KARADENİZ EKONOMİK İŞBİRLİĞİ PARLAMENTER ASAMBLESİ
KEİPA

ULUSLARARASI SEKRETARYA

Doc.: GA51/LC51/REP/18/tr

RAPOR*

KEİ ÜYE DEVLETLERİNDE SİBER GÜVENLİKTE İŞBİRLİĞİNİN GÜÇLENDİRİLMESİ

Raportör: Sn. Eldar Guliyev, Komisyon Başkan Yardımcısı, Azerbaycan

* *Metin, 19 Haziran 2018'de Tirana'daki KEİPA Hukuki ve Siyasi İşler Komisyonunun Elli Birinci Toplantısında müzakere edilmiş ve 20 Haziran 2018'de Tirana'da düzenlenen KEİPA Elli Birinci Genel Kurulu'nda kabul edilmiştir.*

I. GİRİŞ

1. 21. yüzyılda karşılaşılan sorunlar, insanlığın faaliyetleri açısında kapsamlı fırsatların önünü açan yeni bilgi ve iletişim teknolojilerinin (ICT) geliştirilmesi ihtiyacını doğurmaktadır. Karmaşık ve çok katmanlı bilgi akışları insanlığın potansiyelini geliştirme ve güçlendirmeye katkıda bulunmakta ve dünyanın dört bir yanında milyonlarca insanın faydalanabileceği bir biçimde üst düzey kalkınmayı sağlama amacını gütmektedir. Yeni bilgi teknolojileri zaman ve mekanı daha sıkışık hale getirmekte ve global bilgi ve enformasyon alış verişine erişim yelpazesini geliştirme fırsatını doğurmaktadır.

2. Önde gelen ülkeler halihazırda e-devlet, e-imza, dijital ekonomi gibi konseptleri hayata geçirmeye başlamıştır. Bilgisayarlar, akıllı telefonlar, tabletler ve diğer cihazlar önemli devlet bilgileri ve gizli bilgileri toplayan ve taşıyan araçlar olarak ortaya çıkarken bir yandan da birkaç saniye içinde bilgi alış verişine olanak tanımakta, devlet işleri ve bankacılık işlemleri gerçekleştirebilmekte, kredi kartı ya da sanal para kullanarak internet üstünden alışverişler yapmayı ve hizmet alımları gerçekleştirmeyi mümkün kılmaktadır. Bu cihazlar aynı zamanda değerli bilgiler de taşımaktadır: devlet belgeleri, bilgileri ve diğer önemli gizli bilgiler. Her yıl kilit önemdeki sektörlerin hemen her alanda bilgi teknolojilerine bağımlılığı artmakta ve dolayısıyla siber güvenlikle ilgili sorunlar dünya ölçeğinde önem kazanmaktadır.

3. Bilgi ve iletişim teknolojilerindeki (ICT) gelişim ve teknolojik ilerlemelere paralel olarak siber terör, siber suç ve siber saldırılar her geçen gün artış göstermektedir. Bu ise ülkeler, büyük şirketler ve toplum açısından, önemli bilgisayar ağları ve programlarına saldıran kimliği bilinmeyen bilgisayar korsanları tarafından gerçekleştirilen siber terör, siber suç ve siber saldırılarla ilgili endişeleri artırmaktadır.

4. Dolayısıyla, Hukuki ve Siyasi İşler Komisyonu, 25 Ekim 2017'de Rostov-on-Don'da gerçekleşen Ellinci Toplantısında, KEİ üye devletlerinde siber güvenlik sorununu ele almaya karar vermiştir. Komisyonun Elli Birinci Toplantısı, "KEİ Üye Devletlerindeki Dijital Ekonominin Gelişim Beklentileri" konusuna ve Haziran 2018'de Tiran'da gerçekleştirilecek Elli Birinci Genel Kurul Oturumunda ele alınmak üzere bir Rapor ve Tavsiye Kararı hazırlanmasına ayrılmıştır.

5. KEİPA siber güvenlik konusunu 2012'de Bakü'de gerçekleştirilen Kırkıncı Genel Kurulunda ele almış ve parlamentoların bu alandaki işbirliğini güçlendirmedeki rolüne odaklanmıştır. Kabul edilen belgeler potansiyel sorunların çözümüne katkıda bulunma ve güvenli bir ortamda bilgi ve iletişim teknolojilerinin faydalarını azamiye çıkarırken sağladığı fırsatları geliştirmeyi sürdürülebilir kalkınmayı sağlamanın önemli bir unsuru olarak vurgulamaktadır. Bu belgeler aynı zamanda parlamentoların bilim, teknoloji ve inovasyon konularında sağlanan finansmana öncelik vermesi ve bu yolla bu tehditlere yeterli düzeyde yanıt verebilmek ve bunları gereğince ele alabilmek için yapılan araştırmaların kapsamını genişleterek bu çabalara hız vermesi gerektiğini de vurgulamaktadır.

6. Rapor, Azerbaycan, Bulgaristan, Gürcistan, Moldova, Romanya, Sırbistan, Türkiye, Ukrayna ve Yunanistan ulusal delegasyonlarının yaptığı katkılara dayanmaktadır. Bunlara ek olarak KEİPA Uluslararası Sekretaryasınca ilgili internet kaynakları ve yayınlardan referans materyalleri temin edilmiştir.

II. KEİ ÜYE DEVLETLERİNDEKİ DİJİTAL EKONOMİNİN GELİŞİM BEKLENTİLERİ

7. Siber güvenlik, bilgi ağlarının ve verilerin yetkisiz erişime karşı korunmasını sağlamaya yönelik araç ve stratejilerin bir kombinasyonunu ifade eder. Siber güvenliğin unsurları arasında erişim kontrolü, personelin eğitimi, raporlama, potansiyel risklerin değerlendirilmesi, penetrasyon testleri ve yetki talepleri sayılabilir. Siber güvenliğin en sorunlu unsurlarından biri telekomünikasyon sektörünün güvenliğini hedef alan tehditlerin niteliğindeki hızlı ve sürekli değişimdir. Bu konudaki alışılmış yaklaşım kaynakları bilgi güvenliğinin en önemli unsurlarına odaklamakta ve bilgisayar korsanı saldırısı tehditlerine karşı koruma sağlamaya çalışmaktadır. Dolayısıyla bugün siber güvenlik bilgi toplumunun daha da gelişmesi ve konsolidasyonu açısından bir ön şart niteliğindedir.

8. Siber alem global bilgisayar ağlarından oluşmakta olup bu ağlar fiber optik ve diğer kablolar ve kablosuz bağlantılar üzerinden kontrol edilmekte ve birbirlerine bağlanmaktadır. Siber alem interneti ve çeşitli bölgelerde veri aktarımı sağlayan ulus aşırı ağları birbirine bağlamaktadır. Ayrıca makineleri kumanda tabloları ve radyo frekans belirleme yoluyla birbirine bağlayarak veri alan ve kontrol eden sistemler de bulunmaktadır ve bunlara genel olarak Nesnelerin İnterneti adı verilmektedir. Siber alemdeki tehditler siber alemin kendisi kadar çeşitlilik sergilemekte ve ayrıntılı inceleme ve yanıt gerektirmektedir.

9. Bugünün dünyasında siber alem, bilgisayar ağlarını birbirine bağlayan global bilgi sisteminin bir parçası olan herkes açısından bir dikkat gerektiren bir alandır. Birbiriyle bağlantılı dijital bilgi ve iletişim altyapısı modern yaşamın neredeyse tüm alanlarının temelini oluşturmakta ve ekonomiye, kamusal altyapıya, kamusal ve ulusal güvenliğe önemli destek vermektedir. Birbirleriyle bağlantılı çalışan yüzbinlerce bilgisayar, sunucu, yönlendirici, ağ ekipmanı ve fiberoptik kablo sistemleri, tarım, gıda, su, halk sağlığı, acil durum hizmetleri, yönetim, bilgi ve telekomünikasyon, enerji, ulaştırma, bankacılık ve finans sektörleri, posta hizmetleri gibi bir çok alanda sistemlerin işleyişine destek vermektedir. Bu sistemlerin sürekli olarak incelenmesi ve izlenmesi gerekmektedir.

10. Sosyal medya da hızla gelişen alanlardan biri olarak insanlara iletişim ve bilgi alışverişi konusunda yeni fırsatlar sağlamaktadır. Ancak bir o kadar önemli olan bir diğer husus da siber güvenliğin sistemleri veri tabanlarının ve toplanan kişisel bilgilerin yetkisiz kullanımına karşı korumasını sağlamaktır.

11. Toplumlar ve insanlar hiç bir zaman bugün olduğu kadar birbirleriyle bağlantılı bir yapı içinde yer almamışlardır. Elektronik bilgi akışını sağlayan ağların neredeyse yaşamın her boyutuyla bağlantısı vardır. Bugün siber alem hayati sistemleri kontrol eden başlıca yapıdır. Kapsamlı ve kolay yönetilen elektronik alt yapının geniş kullanım alanı da güvenlik zaafı riskini artırmaktadır. Bilgi ve İletişim Teknolojilerinin dünya genelinde artan kullanımı bağlamında bilgi güvenliği dünya toplumları, devletler ve bireyler açısından başlıca sorun halini almaktadır. Dolayısıyla yapmamız gereken başlıca işlerden biri bu alandaki riskleri asgariye indirmektir.

12. Günümüzde karşılıklı bağlantıların ulaştığı boyut da bir yerdeki sorunların bir başka konumdaki bilgisayarları etkileyebilmesi potansiyelini doğurmakta; teknolojideki gelişmenin dinamizmi siber güvenlik endişelerini de beraberinde getirmektedir.

Günümüzde bilgisayar korsanları daha önce görülmemiş genişlikte bir yelpazeden araçlara sahip olup bunları en büyük etkiyi yapacak şekilde kullanabilmektedirler. İnternetin trafik kapasitesinin ve mobil cihazların sayısının sürekli olarak artması da çok geniş bir hedef yelpazesi doğurmakta ve bunları etkileyebilmenin farklı yollarını açmaktadır. Bu çerçevede sürekli olarak gelişen ve karmaşıklaşan tehditlere karşı etkili bir koruma sistemi geliştirmek gerekmektedir. Zararlı yazılımlar saldırganların savunmasız cihazlara hızla erişim sağlayıp veri çalabilmesini mümkün kılmaktadır. Modern teknolojiler, modern terörün temelini oluşturan yasa dışı finansal işlemlerin yapılabilmesine ve kontrolüne olanak tanımaktadır. Günümüzde teröristler basit bir klavye ile bile ciddi zarara neden olabilmektedirler. Dolayısıyla siber güvenliği ve bilgi ve iletişim teknolojileri alanında güvenliği geliştirmek tüm dünya açısından önemli bir görevdir. Bunun sonucu olarak da terör saldırılarındaki artışın ışığında bunları önlemeye ve ortadan kaldırmaya yönelik metotların geliştirilmesi de elzemdir.

13. Cisco firmasının güvenlik araştırmacıları, son yıllardaki siber suçlar hakkında verileri ve analizi ortaya koyan 2018 Bilgi Güvenliği Raporunu yayınlamış bulunmaktadır. Söz konusu rapora göre 2017'deki en önemli trendlerden biri verilerin ele geçirilmesi ve silinmesine olanak tanıyan zararlı yazılımların evrimi olarak öne çıkmıştır. Araştırmacılar bir yandan da karmaşık kum havuzu ortamlarını aşabilen ve tespit edilme ihtimalinin önüne geçmek için şifrelemeyi kullanan siber tehditlerin ortaya çıkışına da dikkat çekmektedir. Cisco'ya göre, Ekim 2017 itibarıyla küresel internet trafiğinin %50'si kadarı şifreli biçimde iletilmiştir. Aynı zamanda 400 binden fazla zararlı yazılımın analizi, Ekim 2017 itibarıyla trafiğin %70 kadarının şifreleme kullandığını göstermektedir.

14. Cisco'nun raporuna göre siber tehditlerden korunma bağlamında öne çıkan başlıca sorunlardan biri Nesnelerin İnterneti (IoT) aygıtlarını ve bulut hizmetlerini kullanan saldırılardır. Söz konusu raporda IoT aygıtlarının günde 24 saat çalıştığı ve neredeyse anlık olarak zararlı faaliyetler gerçekleştirmede kullanılabileceği belirtilmektedir. Saldırganların kullandıkları robot aygıt ağlarının ölçeğini sürekli olarak büyüttüğü ve karmaşık programlar ve zararlı yazılımlardan yararlanarak giderek daha gelişmiş hizmeti engelleme (DoS) saldırıları düzenleyebildiği bir ortamdan bahsedilmektedir.

15. Robot aygıt ağları, zararlı yazılımların bulaştığı makinelerden oluşan bilgisayar ağlarını ifade etmektedir. Robot yazılım, hedef bilgisayarda yetkisiz kullanım sağlamak üzere kurulmuş gizli bir yazılımı ifade eden bir terimdir. Robot yazılımları bilgisayarın kontrolünü ele geçirmek için gizlice kurulmakta ve gündelik rutin kullanımda tespit edilmeleri genellikle güç olmaktadır. Robot aygıtın ele geçirilmesi kullanıcının gereken dikkati göstermemesi sonucu gerçekleşebilmektedir; zira otonom robot yazılım yararlı bir diğer yazılımın bir parçası olarak yansıtılmaktadır. Robot yazılımlar bu tehditten şüphelenmeyen kullanıcıların dikkatini çekmeden çalıştırılmakta ve bir koruma kalkanı ile korunmaktadır. Koruma mekanizması alışılmamış program çalıştırma yollarına başvurmakta, sistem dosyalarının yerine geçmekte, ve otomatik indirme anahtarlarına erişim sırasında makineyi yeniden başlatmaktadır. Robot aygıt ağları siber suçluların etkin araçları arasında olup, bilgisayarları ele geçiren kötü niyetli kişilerin dünyanın herhangi bir yerinden kimliklerini saklayarak bu işi yapabilmesinden ötürü belirgin bir zaaf sergilememektedir.

16. Güvenlik altyapılarının giderek artan düzeyde karmaşıklaşması ve gelişen analitik olanaklarının ışığında her geçen gün daha fazla sayıda araştırmacı yapay zeka ve

bilgisayarın öğrenmesi teknolojilerinin kullanımını önermektedir. Cisco'ya göre güvenlik uzmanlarının %39'u tümüyle otomasyon teknolojilerine dayanmakta, %34'ü bilgisayarın öğrenmesi, %32'si ise yapay zeka araçlarını değerlendirmektedir. Siber tehditlere karşı tedbir alma bağlamında uzmanlar sürekli olarak düzeltici çalışmaları, ve mümkün olduğunca da açıkların kapatılmasını önermekte, bunların yanında düzenli olarak veri yedeklemesi yapılmasını ve bilgisayarın öğrenmesi ve yapay zeka olanaklarını da kapsayan gelişmiş güvenlik teknolojilerinin uygulamaya geçirilmesini tavsiye etmektedir.

17. Siber alemin sağlıklı bir biçimde işlemesi gelişim ve ilerleme açısından faydalıysa da, siber saldırılar güvenlik açıklarının yıkıcı etkiler doğurabilmesini ve ciddi sonuçlara yol açabilmesini mümkün kılmaktadır. Kritik önemdeki altyapıyı oluşturan sitelere yapılan saldırılar giderek daha sık görülmektedir. Bu tür saldırılarla mücadele edebilmek için güvenlik açığı sorununu yeterli düzeyde ele alacak daha geniş kapsamlı fırsatların ortaya konması gerekmektedir.

18. Siber alem ulusal güvenliğin de önemli bileşenlerinden biridir. Güvenli bir siber alem, tüm toplum, devlet, özel sektör ve halkın koordineli ve sonuç odaklı çabalarını gerektiren karmaşık bir stratejik sorundur. Siber güvenlik politikalarının, küresel bilgi ve iletişim altyapısının güvenlik ve istikrarıyla ilgili olduğu ölçüde siber alemdeki faaliyetlere olarak tehdit ve zaafların azaltılması, olaylara yanıt, dayanıklılık, bilgi güvencesi, hukukun uygulanması ve istihbarat misyonları gibi çeşitli unsurları kapsayan yönelik yeni standartlar ve stratejiler içermesi gerekmektedir.

19. Bir diğer sorunsa İnternet üzerinde çeşitli kanallarda akan verinin güvenliğini artırmaktır. Güvenlik sağlamaya yönelik tüm mühendislik yaklaşımlarının yanında izleme herhangi bir güvenlik sorununu hızlıca tespit etme yöntemlerine de yer verilmelidir. Siber güvenlik sisteminin başarısı, sadece sistemin bazı parçalarını korumaktan ziyade tüm sistemin güvenliğini anlamaya dayanır. Dolayısıyla siber suç ve siber terörle mücadele, dijital cephenin yanında kişisel, sosyal ve siyasi boyutta da yürütülmelidir.

20. Siber alemdeki güvenlik zaaflarını ele almak devletlerin temel sorumlulukları arasındadır. Ancak bu sistemlerin güvenliğinde ciddi ilerleme kaydedilmedikçe ya da bunların yapılanması veya işletimi boyutunda ciddi bir değişim söz konusu olmadıkça devletlerin kendilerini siber suç ve ihlallerin büyüyen tehdidine karşı koruyabilmesi de mümkün görünmemektedir. Devletler bir yandan siber güvenlik açıklarını ele almaya yardımcı olabilecek araştırmalara yatırımı artırırken bir yandan da ekonomideki ihtiyaçları ve ulusal güvenliğin gereklerini de karşılamalıdır.

21. Uluslararası Telekomünikasyon Birliği (ITU) her yıl Küresel Siber Güvenlik Endeksini yayınlamaktadır. Bu anketin sonuçlarına göre devletlerin siber güvenlik düzeyi başlıca beş alandaki göstergelere göre somutlaşmaktadır: hukuki, teknik, örgütsel, kapasite oluşturma ve işbirliği. 2017'de endeks 193 ülkeyi incelemiştir. Bu ülkeler arasında KEİ üyesi olanlar şu şekilde sıralanmıştır (siber güvenlik tehditlerinin düzeyine göre): Gürcistan - 8, Rusya - 10, Romanya - 42, Türkiye - 43, Bulgaristan - 44, Azerbaycan - 48, Ukrayna - 59, Yunanistan - 64, Moldova - 73, Arnavutluk - 89, Sırbistan - 90, Ermenistan – 111.

22. Dünyanın birçok ülkesi gibi KEİPA üye devletleri de inovasyonu ve teknolojik gelişmeyi teşvik ederken bir yandan da güvenlik ve özel hayatın gizliliğine ilişkin

hakları da öne çıkaran bir ortamı muhafaza etme bağlamında siber güvenlik sorunlarının üstesinden gelmek için kapsamlı tedbirler almaktadırlar. Konuyla ilgili inisiyatiflerin korunmasına yönelik olarak, bir dizi araştırma ve geliştirme faaliyetini de kapsayan bir yanıt mahiyetinde siber güvenlik düzeyini artırmaya yönelik büyük ölçekli program ve girişimler başlatmaktadırlar.

23. Ülkelerin karşı karşıya olduğu siber güvenlik sorunlarını ele almaya yönelik olarak bütüncül bir vizyon ve plan türetmek üzere çıkarları bir araya getirmek elzemdir. Siber güvenlikle ilgili riskleri azaltmaya yönelik politikaları geliştirmek şarttır. Ayrıca siber alemde güvenlik ihtiyacına yönelik olarak bütünleşik bir yaklaşım sağlamak ve risk ve tehditlerle ilgili olarak kamuoyunu bilinçlendirmek de önemlidir. Ayrıca ilgili mevzuatın oluşturulması ve tahkimi de gerekmektedir. Bir yandan da devleti, bankacılık, enerji ve ulaştırma sektörlerini, ticari yapıları ve telekomünikasyon sektörünü de kapsar şekilde ilgili tüm sektörlerden uzmanların etkileşimini sağlayan bir ağ oluşturmak da mühimdir.

24. 26 Eylül 2012 tarih ve 708 sayılı "Bilgi Güvenliği Faaliyetlerini Geliştirmeye Yönelik Tedbirler" hakkındaki ***Azerbaycan Cumhuriyeti*** Cumhurbaşkanlığı Kararnamesiyle Azerbaycan Cumhuriyeti Haberleşme ve Bilgi Teknolojileri Bakanlığına ülkede siber güvenliğin genel durumu konusunda düzenli incelemeler gerçekleştirme, kamuyu, özel sektörü ve diğer yapıları mevcut ve potansiyel siber tehditler hakkında bilgilendirme, ve global siber saldırılarla mücadelede teknik ve metodolojik destek sağlama yönünde talimat verilmiştir.

25. Bilgi altyapısı birimlerinin siber güvenlik faaliyetlerini koordine etme, ulusal düzeyde mevcut ve potansiyel elektronik tehditler hakkında bilgi verme, kamuyu, özel sektörü ve diğer yapıları siber güvenlik alanında eğitme ve onlara metodolojik destek sağlama amacıyla Azerbaycan Cumhuriyeti Haberleşme ve Bilgi Teknolojileri Bakanlığı bünyesinde bir koordinasyon merkezi olarak Elektronik Güvenlik Merkezi kurulmuştur.

26. 2016'da Merkez, Karşılıklı İlerleme Sağlamaya Yönelik Siber Güvenlik İttifakının (CAMP) üyeleri arasına katılmıştır. Bu kurumun ve siber alemde güvenlik sağlamak üzere kurulan ittifakların yardımıyla üyelere siber güvenlik, yeni siber tehditler, siber saldırılar ve bunlarla mücadeleye yönelik yeni yöntemler konularında gereken metodolojik destek sağlanmaktadır.

27. KEİ üye devletleri arasında siber güvenlik alanında işbirliği sağlamaya yönelik olarak şu öneriler getirilmiştir: KEİ üye devletlerinin siber güvenlik kurumları arasında, siber etkinlikler, siber saldırılar ve siber tehditler konusunda operasyonel bilgi alış verişini sağlamak üzere çok dilli bir internet platformu oluşturulması; KEİ üye devletlerinde siber güvenlik haftası organize edilerek sosyal ağların güvenliği ve kişisel bilgilerin korunması, istenmeyen e-postaları azaltmanın yolları, bilgisayarları bloke eden ve açmak için fidye talep eden yazılımlar ve bunlardan korunmanın yolları konularına eğilinmesi; okul ve üniversitelerde seminerler düzenlenmesi; kamuoyunun bilinçlendirilmesi; konuyla ilgili broşürlerin dağıtılması; KEİ üye devletlerinin ilgili kurumlarından uzmanların katılımıyla ortaklaşa eğitimlerin düzenlenmesi.

28. Avrupa Birliği üyesi olan ***Bulgaristan,*** Birliğin genel anlamda siber güvenliği geliştirmeye yönelik politika ve enstrümanlarının geliştirilmesi ve koordinasyonu süreçlerine katılmaktadır. Bulgaristan Yeni bir Avrupa Birliği Siber Güvenlik Ajansı kurulması ve dijital dünyadaki ürün ve hizmetlerin güvenle kullanılabilir olmasını sağlamaya yönelik yeni bir Avrupa sertifikasyon sisteminin hayata geçirilmesi

yönündeki önerileri aktif biçimde desteklemektedir. Estonya'nın AB Dönem Başkanlığı sırasında start verilen "Siber Güvenlik Paketi", içinde bulunduğumuz 2018 yılı içinde de Bulgaristan'ın AB Dönem Başkanlığı çerçevesinde değerlendirilmeye devam edecektir. Bulgaristan'da, Avrupa'da siber güvenlik konusundaki öne çıkan hususları değerlendirmek üzere bir Siber Sorunlar Konferansı düzenlenmesi planlanmaktadır.

29. Ulusal düzeydeki siber güvenlik standartları üst düzey ağ ve bilgi güvenliğine yönelik tedbirler konulu AB Yönergesinde ortaya konmuştur. Bulgaristan'da yürürlükteki mevzuat kapsamında, Elektronik Devlet Kurumunun yönlendirmesi çerçevesinde devlet kurumları arasında bir çalışma grubu oluşturulmuş olup, bu çalışma grubu Yönerge maddelerinin bir Siber Güvenlik Yasası taslağına entegre edilmesini amaçlamaktadır. 2009'da Bulgaristan Cumhuriyeti Bakanlar Kurulu kararıyla Ulusal Siber Güvenlik Koordinatörü pozisyonu oluşturulmuştur.

30. 2016'da Bulgaristan Cumhuriyeti Bakanlar Kurulu "Siber Sürdürülebilir Bulgaristan 2020" Ulusal Siber Güvenlik Stratejisini kabul etmiştir. Bu strateji çerçevesinde Bulgaristan Cumhuriyetindeki paydaşların ulusal siber sistem güvenliğini geliştirme boyutundaki sorumluluklarının artması ve açık ve güvenli bir siber alem hedefine ulaşılması öngörülmektedir. Siber tehditlerle mücadele üç aşamalı bir süreçtir. Bunların ilki (2016), ICT ile ilgili güvenlik hizmetleri ve kamu kurumlarının yanı sıra İçişleri Bakanlığı ve Savunma Bakanlığı, Ulaştırma, Bilgi Teknolojileri ve İletişim Bakanlığı ve Elektronik Devlet Kurumunu kapsayan bir Ulusal Siber Güvenlik Koordinasyon ve Organizasyon Ağının (NCSCON) kurulması suretiyle siber savunma sürecinin kurumsal bağlamda güçlendirilmesidir. Sonraki aşama iletişim ve bilgi sistemlerinin ve ulusal bağlamda kritik önem taşıyan altyapı unsurlarının gözden geçirilmesi de dâhil olmak üzere acilen alınması gereken tedbirlere odaklanmaktadır. Son aşama ise 2018-2019 döneminde Bulgaristan'da siber saldırılara yanıt verme bağlamında yeterli bir sistemin kurulmasını öngörmektedir. 2020'ye gelindiğinde ulusal düzeyde siber sürdürülebilirliğin ve bölge, Avrupa Birliği ve NATO ekseninde uluslararası düzeyde etkili etkileşimin sağlanması planlanmaktadır. Dört yıl içinde ülkenin bölgede siber güvenlik alanında liderliği üstlenmesi planlar arasındadır.

31. **Gürcistan** Hükûmeti, 2008'de ülkede siber alem bağlamında gerçekleştirilen büyük ölçekli siber saldırılar sonrasında kamuya açık BT sistemlerini korumaya yönelik çalışmalara büyük destek vermektedir. "Gürcistan'ın Ulusal Siber Güvenlik Stratejisi (2013-2015)" ve bu stratejiyle ilgili Eylem Planı 2013'te Ulusal Güvenlik Konseyinin yönlendirmeleri ile kabul edilmiştir. 2016'da, Devlet Güvenliği ve Kriz Yönetimi Konseyine bağlı Ulusal Güvenlik Konsept Belgelerinin Hazırlanması Kurumlar Arası Daimi Komisyonu 2017-208 Siber Güvenlik Stratejisini ve buna tekabül eden Eylem Planını hazırlamıştır. Söz konusu Strateji siber güvenliğin daha da tahkim edilmesi konusuna odaklanmaktadır. Yeni strateji, araştırma ve analizlerin kapsamını genişletmeye, yeni mevzuat hazırlamaya, kamuoyunu bu konuda bilinçlendirmeye, bilgi alış verişine hız kazandırma amacıyla siber güvenlik alanında eğitim ve uluslararası işbirliğini geliştirmeye, risk yaratan açıkları azaltmaya, ve siber alemde hasmane ya da zarar verici uygulamaları tespit ederek önlemeye yönelik stratejileri geliştirmeye odaklanmaktadır.

32. 2012'de "Bilgi Güvenliği" Kanunu kabul edilmiş ve böylelikle bilgi güvenliğini geliştirmeye yönelik etkin ve etkili tedbirlerin alınmasına yönelik çerçeve oluşturulmuştur. Söz konusu kanunla başlıca görevi Gürcistan Savunma Bakanlığının en

kritik Bilgi ve İletişim Teknolojileri (ICT) sistemlerini korumak olan Siber Güvenlik Bürosu kurulmaktadır. ICT sistemlerine yetkisiz erişim veya müdahaleler ile teknolojik aygıtların düşmanca kullanımı ülkenin Ceza Kanununda suç olarak tanımlanmıştır. Kişisel verilerin işlenmesi sırasında mahremiyet hakkı gibi insan hak ve hürriyetlerini korumaya ve ilgili devlet kurumlarının yetki ve sorumluluklarını belirlemeye yönelik olarak çıkarılan Kişisel Verilerin Korunması Kanunu, 2011'de Parlamento tarafından kabul edilmiştir. Kanun hükümleri uyarınca Gürcistan Adalet Bakanlığı Veri Alış Verişi Kurumu (cert.gov.ge) ve Gürcistan Savunma Bakanlığı Siber Güvenlik Bürosu Gürcistan'da siber güvenliği temin etmekle sorumlu tutulmuştur. 2012'de İçişleri Bakanlığı bünyesinde, siber suçlarla ilgili soruşturmaları yürütmek üzere Siber Suçlar Dairesi kurulmuştur. Söz konusu dairede, Avrupa Konseyi Siber Suçlar Sözleşmesine göre kurulmuş olan ve 24 saat temasa geçilebilecek bir İletişim Grubu da yer almaktadır.

33. 2013'te NATO İrtibat Bürosu (NLO) ile işbirliği içinde, Savunma Bakanlığından bir çalışma grubu, Estonyalı bir uzmanın da katılımıyla savunma sisteminde siber güvenlik konusunu incelemiştir. Bu çalışmaların sonucunda Siber Güvenlik Bürosunun kuruluş zeminini oluşturan bir yol haritası hazırlanmıştır. 2017'de ülke güvenliğine karşı yapılan siber saldırılara yanıt veren bir operasyonel ve teknik servis oluşturulmuştur. Siber Güvenlik Bürosu NATO ile gerek ikili gerekse çok taraflı çerçevede aktif bir işbirliği içindedir. Ofis iki akıllı savunma projesine katılmaktadır: zararlı yazılımlar hakkında bilgi alış verişine yönelik çok uluslu bir program (MN MISP) ve siber suçlar hakkındaki bilinç düzeyini artırmaya yönelik çok uluslu bir program (MN CD E & T).

34. ***Yunanistan***'da Siber Suçlar Birimi, Yunanistan Emniyet Teşkilatının siber güvenlik ve siber suçlarla mücadele konularıyla ilgilenen bağımsız bir alt birimidir. Başlıca amacı internet üzerinden gerçekleştirilen suçların ve diğer çevrimiçi suç davranışlarının önlenmesi, soruşturulması ve yargı süreçlerine tabi tutulmasıdır. Birim, vatandaşların korunması ve siber güvenlik alanlarında geniş bir yelpazede faaliyet gösteren beş daireden oluşmaktadır: İdari Destek ve Bilgi İşlem Dairesi, Yenilikçi Eylemler ve Strateji Dairesi, Elektronik İletişim ve Telefon İletişimi Güvenliği ve Yazılım ve Telif Hakkı Koruma Dairesi, Reşit Olmayanlara Yönelik Siber Güvenlik ve Dijital Soruşturmalar Dairesi, Özel Çalışmalar ve Elektronik Suçların Yargı Süreçlerine Tabi Tutulması Dairesi. Siber Suçlar Birimi siber suçları başarıyla soruşturmaktadır.

35. Yunanistan, Avrupa Konseyinin elektronik suçlarla mücadele alanında Siber Suçlara ilişkin Sözleşmesi hükümlerini ulusal hukuka geçirme sürecini tamamlamıştır. Yunanistan kurumsal bilgi ve iletişim kanalları üzerinden ikili ve çok taraflı işbirliği anlaşmalarına dayanarak suç konusunda sürekli bir bilgi alış verişi sağlanması yönünde aktif çaba sarf etmektedir. Europol'ün Avrupa Siber Suçlar Merkezi-EC3 ve İnterpol'ün Küresel İnovasyon Kompleksi kapsamında sağlanan mevcut araçlar ve hizmetler tam anlamıyla değerlendirilmektedir. Dijital güvenliği sağlamak ve devlet altyapısının korunması amacıyla kamu kurum ve kuruluşlarıyla yakın işbirliği yapılmaktadır.

36. Ulusal Siber Alem Acil Durum Müdahale Ekibi (CERT), siber saldırılarla mücadeleye yönelik bir kurumdur. Elektronik saldırıların ortaya çıkış sürecini kontrol altına almakta, bu saldırıları analiz ederek veri tabanlarının bilgi güvenliğini sağlamaktadır. Daha büyük ölçüde etkinlik sağlayabilmek amacıyla grup diğer ülkelerin CERT yapılanmalarının yanı sıra ülke içinde de diğer kamu kurumlarıyla işbirliği yapmaktadır. İçişleri Bakanlığı Güvenlik Çalışmaları Merkezi, Araştırma ve Teknoloji Vakfı (FORTH), Selanik Aristo Üniversitesi ve Yunanistan İnternet'teki İçerik Öz Denetim Kurumu (Safenet) ile AB'nin

DG HOME AFFAIRS Avrupa Programı kapsamında işbirliği yaparak Yunanistan Siber Suçlar Merkezini (GCC) kurmuştur. Merkez siber suçlar konusunda eğitimi büyük ölçüde geliştirme olanağı sunan koordineli yeni bir Avrupa inisiyatifinin bir parçasıdır.

37. ***Moldova Cumhuriyeti*** Hükûmeti, 31 Ekim 2013 tarih ve 857 sayılı Kararı ile Bilgi Toplumunun Gelişimine Yönelik Ulusal Strateji'yi "Moldova digitală 2020" (Dijital Moldova 2020) ve bu planın uygulanmasına yönelik olarak Bilgi Teknolojileri ve İletişim Bakanlığınca hazırlanan Eylem Planı'nı onaylamıştır. Moldova Cumhuriyetinin Siber Güvenliği Ulusal Programı 2016-2020 29 Ekim 2015 tarih ve 811 sayılı Hükûmet Kararı ile onaylanmıştır. Bu kararlar ve programlar, bilgi güvenliğini sağlama bağlamında ulaşılması gereken hedefleri ve siber güvenliğin temelini oluşturmaktadır. Bu hedeflere ulaşmak amacıyla hükûmet bilgi sistemleri için zorunlu tutulan asgari şartları ve mevcut bilgi sistemlerinin yeterli düzeyde koruma sağlaması için gerekenleri belirlemiştir (28.3.2017 tarih ve 201 sayılı Hükûmet Kararı).

38. Yüksek Güvenlik Konseyi 7.10.2014 tarih ve 01 / 1-02-05 sayılı kararıyla bilgi güvenliğinin sağlanmasının ulusal güvenliği sağlamanın önde gelen unsuru olduğunu ve Moldova Cumhuriyetinde vatandaşların bilgi teknolojisine ve elektronik iletişime güvenine dayanan bir bilgi toplumu inşa etmeye katkıda bulunduğunu teyit etmiştir. 18 Ağustos 2010 tarih ve 746 sayılı Hükûmet Kararı uyarınca Moldova-NATO Ortaklığına ilişkin güncellenmiş Bireysel Eylem Planı çerçevesinde Özel Telekomünikasyon Merkezi bünyesinde Siber Güvenlik Merkezi (CERT-GOV-MD) kurulmuştur.

39. CERT-GOV-MD'nin görevi, siber saldırılara ilişkin bilgi toplama ve analizi yoluyla siber alemde devlet kurumlarının bilgi güvenliğini sağlamak ve kamu kurumlarının bilgi kaynaklarını korumak için acilen alınması gereken etkin tedbirlerin kabulü olarak tanımlanmıştır. Merkez, ülkedeki bilgi sistemleri ve internet kullanıcılarına karşı gerçekleşmiş veya gerçekleşebilecek bilgisayar olaylarına ilişkin bilgi kabul etmekte ve bu bilgileri işlemekte, bilgisayarla ilgili tehditler karşısında bilginin korunmasına yönelik tavsiyelerde bulunmakta, kullanıcılara ve Moldova Cumhuriyeti devlet kurumlarına bilgisayar olaylarını soruşturmada yardımcı olmakta, ve bilgi güvenliği konusunda eğitimler düzenlemekte ve gerçekleştirmektedir.

40. Moldova Cumhuriyeti siber güvenlik alanında kurumsal kapasitesini artırma ve stratejik iletişim ve bilgi sistemlerini siber saldırılara karşı çabalarına devam etmekte ve NATO ile siber güvenlik ve modern güvenlik tehditleriyle mücadele alanında işbirliğini geliştirmeye sıcak bakmaktadır.

41. ***Romanya*** siber güvenlik tedbirlerinin uygulanmasına destek vermektedir ve Ulusal Siber Güvenlik Stratejisi uyarınca Ulusal Siber Güvenlik Sistemi (NCSS) bu alanda uzmanlaşan kamu kurum ve kuruluşlarını siber alemde güvenliği sağlamaya yönelik ulusal edimleri koordine etmek üzere bir araya getiren genel işbirliği çerçevesini oluşturur.

42. CERT-RO, Romanya Ulusal Bilgisayar Güvenliği Olaylarına Müdahale Ekibi ulusal siber alemi tehdit eden güvenlik olaylarını önleme, tespit etme ve bunlara müdahale etme amacını taşıyan bağımsız bir kuruluştur. Söz konusu ekip alınan uyarılara dayalı bir Erken Uyarı Sistemi işletmekte ve işleme konu edilen siber güvenlik uyarılarını veritabanında tutmaktadır. CERT-RO bilinçlendirme kampanyaları düzenlemekte, danışmanlık hizmetleri vermekte ve Romanya, Avrupa Birliği ve ötesinde diğer kurumlarla işbirliği yapmakta, ve bu yolla siber tehditler konusunda bilgi düzeyini

artırmayı ve olaylara verilen yanıtın düzeyini geliştirmeyi amaçlamaktadır. CERT-RO İletişim ve Bilgi Toplumu Bakanlığının koordinasyonunda faaliyet göstermekte olup tümüyle devlet bütçesinden finanse edilmektedir.

43. Avrupa Parlamentosunca 2016'da kabul edilen ağ ve bilgi sistemlerinin güvenliği Yönergesi (NIS) çerçevesinde İletişim ve Bilgi Toplumu Bakanlığı, CERT-RO'nun da desteğiyle Yönergenin iç hukuka aktarımına yönelik bir proje hazırlamış ve hazırlanan taslak yayınlanarak kamuoyuyla istişare sürecine sunulmuş olup halen onay aşamasındadır. Söz konusu proje, esas itibarıyla bilgi alış verişine ilişkin stratejik hedeflere ulaşma çabalarını kolaylaştırma ve bunların uygulanmasına yönelik kurumsal çerçevenin yanı sıra ulusal düzeyde ve Avrupa'dan ortaklarla işbirliği mekanizmalarını tesis etmektedir.

44. Avrupa 2020 Dijital Gündemi çerçevesinde Romanya öncelikli dört yönelim belirlemiştir: (1) e-Devlet, Siber Güvenlik, Bulut Bilişim, Açık Veri, Sosyal Medya; (2) Eğitim, Sağlık ve Kültür alanında ICT; (3) e-Ticaret, ICT alanında Araştırma, Geliştirme ve İnovasyon; (4) Geniş Bant Ağlar ve Dijital Hizmetler Altyapısı.

45. ***Sırbistan Cumhuriyetinde***, Bilgi Güvenliği Kanunu (6/16 ve 94/17 sayılı "Sırbistan Cumhuriyeti Resmi Gazetesi") yürürlükte olup, bilgi ve iletişim sistemlerinin kullanımı ve bilgi güvenliğini artırmaya yönelik tedbirleri düzenlemektedir. Kanuna göre Sırbistan'da bilgi güvenliğinden sorumlu kurum Ticaret, Turizm ve Telekomünikasyon Bakanlığıdır. Kanunla ayrıca Ulusal CERT (Elektronik İletişim ve Posta Trafiği Düzenleme Kurumu) ve kamu kurumlarına yönelik CERT (Bilgi Teknolojisi ve E-Devlet Dairesi) de kurulmaktadır. Ayrıca Yüksek Teknolojili Suçlarla Mücadeleye Yönelik Devlet Kuruluşlarının Yapılanması ve Yetkileri Kanunu (61/05 ve 104/09 sayılı "Resmi Gazete") ile Cumhuriyet Savcılığının ve İçişleri Bakanlığının Yüksek Teknolojili Suçlarla Mücadele konusuna odaklanan özel birimlerinin yetkileri de belirlenmektedir.

46. Sırbistan Cumhuriyeti Hükûmeti 2017-2020 Dönemi için Sırbistan Cumhuriyetinin Bilgi Toplumunu Geliştirme Stratejisini kabul etmiştir (53/17 sayılı "Sırbistan Cumhuriyeti Resmi Gazetesi"). Strateji Sırbistan Cumhuriyetinde bilgi güvenliğinin geliştirilmesi için başlıca dört öncelik alanı ortaya koymaktadır: (1) ICT sisteminin güvenliği, (2) vatandaşların bilgi güvenliği, (3) yüksek teknolojili suçlarla mücadele, (4) Sırbistan Cumhuriyetinin bilgi güvenliği, ve (5) uluslararası işbirliği. Sırbistan Cumhuriyeti Hükûmeti, bilgi güvenliği alanıyla ilgili kurumların temsilcilerinden oluşan Bilgi Güvenliği İşleri Koordinasyon Birimini kurmuştur. Koordinasyon Birimi bilgi güvenliğini artırmaya ve siber güvenlik alanında ilerleme kaydetmeye yönelik tedbirler almak üzere ilgili kurumlar arasında işbirliği sağlar.

47. Sırbistan Cumhuriyeti yüksek teknolojili suçlar alanında diğer devlet ve uluslararası kuruluşlarla işbirliği yapmaktadır. Sırbistan Cumhuriyeti Uluslararası Telekomünikasyon Birliği ve Avrupa Güvenlik ve İşbirliği Teşkilatının (AGİT) çalışmalarına katılmaktadır. Bu bağlamda, bilgi sistemlerine yapılan saldırıların önlenmesi ve bertaraf edilmesi amacıyla ulusal ve uluslararası merkezlerin bilgi ve deneyimlerinin paylaşılması yoluyla KEİPA üye devletlerinin arasında siber güvenlik alanındaki işbirliğinin geliştirilmesi önerilmektedir.

48. ***Türkiye***'de Siber Güvenlik Stratejisi esas itibarıyla şu ana alanlara odaklanmaktadır: siber savunma ve siber önleme operasyonları, siber suçlarla mücadele, kriz yönetimi,

internet ağ yönetimi, ilgili kurumlar arasında çalışmaların koordinasyonu. Hükûmetin başlıca amaçlarından biri siber güvenliği Türkiye'nin ulusal güvenlik sistemine entegre edebilmektir.

49. Siber güvenlik politikası ile ilgili olarak atılan en önemli adımlardan biri, Bakanlar Kurulunun "Ulusal siber güvenlik çalışmaların yürütülmesi, yönetilmesi ve koordinasyonu " hakındaki Haziran 2012 tarih ve 3842 sayılı Kararı olmuştur. Söz konusu Karar uyarınca, bir siber güvenlik politikası, stratejisi ve eylem planını hazırlamak üzere Siber Güvenlik Komisyonu (SGK) kurulmuştur. Ülkede siber güvenliği sağlama sorumluluğu Ulaştırma, Denizcilik ve Haberleşme Bakanlığına aittir. Siber Güvenlik Komisyonu Kararıyla, 2013'te, Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur.

50. 2013-2014 dönemi Ulusal Siber Güvenlik ve Eylem Planı, Türkiye'de ulusal siber güvenlik politikalarını etkileyen başlıca etkenleri dikkate almakta ve aşağıdaki hedefleri belirlemektedir: siber güvenlik alanında yeni kanunların kabulü ve mevcut kanunların geliştirilmesi; USOM bünyesinde bir siber olaylara müdahale ekibinin (SOME) kurulması; siber saldırının kaynağını ve etkisini tespit etmeye yönelik güvenilir yedekleme mekanizmalarının geliştirilmesi; kamu bilgi sistemlerinin güvenliğinin artırılması ve yeni teknolojilerin sağlanması; siber güvenlik alanında insani kapasitenin artırılması ve bilinçlendirme sağlamaya yönelik faaliyetlerin düzenlenmesi; siber güvenlik sağlamaya yönelik yerel teknolojilerin geliştirilmesi ve ulusal siber güvenlikten sorumlu kurumların çalışmalarının kapsamının genişletilmesi.

51. Siber tehditlerle daha etkili bir biçimde mücadele edebilmek bağlamında, siber güvenlik alanında kapasite geliştirme ve bilinçlendirme sağlamaya yönelik ikili ve çok taraflı işbirliğini artırmak şarttır. KEİ üye devletleri arasındaki işbirliği çerçevesinde aşağıdaki alanlara dikkat çekilmesi önerilmektedir: siber güvenlik konusundaki ulusal yasal çerçeve hakkında bilgi alış verişi; çalışma gezilerinin düzenlenmesi; uzman değişim programları; karşı tehditler konusunda istihbarat bilgilerinin alış verişi; siber güvenlik alanında ortak tatbikatlar düzenlenmesi; siber güvenlik alanında ortaklaşa konferans ve seminerler düzenlenmesi.

52. ***Ukrayna***'da yakın dönemde kabul edilen "Ukrayna'nın Siber Güvenliğinin Temel İlkeleri" hakkındaki Kanunda insanların, kamunun ve devletin kritik çıkarlarının korunmasını sağlamaya yönelik başlıca hukuki ve örgütsel zeminler, Ukrayna'nın siber alemdeki ulusal çıkarları, siber güvenlik alanında devlet politikasının başlıca hedef, yönelim ve ilkeleri, devlet kurumları, şirketler, kuruluşlar, örgütler, bireyler ve vatandaşların bu alandaki sorumlulukları tanımlanmaktadır.

53. Avrupa Konseyi ve Avrupa Birliğinin yürüttüğü "Siber Suçlar ve Doğuyla Ortaklık" projesi çerçevesinde, Siber Suçlar Sözleşmesinin gereğince uygulanabilmesini sağlamak üzere Ukrayna Ceza Muhakemeleri Usulü Kanununda yapılacak değişikliklere ilişkin taslak metin hazırlanmıştır. Elektronik ortamda delil toplamaya yönelik usullerin geliştirilmesi ve yargılama öncesi soruşturma sırasında mahkeme kararıyla telekomünikasyon kanallarından bilgilerin kaldırılmasına yönelik özel bir prosedürün hayata geçirilmesi önerilmektedir. Ayrıca elektronik verilerin hızlı bir biçimde sabitlenip depolanmasına yönelik prosedür de öngörülmektedir. Bunların yanında belirli (tespit edilmiş) bir bilgi kaynağının (bilgi hizmetinin) engellenmesine yönelik mekanizma da tanımlanmaktadır. Söz konusu Kanunun aynı zamanda kanunların icrasıyla sorumlu

kurumlar ve hizmet sağlayıcılar arasındaki ilişkilerin yanında polis, istihbarat ve karşı istihbarat kurumları arasındaki ilişkileri de düzenlemesi beklenmektedir.

54. Ukrayna Emniyet Teşkilatı, Ukrayna İstihbarat Teşkilatı, Adalet Bakanlığı, haberleşme ve enformasyon alanında devlet düzenlemelerini uygulamaktan sorumlu Ulusal Komisyon temsilcileri arasında da bir dizi çalışma toplantısı gerçekleştirilmiş ve bu toplantılarda mevzuatta yapılması öngörülen değişiklik önergeleri ele alınarak bunların daha da etkin hale getirilmesi için yorum ve öneriler getirilmiştir. Bunların yanında "Ukrayna Telekomünikasyon Odası" Birliği uzmanlarının katılımıyla bir çalışma toplantısı da gerçekleştirilmiştir. İşletmelerin bilgi güvenliği ve siber güvenlik sağlamaya yönelik faaliyetlere katılımını düzenlemeye yönelik tedbirler almak ve özellikle de devletin kriptolama ve bilginin teknik açıdan korunması konusundaki kontrolünü güçlendirmeye ve bu tür kurumların ürün, teknoloji ve hizmetlerinin kullanımını kısıtlamak amacıyla Emniyet Teşkilatı "Ukrayna'nın Siber Güvenlik Stratejisinin Uygulanmasına Yönelik Tedbirlerin Düzenlenmesi" konulu yönetmeliği hazırlamıştır.

55. Siber güvenlik yaklaşımları alanındaki önemli sorumluluklar arasında öneli kaynakların ve kritik önemdeki altyapının güvenliğini sağlamaya yönelik kapsamlı bir ulusal plan hazırlanması; özel sektöre ve diğer devlet kurumlarına kritik bilgi sistemlerinin devre dışı kaldığı durumlar için acil durum kurtarma planlarıyla ilgili olarak teknik destek verilmesi; devlet kurumları, yerel kurumlar ve özel sektör, üniversiteler ve kamuoyu da dâhil olmak üzere sivil toplum kuruluşlarına belirli uyarılar ve uygun korunma tedbirleri ve karşı tedbirler hakkında bilgi vermek üzere diğer devlet kurumlarıyla koordinasyon sağlanması; ve siber güvenliği destekler mahiyette yeni bir bilimsel anlayış ve teknolojilerin önünü açacak biçimde diğer kurumlarla birlikte araştırma ve geliştirme çalışmaları yürütülmesi ve bu çalışmalara finansman sağlanması sayılabilir.

56. Siber alemdeki unsurları korumak birden çok ülkenin ve bunların vatandaşlarının çabasını gerektirir. Siber alemi oluşturup destekleyen teknolojiler hızla gelişirken tehdit ve zaaflar da değişim göstermiştir. İyi uygulamaların paylaşımı ve yeni teknolojilerin değerlendirilerek uygulanması gibi işbirliğine dönük faaliyetler üzerinden en ciddi siber zaafları tespit etmek ve gidermek için koordineli çabalar sarf edilmelidir.

57. Ülkelerin ekonomileri ve ulusal güvenlik giderek bilgi teknolojilerine ve bilgi altyapısına daha çok dayalı bir hal almaktadır. Küresel ölçekte siber alem ekonominin tüm sektörlerinin faaliyetlerini desteklemektedir: enerji (elektrik, petrol ve doğal gaz), ulaştırma (demiryolu, havayolu, deniz taşımacılığı), finans ve bankacılık, bilgi ve telekomünikasyon, halk sağlığı, acil durum hizmetleri, su, kimya, savunma, sanayi, gıda, tarım, ve posta hizmetleri. Dolayısıyla bilgi ağlarına yapılan siber saldırıların kritik operasyonlar üzerinde ciddi etkileri olabilir. Bu tür saldırılara yanıt vermek ve zaafları gidermek için farklı düzeylerde bütünleşik yeteneklerin geliştirilmesi gerekmektedir.

Uluslararası İşbirliği

58. Uluslararası ölçekte siber güvenliği geliştirmenin başlıca araçlarından biri Avrupa Konseyinin 2001'de kabul edilen ve 2004'te yürürlüğe giren Siber Suçlar Sözleşmesi'dir. Söz konusu sözleşme ulusal yasal çerçevelerin uyumlu hale nasıl getirilebileceği ve siber suçlarla mücadele konusunda uluslararası işbirliğinin unsurları hakkında yönlendirmeler sağlamaktadır. Bu yasal enstrüman hem pratik hem de siyasi açıdan önem arz etmektedir. Siber suçlarla mücadeleye yönelik olarak ilgili ulusal yasal çerçevelerin oluşturulmasına dair ilkeleri ortaya koymasıyla bu konuda Avrupa'da geçerli kuralların başka alanlara da

uyarlanması açısından faydalı bir araçtır. Dahası, Sözleşmeye taraf olmak siber suçları işleyenlerin iadesi de dâhil olmak üzere operasyonel konularda uluslararası işbirliğini kolaylaştırmaktadır. Sözleşmenin siyasi açıdan önemiyse siber güvenlik konularındaki bağlayıcı tek uluslararası sözleşme olmasından ve Sözleşmeye taraf olmanın ilgili ülkenin mevzuatını uluslararası düzenlemelerle uyumlu hale getirme ve siber suçlarla ciddi anlamda mücadele etme yönündeki kararlılığını göstermesinden kaynaklanmaktadır. Avrupa Konseyi, özel sektör ve üye devletlerle birlikte Sözleşmenin dünya genelinde kabulünü teşvik etmeye yönelik bir Küresel Siber Suçlar Projesine start vermiştir. Söz konusu Sözleşmeye katılan devletlerin sayısı artmakta ve bu ülkeler suç örgütlerini ve kendi topraklarında göz yumdukları aracı yapılanmalar üzerinden siber saldırıları teşvik eden hükûmetleri caydıran önemli bir yapı teşkil etmektedir. Sözleşme, 1 Mart 2006'da yürürlüğe giren Bilgisayar Sistemleri üzerinden gerçekleştirilen Irkçı ve Yabancı Düşmanı Nitelikteki Fiiller Protokolü ile tamamlanmaktadır. *(Rusya dışında tüm KEİ üye devletleri Sözleşmeyi imzalamış ve onaylamıştır; Azerbaycan, Bulgaristan, Gürcistan ve Rusya dışında tüm KEİ üye devletleri Protokolü imzalamış ve onaylamıştır; Türkiye Protokolü imzalamış ancak henüz onaylamamıştır).*

59. Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) siber güvenlik konusunu 2008'de ele almaya başlamıştır. O tarihten bugüne kadar AGİT üyesi devletler siber güvenlik konusunda çok sayıda üst düzey toplantı gerçekleştirmiş ve bu toplantılarda siber güvenlik konusunda bilinç düzeyini artırma, ülkelerin siber suçlar ve terörle mücadele alanında kapasitelerini geliştirmeleri ihtiyacı, ve siber alemde devletlerin sorumlu davranışının ne şekilde olabileceği gibi konular ele alınmıştır. AGİT bünyesinde kabul edilen güven artırıcı tedbirler uluslararası ölçekte bilgi güvenliğini sağlamanın başlıca araçları arasındadır. Güven artırıcı tedbirlerin amacı bilgi ve iletişim teknolojilerinin kullanımı sırasında çatışma risklerini azaltmaktır. Teşkilatın bu konuda, AGİT Daimi Konseyinin 2012 tarih ve 1039 sayılı Kararı uyarınca kurulmuş bir gayrı resmi çalışma grubu bulunmaktadır. 2016'da, "AGİT bünyesinde bilgi ve iletişim teknolojilerinin kullanımından kaynaklanan çatışma risklerini azaltmaya yönelik Güven Artırıcı Tedbirler" konusunda 1202 sayılı Karar kabul edilmiştir.

60. Dünyanın neredeyse tüm ülkelerinin çıkarlarını etkileyen küresel siber güvenlik meseleleri Birleşmiş Milletler şemsiyesi altında da ele alınmaktadır. BM Genel Kurulu siber güvenlik konusunda kararlar almıştır. 2009'da kabul edilen "Uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler" konulu 64/386 sayılı BM Kararı, uluslararası güvenlik bağlamında siber güvenlik konusunda değerlendirmelere devam edilmesini ve bu konuda daha kapsamlı tavsiyeler ortaya koyacak bir uzmanlar grubu oluşturulmasını önermektedir. 2010'da, Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanındaki Gelişmeler Konusunda Devletlerin Uzmanlarından oluşan BM Grubu ülkeleri bilgi güvenliği ve uluslararası işbirliğini geliştirmek için birlikte çalışmaya davet eden bir rapor hazırlamıştır. Uluslararası güvenlik sisteminin kilit unsurlarından biri olarak uluslararası bilgi güvenliğine önem veren BM Siber Güvenlik alanında bir Sözleşme hazırlamak için çalışmaktadır.

61. NATO, bu alandaki diğer strateji belgeleri ve faaliyetlere zemin oluşturan ilk Siber Savunma Politikasını, 2007'de geliştirmiştir. NATO, yeni stratejik ortama hızla uyum sağlayan ilk uluslararası örgüt olup, İttifak Üyesi Devletlerin ulusal güvenliği açısından büyük önem taşıyan alışılmışın dışındaki güvenlik tehditlerini fark etmiştir. NATO'nun 2007 Siber Savunma Politikası NATO'nun kendi ağlarının siber savunma yeteneklerini

geliştirmeye dönük hedefler belirlemiş ve üye devletlerle siber savunma konularında istişare için gereken ilk mekanizmaları oluşturmuştur. Kasım 2010'daki Lizbon Zirvesinde kabul edilen NATO Strateji Konsepti, NATO'nun siber saldırı tehdidine yanıt vermeye yönelik çabalarını hızlandırması gereğini vurgulamaktadır. Lizbon Zirvesi NATO'yu ve Müttefikleri yeni güvenlik sorunlarını ele alma yükümlülüğüne sokmakta ve diğer hedeflerin yanı sıra İttifakın siber gündemi için son derece iddialı bir yol haritası çizmektedir. NATO'nun tüm askeri ve sivil yapılarını merkezi koruma sistemi altına almak, savunma planlama sürecine siber bileşen eklemek ve bilgi paylaşımı ve erken uyarı olanaklarını geliştirmek bu yol haritası kapsamında yer alan unsurlardır. 2017'de NATO İşbirliğine Dayalı Siber Savunma Mükemmellik Merkezi Estonya'nın Tallinn kentinde kurulmuş ve Avrupa'da siber güvenlik alanında başı çeken girişim konumunu almıştır. Merkez her yıl, siber savunma alanındaki uzmanlar için dünyanın en büyük siber savunma tatbikatı olan "Kilitli Kalkanları" gerçekleştirmektedir. Merkez ayrıca siber savunma konusunda bir doktrin geliştirmekte olup bu kapsamda saldırı durumunda ülkelerin izleyeceği yolu çizen tek bir algoritma belirlenmektedir. Yeni doktrinin 2019'da NATO tarafından onaylanması beklenmektedir. NATO ve AB modern siber tehditlere yanıt verebilme yeteneklerini test eden paralel ve koordineli tatbikatlar yürütmektedir.

62. Mayıs 2010'da Avrupa Komisyonu tarafından, Avrupa'da ekonomik büyümeyi desteklemek ve Avrupa'daki vatandaşlara ve işletmelere dijital teknolojinin etkisini azamiye ulaştırmada destek vermek amacını güden Avrupa Dijital Gündemine (DAE) start verilmiştir. 2013'te Avrupa Birliği bir Siber Güvenlik Stratejisi geliştirmiş ve onaylamıştır. Avrupa Birliğinin Siber Güvenlik Stratejisinin amacı: Açık, Güvenli ve Emniyetli bir Siber Alem AB üye devletlerinin siber güvenlik alanındaki dayanıklılık ve kapasitesini artıracaktır (siber suçlarla mücadeleye hız kazandırmak, etkili bir güvenlik altyapısı tesis etmek, siber güvenlik alanında uluslararası politika ilkelerini değerlendirmek). 2017'de yeni sorun ve teknolojileri de dikkate alacak şekilde mevcut stratejiyi güncelleme yönünde karar alınmıştır. Avrupa Komisyonu siber güvenlik alanında mesafe kat etmeye yönelik olarak bir dizi tedbir önermiştir. AB Siber Güvenlik Ajansının kurulması da bunlardan biridir. Ajans, mevcut Avrupa Ağ ve Bilgi Güvenliği Ajansının (ENISA) yapısı üzerine kurularak AB ülkelerine siber saldırılarla mücadelede yardımcı olacaktır. Bilgisayar Acil Durum Müdahale Ekipleri (CERT) kritik önemdeki bilgi altyapısını korumaya yönelik kilit bir araç olarak görülmektedir. Bu ekipler AB ülkelerinde halihazırda oluşturulmuş olup devlet ve vatandaşlara güvenlik hizmetleri sağlayan başlıca yapı olmanın dışında eğitim faaliyetleri de yürütmektedirler. Üye devletlerse siber güvenliği sağlamak için gereken ulusal kapasite ve kaynakların mevcut olmasını sağlamaktadır.

III. SONUÇ

63. Son birkaç yılda siber alemdeki tehditler ciddi bir artış göstermiştir. Siber alemin hayatın neredeyse tüm alanlarında artan önemini göz önünde bulunduran ülkeler ve uluslararası örgütler bilgi sistemlerinin çalışmasını kesintiye uğratan durumlara karşı koruma sağlamak ve siber alemde güvenlik müdahaleleri yapabilmek için tasarlanan politikalar geliştirmeye başlamıştır.

64. Güvenli ve emniyetli bir internet sistemi ekonomiler ve toplumlar açısından çok önemlidir. Siber alemi oluşturan altyapı tasarımı ve gelişimi itibarıyla global niteliktedir. Siber alemde ulusal sınırlar pek bir şey ifade etmemektedir. Siber alemin küresel niteliğinden dolayı ortaya çıkan zaaflar tüm dünyaya açık ve istismar etmek isteyen

herkesin erişebileceği bir nitelik almaktadır. Siber güvenliği sağlamak gerek ulusal gerekse uluslararası düzeyde devletler, işletmeler ve toplumlar açısından çözülmesi gereken bir sorundur.

65. Tüm ülkelerin bilgi güvenliği alanında çalışanların eğitimi ve becerilerine ve kapasitelerini artırmaya yatırım yapması ve kamu, özel sektör ve akademide işbirliğini sağlaması gerekmektedir. Siber güvenlik tehditleri ve zaaflarını azaltmaya yönelik programların yanı sıra siber alem güvenlik bilincini oluşturma ve eğitime yönelik programların uygulanması elzemdir. Siber güvenlik konusunda global kültürün teşvik edilmesi, desteklenmesi, geliştirilmesi ve kararlılıkla uygulanması gerekmektedir.

66. Siber güvenlik alanındaki kanun ve yönetmeliklerin kabulü ve sürekli olarak güncellenmesi gerekmektedir, zira yalnızca kanunların kabulü ve uygulanması günümüzün siber güvenlik sorunlarının üstesinden gelmek için yeterli değildir. Siber güvenlik konusu, kamu ve özel sektör arasında ortaklığın yanı sıra uluslararası ölçekte işbirliği ve kuralların siber güvenlik stratejilerinin temel bileşenleri arasında yer bulmasını gerektirmektedir.

67. Bilgisayarlar, akıllı telefonlar ve tabletler gibi çok çeşitli cihazlarla donanmış bağlantılı bir dünyada herkes aynı iletişim kanallarını paylaşmakta ve her bir tüketici siber alemde kendi alanının güvenliğini sağlamada rol üstlenmektedir. İnternetin ve diğer dijital kaynakların korunması paylaşılan bir sorumluluktur. Siber güvenliğin ilgili kullanıcının siber alemdeki sorumlu davranışı ile başladığı unutulmamalıdır.

68. Daha güçlü bir siber güvenlik yapısı sağlamaya yönelik çabalara hız kazandırmak, siber saldırılara verilen yanıt bağlamında koordinasyonu geliştirmek, bilgi altyapısını korumada ortaklıkları teşvik etmek ve siber saldırıların ortaya çıkma sürecinde bunları izleyip önlemeye yönelik ulusal ve uluslararası sistemlerin kurulmasını desteklemek son derece önemlidir. Siber alemde güvenlik açıkları son derece somut, ciddi ve hızla büyüyen bir sorundur.

69. Günümüzde, küresel ölçekte bilginin giderek artan önemi toplumun gelişiminin belirleyici trendleri arasındadır. Bu bağlamda bilgi ve iletişim teknolojilerinin güvenliği uluslararası gündemin başlıca odak noktalarından biri halini almaktadır. Siber güvenlik dünya toplumlarını bir araya getiren bir konu olup, siber tehditlerin gerçek tehlikesini daha iyi anlayan bir perspektif geliştirmek yoluyla gündem gerçek anlamda güvenilir ve güvenli bir bilgi ortamı yaratmak üzere şekillendirilebilir.