2. İSTANBUL SİBER-GÜVENLİK FORUMU
KAĞITHANE DEKLARASYONU

2. İstanbul Siber-Güvenlik Forumu; "Yeni Siber Ekonomi ve Türk Ürünleri" ana temasıyla TASAM Millî Savunma ve Güvenlik Enstitüsü tarafından, **23 Kasım 2023** tarihinde, **İstanbul Kent Üniversitesi Kağıthane Kampüsü**'nde yapılan 9. İstanbul Güvenlik Konferansı eş-etkinliği olarak birlikte 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; "Kritik Altyapılarda Siber-Güvenlik, Mobilite ve Siber-Güvenlik", "Nesnelerin İnterneti ve Siber-Güvenlik", "Yeni Siber Ekonomi ve Türk Ürünleri", "Yapay Zekâ, Sanal Gerçeklik ve Siber Güvenlik", "Derin Sahte ve Siber-Güvenlik", "Karar Vericiler için Siber-Güvenlik" ve "Endüstriyel 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. Teknolojinin hızla gelişimiyle beraber yeni ilerlemeler meydana gelmiştir. Bu ilerlemelerin en önemli gelişmelerinden birisi de yapay zeka alanında yaşanmıştır. Bu alandaki ilerlemelerin mevcudiyeti çeşitli güvenlik tehditlerini oluşturması da kaçınılmaz olmuştur. Bunlardan birisi de yapay zekanın otonom hale gelip kendi kendine karar verebilmesi ve suç işleyebilirliği olmuştur.

2. Bazı görüşlere göre, yapay zekâ sistemleri belirli görevleri gerçekleştirmek üzere programlanır ve suç işlemek için gerekli kasıt veya bilinçten yoksun olabilir. Ancak, algoritmaları tasarlayan insanlar, yapay zekânın kötü niyetli kullanımına ve potansiyel yasa dışı faaliyetlere zemin hazırlama riski taşıdıklarından dolayı bu durumdan sorumlu tutulabilirler. Yapay zekanın suç işleyebilmesi özerklik, farkındalık ve suç kastı/manevi unsur bağlamında değerlendirildiğinde yapay zekanın suç işlediğini kabul edebilmemiz mümkündür.

3. Bazı bakış açılarına göre, günümüzde yapay zeka, tabanca, bıçak veya sahtecilik araçları gibi suçların işlenmesinde bir tür araç olarak kabul edilebilir. Ancak, gelecekte yapay zeka üreten yapay zekaların, canlılara veya diğer yapay zekalara karşı işlenen suçlarda önemli bir rol

oynayabileceği, hatta yeni suç formları yaratabileceği vurgulanmıştır. Bu suçların sonucu yaşanabilecek olumsuz sonuçlarla birlikte cezalarının ne olacağı da bu süreçte önemli konular arasındadır.

4. Teknolojinin ilerlediği bir diğer gelişme ise kuantum teknolojilerinde yaşanmıştır. Kuantum teknolojileri kırılamayan şifrelerle birlikte askeri ve sivil alandaki birçok uygulamada hızla gelişirken, özellikle kuantum radarları gibi teknolojilerle; bilgi güvenliği ve iletimindeki mevcut tehditlerin aşılma potansiyeli yüksektir.

5. Kuantumun birinci devrimiyle beraber kuantum mekaniğinde süper pozisyon, bağımlılık ve fiziksel unsurların kapsadığı teknolojiyle birlikte şifrelerin kolaylıkla kırılabildiği öngörülmüştür. İkinci devrimde teoride yer alan kuramlar vücut bulmaya başlamıştır. Meskun - Mahal muharebelerinde kullanılan hassas nano sensörler, mayın tespiti ve terör unsurlarının tespitini kuantum teknolojisi kolaylaştıracaktır. Bilginin depolanması ve aktarılmasındaki tehditi de yine kuantum teknolojisiyle aşmak mümkündür.

6. Ulusal kamu diplomasisi devletlerin dış politikada çıkarlarını gözeterek kendini korumak için geliştirdiği diplomasidir. Ulusal kamu diplomasisi ve güvenlik stratejileri, siber güvensizlik ve kuantum bilgisayarlarının yükselişiyle birlikte değişen güvenlik ortamına adapte olmayı gerektirmektedir. Siber terörizm ve veri ihlalleriyle birlikte "Siber Güvensizlik" kavramının ortaya çıkışı kuantum bilgisayarların önemini arttırmıştır. Bu bilgisayarla birlikte karmaşık programların çözümü güvenlik alanında önemli bir atılım olacaktır.

7. Birinci sanayi devrimiyle birlikte buhar makineleri icat edilmiş, ikinci sanayi devrimiyle birlikte ise elektrik keşfedilmiştir. Üçüncü sanayi devriminde elektronik bilgisayarlar ve teknolojiler insan hayatının içine dahil olmuş ve son olarak dördüncü sanayi devrimiyle birlikte Endüstri 4.0 ve yapay zeka teknolojileri hayatımıza girmiştir. Kuantum bilgisayarların üstün işlem kapasitesi, özellikle büyük veri analizi gücünü artırmak için kullanılmaktadır. Bu sayede, yalnızca aranan kelimeleri değil, aynı zamanda kurulan cümleleri de anlama yeteneğine sahip akıllı web arama motorları ortaya çıkmaktadır. Kuantum bilgisayarların temel özelliği, aynı anda birçok işlemi hızla gerçekleştirebilme kapasitesidir. Geleneksel bilgisayarların aksine, kuantum bilgisayarlar şifreleri hızla çözebilme yeteneğine sahiptir. Bu durum, kuantum bilgisayarların devlete ait kurumlar veya özel sektör gibi her türlü kuruluşun güvenlik sistemlerini kolayca çözebilme potansiyelini içermektedir.

8. Devletler, kuantum bilgisayarların ortaya çıkardığı yeni güvensizlik dönemine uygun stratejilerini belirlemeli ve ulusal kamu diplomasisini, teknolojik ilerlemelere paralel olarak değiştirmelidirler. Güvenlik stratejileri zaman içinde evrim geçirmiştir, özellikle siber güvensizlik kavramı ortaya çıktıkça; siber terörizm, veri ihlalleri gibi tehditler ön plandadır.

9. Nano teknolojinin hayvanların genetiğinin değiştirilerek faklı bir forma dönüşmesini sağlaması ile biyolojik savaşta bu hayvanların kullanılabileceği öngörülerek tedbirler alınmalıdır. Ahtapot, köpek, kene gibi hayvanlarla yapılacak bir müdahale ve hastalık yayma, biyolojik savaş içerisinde yer alan tehditler olarak görülebilir. Antik çağ hayvanlarının kolonları kopyalanarak tekrardan hayata geçirilme projeleri de bulunmaktadır. Bu hayvanların beyinlerine yerleştirilen çiple silah olarak kullanılması muhtemeldir.

10. Ayrıca farklı canlıların genleri birbirlerine aktarılarak başka canlı tipolojileri de elde etmek mümkündür. Bu canlıların silah olarak kullanılması da yine büyük risk teşkil etmektedir. Biyolojik savaşlar daha büyük zararlara ve kitlesel ölümlere yol açabilir. Büyük Sıfırlama gibi planların bu alanda geliştirilen teknolojilerle gerçekleştirilmesi mümkündür.

11. Geliştirilen teknolojilerle çekirge gibi hayvanlar kullanılarak savaşlar yürütülebilir ve bu savaşların sonuçları olarak ekonomiler ağır bir şekilde etkilenebilir. Bunun örnekleri Somali ve Hindistan'da görülmüştür.

12. Türkiye'de ise kene gibi hayvanlar kullanılarak Kırım Kongo hastalığını yayma iddiaları yer almakta olup Marmara denizinde görülen köpekbalıkları farklı bir konseptte küçük çaplı çalışmaların yapıldığı iddialarını güçlendirmektedir.

13. Firewall sistemleri, kritik altyapıları korumak için büyük önem taşır ve aynı zamanda network segmentasyonu sağlayarak erişimi kontrol altında tutar. Gartner raporlarına göre, firewall sızıntılarının %99'u konfigürasyon hatalarından kaynaklanır ve bilinen saldırıların büyük bir kısmı aynı hatalardan gelir. Bu nedenle, firewall kurallarının düzenli gözden geçirilmesi hayati önem taşır. Ancak dijitalleşme, siber güvenlik uzmanları arasında yetersizlik ve artan kural sayısı gibi zorluklara yol açmaktadır, bu da güvenlik ekiplerinin zamanını etkiler. Bu minvalde Opinnate teknoloji şirketi gibi kurumlar firewall sistemleri üzerinde kural analizi ve raporlama ihtiyaçlarını karşılayan, otomasyon gücünü kullanarak güvenlik ekiplerinin zamanını daha etkili bir şekilde yönetmelerine yardımcı olan çözümler geliştirmiştir. Firewall teknolojilerinin güncelleştirilmesi ve daha güvenlikli hale getirilmesi gerekmektedir. Bu gibi teknolojilerin gelişmesi istihdam ihtiyacının artmasını da mümkün kılmaktadır ve global dünyada ulusal şirketlerin önünü açma potansiyeline sahiptir.

14. Teknolojinin bu denli ilerlemesiyle beraber birçok teknoloji şirketi de çeşitli hizmetler sunmaya başlamıştır. Bu teknoloji şirketlerinin önde gelen isimlerinden biri olan KOBIL küresel bir teknoloji şirketi ve global bir firma olarak müşterilerine dijital kimlik çözümleri sunarak, güvenlik odaklı ve sürekli değişen dijital ihtiyaçlara uyum sağlamayı hedeflemektedir. İhtiyaçların sürekli değişimi, mobil deneyimlerin merkezi bir noktadan yönetilme ihtiyacı ve yeni iş modellerinin ortaya çıkması için gereken platformlar, dinamik bir dijital ortamda önemli bir rol oynamaktadır. Üretici, aracı ve müşteriler arasında birbirine güvenen bir ekosistem oluşturabilmek için ortak bir paydada buluşma gerekliliği önemlidir.

15. Dijitalleşme, mobil uygulamaların sunduğu avantajların yanı sıra güvenlik endişelerini de beraberinde getirmektedir. Uluslararası araştırma şirketlerinin yayımladığı çeşitli çalışmalarda, önümüzdeki yıllarda şirketlerin %50'sinin veri sızıntısı yaşayabileceği ve bu durumun dijitalleşme süreçleri ile değişen saldırı yöntemlerinin ana sebeplerinden biri olacağı öngörülmektedir. Pazar baskısı, güvenlik zafiyetlerinin ortaya çıkmasına neden olabilmektedir. Örneğin, 2021 yılında yapılan bir çalışma, e-ticaret sektörünün 2025 yılına kadar %90 oranında yeni düzenlemelere tabi tutulacağını öne sürmüştür. Bu düzenlemelerin farklı sektörlere de yayılacağı öngörülmektedir.

16. İnternetin geleceği olarak görülen yeni gelişmelerden birisi de Metaverse veya Türkçe karşılığı ile sanal/kurgusal evrendir. Metaverse'le ilgili olarak şirketlerin sanal paralar kullanarak gerçek para birimleriyle ticaret yaptığı üç boyutlu sanal bir evren olduğu açıklanmıştır. Çin gibi büyük ölçekli teknoloji ülkelerinin ilerleyen yıllarda Metaverse kullanımının oluşturduğu pazarı büyüteceği öngörülmektedir. Türkiye'de ise henüz resmi bir Metaverse politikası bulunmamakla birlikte, ülkenin milli Metaverse platformları ve içerik oluşturmayla ilgili adımlar atması gerekmektedir.

17. Teknolojinin ulaştığı en farklı alanlardan birisi ise "İnsan Sonrası Yeni Irksal Yaratılışlar ve Ülkeler" başlığı altında incelenmiştir. NBIC (nano teknoloji, biyo teknoloji, bilgi teknolojisi, kognitif teknoloji) teknolojileri, fiziksel ve zihinsel becerileri artmış yeni insan türlerinin yaratılmasında kullanılan bir kombinasyonu temsil etmektedir.

18. Öjeni, insanları genetik açıdan kontrol altında tutan, sağlıksız ceninleri ayıklamayı ve insan ırkını ıslah etmeyi amaçlayan tartışmalı bir bilimsel akımdır. Bu akım, körler, sağır ve şizofren hastaların kısırlaştırılması gibi uygulamaları içermekte olup ABD'de 1960'a kadar öjeni kısırlaştırmaları örnek olarak gösterilebilir. Aynı zamanda, Almanya'da Hitler döneminde ari ırk yaratma projeleri ve insan çiftlikleri gibi uygulamalar, öjeninin aşırı ve etik dışı biçimlerini temsil eder. Çin'de ise üstün insan yaratma projeleri, öjeninin modern bir örneğini oluşturmaktadır. Bu tür müdahaleler evrimsel gelişmeye zarar vererek ırkçılığı teşvik edebilir ve toplumda ciddi etik sorunlara yol açabilir. 2002 yılında Amerikan Ulusal Bilimler Merkezi tarafından yayımlanan "Converging Technologies for Improving Human Performance, Nanotechnology, Biotechnology, Information Technology and Cognitive Science" başlıklı rapor ile bu konsept dünya çapında tanıtılmıştır. Bu çalışmalarla birlikte teknolojik unsurlarla yeni insan deneyleri oluşturulmaya başlandığı iddiaları yer almaktadır.

19. Teknoloji alanında yaşanan gelişmelerle kötüye kullanımla da sonuçlanabilmektedir. Siber suçlar altında toplanan bu suçlarla ilgili olarak ceza hukuku önleyici değil bastırıcıdır. Bu durumun etik çerçevede tartışılması önerilmektedir.

20. Siber saldırılarla birlikte siber savunmadaki teknolojiler de bu alanla iç içe geçmiş durumdadır. Birbirlerine karşı bağımlı yapıdadırlar. Yapay zeka ve makine öğrenmesi gitgide siber güvenlik alanına girmektedir. Bu konuyla ilgili olarak Türkiyede birçok farklı kurum tarafından eğitimler verilmektedir. Bu programlardan biri olan Siber Vatan Programı Sanayi ve Teknoloji Bakanlığı'na bağlı olarak birçok devlet/ özel kurumdan alınan destekle kalkınma ajansları tarafından

yürütülmektedir. Bu programa seçilen öğrencilere belirli bir süreçten geçtikten sonra staj ve istihdam olanakları sağlanmaktadır.

21. Yapay zeka sistemlerinin askeri alandaki etkisi ise küresel rekabet ve teknolojik gelişmelerle birlikte artmaktadır. Özellikle savunma sanayiindeki otonom silah sistemleri ve robotik kullanımıyla bu alan dikkat çekmektedir. Ancak, bu teknolojinin kötüye kullanımı, otomatik silah ticaretinin kontrol altında tutulmasını zorunlu kılmaktadır. Suriye ve Gazze gibi bölgeler bu durumun yaşanma ihtimalinin yüksek olduğu bölgelerdendir. Türkiye'nin, Ukrayna tarafından boru hatlarına yapay zekayla yapılan saldırılar örneğinden yola çıkarak tehditlere karşı kendini bu alanda önemli güç haline getirmesi, ticaret ve kritik yolları kontrol etmesi elzem hale gelmiştir.

23 Kasım 2023, İstanbul