



## 3. İSTANBUL SİBER-GÜVENLİK FORUMU

### SONUÇ DEKLARASYONU

**3. İstanbul Siber-Güvenlik Forumu;** “Yeni Siber Ekonomi ve Türk Ürünleri” ana temasıyla TASAM Millî Savunma ve Güvenlik Enstitüsü tarafından, **21 Kasım 2024** tarihinde, **Wish More Hotel İstanbul**’da yapılan **10. 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 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”, “Siber-Uzay ve Milli Güvenlik”.

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

1. Dijitalleşmenin ve teknolojik gelişmelerin hızla ilerlemesi, beraberinde sosyo-kültürel sonuçlara yer açmaktadır. İnsanların cinsel yönelimlerinin etkilenmesi, sosyal medya mecraları üzerinden tek tip yaşam tarzlarının dayatılması, yeni bir toplum inşasını işaret etmektedir. Özellikle gençlere yönelik LGBTQ+ haklarının yaygınlaşması, cinsiyet değişimi ameliyatlarının artışı ve güzellik saplantıları gibi manipülasyonlar toplumun temel dinamikleri için büyük bir tehdit oluşturmaktadır. Bu tarz dejenere olmuş toplumlarda intihar oranlarının da oldukça yüksek olduğu görülmektedir.
2. Bu etkiler özellikle gençlerin Homo Distractus (Odağını Şaşırmış) olma durumunu tetiklemektedir. Güç odakları hegemonyalarını devam ettirme stratejilerinden biri olarak toplumlarda IQ seviyesini azaltmaya çalışmaktadırlar. İngiltere ve Amerika’nın kontrol ettiği Hindistan örneğinde de bu durumun işlerliği görülmektedir. Bu stratejinin çeşitli kanallarla, özellikle sosyal medya mecraları üzerinden günümüz gençlerine de uygulandığı görülmektedir. Bu şekilde odağı şaşırmış gençlere gerçek yansıtılmazsa, gelecekte oldukça büyük sorunlar eşiktir.



3. Günümüzdeki dünya sistemi bilgi üretimi ve kullanımı üzerinden şekillenmektedir. Böylelikle bilgi doğrudan bir güç vasıtası haline almıştır. Bilginin güç ile olan ilişkisi, bilginin manipülatif bir şekilde kullanma riskini artırmaktadır. Bilginin Güvenliği, bireyden uluslararası topluma kadar çok boyutlu bir güvenlik kapsamı ortaya koymaktadır. Böylelikle “Bilginin Güvenliği” kavramı hayatın doğasının ne olacağı ile ilgili önemli bir aşamaya evrilmektedir. Bu kapsamlı güvenlik alanı yine kapsamlı bir bilginin korunması ihtiyacını doğurmaktadır.
4. Günümüz çağında asıl mücadeleler internet ortamına taşınmış durumdadır. Ülkelerin alt yapı sistemleri, güvenlik duvarları ve açıkları milli güvenlik meselesi konumundadır. Bu durumda siber saldırılar ve siber tehdit grupları, devletler için oldukça büyük bir tehdit oluşturmakta ve savaşlar “Hibrit Savaşlar” a evrilmektedir. Hibrit Savaşın en belirgin özellikleri, yüksek teknolojik araçlar ve yöntemler ile sivil-asker tanımının bulanıklaşmasıdır. Böylelikle Hibrit Savaş günümüz savaş düzenini yeniden belirlemektedir. Burada en etkileyici olan saldırılar ise alt yapı sistemlerine gerçekleştirilen siber saldırılardır.
5. Günümüzde artık beş savaş boyutu bulunmaktadır, beşinci boyut olan uzay, uyduların olduğu boyuttur ve ezber bozmaktadır. Yörüngelerde bulunan uydulara yönelik olası kinetik saldırılarla, yeryüzünde bulunan sistemlerin yanında doğrudan yörüngedeki uydu sistemlerinin de artık saldırıya açık halde bulunuyor olması Uzay ve Siber Uzay güvenliğinin daha kritik bir noktaya taşımaktadır. Bugün ve gelecekte Siberuzayın millî güvenliğin bir parçası olarak ele alınması, önlemlerin barış-kriz ve sıcak çatışma/savaş süreçlerine göre alınması ve yönetilmesi elzemdir.
6. Barış, kriz ve sıcak çatışma süreçlerini kapsayan tüm pasif, reaktif, aktif ve proaktif siber çatışma hukuku düzleminde uluslararası ve ulusal yasalar, Birleşmiş Milletler Güvenlik Kurulu kararları ve ilgili Angajman Kuralları uygulanmalıdır. NATO’nun siber uzaya yaptığı ciddi yatırımlar göz önünde bulundurulmalı ve alınacak olan güvenlik önlemlerinin uluslararası standartlar çerçevesinde gerçekleşmesi sağlanmalıdır.
7. Teknoloji, artık yalnızca bir araç değil, küresel güç dengelerini belirleyen ve uluslararası ilişkilerde stratejik unsur olarak kullanılan bir güç haline gelmiştir. Teknolojik gelişmeyi elinde tutan ülkelerin küresel güç dengelerini de etkilediklerini göz önünde bulundurduğumuzda “Dijital Egemenlik” kavramı önemli bir nokta olarak karşımıza çıkmaktadır.
8. Teknolojik gelişmeyi tetikleyen en önemli nokta askeri olarak karşımıza çıkmaktadır. Aktif savaşlar ve güç mücadeleleri, teknolojik gelişmenin en önemli temel faktörü olmuş durumdadır. Burada gelişmiş silahlar, İHA’lar, caydırıcı hipersonik silahlar gibi çok önemli yatırımlar ön plana çıkmaktadır.



9. Askeri alandaki gücün etkin olabilmesi için askeri sistemlerin sürdürülebilir, dayanıklı ve yeni teknolojik gelişmelere entegre olması gerekmektedir, kritik altyapılar oldukça önem arz etmektedir. Uydu sistemleri, 5G ve askeri haberleşme bu noktada ön plandadır. 5G ile gerçek zamanlı iletişimin sağlanması; otonom sistemlerde, İHA'larda, siber güvenlik vb. pek çok alanda entegrasyonu sağlayabilmek adına kilit bir noktayı oluşturmaktadır. Bunun için 5G yatırımlarının ve uydu sistemlerinin olabildiğince hızlı bir şekilde desteklenip geliştirilmesi elzemdir.
10. Siber güvenlik alanında koruma sistemleri ve güvenlik açıklarının oluşması, siber veri giriş ve çıkışları sürecinde gerçekleşmektedir. Bu durum Siber koruma sistemlerini oldukça hassas ve dış müdahaleye açık konuma getirmektedir. Bu sebepten dolayı güvenlik tedbirleri hangi düzeyde olursa olsun, yüzde yüz bir koruma sağlamamaktadır.
11. Verinin güvenliğinin sağlanması ile sistem bütünlüğü ve güvenliği arasında doğru orantı bulunmaktadır. Bankacılık sektörlerindeki gibi kredi kartı ödemeleri ve diğer kritik işlemlerin yönetimi için oluşturulmuş bulunan mevcut yapıların güvenliği sorgulanmalıdır. Özellikle finansal analizler gibi kritik alanlarda verinin güvenliği ve başarılı bir şekilde entegrasyonunun sağlanması, güvenlik açıklarının minimize edilmesi adına oldukça hayati bir önem taşımaktadır.
12. Entegrasyon süreçleri sırasında "entegrasyon uzmanı" kavramının gerekliliği göz önünde bulundurulmalıdır. Veri açıklıklarını önlemek adına şifreli algoritmaların standart hale getirilmesi ve farklı sistemler arasında entegrasyonu sağlayacak projelerin geliştirilmesi gerekmektedir. Yeni dijital dünya sisteminde verinin gücünün mermiden, bombadan daha etkin olduğu göz önüne alındığında, veri güvenliğinin sağlanmasının ne kadar büyük bir önem arz ettiği daha iyi anlaşılmaktadır.
13. Büyük güç rekabeti yapay zeka alanında gerçekleşme, uluslararası arenadaki önemli aktörler arasında iş birliği ve rekabet önemli ölçüde bu ekseninde dönmeye başlamaktadır. Avrupa Birliği bu konuda Yapay Zeka Yasası yayımlamıştır. Yapay zekanın 3D yazıcılar, robotlar, hatta giyilebilir teknolojiler ile hayatımızın ne kadar içerisinde bulunduğunu görmek mümkündür.
14. Çin ve Amerika arasındaki ilişki hem iş birliği hem de rekabet çerçevesinde ilerlemektedir. Bu büyük güç yarışı ekonomik rekabetin ötesinde yapay zeka ve teknoloji savaşlarına dönüşmektedir. Günümüzde gerçekleşen savaş artık teknolojinin, fikirlerin savaşlarıdır. Bu süreçte odaklanmamız gereken nokta yeni teknolojik gelişmelere ne kadar hazır olup olmadığımızdır. Güvenlik stratejilerimizi bu ekseninde inşa etmemiz gerekmektedir.



15. Bir değerin sanal temsili olarak da tanımlayabileceğimiz dijital paralar (CBDC) günümüz gerçekliğinin ayrılmaz bir parçası haline gelmiş bulunmaktadır. Dijital para sistemleri ile finansal işlemlerin hızlanması, işlem maliyetlerin azalması, vergi kontrolünün daha yüksek seviyede sağlanabilir olması gibi avantajlar; bu para birimlerini daha cazip kılmaktadır. Böylelikle geleneksel para sistemlerinin yerini artık dijital para sistemlerine bırakmaya başladığı görülmektedir. Fakat dijital para sistemlerinin piyasa manipülasyonları, siber güvenlik tehditleri gibi zafiyetlerinin de bulunduğu göz ardı edilmemelidir.
16. Günümüzde dijital para sistemleri ile fiziki paranın önemini yitireceği, piyasada sanal paranın etkin olacağı dile getirilmektedir. Türkiye özelinde 2021 yılı itibariyle dijital para aktifleştirilmiş bulunmakta ve HAVELSAN - ASELSAN aracılığı ile geliştirilmekte olsa da merkez bankasının bu hususta aktif olmadığı görülmektedir. Dijital para sistemleri için gerekli hazırlıkların yapılması en çok gelecek adına önem arz etmektedir. Halka bu sistemlerin eğitim vb. yollarla anlatılması, CBDC sistemleri için gerekli yasaların düzenlenmesi elzemdir.
17. İsrail'in çağrı cihazlarını patlatması ile dijitalleşmenin aynı zamanda nasıl bir tehdit oluşturduğunu, dijital bağımlılığın bizi dış tehditlere nasıl açık bıraktığını göstermede önemli bir örnek olmuştur. İlk bakışta güvenlikle ilgisiz birçok dijital teknoloji alanının dahi saldırı veya savunma boyutu bulunmaktadır. Günümüz dijital teknolojileri açısından geri sayılabilecek cihazlara saldırılar dikkate alındığında daha gelişmiş olanlar üzerinden de birçok saldırı projesinin hazırlandığı tahmin edilmektedir. Bu tür tehditlerden kaçınmak adına üretim ve birikimde ulaştığımız seviyeyi iç piyasaya entegre etmek, bunu bir yasa haline getirmek hayati önem taşımaktadır.
18. Ülkemizde de farklı kurumlar aracılığıyla bu kapsamda önemli araştırma ve üretim birimleri bulunmakta, terörle mücadelede kullanılan araçlarla bu teknolojilerden yoğun bir şekilde yararlanılmaktadır. Belirtilen gerçeklere karşın yapay zeka kapsamında ilk bakışta ilgisiz veya demode bir teknoloji ile yeni bir saldırı/savunma/güvenlik tehdidi söz konusu olabilmektedir. Dolayısıyla ileri teknolojik alanlara ve yazılım sistemlerine odaklanırken sıradan gibi görünen alanların ihmal edilmemesi son derece önemlidir.
19. Başta cep telefonu olmak üzere bütün elektronik aletlerde, aparat ve ürünlerin daha ekonomik gerekçelerle uluslararası piyasadan tedarik etme yanlısına düşülmemelidir. Elektronik cihazların sıradan parçaları için de yerli üretimin teşviki, desteği, kontrolü, geliştirilmesi, güvenilir yerli firmalar üzerinden tedariki oldukça büyük önem arz etmektedir.



20. İsrail askeri kapasitesi, entelektüel birikimi ile oldukça dikkat çeken ve bölgesinde güç sahibi olan bir ülke olarak Ortadoğu coğrafyasında bulunmaktadır. Bölgesinde ulusal güvenliğini sağlama adına ileri teknoloji yatırımlarıyla, dışa bağımlılığın minimize edilmesiyle, Ar-Ge yatırımlarıyla savunma teknolojilerinde dünyanın en ileri ülkelerinden biri olarak bulunmakta, yüksek kapasiteli askeri altyapıya sahip, Ar-Ge yatırımlarında öne çıkan bir ülke olarak karşımıza çıkmaktadır. Gelecek 20 yıl içinde Orta Doğu'da Ar-Ge ve teknoloji alanında üstünlük sağlaması muhtemeldir. Bölgedeki stratejik hamleleri, uluslararası ilişkilerdeki gücü ve yüksek Ar-Ge yatırımları, İsrail'i dikkate alınması gereken önemli bir aktör haline getirmektedir.
21. Yolsuzluk, insanlığın ortak problemlerinden biri olarak karşımıza çıkmaktadır. Teknolojik gelişmeler, medya ve iletişimin gelişimi, küresel pazarların ve şirketlerin oluşumu yolsuzluğun küresel bir olgu haline gelmesini sağlayan temel etmenlerden bazılarını oluşturmaktadır. Batı menşeli şirketlerde de görülen yolsuzluk, piyasa ve hacmin büyümesiyle daha karmaşık hale gelmekte ve tespitini zorlaştırmaktadır.
22. Batılı şirketlerin yolsuzlukları uzun süre gizlenip büyüdükçe etkileri de büyük ve yıkıcı olmaktadır. Bu şirketler, yüksek teknolojik imkânlarla sahip olmaları sayesinde yolsuzlukları daha kolay gerçekleştirebilmektedir. Ancak bu durum, yolsuzlukla mücadele eden yasal otoritelerin daha gelişmiş teknolojik donanımlara sahip olmalarını gerektirdiğinden, mücadeleyi daha zor ve maliyetli hale getirmektedir. Yolsuzlukların tespiti ve ifşası, Batılı kurum ve kuralların daha da güçlenmesine ve Batı hegemonyasının yeniden pekişmesine yol açmaktadır.
23. Dijital çağın gelişmesiyle birlikte, özellikle sosyal medyanın hayatımıza girişi dijital etik ve güvenlik kavramlarını daha da kritik hale getirmiştir. Dijitalleşmenin hayatımızın her noktasına yerleşmesi, "post-truth" (hakikat sonrası) olgusunun önem kazanmasına yol açmaktadır. Bu dönemde, çevrimiçi davranışlar, bilgi manipülasyonu ve yanlış bilgilendirme yaygınlaşmış ve bunlar sosyal medya aracılığıyla hızla yayılarak toplumsal algıları etkilemeye evrilmiştir. Türkiye'de, bu soruna karşı, İletişim Başkanlığı bünyesinde yalan haberlerin takip edilmesi gibi önlemler alınmış olsa da sosyal medya, insanların düşünce ve davranışlarını değiştiren güçlü bir araç haline gelmiştir.
24. Post-truth çağında, hakikat yerine duygular ve kişisel inançlar ön plana çıkarken, bilgi güvenliği ve dijital etik sorunları derinleşmektedir. Devletler, yalnızca fiziksel tehditlerle değil, siber saldırılar ve dijital manipülasyonlarla da karşı karşıya kalmaktadır. Yanlış haberler ve propaganda, toplumların algısını değiştirebilir ve sosyal, politik istikrarsızlıklara yol açabilir. Bu nedenle, halk doğru bilgilendirilmelidir ve algı yönetimine karşı doğru yönlendirme yapılmalıdır. Devletlerin güvenliği, artık dijital tehditlere karşı güçlü bir savunma stratejisi gerektirmektedir.



25. Devletlerin güvenlik stratejileri, dijital çağın getirdiği yeni tehditlere karşı yeniden şekillendirilmelidir. Enformasyon savaşları, hibrit tehditler ve siber güvenlik, devletlerin karşı karşıya olduğu en önemli tehlikeler arasında yer almaktadır. Komploları, siber saldırılar ve medya manipülasyonları halkla devlet arasındaki güveni zedelemekte ve devletlerin istikrarını tehdit etmektedir. Bu sebeple, dijital güvenliği sağlamak ve doğru bilgi akışını kontrol altına almak için devletlerin etkili güvenlik ağları geliştirmesi ve dijital etik ilkelere uygun politikalar oluşturması gerekmektedir.

22 Kasım 2024, İstanbul