ise görünürlük, hazırlık ve iş birliğinin en güçlü savunma olduğunu gösteriyor.

Bu vesileyle Siber Güvenlik Başkanlığına ve Bilgi Güvenliği Derneğine bir kez daha teşekkür ediyor, konferansın ülkelerimize hayırlı sonuçlar getirmesini diliyorum. Siber alanda da “iki devlet, tek millet” anlayışıyla omuz omuza yürümeye devam edeceğimize yürekten inanıyorum. Beni sabırla dinlediğiniz için teşekkür ederim. Sağ olun, var olun.

04:40:36 Hüseyin KURU – Jandarma Muhabere Yarbayı, Jandarma Genel Komutanlığı MEBS ve Siber Güvenlik Komutanlığı

Değerli Genel Müdürüm, değerli hocalarım, değerli kurumların, firmaların, üniversitelerin çalışanları; hepinizi saygıyla selamlıyorum.

Tabii günün sonndan bir önceki konuşmasını yapmakta olduğum için sizin de biraz yorgunluğunuz var. Bugün sizlerle ülkelerin teknolojik üstünlük elde etmek ve bu üstünlüğü korumak için yürüttükleri küresel rekabeti, bu rekabetin giderek daha önemli hale gelen boyutlarından biri olan siber casusluk faaliyetlerini ve bütün bunların ulusal güvenlik üzerine etkilerini konuşmak istiyorum.

Aslında teknoloji savaşları dediğimiz bu mücadele yalnızca yeni ürünler geliştirmekten ibaret değil. Ülkeler mevcut teknolojileri iyileştirmeye, yeni yetenekler kazandırmaya, yerleştirilerek dışa bağımlılıklarını azaltmaya, rakiplerinin sahip olduğu kritik bilgi birikimine ulaşmaya çalışırken diğer yandan onların kritik mühendislik bilgilerine erişimini kısıtlamaya çalışıyorlar. Siber casusluk da bu rekabetin en kurnasız boyutlarından bir tanesini teşkil ediyor.

Teknoloji tarihine baktığımızda önemli bir gerçeği görüyoruz: Bir teknoloji ne kadar köklü dönüşüm yaratıyorsa zamanla ona duyulan ihtiyaç da o ölçüde artıyor. Yani entegrasyon artık bir zorunluluk haline geliyor. Ya entegre oluyorsunuz ya da aslında teknolojiyi arkadan takip ediyorsunuz. Elektriğin icadını, bilgisayarları, interneti ve akıllı telefonları düşünelim. Bugün benzer bir dönüşümü yapay zekâda yaşıyoruz. Yine robotik teknolojiler, elektrikli araçlar, İHA sistemleri bugün entegre olmak zorunda olduğumuz, aslında devrimsel nitelikteki teknolojiler. Bundan sonra da, belki gelecekte, yarın kuantum bilgisayarları konuşuyor olabiliriz; kuantum bilgisayarların yarattığı hassasiyeti, kuantum anahtar dağıtımını, kuantum şifrelemeyi, kuantum güvenli haberleşmeyi konuşuyor olabiliriz. Belki bugünden bu alanlarda tedbir almak durumundayız. Bununla ilgili yerli firmaların da açıkçası çalıştığını görüyoruz.

Başlangıçta devrimsel bir yenilik olarak görülen bu teknolojiler zamanla ekonominin, sanayinin, savunmanın ve günlük yaşamın vazgeçilmez parçalarına dönüşüyor. İşte bu noktada teknoloji yalnızca bir ürün olmaktan çıkıp stratejik güç unsuruna dönüşüyor. Bir ülkenin gücünü artık sadece ekonomik büyüklüğü, askeri kapasitesi veya doğal kaynaklarıyla ölçemeyiz. Hangi teknolojileri geliştirebildiği, onları ne kadar kullandığı ve kritik alanlarda ne ölçüde bağımsız hareket edebildiği de belirleyici. Kısaca teknoloji ekonomik ve askeri gücün alternatifi değil; bu güçler üzerinde aslında çarpan etkisi yaratan bir pozisyonda.

Peki ülkeler teknolojik yetkinliklerini geliştirmek ve bu rekabette üstünlük sağlamak için hangi yöntemleri kullanıyor? Bunun farklı yolları var. İlk olarak ihtiyaç duydukları teknolojileri doğrudan satın alabiliyor veya teknoloji transferi yoluyla edinebiliyorlar. Ancak bir teknolojiyi satın almak, o teknolojiyi geliştirebilecek bilgi birikimine ve mühendislik yetkinliğine sahip olmak anlamına gelmiyor.

Bir başka yaklaşım mevcut teknolojileri daha ileriye taşımak; yani kullanılan teknolojilere yeni özellikler kazandırmak, performanslarını artırmak ve zaman içerisinde bunları yerli imkânlarla geliştirilebilir ve üretilebilir hale getirmek. Aslında siber güvenlik ekosisteminde de en çok gördüğümüz örnekler bu yolla edinilen tecrübeye yeni ürünler geliştirmek üzerine. Örneğin yerli firewall'larımıza, yerli WAF'larımıza baktığımızda yabancı muadillerinin çok daha ötesinde yeni yetenekler kazandırarak kamu kurumlarına entegre etmeye çalıştıklarını görüyoruz. Aslında burada gerçekten mühendislik örneklerini, belki tersine mühendislik çalışmalarının başarılı örneklerini de görmüş oluyoruz. Tersine mühendislik bu süreçte kullanılan yöntemlerden bir tanesi: Mevcut ürünlerin çalışma prensiplerini ve teknik yapılarını analiz ederek benzer teknolojiler geliştirmek, hatta bazı alanlarda mevcut ürünlerin ötesine geçmek mümkün olabiliyor.

Ülkeler bir yandan teknoloji edinmeye çalışırken diğer yandan sahip oldukları üstünlükleri korumak istiyor. ABD'nin F-22 savaş uçağına veya yarı iletkenlere koyduğu kısıtlamalar aslında bunun örneklerinden birkaç tanesi.

Ancak rekabet her zaman meşru sınırlar içerisinde yürümüyor. Bir ülkenin yıllarca çalışarak, binlerce mühendis ve milyarlarca dolar yatırımla oluşturduğu bilgi birikimine başka bir ülke çok daha kısa sürede ulaşmaya çalışırsa ortaya aslında siber casusluk diye bir kavram çıkmış oluyor. Casusluk elbette yeni değil. Geçmişte gizli belgelere ulaşmak için hedef ülkeye fiziksel olarak gitmek, istihbarat elemanları yetiştirmek veya devşirmek, onları o ülkedeki kurumlara yerleştirmek gerekebiliyordu. Bu süreç uzun, maliyetli ve fiziksel açıdan riskliydi.

Peki bugün ne değişti? Mühendislik çizimleri, kaynak kodları, araştırma sonuçları ve savunma projeleri artık dijital sistemlerde işleniyor, saklanıyor ve iletiliyor. Siber ortam fiziksel mesafeyi büyük ölçüde önemsizleştiriyor. Dünyanın diğer ucundaki bir kurum uzaktan hedef alınabiliyor. Aynı anda çok sayıda hedefe yönelik keşif ve sızma faaliyetleri siber ortam üzerinden yürütülebiliyor. Saldırganın kimliğini kesin olarak belirlemek de her zaman kolay değil. Yapay zekâ, hedef araştırması ve büyük veri analizinde bu faaliyetlerin hızını ve ölçeğini artıracak yeteneklere artık sahip.

Geleneksel casuslukta fiziksel erişim ve insan ilişkileri çoğu zaman belirleyiciydi. Siber ortamda ise zayıf bir parola, güncellenmemiş bir sistem veya tedarikçi üzerinden açılan bir erişim saldırgan için fırsat oluşturabiliyor. Bir kez elde edilen yetki, farklı sistemlere ilerlemek ve büyük miktarda veriyi kopyalamak amacıyla kötüye kullanılabilir. Bu yüzden kurumların yalnızca dış ağlarını değil; kimlik ve erişim yönetimini, tedarikçi bağlantılarını ve hassas verilerini kullanırken aynı zamanda koruması elzem bir konu haline geldi.

Siber casusluk risksiz değil; fakat geleneksel yöntemlere göre çok daha düşük fiziksel riskle daha geniş bir alana ulaşabiliyor. Bunun dikkat çekici örneklerinden biri F-35 savaş uçağı programı. F-35 yalnızca bir uçak değil; gelişmiş sensörleri, yazılımları ve düşük görünürlük teknolojileriyle büyük bir mühendislik bilgi birikimini teşkil ediyor. Bu programa ilişkin hassas bilgilerin geçmişte Çin bağlantılı siber casusluk faaliyetlerinde hedef alındığı kamuya yansdı. Ele geçirilen bilgilerin başka uçak programlarına ne ölçüde katkı sağladığı kesin olarak ortaya konmuş değil. Ancak temel ders açık: Bir

ülkenin teknolojik üstünlük için yıllarca yaptığı yatırım, başka bir ülkenin istihbarat hedefi haline gelebiliyor. Dolayısıyla teknolojiyi üretmek kadar onun arkasındaki fikri sermayeyi korumak da önemli.

F-35 örneği rekabetin ne kadar büyük ekonomik ve stratejik değer taşıdığını da hatırlatıyor. Bir savunma platformu yalnızca metalden ve elektronik bileşenlerden oluşmaz. Onu asıl değerli kılan, yıllar boyunca edinilen test sonuçları, tasarım tercihleri, yazılım mantığı ve mühendislik deneyimidir. Bu bilgi birikiminin kaybı yalnızca tek bir projenin değil, sonraki nesil ürünlerin rekabet avantajını da etkileyebilir.

Üstelik hedef yalnızca savunma sanayii değil. 2000-2020 döneminde gerçekleşen Çin bağlantılı 595 casusluk vakasının incelendiği bir araştırmada havacılık, uzay ve bilgi teknolojileri ön plana çıkıyor. Yani bu alanlara yönelik siber casusluk faaliyetleri yoğun olarak gerçekleşiyor. Onları biyoteknoloji, ilaç, ileri malzemeler ve enerji gibi alanlar takip ediyor. Çünkü bugünün araştırmaları yarının ekonomik ve askeri üstünlüğünü belirleyebiliyor. Bir üniversitenin yayınlanmamış çalışması veya bir girişimin kaynak kodu da stratejik değer taşıyabiliyor.

Ancak bazen hassas bir bilginin açığa çıkması için karmaşık bir siber saldırıya bile ihtiyaç kalmıyor. Bu olay 2026 yılında oldu: Fransa'nın Charles de Gaulle uçak gemisi ile ilgili bu yıl içerisinde kamuoyuna yansıyan konum paylaşımı olayını hatırlayalım. Gemideki bir personelin spor aktivitesine ilişkin konum verilerini, Strava'ya galiba uygulamanın ismi, herkese açık paylaşması geminin bulunduğu bölgeye ilişkin bilgi edinilmesine neden oldu. Milyarlarca euroluk gelişmiş bir askeri platformun operasyonel güvenliği sıradan bir dijital alışkanlık nedeniyle riske girebiliyor. Bu olayın bize hatırlattığı şey şu: Güvenlik yalnızca güvenlik duvarı veya şifreleme değildir. İnsan, süreç, teknoloji ve operasyonel disiplin birlikte ele alınmalıdır.

Peki bir ülke kendi teknolojilerini çok iyi koruyor olsa bile kritik altyapılarında başka ülkelere bağımlıysa ne ölçüde bağımsızdır? Bu soru bizi dijital egemenliğe götürüyor. Fransa'nın kamu dijital hizmetlerinde Avrupa merkezli alternatifleri değerlendirmesi, teknoloji bağımlılığını azaltma arayışının örneklerinden bir tanesi. Benzer tartışmalar 5G ve 6G ağlarında Çin merkezli Huawei ve ZTE gibi tedarikçiler etrafında da yaşandı. Bazı Avrupa ülkeleri ulusal güvenlik kaygıları nedeniyle bu şirketlerin kritik ağ bileşenlerinde kullanılmasına kısıtlamalar getirdi, bazıları yasakladı.

Ancak burada önemli bir ayrım yapmamız gerekiyor. Dijital egemenlik bütün yabancı teknolojilerden vazgeçmek veya her teknolojiyi sıfırdan geliştirmek anlamına gelmiyor. Böyle bir yaklaşım ne gerçekçi ne de ekonomik açıdan sürdürülebilir. Asıl mesele kritik teknolojilerde dışa bağımlılığın oluşturabileceği riskleri yönetebilmek.

Bu risklerin yönetilmesinde teknoloji tedarik zincirinin güvenliği de kritik önem taşıyor. Kullandığımız ürünlerin güvenliğini yalnızca satın alma aşamasında değil, bütün yaşam döngüsü boyunca değerlendirmeliyiz. Yazılım güncellemelerinden üçüncü taraf bileşenlere kadar ortaya çıkabilecek güvenlik zafiyetlerini tespit edecek ve giderecek mekanizmalar oluşturmamız. Özellikle kamu hizmetlerinde önceliğimizi yerli üretime vereceğiz; ancak açık standartların kullanılması, açık kaynak kodlu yazılım ve uygulamaların kullanılması, verilerin farklı sistemlere taşınabilmesi ve teknolojilerin birlikte çalışabilir olması, monolitik mimariden mikroservis mimarisine geçiş gibi hususlar

uzun vadeli tedarikçi bağımlılığını azaltmak açısından büyük önem taşıyor. Çünkü teknolojik egemenlik yalnızca kullandığımız teknoloji üzerinde söz sahibi olmak değil, o teknolojinin güvenliğini ve sürekliliğini de kontrol edebilmek anlamına geliyor.

Elbette bütün bunları gerçekleştirmek için güçlü bir teknolojik altyapıya ve ciddi yatırımlara ihtiyaç var. Ancak teknolojiye sahip olmakla o teknolojiyi geliştirebilecek ve gerektiğinde bağımsız olarak sürdürebilecek yetkinliğe sahip olmak aynı şey değil. İşte bu noktada teknoloji rekabetinin belki de en önemli unsurlarından biri karşımıza çıkıyor: nitelikli insan kaynağı.

Bugün çipleri, veri merkezlerini, yapay zekâ sistemlerini ve milyarlarca dolarlık yatırımları konuşuyoruz. Ancak bazen birkaç araştırmacının geliştirdiği yeni bir algoritma, milyarlarca dolarlık bir altyapının performansını önemli ölçüde artırabiliyor. Bu nedenle dünyanın önde gelen teknoloji şirketleri arasında yalnızca teknoloji geliştirme yarışı değil, yetenekli insanları kazanma yarışı da yaşanıyor. İşte Meta olsun, OpenAI olsun, Apple olsun; bunların arasında özellikle “AI talent wars” dediğimiz yetenek savaşları yaşanıyor. En son Ruoming Pang diye bir adam var, belki duymuşsunuzdur; 200 milyon dolara Apple’dan Meta’ya transfer edildi. Yani tek imza parası 200 milyon dolar. Demek ki bu adamın kullanılan altyapıdaki verimliliği artıracak o algoritmaya katkısı çok daha büyük seviyede olacak. Böyle dâhileri büyük firmalar kendi bünyelerine katmak için inanılmaz bir savaş veriyor. O yüzden buradan yola çıkarak biz de insan kaynağına yapılan yatırımı belki de çok önceliklendirmemiz gerekiyor. Dolayısıyla günümüzde finansal sermaye kadar insan kaynağı ve bilgi birikiminden oluşan entelektüel sermaye de stratejik bir güç unsuruna dönüşmüş durumda.

Bir ülkenin güçlü teknolojik altyapılar kurması elbette önemli. Ancak bu altyapıları geliştirecek, yeni teknolojiler üretecek ve bunların güvenliğini sağlayacak insanları yetiştirmesi, ülkesinde tutması ve onlara uygun araştırma ortamları sunması da en az bunun kadar önemli. Burada gençlerin erken yaşta bilim ve teknoloji ile tanışması kadar araştırmacıların hata yapmaktan korkmadan deneyebileceği ortamların kurulması da değerli. İyi bir fikrin ürüne dönüşebilmesi için laboratuvar, finansman, mentorluk ve kamu ile özel sektörün ihtiyaçlarına erişim gerekiyor. Yetişmiş insanı yalnızca bir istihdam kalemi olarak değil, ülkenin uzun vadeli bilgi birikimini taşıyan stratejik bir varlık olarak görmek durumundayız.

Ancak nitelikli insan kaynağına sahip olmak da tek başına yeterli değil. Bu insanları destekleyecek, araştırmayı teknolojiye dönüştürecek güçlü bir ekosisteme de ihtiyaç var. Bu noktada 2026 yılında yayınlanan, ABD ve Çin’in yapay zekâ alanındaki rekabetini inceleyen bir akademik araştırmaya değinmek istiyorum. Araştırma iki ülkenin teknolojik üstünlüğe ulaşma süreçlerini beş faktör üzerinden değerlendiriyor: devlet yatırımları, askeri entegrasyon, özel sektörün gücü, düzenleyici politikalar ve yarı iletken teknolojilerine bağımlılık. Araştırmanın en dikkat çekici sonucu ise şu: ABD ve Çin farklı ekonomik ve siyasi modeller izlemelerine rağmen iki ülkenin teknolojik üstünlük yarışında iki ortak unsur öne çıkıyor: güçlü devlet yatırımları ve yapay zekânın askeri sistemlerle entegrasyonu.

ABD’de özel sektörün ve üniversitelerin öncülük ettiği, devletin araştırma ve savunma yatırımlarıyla desteklediği bir yapı görüyoruz. Çin’de ise devletin daha merkezi bir

yönlendirme yaptığı, sivil ve askeri teknolojilerin birlikte geliştirilmesine ağırlık veren bir yaklaşım bulunuyor. Yani yöntemleri farklı olsa da her iki ülke de yapay zekâyı yalnızca ekonomik bir fırsat olarak değil, ulusal güvenliği ve askeri üstünlüğü doğrudan etkileyen stratejik bir teknoloji olarak değerlendiriyor. Elbette iki ülkeyi inceleyen tek bir araştırmadan bütün dünya için geçerli bir başarı formülü çıkaramayız. Ancak buradan alabileceğimiz önemli bir ders var: Teknolojik üstünlük için yalnızca yetenekli insanlara ve güçlü şirketlere değil, devletin stratejik desteğine ve araştırma sonuçlarını somut yeteneklere dönüştürebilen bir ekosisteme ihtiyaç var.

Peki Türkiye açısından önceliklerimiz ne olmalı? Öncelikle hangi kritik teknolojilerde bağımlılığın ulusal güvenlik riski yarattığını belirlemeliyiz. İkinci olarak tedarik zincirini yalnızca fiyat ve performansa göre değil, sürdürülebilirlik ve alternatif kaynaklara erişim açısından da değerlendirmeliyiz. Üçüncü olarak siber tehdit istihbaratını kurumlar arasında hızla paylaşmalı, bir kurumun öğrendiği tehdidi diğerinin savunma kapasitesine dönüştürmeliyiz. Dördüncü olarak araştırma geliştirme çalışmalarını, fikri mülkiyeti ve henüz ticarileşmemiş bilgiyi de korumalı düşünmeliyiz. Ve elbette nitelikli insan kaynağını yetiştirmeye, elde tutmaya ve desteklemeye devam etmeliyiz.

Bu öncelikler birbirinden bağımsız değil. Yerli bir teknolojiyi geliştirirken tedarik zincirini güvenceye almazsak yeni bağımlılıklar yaratabiliriz. İyi yetişmiş insanlarımızı desteklemezsek altyapı yatırımlarının potansiyelini kullanamayız. Bilgi paylaşımını ve güvenlik kültürünü geliştirmezsek ürettiğimiz değeri koruyamayız. Dolayısıyla üretim, güvenlik ve yönetim aynı stratejinin parçaları olarak düşünülmeli.

Değerli katılımcılar, teknolojik egemenlik bütün teknolojileri tek başımıza üretmek demek değildir. Kritik bağımlılıkları yönetebilmek, stratejik bilgi birikimini koruyabilmek ve gerektiğinde bağımsız karar alabilmektir. Bu konuşmadan üç kelimenin akılda kalmasını isterim: Üret, koru, kontrol et. Hepinize teşekkür ediyorum.

05:00:35 Hasan YAMAN – EGM Siber Suçlarla Mücadele Daire Başkanlığı Bilgi Teknolojileri Şube Müdürü – Emniyet Amiri

Kıymetli başkanlarım, protokol üyeleri, değerli akademisyenler, sektör temsilcileri ve katılımcılar; Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı adına hepinizi saygıyla selamlıyorum. Konferansın ülkemize katkı sağlamasını temenni ediyorum.

Bu yılın ana teması “Yeni Dünya Düzeninde Siber Savaşlar” olarak belirlenmiştir. Gün boyunca siber dayanıklılık ve caydırıcılık ile platform güvenliği başlıkları değerli konuşmacılar tarafından ele alındı. Bu son oturumda ise küresel rekabette teknoloji savaşları ve siber casusluk konusunu bir kolluk birimi olarak sahada gördüğümüz yönüyle, yani suç ve delil boyutuyla sizlerle paylaşmak istiyorum.

Değerli katılımcılar, siber alandaki gelişmeleri değerlendirirken artık yalnızca saldırının yöntemine bakmak yeterli değildir. Bir olayın hangi hizmeti aksattığı, hangi veriyi tehlikeye attığı, hangi kurumsal bağımlılığı ortaya çıkardığı ve ne ölçüde güven kaybına yol açtığı da en az teknik ayrıntılar kadar önemlidir. Kamu hizmetlerinin, üretimin,

haberleşmenin ve finansal işlemlerin dijital sistemlerle iç içe geçtiği bir ortamda siber güvenliğin etkisi doğrudan gerçek hayatta görülmektedir.

Özellikle siber casusluk faaliyetlerinde amaç her zaman bir hizmeti durdurmak ya da görünür bir hasar oluşturmak değildir. Bazen hedef, uzun süre fark edilmeden erişimi sürdürmek; teknik tasarımları, kurumsal yazışmaları, araştırma sonuçlarını veya karar süreçlerine ilişkin bilgileri elde etmektir. Böyle durumlarda olayın büyüklüğü, sistemin ne kadar süre kapalı kaldığıyla değil, hangi bilginin kimlerin eline geçtiğiyle anlaşılır.

Bu durumu en iyi anlatan olaylardan birini sizlerle paylaşmak istiyorum. 2024 yılının Mart ayında Microsoft'ta çalışan Andres Freund isimli bir yazılım mühendisi, üzerinde çalıştığı bir Linux sistemine uzak bağlantıların normalden yaklaşık yarım saniye geç geldiğini fark eder. Bu, çoğumuzun üzerinde durmayacağı kadar küçük bir rakamdır. Ancak Freund nedenini araştırdığında gecikmenin, dünyadaki Linux sistemlerinin büyük bir bölümünde kullanılan XZ Utils adlı bir sıkıştırma kütüphanesinden kaynaklandığını görür. İnceleme derinleştirildiğinde bu kütüphaneye, bulunduğu sunuculara şifre gerektirmeden uzaktan erişim imkânı veren bir arka kapı yerleştirildiğini fark eder. Test aşamasındaki bu zararlı yazılımın birkaç hafta içinde yaygın Linux dağıtımlarına, dolayısıyla milyonlarca sunucuya ulaşması hedefleniyordu. Arka kapıyı yerleştiren kişi ise iki yılı aşkın süredir projeye gönüllü olarak katkı sağlayan birisi. Onun daha arkasındaki kişiler ise bilinmiyor. Yıllara yayılan bir sabır, güvene dayalı bir ilişki ve küresel ölçekte bir bağımlılık vardır. Olayın ortaya çıkması ise herhangi bir güvenlik ürününe değil, bir mühendisin dikkatine bakmaktadır.

Teknoloji savaşları denildiğinde aklımıza çoğunlukla çip üretimi, yarı iletkenler ve ihracat kısıtlamaları gelmektedir. Ancak bu rekabetin sahada bizi doğrudan ilgilendiren yüzü bağımlılıklardır. Donanımdan yazılıma, bulut hizmetlerinden haberleşme altyapılarına uzanan bağımlılıklar güvenlik değerlendirmesinin ayrılmaz bir parçası hâline gelmiştir. Saldırgan da bunun farkındadır ve çoğu zaman hedef kurumun kendisine değil, o kurumun güvendiği tedarikçiye saldırmaktadır.

Bir başka örnek daha vermek gerekirse: 2024 yılında, birçoğunuzun bildiği gibi, Amerika Birleşik Devletleri'nde Salt Typhoon olarak adlandırılan bir grubun dokuz büyük telekom operatörünün sistemlerine sızması olayı yaşandı. Grubun hedefi, mahkeme kararıyla yapılan dinlemeler için kurulan yasal sistemlerdi. Bir başka deyişle saldırı, kimlerin takip edildiğini öğrenmek için bizzat sistemin kendisine saldırmıştır. Bir kolluk mensubu olarak bu olaydan çıkardığım sonuç şudur: Yasal yetkiyle kurduğumuz her erişim kapısı aynı zamanda saldırıların da ilgisini çeken bir kapıdır. Bu kapıların güvenliğini sağlamak, suçla mücadelenin kendisi kadar önem taşımaktadır.

Bununla birlikte her siber saldırıyı siber savaş kapsamında değerlendirmek de doğru değildir. Devletlerin stratejik faaliyetleriyle ekonomik kazanç amacı güden suç yapıları farklı niteliklerdedir. Ancak kullandıkları altyapıların, yöntemlerin ve zafiyetlerin zaman zaman örtüşmesi, tehditlerin doğru değerlendirilmesini güçleştirmektedir. Bu örtüşmeyi iki örnekle açıklamak istiyorum.

2024 yılının Şubat ayında Çin'de i-Soon adlı özel bir şirketin iç belgeleri internete sızar. Belgelerden, yüzden fazla çalışanı bulunan bu şirketin devlet kurumlarına sözleşme

karşılığında siber saldırı hizmeti sattığı, hedef listeleri ve fiyat teklifleriyle çalıştığı anlaşılır. Yani devlet adına yürütülen casusluk faaliyeti özel bir şirkete ihale edilmiştir.

Bunun tersi de yaşanmaktadır. 2025 yılının Şubat ayında Bybit adlı kripto para borsasında tek bir işlemle yaklaşık 1,5 milyar dolar değerindeki varlık çalınır. Bugüne kadarki en büyük dijital hırsızlık vakasıdır. FBI, olaydan beş gün sonra saldırının Kuzey Kore bağlantılı Lazarus grubu tarafından gerçekleştirildiğini tespit eder. Burada da yöntem tedarik zinciridir. Saldırganlar borsanın kendi sistemlerine değil, borsanın kullandığı cüzdan yazılımını geliştiren bir mühendisin bilgisayarına girer. Yerleştirdikleri kod iki gün boyunca bekler ve borsa bir sonraki transferini başlattığında devreye girer.

Bir devlet aktörünün suç örgütü gibi hırsızlık yaptığı, özel bir şirketin ise devlet adına casusluk yürüttüğü bir ortamdayız. Bu örtüşmenin bizim açımızdan anlamı şudur: Sıradan bir dolandırıcılık ya da hesap ele geçirme soruşturmasında karşımıza çıkan bir sunucu kimi zaman çok daha büyük bir faaliyetin parçası olabilir. Bu nedenle siber suçla mücadele, casusluğun tespitine de doğrudan katkı sağlayan bir alandır.

Yapay zekâ bu ortamı iki yönden değiştirmektedir. Bir tarafta büyük hacimli veriyi değerlendirmek, olağan dışı davranışları belirlemek ve olay incelemelerini desteklemek için yeni imkânlar sunar. Diğer tarafta ise kimlik taklidi, sahte içerik ve hedefe uyarlanmış sosyal mühendislik faaliyetlerini daha erişilebilir hâle getirir. Bir başka örnekte, Hong Kong'da uluslararası bir mühendislik şirketinin finans biriminde çalışan bir personel, e-posta üzerinden gelen davetle bir video görüşmesine katılır. Görüşmede şirketin finans direktörü ve birkaç yöneticisinin yüzleri ve sesleriyle bir görüşme yapar. Bu görüşme personelin şüphesini giderir; 15 ayrı işlemde yaklaşık 25 milyon dolar transfer eder. Daha sonra anlaşılır ki görüşme tamamen yapay zekâ ürünüdür. Burada belirleyici olan, kullanılan teknolojinin yeniliğinden çok kurumların doğrulama ve güvenlik süreçlerinin bu değişime ne kadar ayak uydurabildiğidir. Bir video görüşmesi ya da tanıdık bir ses artık tek başına kimlik doğrulaması için yeterli değildir.

Yapay zekânın kurumlar tarafından kullanımı da dikkatle ele alınmalıdır. Herkese açık yapay zekâ hizmetlerinde yazılan her soru, yüklenen her belge, paylaşılan her tablo kurumun dışına çıkmakta; nerede saklandığı, kimler tarafından görülebildiği veya hangi modelin eğitiminde kullanıldığı çoğu zaman bilinmemektedir. Bir ihale dosyasının, bir soruşturma evrakının ya da bir teknik şartnamenin özetlenmek üzere bu hizmetlere verilmesi, biraz önce anlattığım casusluk faaliyetleri için aylarca uğraşarak elde edilmeye çalışılan bilgiyi bir anda kendi ellerimizle vermek anlamına gelmektedir.

Bu konuda Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı olarak paylaşabileceğimiz bir tecrübemiz bulunmaktadır. Başkanlığımız, yapay zekânın henüz bugünkü kadar gündemde olmadığı 2018 yılından itibaren bu alanda yatırım yapmaya başlamış ve kamu kurumları arasında bu alanda en erken adım atan birimlerden biri olmuştur. Bugün geldiğimiz noktada kendi altyapımızda çalışan ve kurum verisinin tek bir satırının dahi dışarı çıkmadığı dil modellerimiz geliştirilmiştir. Bu modelleri kurumsal bilgiyle buluşturan erişim destekli üretim mimarileri ve vektör veri tabanları üzerinde yıllar içinde edindiğimiz bilgi birikimi, dijital delil incelemelerinden ihbarların değerlendirilmesine kadar sahadaki pek çok işimizi hızlandırmaktadır. Bu çalışmalarını bir milli teknoloji hamlesi olarak görüyor; yurt dışındaki hizmetlere bağımlı kalmadan

güvenli ve milli bir yol izlenebileceğini kendi tecrübemizle göstermiş bulunuyoruz. Bu birikimi, benzer ihtiyaç duyan diğer kamu kurumlarıyla bilgi güvenliği çerçevesinde paylaşmaya hazır olduğumuzu da belirtmek istiyoruz.

Değerli katılımcılar, caydırıcılık yalnızca saldırıyı önleyebilen bir teknolojiye sahip olmakla açıklanamaz. Saldırıların tespit edilmesi, izlerin korunması, olayın teknik yönünün aydınlatılması ve suç teşkil eden fiiller bakımından adli sürecin işletilebilmesi de caydırıcılığın önemli unsurlarındandır. Bu noktada Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Dairesinin sorumluluk alanı öne çıkmaktadır. Siber suçla mücadele, teknik bir olayı tespit etmekle tamamlanmaz. Olayın nasıl gerçekleştiğinin, hangi hesap ve altyapıların kullanıldığının, mağduriyetin nasıl oluştuğunun ve fiilin kimler tarafından gerçekleştirildiğinin delillerle ortaya konulması gerekmektedir.

Bir IP adresi, bir kullanıcı hesabı, bir zararlı yazılım benzerliği tek başına tespit anlamına gelmez. Saldırganlar da bunu bildikleri için kimi zaman kasıtlı olarak yanıltıcı izler bırakmaktadır. 2018 yılında PyeongChang Kış Olimpiyatları'nın açılış töreni sırasında organizasyonun sistemlerini çökerten zararlı yazılımın içine, başka bir ülkenin saldırı grubuna ait izler bilerek yerleştirilmiştir. Ayrıntılı inceleme sonucunda izlerin sahte olduğu anlaşılır. Dolayısıyla teknik iz ile failin kimliği arasında doğrudan, otomatik bir eşitlik kurulamayacağı unutulmamalıdır.

Soruşturmaların bir diğer güçlüğü, suçun çoğu zaman birden fazla ülkeye ve hizmet sağlayıcıya yayılmasıdır. Mağdurun bulunduğu ülke, kullanılan sunucunun konumu, iletişim hizmetini sağlayan platformun yönetildiği yer ve suçtan elde edilen menfaatin aktarıldığı alanlar farklı olabilir. Bu nedenle ulusal kurumlar arasındaki eş güdümün yanında uluslararası adli iş birliği ve zamanında bilgi temini de önem taşımaktadır.

Genel Müdürlüğümüzce yürütülen siber suçlarla mücadele çalışmalarında suçların tespiti ve soruşturulmasına yönelik faaliyetler, dijital delil incelemeleri, ilgili kurumlarla koordinasyon ve vatandaşlarımızın bilinçlendirilmesine dönük çalışmalar birbirini tamamlamaktadır. Sahada karşılaştığımız dolandırıcılık, hesap ele geçirme, kişisel verilerin kötüye kullanımı benzeri suç türleri, teknik açıkların yanı sıra güven ilişkilerinin de hedef alındığını göstermektedir. Bir soruşturmada ortaya çıkan yöntem ve kötüye kullanılan bir hizmet, başka kurumların alacağı önlemler açısından da değerli olabilir. Bu bilginin gerekli gizlilik ve hukuki güvenceler gözetilerek ilgili taraflarla paylaşılması, benzer mağduriyetlerin önlenmesine katkı sağlar.

Değerli katılımcılar, önümüzdeki dönemin temel ihtiyacı daha fazla güvenlik ürünü elde etmekten ibaret değildir. Kurumların kendi varlıklarını ve bağımlılıklarını doğru tanıması, güvenliği hizmet tasarımının başından itibaren dikkate alması, yetişmiş insan kaynağına yatırım yapması ve başta gerçek olaylardan edinilen tecrübeyi kalıcı iyileştirmelere dönüştürmesidir.

Konuşmamın başında bir mühendisin fark ettiği yarım saniyelik bir gecikmeden söz etmiştim. O arka kapıyı herhangi bir güvenlik ürünü ya da bir savunma sistemi bulmadı; işini ciddiye alan bir mühendisin dikkati sayesinde ortaya çıktı. Teknolojinin ve rekabetin bu kadar hızlandığı bir dönemde en belirleyici unsur hâlâ insandır. Kamu kurumlarının saha tecrübesi, akademinin araştırma birikimi ve özel sektörün geliştirme kapasitesi aynı amaca hizmet ettiğinde bu insanı yetiştirmek de mümkün olacaktır.

Emniyet Genel M¼d¼rl¼ğ¼ Siber Suçlarla M¼cadele Dairesi olarak g¼rev ve yetkilerimiz çerçevesinde siber suçla m¼cadeleye, dijital delil inceleme kapasitesinin geliştirilmesine, kurumlar arası iş birliğine ve toplumsal farkındalığın artırılmasına yönelik çalışmalarımızı sürdüreceğiz. 19. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nın ÷lkemizin siber dayanıklılığına ve ilgili kurumlar arasındaki iş birliğine katkı sağlamasını diliyor, düzenlenmesinde emeğİ geçenlere teşekkür ediyorum. Hepinizi saygıyla selamlıyorum.