4. İstanbul Güvenlik Konferansı 2018

İstanbul Deklarasyonu (TASLAK)

Türkiye'de ilk kez 2015 yılında düzenlenen ve bu yıl dördüncüsü gerçekleştirilen **İstanbul Güvenlik Konferansı**, "Geleceğin Güvenliği" ana teması altında TASAM Millî Savunma ve Güvenlik Enstitüsü (MSGE) tarafından, Deep Learning Türkiye stratejik paydaşlığında, **08-09 Kasım 2018** tarihinde İstanbul'da Elite World Europe Oteli'nde icra edilmiştir. Bölgesel ve küresel ölçekte markalaşan **İstanbul Güvenlik Konferansı 2018**'de değişik ülke ve bölgelerden her disiplinde geniş konuşmacı ve protokol katılımı sağlanmıştır. Türkiye'den ilgili tüm otoriteler de Konferans'ta temsil edilmiş, tüm oturumlar kurumsal olarak takip edilmiştir.

Konferans'ta, önceki yıl olduğu gibi Katar Savunma Bakanlığı Stratejik Araştırmalar Merkezi (QSSC) işbirliğinde "Körfez'de Güvenliğin Geleceği" başlıklı **Türkiye - Körfez Savunma ve Güvenlik Forumu 2018** ile "Afrika'da Güvenliğin Geleceği ve Türkiye" başlıklı **Türkiye - Afrika Savunma Güvenlik ve Uzay Forumu 2018** de alt etkinlikler olarak eş zamanlı yapılmıştır.

ABD'den Çin'e, Rusya'dan İran'a 40'a yakın ülkeden katılımcıları buluşturan **İstanbul Güvenlik Konferansı 2018**; "Endüstri 4,0" ve "Yapay Zekâ" olgularının ışığında, güvenliğin mimarisinde Türkiye merkezli rekabetçi yeni perspektifler hedefinde önemli görüş ve düşüncelerin paylaşıldığı bir platform olmuştur.

Açılış konuşmalarında konvansiyonel güvenliğin son yıllarını yaşadığı ve "geleceğin güvenliğinin" değişen devlet doğası çerçevesinde şekilleneceği belirtilmiştir. Konferans'ta, geleceğin güvenliğinin bütün boyutlarına etki etmesi muhtemel faktörler kapsamlı bir şekilde incelenmiştir. Konferans kapsamında "Siber Güvenlik", "Derin Öğrenme" ve "Geleceğin Güvenliğinde Yapay Zekâ" panelleri düzenlenmiştir. Konferans sürecinde düzenlenen bir törenle, stratejik vizyon sahibi başarılı kişi ve kurumlara, TASAM tarafından 11 yıldır geleneksel hâle getirilen **TASAM Stratejik Vizyon Ödülleri** de tevdi edilmiştir.

Konferans sonucunda, aşağıdaki tespitler ve öneriler yapılmış, ilgili tüm otoritelerin ve kamuoyunun dikkatine sunulması kararlaştırılmıştır:

1. Katar Devleti'ne uygulanan ambargonun başlangıcından bugüne 500 gün geçmesine rağmen ambargonun uygulanma nedenleri konusunda somut bir veri hâlâ sunulamamıştır. Körfez'de özellikle yöneticilerin hatalarını düzeltmesi için bir fırsat olarak görmesi gereken "Kaşıkçı" olayı, dünyanın vicdanını yaralayan ve tamamen siyasallaşan bir konu hâline gelmiştir.

2. Güçlü Türkiye, Körfez güvenliğinin de garantörüdür. Ayrıca Batı Balkanlar da güvenlik açısından çok kırılgan durumdadır. Bu bölgelerdeki çatışmalar, büyük güçlerin çıkarlarını yansıtacak şekilde gerçekleşmekte ve insan hayatı siyasetin önünde görülmemekte, öncelikli olarak nitelendirilmemektedir.

3. Ülkeler ithal güvenliğe bel bağlamadan kendi güvenlik sistemlerini oluşturmalıdır, aksi takdirde yönetimlerinin zayıflaması söz konusudur.

4. Hiçbir silahlı güç sayı olarak mutlak bir değer ifade etmeyecektir, ancak siyasi makamlar tarafından kendisine verilecek "caydırıcılık", "müdahale" gibi görevleri yerine getirmesi hâlinde bir değer ifade edebilir. Konvansiyonel savaş var olmaya devam edecektir. Hibrit savaş gibi yeni savaş türlerinin tek savaş yöntemi olacağı yönündeki düşünceler tekrar değerlendirilmelidir.

5. Çatışmalar sınır tanımasa da yayılmalarında etkisi azalan sınırlar tekrar önem kazanmaya başlamaktadır. Küresel düzeyde sayıca 60'ın üzerindeki ülke komşularına karşı duvar inşa etmekte, güvenlik giderek bölgeselleşmektedir. Dünya genelinde akıllı şehir çalışmaları, sadece teknoloji ile değil asimetrik şekilde değişen güvenlik tehditleriyle de ilişkilendirilerek kurgulanmalıdır.

6. Hibrit savaş; yapay zekâ, uzay savaşı ve siber saldırı konularında analitik bir bakış açısıyla ele alınmalıdır. Bu konuda Çin 2025 yılına kadar dünya lideri olabilmek için etkin bir şekilde çaba göstermektedir. ABD, "güvenlik güç unsuru" olarak uzay komutanlığı oluşturmuştur. Çin de uzay savaşı konusunda çok mesafe kat etmiştir. Bu alanda yapılan çalışmaların hedefi, alçak dünya yörüngesindeki askerî uydulardır. Devlet-dışı aktörlerin anti-uydu-savar sistemi geliştirme veya elde etmeleri engellenmelidir.

7. 2018 yılında yayınladığı siber güvenlik stratejisinde saldırı amaçlı siber operasyonlar yapacağını ifade eden ABD, siber saldırılar konusunu daha geniş bir boyuta taşımıştır. Dünya genelinde siber savaşlara harcanan mali kaynak 8 trilyon dolara ulaşmıştır. 5 milyon personelin verisinin çalındığı rapor edilmiştir. 2022 yılına kadar dünya genelindeki siber güvenlik uzmanı ihtiyacı 1,8 milyon kişi olarak öngörülmektedir. Bunların istenen nitelikte eğitilerek göreve başlamamaları hâlinde siber saldırıların etki boyutu çok daha büyük olacaktır.

8. Geleceğin güvenliğinde savunma sektörü, her ülkenin kendi güvenlik ihtiyacına göre yapılandırılmalıdır. İnsancıllık ve askerî genellilik gibi silahlı çatışma hukukunun göz ardı edilmesi nedeniyle operasyon sahalarında çok sayıda sivil hayatını kaybetmektedir. Yakın gelecekte orduların envanterine yaygın şekilde girmesi beklenen lazer silah sistemleri, otonom sistemler ve benzeri sistemlerin yönlendirilmesinde insan ihtiyacı önemini koruyarak devam edecektir.

9. Küresel köyde hızla yıpranan ABD meşruiyeti yerine aday olan Çin, tarih boyunca olduğu gibi kapalı bir kutu olarak görülmekte, üstleneceği meşruiyet konusunda şüphelere yol açmaktadır.

10. Afrika ve Çin'in eşit ortaklık kazanması konusu çok zordur ve bu çalışma yolu daha tamamlanmamış olmasına rağmen ilişkilerinde Afrika - Amerika ile Afrika - Avrupa'dan çok daha eşit olduğu görülmektedir.

11. 1990'ların başında "yumuşak güç" kavramı ilk defa kullanılmaya başlandığında, kavramı ortaya koyan otoriteler artık "sert güç" kavramının dış politika ve ulusal hedeflere ulaşmada etkin bir araç olmadığını, buna karşın yumuşak güç nosyonunun dış politika uygulamalarında yeni enstrüman olacağını vurgulamıştır. Ancak bugüne dek yumuşak güç ve sert güç kavramlarının gerçeği ortaya koymakta yetersiz olduğu görülmüş, dış politikayı açıklamakta yetersiz kaldıkları, gerçekçi olmadıkları tespit edilmiştir. Yeni "akıllı güç" kavramı üzerinde önemle durulmalıdır.

12. Dış politika uygulamalarında artık devletler yegâne aktör değildir. Devlet-dışı aktörlerin; sivil toplum kuruluşlarının, çok-uluslu şirketlerin, hatta terör örgütlerinin dahi devletleri etkilediği bir sistem halen yerini korumaktadır. Tek başına çok boyutlu düzlemde yumuşak güç nosyonu yeterli olamaz ve yeri geldiğinde sert güç de yöntem olarak benimsenebilir. Güç bileşenleri dengelenebilir ve böylelikle akıllı güç nosyonu ortaya çıkarılır.

13. Son yıllarda, akıllı güç kullanımında Çin'in önemli bir emsal teşkil edebileceği tespit edilmiştir. Ekonomik kalkınma, işbirliği gibi değerleri politik yapıdan ayırmak oldukça zor olduğundan Çin, Bölge'deki ve Bölge dışındaki devletlere ekonomik işbirliği teklif ederken politik dayatmalardan kaçınmakta ve böylelikle son yıllarda küresel bir cazibe oluşturmaktadır. Türkiye'nin bölgesinde insani yardım faaliyetlerinde bulunması ve bu çabalarını son yıllarda gitgide artırması, Bölge'de Türkiye lehine önemli bir yumuşak güç kapasitesi oluşmasını sağlamaktadır.

14. "Yumuşak Güç" kavramının ortaya atıldığı yıllardaki güç dağılımı Soğuk Savaş döneminin çift kutuplu düzenidir, ancak günümüzde çift kutuplu güç dağılımından söz etmek yerinde bir ifade olamaz. Yumuşak güç içerikli bir gelecek perspektifinin ortaya konabilmesi için sistem perspektifi göz ardı edilmemelidir, sistem yaklaşımı ihmal edilerek ne yumuşak güç ne de akıllı güç çıkarımları ortaya konabilir.

15. Son yıllarda savunma endüstrileri robotik atılımlar gerçekleştirmekte ve robotik savaş konseptine yönelik ar-ge çalışmaları yürütmektedir. Özellikle 11 Eylül saldırılarından sonra yarı-otonom kabul edilebilecek insansız hava aracı teknolojilerinde dramatik bir artış olmuştur. Otonom silah sistemleri de bu dramatik yükselişin geldiği son aşamadır. Bunun yanında otonom silah sistemleri için uluslararası hukukta herhangi bir kodifikasyon bulunmamakta, kullanımı esnasında uluslararası insan hakları, insancıl hukuk, ceza hukuku ile sorumluluk bağlamında ciddi boşluklar bulunmakta ve bu boşlukların ivedilikle kodifiye edilmesi gerekmektedir.

16. Devletlerin karar verme yapılarındaki zaaflardan faydalanarak doğrusal olmayan metotlarla saldırılar geliştirmesi sebebiyle hibrit savaşlar, iç ve dış güvenlikle ilgili her alanı kapsamaktadır. Demokratik toplumlar, sahip oldukları kırılganlıktan dolayı hibrit saldırı ve tehditlere açıktır. Bu sebeple hibrit tehditlerle başa çıkabilmek ve hibrit savaşa hazır olabilmek için devletlerin bütüncül ve kapsamlı bir yaklaşımla, koordinasyonlarını ve işbirliklerini artırması çok önemlidir.

17. Çin 2017 yılında "Yeni Nesil Yapay Zekâ Geliştirme Programı" adı altında bir hükümet programı başlatmış ve yapay zekâ alanında atacağı adımları bir strateji belgesinde formüle etmiştir. Bu perspektifteki en dikkat çeken unsurlardan biri ise; Çin'in 2025 yılına kadar, yapay zekâ alanında atılacak adımlarla küresel liderliği hedeflemesidir.

18. Ağ teknolojilerinin gelişmesiyle "siber güvenlik", dünya gündeminde önemi günden güne artan bir konu haline gelmiştir. Buna bağlı olarak, risk tabanlı yaklaşımlardan dolayı devletler yüksek derecede harcamalar yapmaktadır. İhlallerin bertaraf edilebilmesi için uyumluluk anlaşmaları yapılmaktadır. Bilgi teknolojilerinin gelişimi, asimetrik savaş nosyonunu ortaya çıkarmaktadır.

19. Türkiye'deki yapay zekâ çalışmalarının daha ileriye götürülmesi için finansman desteği artırılmalıdır. Bunun yanında "derin öğrenme" sisteminin eğitime ve savunmaya entegrasyonu da büyük öneme sahiptir.

20. Geleceğin güvenliğinde yapay zekâ ve derin öğrenme çalışmalarının katkılarıyla güvenlik kameraları da anahtar öneme sahiptir. Dünya üzerinde 256 milyon güvenlik kamerası vardır ancak bunlar akıllı kameralar değildir ve uzmanların güvenlik sorunlarına çözüm arayabileceği bulguları öne çıkaramamaktadır. Akıllı kameralar, niteliksel özellikleri ile; eğitim kurumlarındaki öğrencilerin gözleminde, herhangi eğlence mekanına gelen kötü niyetli kişilerin tespitinde, kalabalık bir havalimanı, alışveriş merkezi, otobüs/tren garı veya şehir meydanındaki olası güvenlik problemlerinin ortaya çıkarılmasında ve önlenmesinde, eylemlerdeki provokatif ve art niyetli kişilerin teşhisinde kullanılmakta ve bunlara bağlı olarak şehirlerdeki güvenlik açıkları akıllı kameralarla giderilebilmektedir.

21. Dünyada hukuk alanında da yapay zekâ çalışmaları yapılmakta, kullanımının etiği ile yargısal sürecin nasıl kat edileceği üzerinde durulmakta, gelecekte yargıç yerine yapay zekânın görev yapabileceği ön görülmektedir. ABD son yıllarda bu alanda çalışmalar yapmaktadır.

22. Ar-ge başlangıç firmaları Türkiye'de fon ve yatırım sorunları yaşadığı için maddi kaynaklar bakımından desteklenmelidir. Kamuya ve özel sektöre adaptasyonu üzerine düşünülmesi gerekmektedir.

23. ABD güvenlik raporlarına göre Çin ve Rusya ABD'nin askerî uydularını devre dışı bırakabilecek silah sistemleri geliştirmektedir. 2018 yılında ABD Başkanı Donald Trump'ın Pentagon'a bağlı uzay kuvvetlerini 6. kuvvet olarak inşa ettiğini açıklaması, geleceğin güvenliğinin uzay alanında hangi aşamaya geldiğinin anlaşılmasında mühim bir olgudur. Bunun paralelinde, yakın gelecekte ABD ve Çin arasında bu alanda örtülü bir mücadele öngörülmektedir.

24. Uzay savaşında hedef noktası LEO (Low Earth Orbit) olarak ifade edilen Alçak Dünya Yörüngesi kapsamında askerî casusluk için kullanılan uydular mevcuttur. Özellikle ABD, Irak Savaşı'nda kullandığı "Küresel Ağ Tabanlı Savaş Doktrini" yaklaşımını ortadan kaldırabilmek, enformasyonu ve bilgiyi kesebilmek, devletleri savaş ortamlarında kör ve sağır kılabilmek amacıyla yeni silah sistemleri ve savaş yaklaşımları geliştirmektedir.

25. ABD'nin uzay savaşı için resmî bir tanımlaması olmasa da Çin bu hususta; "dış uzay adı verilen bir bölgede iki devletin saldırı ve savunma amaçlı karşılıklı operasyonlarına dayanan bir mücadele tekniği" şeklinde bir tanımlama geliştirmiştir.

26. Askerî casusluk kapsamında ABD özellikle askerî uydular sayesinde dünyanın her yerine ait yüksek çözünürlüklü fotoğraflar çekebilmekte, özel iletişim imkanlarına sahip olmakta, gizli dinleme kapasite ve imkanları edinmektedir. ABD ayrıca yine uzaydan dünyanın her yerine 30 ila 60 dakika içinde gönderebileceği ve nokta atışı yapabileceği uzun menzilli füzelere sahiptir. Tüm bu konular önemle takip edilmeli ve değerlendirilmelidir.

27. 2015 yılındaki Ukrayna Krizi sırasında Rusya, enformasyon savaşını askerî savunma stratejisi belgesine dâhil etmiştir. Hasmın savaş ve benzeri durumlarda tüm bilgi desteğini kesmeyi amaçlayan Rusya'nın hedeflerinden biri de alçak yörüngedeki ABD casus uydularıdır.

28. Devlet-dışı aktörler uzayda propaganda, dezenformasyon ve bilgi kirliliği oluşturmak için televizyon yayını yapan uydular satın alabilmekte, benzeri uydular terör örgütleri tarafından da satın alınabilmektedir.

29. ABD, uydularının devre dışı bırakılarak kör ve sağır bırakılması ihtimaline karşı geliştirdiği B52 uçağı ile uydu sistemini yeniden hayata geçirebilecek yedek bir mekanizma oluşturmuştur. Bu bile ABD'nin uzay alanındaki mücadeleyi ne kadar dikkate aldığına, tehdit hissederek uzay teknolojilerini ne kadar ciddiye aldığına dair bariz bir örnektir. Türkiye'nin, başkent Ankara'da kurmayı planladığı uzay üssü ile rekabete ortak olacağını açıklaması da geleceğin güvenliğinde Türkiye adına inovatif adımlardan biridir.

30. Her yıl Güney Çin Denizi'nden 28 milyar varil petrolün transferi, üstünde durulması gereken ticari bir istatistiktir. Keza sahildar devletlerin geçmişte ve günümüzde birbirleriyle yaşadığı politik sorunlar Güney Çin Denizi'ni dünyanın en problemli sularından biri haline getirmiştir. Nitekim bu durum, gelecek perspektifinde Güney Çin Denizi içerikli konuları akademik gündeme de taşıyacaktır. Güney Çin Denizi'nde yaşanabilecek problemler vahim bir şekilde tüm Asya'ya sirayet edebilir. Bölgedeki endişelerin yatıştırılması için bölgesel diyaloğun artırılması gereklidir.

31. İnternetin yaygınlaşması, terörizmin boyut değiştirmesine ve yeni kavramların doğmasına yol açmıştır. Terör örgütleri sosyal medya alanında uzmanlaşmış, bu durum "yeni terörizm" olarak bilinen nosyonu ortaya çıkarmıştır. Buna bağlı olarak terör örgütleri; manipülatif bilginin daha geniş kitlelere yayılabilmesi ve daha geniş kitlelerden destekçi toplanabilmesi imkanlarını elde etmeye başlamıştır. Bu kolaylıkların terör örgütlerince elde edilmesi, güvenlik güçlerinin de iletişim, koordinasyon ve eşgüdüm yeteneklerini geliştirmesini gerektirecektir.

32. Terörle mücadelede; bilgiyi elde etmek öngörü gücünü artıramaz. Gelebilecek sürpriz saldırılar için öngörülerin üretilmesinde analiz birimlerinin yeterli sayıya ulaştırılması ve yetiştirilmesi hayati önem arz etmektedir.

33. Uluslararası örgütlerin barış ve istikrar bağlamında meşruiyetlerini koruyabilmeleri için benimsemeleri gereken bazı prensipler olmalıdır; uluslararası örgütler çatışmalara müdahaleye değil, çatışmaların önlenmesine odaklanmalıdır. Bu husus, savaşların ortaya çıkmasını önleyecek ve insani kayıpları azaltacaktır. Bu sebeple savaşların önlenmesine yönelik plan ve projeler üzerinde durulması gerekmektedir.

34. Uluslararası düzeyde stratejik ve kapsayıcı ortaklıklar hayati öneme sahiptir. Yerel ve bölgesel düzeyde; emniyet güçleriyle, STK'larla, devlet-dışı örgütlerle gerekli eşgüdüm sağlanmalıdır. Tüm bu unsurlar, barışı koruma noktasında devlet kadar rol sahibidir.

35. Barış inşasına ilişkin programların başarısız olmaması, sürdürülebilir olmasıyla doğrudan ilgilidir. Bu sebeple uluslararası örgütlerin sürdürülebilir kalkınma programlarına azami ölçüde titizlikle yaklaşmaları gerekmektedir.

36. Uluslararası kadar ulusal düzeyde de barışı korumaya motive olunması krizlerin çözümünde uluslararası örgütlerin yükünü azaltacaktır. Uluslararası barışın tesis edilebilmesi noktasında uluslararası örgütler kadar siyasi partiler, gençlik örgütlenmeleri ve özel sektör de dâhil olmak üzere oldukça geniş bir sorumluluk ağı mevcuttur.

37. Kadınların toplumsal, siyasal, iş yaşamında bulunması ve her alanda daha fazla katkı sağlaması şiddetin azalmasında, barışın inşası ve tesisinde üzerinde durulması gereken en önemli noktalardan biridir.

38. Türkiye'nin Somali'de güvenliği sağlamaya yönelik icra ettiği faaliyetler barışın inşası için aydınlatıcı örneklerden biridir. Keza Türkiye, yakın dönemde 8 ülkeye benzer desteklerde bulunmuştur. Dünyanın her yerine yapılan insani yardımlar hususunda ABD'den sonra 2. sırada yer almıştır, ancak yapılan mali yardımın gayrisafi yurtiçi hasıla oranına bakıldığında dünyada ilk sırada yer almaktadır ki bu da her türlü takdire şayandır.

39. ABD Ülke/Anayurt Güvenliği Teşkilâtı ve 2018 Dünya Ekonomik Forumu değerlendirmelerinde, stratejik düzeydeki siber saldırıların, nükleer savaştan sonra en yüksek yıkım gücüne sahip olduğu ve geleceğin güvenliğinde çok hassas bir konuma sahip olduğu vurgulanmıştır.

40. Siber saldırılar sonrası tahribatın önlenebilmesi, zararlarının en aza indirilebilmesi maksadıyla "büyük veri analizi", "makine öğrenmesi", "derin öğrenme" gibi yeni teknolojilerden azami faydalanılmalı; ayrıca kurumsal farkındalık, üst düzey yönetimler tarafından sahiplenme ve siber saldırılara teknik olarak sistematik ve bütünsel yaklaşım esas alınmalıdır.

41. Siber faaliyetler doğası gereği gayrinizamidir. Bunun yanında siber faaliyetlerde de asimetrik etki ile birlikte, bilinmezlik ve süreklilik sürecin merkezine oturur. Bu çerçevede düşünülürse bahsedilen savaş değil, mücadeledir ve özelleşmiş her mücadele için özel ihtisasa sahip hibrit personel grubu, planlamada esneklik ve manevra kabiliyeti son derece elzemdir.

42. Bilişim Teknolojileri (BT) çok hızlı değişimlere ayak uyduracak şekilde tasarlanarak ihtiyaçlara yanıt vermek için azami 3-4 yılda bir yenilenmektedir. Öte yandan Otomasyon Teknolojileri (OT) herhangi müdahaleye gerek duymayacak şekilde 25-30 yıl çalışacak şekilde tasarlanmaktadır. Bu geçen sürede, dijitalleşme ile beraber BT sistemleri ile OT sistemleri entegre olmaya başlamıştır ve bu entegrasyon, geleceğin güvenliğinde yeni zafiyetler doğurmaya adaydır.

43. Fabrikalar ile enerji tesisleri; uzaktan yönetilebilmesi ve veri toplanıp verimliliğinin ölçülebilmesi için internete bağlanmakta, bu durum beraberinde siber saldırı tehlikesini de gündeme getirmektedir. İstatistiklere göre Türkiye'de günde ortalama 516 saldırı girişimi olmakta, araştırmalara göre dünya genelinde bir siber saldırının fark edilmesi ortalama olarak 5 aylık süre sonunda mümkün olmakta, gün geçtikçe çeşitliliği ve şiddeti artan siber saldırılar karşısında, kurumların direnç göstermesi ve çevik biçimde yanıt vermesi zorlaşmaktadır.

44. Siber güvenlik faaliyetleri ile olası saldırılar gerçekleşmeden önce hazırlık yapıp, karşılaşıldığında hızlı ve doğru tepki verilmesi çok önemlidir. Tehdit ve zafiyetlerin farkında olunup yönetilmesi, saldırıların tespiti için güvenlik olaylarının takibi, saldırı sonrası etkin bir siber olaylara müdahale sürecine sahip olunmasını sağlayacak strateji ve yönetişim, dönüşüm, siber savunma ve siber olaylara müdahale adımlarında etkin bir siber güvenlik çerçevesi oluşturarak en güncel güvenlik standartlarına sahip olunması ancak uçtan uca siber güvenlik çerçevesi ile mümkün olacaktır.

45. Siber güvenlik alanında; geleneksel yönetim sistemlerinde önerilen kontrol esaslı yaklaşımdan, "teknik zafiyetlerin güncel tehdit bilgileri ışığında sürekli taranması, belirlenmesi ve giderilmesi, sistemlerin de bu doğrultuda sürekli izlenerek vakalara doğru ve zamanında yanıt verilmesi" yaklaşımına doğru bir yönelim söz konusudur.

46. Son dönemde, siber güvenlik operasyon merkezleri, siber tehdit simülasyonları, kırmızı takım uygulamaları, siber suistimal inceleme ve siber risk sigortası kavramları siber güvenlik trendleri olarak karşımıza çıkmaktadır.

47. Devletin görevi halkını sürekli güvenlik ve sürdürülebilir refah içinde geleceğe taşımaktır. Ancak sağlam bir eğitim ve düzenli mali yapıya sahip bir ekonomi içinde gelişebilen refah ve güvenlik ise sadece silahlı tehdit ile karşı karşıya olmayıp, son dönemlerde Türkiye ve Katar örneğinde de gözlemlendiği gibi, hedef ülkelerde ulusal paralar, dış mali manipülasyonlara da hedef olmakta ve bu yöntemlerle de çökertilmeye çalışılmaktadır.

48. Hedef ülkeler bu saldırıya karşı önlem olarak, uzun vadeli makro analizlerle mali riskleri asgariye indirecek olanaklara sahiptir, ana enstrümanı ise parasal güvenliği sağlamaktır. Nitekim temel gelişmişlik göstergeleri; düşük enflasyon, makbul "çevrilebilir" para birimi, talebi yüksek devlet varlık bonoları, demografik istikrarlı dengeli nüfus artışı ve dijital ağırlıklı teknolojik gelişmedir. Bugün teknolojik gelişme, dijital girdilerle adeta kapitalsiz bir kapitalist sistem inşa etmektedir.

49. Siyasal ekonomi anlayışında ekonomi güvenliği ile ülke güvenliği aynı makro dengeler içinde bir araya gelmektedir. Yaşadığımız dönemde TL'nin dış etkenlerle değer kaybına uğratılması, ABD ile Çin arasındaki ticaret savaşları, İtalyan ulusal bütçesine AB tarafından gösterilen tepki, Brexit, İran yaptırımları vb. gelişmeler yaklaşan yeni ekonomik düzenin işaretlerini içermektedir. Küresel ekonomik lider ülkeler arayışı ortaya çıkmakta, bölgesel ve ulusal planda bu yeni düzen için enflasyonu dizginleyecek mali disiplin içinde uluslararası yatırımcıları çekecek güvenceleri içeren ve ar-ge ile reel sektörü de dâhil edecek süreçlerin başlatılması gereklilik arz etmektedir.

09 Kasım 2018, İstanbul