İSTANBUL SİBER-GÜVENLİK FORUMU

İSTANBUL DEKLARASYONU (TASLAK)

İstanbul Siber-Güvenlik Forumu; "Post-Güvenlik, Dijital Devrim, Döngüsel Ekonomi ve Siber Ekosistem" ana temasıyla TASAM Millî Savunma ve Güvenlik Enstitüsü tarafından, **03 Kasım 2022** tarihinde, **Ramada Hotel & Suites by Wyndham İstanbul Merter**'de yapılan 8. İstanbul Güvenlik Konferansı alt etkinliği olarak eş-zamanlı icra edilmiştir.

Forum'a çeşitli ülke ve bölgelerden, farklı alan ve sektörlerden konuşmacı ve protokol katılımı sağlanmıştır. Farklı ülkelerinden diplomatik temsilciler ve delegasyonlar da yer almıştır. Forum'da yerli/yabancı uzmanlar, akademisyenler ve diplomatlar tarafından konuşma ve sunumlar gerçekleştirilmiştir. Türkiye, Asya, Avrupa, Amerika ve Afrika ülkelerinden ilgili otoriteler de Forum'da temsil edilmiş, tüm oturumlar kurumsal olarak takip edilmiştir.

Forum'da Türkiye, Bölge ve Dünya'nın günümüz ve geleceğinde hayati önem taşıyan şu konular ele alınmıştır; "MENA" (Orta Doğu ve Kuzey Afrika) VD. Bölgelerde Siber-Güvenlik", "Siber-Güvenlikte Standartlar ve Normlar", "Endüstriyel Siber-Güvenlik", "Nesnelerin İnterneti ve Siber-Güvenlik", "Mobilite ve Siber-Güvenlik", "Derin Sahte ve Siber-Güvenlik", "Yapay Zekâ, Sanal Gerçeklik ve Siber-Güvenlik", "Kritik Altyapılarda Siber-Güvenlik", "Karar Vericiler için Siber-Güvenlik".

Forum'da ortaya konan aşağıdaki tespit ve önerilerin, mevcut kazanımları/kurumları yükseltecek bir vizyonla, ilgili tüm otoritelerin ve kamuoyunun dikkatine sunulması kararlaştırılmıştır:

1. Bilgi teknolojilerinin hızlı gelişimi, aynı büyüklükteki güvenlik sorunlarını beraberinde getirmiştir. İnternetin ilk yıllarında bilgi güvenliğinin üç önemli bileşeni olan "erişilebilirlik, gizlilik, bütünlük" kavramlarından "erişilebilirlik" öne çıkmış; önce internetin gelişmesi ve işletilmesi düşünülmüş, "gizlilik ve bütünlük" geri planda kalmıştır. Bu ise internetin temel mimarisinin ve servislerinin zaman içinde gizlilik ve bütünlüğe dair sorunlara yol açmasına neden olmuştur. Hızlı büyümeden ötürü "erişilebilirlik" ile ilgili sorunlar da zaman içinde artarak, gelişmelerin güvenlik kavramının her zaman bir adım geride kalmasına neden olmuştur.

2. Yeni ve gelişmekte olan teknolojilerin, siber tehdit ortamı üzerinde beklenen etkilerinin; geleceğin çok boyutlu güvenlik ortamını şekillendireceği, yapay zekâ ve makine öğrenimi, otonom cihazlar ve sistemler, telekomünikasyon ve bilgi işlem teknolojileri, uydular ve uzay varlıkları, insan-makine ara yüzleri, kuantum hesaplama ve siber-uzaydaki tehditlerin hibrit savaş kapsamında olduğu otoritelerce teyit edilmiş, siber-uzay harbin 5. boyutu kabul edilmiştir.

3. Yeni teknolojiler iş hayatına ve günlük hayata dinamizm kazandırırken, öngörülemez tehlikeleri de içinde barındırmaktadır. Günümüzde "siber" kelimesi ile başlayan birçok yeni olgu ile karşı karşıyayız. "Siber-suç", "siber-dolandırıcılık", "siber-zorbalık", "siber-savaş" vb. kavramlara yönelik toplumsal farkındalık her geçen gün artmaktadır. Siber-güvenlik ihtiyacı ile başlayan farkındalık, siber-güvenlik alanında uzman kişilerin eğitimi ve yetişmesi ile yeni bir meslek alanı olarak çoktan iş hayatındaki yerini almaya başlamıştır.

4. Kovid-19 salgınından sonra beklenen yeni pandeminin, "siber-güvenlik ve ekosistemin rekabetçi yönetişiminde yaşanacak sorunlar" olabileceği güçlü bir tez olarak önemini korumaktadır. Çünkü çok boyutlu siber-güvenlik alanı artık hayatın işleyişi, doğası hâline gelmiştir. Öte yandan mevcut pandemi sürecinde doğrusal ekonomiden "döngüsel ekonomiye" geçmenin bir seçenek değil zorunluluk olduğunun daha iyi anlaşılması ile "yeşil ekonomi", "dijital devrim" gibi kavramların öncülüğünde iş ve sürdürülebilir kalkınma modeli de hızla değişmektedir. Aynı zamanda küresel yeni standartlar demek olan bu dönüşüm, rekabet endekslerini kökten değiştirme potansiyeline de sahiptir. Güç ve mülkiyet kavramının anlam ve değerini yeniden belirleyen "dijital devrim" odaklı bilgi ekonomileri bugünün ve geleceğin belirleyicisi olacaktır.

5. 2022 itibarıyla ilk kez gerçekleştirilen İstanbul Siber-Güvenlik Forumu ile geleneksel güvenlik anlayışı irdelenmiş ve gelinen noktada "siber-güvenlik" olgusuna ne yazık ki gerçek değerinin verilmediği, bu alanın büyük çoğunluk tarafından bilinmediği, anlaşılmadığı veya anlaşılır biçimde aktarılamadığı sonucu ortaya çıkmıştır. Her akşam TV kanallarında üzerine senaryolar yazılan siber-güvenlik, teknik bilgilerle anlatılmaktadır. 7'den 77'ye hemen herkesin elinde akıllı telefonların olduğu düşünüldüğünde siber-güvenlik eğitimlerinin, anasınıfından yükseköğretime her kademede gerçekleştirilmesi ve vatandaşların bilinçlendirilmesi oldukça önemlidir.

6. Küreselleşme ile değişen güvenlik algısının günümüzde en önemli aygıtlarından biri de siber-güvenliktir. Yeni güvenlik teorileri incelendiğinde, devletlerin farklı alanlarda tekelliğini kaybedişi ve toplumsal dinamizm alanı olarak sosyal medyanın ülkelere olan etkileri güvenlik politikalarını da yeniden şekillendirmiştir. Birey ve toplumların algısal mekanizmalarının modern dünyadaki değişimi ve imalat unsuru bağlamında internet devrimi özne olarak alındığında, hem ülkelerin güvenlik stratejilerinde küreselleşen dünyanın doğurduğu güvenlik tehditleri hem de genel kamuoyunun siber aygıtlarla algı yönetimi imkanları, beraberinde pek çok riski getirecektir. Bu noktada ülkelerin yakın dönemde geleneksel savunma aygıtlarının yanı sıra siber-güvenlik alanında farklı savunma unsurları inşa ettiği görülmektedir. Siber güvenliğin, bir tehdit olarak hızla arttığı günümüzde, gelişmiş ülkelerin ordularında siber-güvenlik birimlerinin oluşturulması, kamu politika süreçlerinde siber-güvenliğe yönelik tedbirlerin öncelenmesi ve siber alanda devletlerin resmî muhatap unsuru oluşturacak daha fazla inisiyatif alması ve elbette güçlü kurumsallaşma elzem hâle gelmiştir.

7. Post-Pandemi ile dijitalleşme hayatımızın her alanında artmış ve bireysel kullanımların yanı sıra çalışma koşullarında da dönüşüme yol açmıştır. Şirketler, kurumlar, kişiler ve hatta devletler toplantılarını çevrimiçi olarak gerçekleştirmiştir. Özellikle ekonomik ve ergonomik oluşu sebebiyle dijital araçların kullanımı artmış olsa da insanlık bir anda kendisini planlanmamış ve bilinçsiz bir dijitalleşmenin içerisinde bulmuştur. Sınırları henüz tam anlamıyla bilinmeyen, tüm bilgi ve belgelere kolayca erişilebilen bir dünyaya hızlıca giriş yapılmıştır. Bu doğrultuda kritik altyapı güvenliğinin zayıflığı ise birçok devletin yüzleştiği bir gerçeklik olmuştur. Bu alanda kapasite inşasında geç kalmanın telafisi yoktur.

8. Günümüzde toplantıların, sınavların ve mülakatların büyük çoğunluğunun çevrimiçi yapılması yönünde tercihler artmıştır. Küreselleşen dünyada zamanla yarışıldığı düşünüldüğünde bu tercihler hem ekonomi hem zaman hem de mekândan tasarruflara yol açsa da yapılan tüm bu işlerde "gerçeklik" algısı sorgulanmalıdır. Muhatabın, evrakların, bilgilerin ve belgelerin gerçekliği büyük bir soru işareti taşımaktadır. İşe girişlerde yapılan sahteciliğin %6'lardan %30'lara çıkması söz konusu iken ve sahte belge hazırlayan internet sitelerinin sayısı her geçen gün artıyorken bu durumun tespiti için "doğrulama" kanallarının her alanda kullanılıyor olması elzemdir.

9. Bugün "suç" kavramı hukuk devletinde amir kurumlar tarafından ceza veya güvenlik tedbiri yaptırımına bağlanan fiildir. Suçu işleyen kişiye ise suçlu veya fail denir. Ancak siber dünyada gerçekleşen "siber suç" kavramının tanımı ne yazık ki hâlâ günümüzde net değildir. Bu yüzden Siber Hukuk, Bilişim Suçları, Bilişim Hukuku gibi yeni hukuksal alanların oluşması, yeni suç formlarının oluşturulması ve buna bağlı güçlü regülasyonların sürekli güncellenmesi yeni güvenlik ekosisteminin temellerindendir.

10. Ulus devlet toplumları yerini küresel toplumlara bırakırken günümüzde ise siber ağ toplumlarına dönüşmektedir. Her vatandaş en az bir tane siber ağın (Google, Youtube, Amazon vs.) aktif kullanıcısı olmakta ve bugün bu durumun alışveriş, eğitim veya herhangi hizmetin sunumundan öte adeta devlet - vatandaş ilişkisi hâline dönüştüğü görülmektedir. Bir diğer sorun ise kişisel verilere tek tuşla ulaşabilen ve bünyesinde tutabilen bu siber ağlar sahip oldukları verileri ne yazık ki kuruldukları merkezlerde tutmamaktadır. Örneğin ABD kuruluşu olarak bilinen Amazon şirketi kişisel verileri İrlanda üzerinde tutmaktadır. Burada ise devletlerin karşısına "siber vatan veya siber topraklar nasıl tanımlanacak ve nasıl korunacak?" sorusu çıkmaktadır. Siber dünyanın fiziksel bir karşılığının olmayışı, siber veya sanal dünyaya fiziksel engeller koymanın mümkün olmadığını göstermekte ve farklı çözüm yolları arayışlarını zorunlu kılmaktadır.

11. Metaverse veya Türkçe karşılığı ile sanal/kurgusal evren, internetin geleceği olarak görülmekte; farklı olguların kurgusal evrene taşınması, devletlerin ve çok uluslu şirketlerin programa destek vermesi ve gerçek kentlerin sanal evrene taşınmaya başlaması ile artık mekân kavramında algısal değişimlerin oluştuğu ve günümüzde insanlığın sanal evrende daha çok zaman geçirdiği görülmektedir. Hayali gerçeklikte olmak ve ona yatırım yapmak, yeni dünya düzeninin oluşumuna da farklı bir perspektif getirmektedir. Bu bağlamda yeni teknolojilerin bireyselliğin ötesinde devlet politikaları çerçevesinde ele alınmasının çok önemli olduğu vurgulanmıştır.

12. Sanal evrene geçişten önce günümüz dünyasında popülaritesi hızla artan ve "kimliksiz para" olarak da adlandırılan kripto paralar, blokzincir aracılığıyla devletlerin - meşruiyetini sağlamada tarihsel önem arz eden - para basma tekelinin ellerinden alınma tehdidini ortaya çıkarmış, para basmak adeta kontrolsüz ve aracısız hâle gelmiştir. Bu da finansal güvenlik anlamında birçok paradoks ve tehdidi doğurabilme potansiyeline sahiptir. Devlet'in sahip olduğu para basma tekeline ve vergi toplama gücüne tepki olarak görülen tüm bu "kimliksiz paraların" denetlemesi için derin çalışmalar yapılmasının ve regülasyon ihtiyacının ivedi olduğu belirtilmiştir.

13. Siber savaşlar, devletlerin karşılıklı olarak siber saldırılar gerçekleştirerek birbirlerinin bilişim ağlarına zarar vermesi ya da kesintilere yol açması ile ortaya çıkmaktadır. Bu savaşta rol alan aktörler ise ülkeler, ülkelerin silahlı kuvvetleri, istihbarat örgütleri, kanunî otoriteler, özel sektör, bireyler veya birtakım gruplardır. Siber savaş ve saldırılarda kritik ulusal altyapılar, askerî sistemler veya ülke için önemli endüstriyel yapılar hedef alınmaktadır. Bu çerçevede rekabet gücü yüksek geleneksel güvenlik yöntemlerinden farklı harcama kalemleri ve alt yapıların oluşturulması önerilmiştir.

14. Bir ihtiyaç sonrası oluşan "ulus devlet" kavramı günümüzde yerini farklı devlet yaklaşımlarına bırakma konusunda yol ayrımındadır. Dijitalleşme süreci "elektronik devlet" kavramını farklı bir boyuta taşımıştır ve devletlerin dijitalleşmesi hızlanmıştır. Devletler birer siyasal aktör olarak, bünyelerindeki her kurum için internet siteleri açmış, böylelikle devletin ulaşılamaz ve katı bürokratik yapısı bu gelişmelerle birlikte kolay ulaşılabilir ve esnek bir biçime - hatta hesap verilebilirliğin arttığı bir yapıya - dönüşmüştür. Günümüzde herhangi kurum tarafından talep edilen ve alınması gereken evrak için uzun süren bürokratik süreçlere gerek kalmamış, e-devlet uygulaması sayesinde tek tuşla saniyeler içinde alınılabilir hâle gelmiştir. Kamu sektöründeki dijitalleşme hareketleri Yeni Kamu Yönetimi anlayışına dönüşerek Klasik Weberyan bürokrasi anlayışında büyük çözülmelere yol açmıştır. Bu yenilikler kamu sektörünü geleneksel anlayıştan uzaklaştırmıştır.

15. Geçmişi 1980'lere uzanan Quantum teknolojisi, nükleer etkenleri de barındırması açısından ABD ve Çin gibi ülkeler arasında yeni bir savaşa sebep olabileceği tartışmalarına yol açmaktadır. Bu teknolojiyi bu denli önemli kılan özelliklerden en önemlisi olarak, barındırdığı şifre kırma teknolojisini göstermek mümkündür. Çünkü bu teknolojinin varlığı ve kullanımı ile dünyanın en iyi korunan bilgisayar ağlarının şifreleri saniyesinde çözülebilme riski ile karşı karşıyadır. Çin'in geliştirdiği kuantum ışınlama teknolojisiyle uzaya foton şeklinde bilgi gönderdikleri ve başka ülkelerin kritik bilgilerini aldıklarına dair iddialar mevcuttur. Ayrıca Çin'in, füzelerin yönünü değiştirmekte kullanılabilecek bir teknolojisinin olduğu üzerine teoriler de üretilmektedir. Tüm bu iddialar ve varsayımlardan öte Quantum teknolojisinin, kritik altyapıların ve veri güvenliğinin sağlanması açısından daha fazla çalışma ve yatırım yapılması gereken bir alan olduğu gerçeği vurgulanmıştır.

16. Türkiye'nin dost ve kardeş ülkelerle birlikte yeni büyük siber tehditlere karşı proaktif hareket edebileceği erken-aşama konularından biri "Deepfake" (Derin-sahte) adıyla yaklaşmakta olan siber tehlikedir. Derin-sahte; kişilerin görüntü ve sesinin yapay zekâ destekli sinir ağları kullanılarak başka kişilerinki ile - insan gözü ve kulağının ayırt edemeyeceği boyutlarda - değiştirilebildiği yeni nesil bir medya türüdür. Bu dosya türleri derin makine öğrenmesi teknikleri uygulanarak orijinal medya dosyalarının birebir benzer klonları oluşturularak üretilmektedir. Derin-sahte içeriklerin, ünlülerin sahte uygunsuz videolarının yanı sıra sahte haberler üretmek için de kullanılmaya başlaması ve finansal sahtekârlıklarda bile yer alması dünya çapında ciddi endişeler duyulmasına yol açmıştır. Bu teknolojinin sadece ses kısmının kullanılmasıyla bile kritik emirler ve talimatlar verilmesi, politik krizler çıkarılması, borsa manipülasyonlarına ve ülke çapında acil durum ilanına neden olunması, askerî birimlerin yanıltılması, gizli istihbarat operasyonlarında yer alması gibi sayısız olasılık mümkündür.

17. Derin-sahte teknolojisi dünyada sadece güvenlik boyutu ile değil sivil boyutu ile de çok dikkat çekmektedir. Hayatta olsun veya olmasın bir kişinin çok kısa bir videosu, resmi veya ses kaydıyla derin-sahte içeriklerin oluşturulması eğlence sektörü, eğitim sektörü, kültür, turizm, iletişim, sanat, tekstil, film, reklam, sağlık, perakende gibi birçok sektörde ve alt birimlerinde yer almaya başlamış durumdadır. TASAM tarafından geliştirilen BRAINS^2 Türkiye (Biyoteknoloji, Robotik, Yapay Zekâ, Nanoteknoloji, Uzay, Stratejik Hizmetler) kapsamındaki Sentetik Gerçeklik Teknolojisi adlı ilk uygulama programının; "Derin-Sahte (Deepfake) Ürün ve Savunma Ekosistemi İnşası" teması ile büyük bir vizyon ve işbirliği potansiyeline haiz olduğu teyit edilmiştir.

18. Yine BRAINS^2 Türkiye kapsamında "Yönetişimin İnterneti (Blokzincir) ve Kripto Varlıklar Stratejisi" teması ile geliştirilen "Yıkıcı İnovasyon Blokzincir Teknolojisi" uygulama programı vizyon ve işbirliği potansiyeli ile takdirle anılmıştır. Blokzincir; popüler uygulaması kripto paralar (Paranın İnterneti) üzerinden tarif edilse de Yönetişimin İnterneti olarak tanımlanan Blokzincir

3,0 uygulamaları, ekonomi, güvenlik, akıllı şehirler başta olmak üzere, tüm uygarlık üzerinde devrimsel etki potansiyeline sahiptir. Bu minvalde yalnız teknoloji değil, süreç ve yönetişim inovasyonunu da kapsamaktadır. Özellikle "vatandaş", "devlet", "akademi", "özel sektör" olmak üzere, geleneksel merkezî kurumsal yapıları da ciddi anlamda etkilemesi, hatta kendi aralarındaki iletişimi de dönüştürmesi beklenmektedir. Bu çerçevede Yıkıcı İnovasyon Blokzincir Teknolojisi programı; Türkiye ve dost-kardeş ülkeler için makro ve sektörel boyutlarda ekosistemin tanımlanması, rekabetçi kapasitenin inşası, teşviki, regülasyonu, güvenlik ve ekonomi odaklı yıkıcı riskler ile stratejik fırsatlara odaklanmayı referans almaktadır.

19. Geleneksel meritokratik altyapının kurmay güvenlik merkezli değişim ve dönüşümünde ülkelerin ilgili güvenlik/savunma otoritesi bünyesinde kara, hava, deniz ve uzayın yanı sıra resmî anlamda siber alanın da yeni harekât alanı olarak tanımlanması ve stratejik siber istihbarat üzerine bağımsız bir komutanlık/başkanlık olarak "siber-güvenlik komutanlığı/başkanlığı" kurulması önerilmiştir.

20. Kurulması önerilen siber-güvenlik komutanlığına/başkanlığına bağlı bir muhabere taburunun ofansif siber kuvvet olarak yapılandırılması ve bu yapının temel amaçlarının operasyon-savunma-saldırı- sızma şeklinde olması da ayrıca tavsiye edilmiştir.

21. "Duygusal ve matematik zekâyı birlikte teşvik edecek" çatı bir başlık altında, profesyonel programcı ve kodlayıcılardan oluşan, kimlikleri mahfuz ve sürekli klavye başında olan, birçok alanda faaliyet gösterecek, sıcak bölgelerde ve siber savaşlarda görev yapabilecek personelden oluşan bir ordu kurulması ve bu ordunun gerçek zamanlı siber istihbarat edinmek için "büyük veri" analitiğini kullanarak verilerin otomatik işlenmesini sağlayan teknolojiler geliştirip kullanması önerilmiştir.

22. Türkiye için; dost ve kardeş ülkelere de hizmet verecek şekilde siber endüstrinin ölçek büyüklüğünün gözden geçirilmesi, ekosisteme ulusal bir yatırım ve kapasite programının oluşturulması öncelik arz etmektedir. Ekosistem envanterinin, sektörün temsil ettiği teknoloji de kullanılarak model bir proje olarak oluşturulması ve interaktif güncellenmesi, potansiyeli takip ve doğru kararlar için önceliktir.

23. Klasik dış ticaret ve hizmet ürünlerinden çok daha verimli ve ekonomik dönüşümü stratejik boyutlarda içeren siber endüstrinin temsilcilerinin VIP seyahatlere, ticari temaslara güçlü bir şekilde dâhil edilmesi sektörün motivasyonunu da artıracaktır. Bu alanda var olan ülkeler arası işbirliği mekanizmalarının güçlendirilmesi de tarihî bir farkındalık olacaktır.

24. Yerli ve millî işletim sistemine sahip olunup kademeli geçiş sağlanması, internetin küresel internet sağlayıcılardan bağımsız çalışacak hâle getirilmesi, "büyük verinin" yapay zekâ ile işlenip

olası saldırgan harekâtların öngörülebileceği bir sistem kurulması, yapay zekâ destekli IPS ve IDS sistemler geliştirilmesi ve "siber-güvenlik yasası" çalışmalarına hız verilmesinin önem ve aciliyet arz ettiği, dijital alan düzenlenmesinin ulusal güvenlik/egemenlik sorunu olduğu vurgulanmıştır.

25. Siber Endüstri Bakanlığı kurulması veya Cumhurbaşkanlığı bünyesinde bir başkanlığın oluşturulması önerilmiştir. Aynı zamanda Dışişleri Bakanlığı içerisinde bir "siber endüstri birimi" marifeti ile siber krizlerin ve bu alandaki çok boyutlu dış potansiyelin diplomasi tarafından desteklenmesinin önemi vurgulanmıştır.

03 Kasım 2022, İstanbul