Doc.: GA40/LC40/REP/12/tr

RAPOR *

KEİ Üye Devletlerinde Bilgi (Siber) Güvenliğinin Geliştirilmesinde Parlamentoların Rolü

Raportör: Sn. Mihail Emelyanov, Komisyon Başkan Yardımcısı, Rusya

* *Hukuki ve Siyasi İşler Komisyonu'nun Kırkıncı Toplantısı tarafından, 17 Ekim 2012'de, Atina değerlendirilen ve 27 Kasım 2012'de Bakü'de Kırkıncı Genel Kurul tarafından kabul edilen Metin.*

I. GİRİŞ

Bilgi teknolojilerinin etkisindeki küresel yükseliş bağlamında bu alanın güvenliği, küresel topluluk, her devlet ve her birey için temel bir soruna dönüşmektedir. Yeni bilgi ve iletişim teknolojileri, yepyeni fırsatların kapısını açmaktadır. Bilginin çok-katmanlı kanalları, tüm dünyada milyonlarca kişinin yararına olan kapasite gelişiminin artmasını teşvik etmekte ve daha yüksek düzeyde kalkınmayı hedef olarak getirmektedir. Bilgi teknolojilerine bağımlılık yaşamın neredeyse her alanında, her yıl artmakta ve bununla birlikte siber alanla ilgili sorunlar daha da küresel bir nitelik kazanmaktadır. Sonuç olarak siber güvenlik riskleri, 21inci Yüzyılın en ciddi ekonomik ve ulusal güvenlik sorunlarından bazılarını ortaya çıkarmaktadır.

Hukuki ve Siyasi İşler Komisyonu, teknolojik ilerlemelerin bu sosyal geçişli etkileri ve sonuçları ışığında 4 Nisan 2012'de Tiflis'te yapılan Otuz Dokuzuncu Toplantısı'nda KEİ üye devletlerinde siber güvenlik sorununa, bu süreci parlamenter katkı perspektifinden ele almaya karar vermiştir.

Bu itibarla Komisyon'un 17-18 Ekim 2012'de Atina'daki Kırkıncı Toplantısı, Genel Kurul'un Kasım 2012'de Bakü'deki Kırkıncı Toplantısı'nda Rapor'un ve Tavsiye Kararı'nın görüşülmesi düşüncesiyle "KEİ Üye Devletlerinde Bilgi (Siber) Güvenliğinin Geliştirilmesinde Parlamentoların Rolü" konusuna ayrılmıştır.

KEİPA, Asamble faaliyetleri çerçevesinde bilgi toplumunun güçlendirilmesi ve teknolojik kalkınma konusuna özel bir önem atfetmektedir; ve bilgi ve iletişim teknolojilerinin güvenli bir ortamda herkese sağladığı faydaların maksimize edilmesi ve fırsatların geliştirilmesi amacıyla güvenli bilim, teknoloji ve yenilik sistemlerinin güvence altına alınmasının yanısıra bu alandaki potansiyel sorunlarla mücadeleye katkıda bulunma sorumluluğunu paylaşmayı vurgulayan ilgili raporlar ile tavsiye kararlarını[1] kabul etmiştir.

Hazırlanan Rapor'da Gürcistan, Romanya, Rusya, Sırbistan ve Ukrayna ulusal delegasyonlarının yaptığı katkıdan yararlanılmıştır. Bununla birlikte, KEİPA Uluslararası Sekreteryası tarafından ilgili internet kaynakları ve yayınları üzerinden referans belgeleri edinilmiştir.

II. KEİ ÜYE DEVLETLERİNDE BİLGİ (SİBER) GÜVENLİĞİNİN GELİŞTİRİLİMESİNDE PARLAMENTOLARIN ROLÜ

1. Çağdaş dünyada siber alan, pratikte herşeye ve herkese dokunmaktadır. Dünya çapındaki internet ağı, bilgisayar ağları arasında karşılıklı işleyişi mümkün kılan bir gezegen bilgi şebekesidir. Yeni bilgi teknolojileriyle uzay ve zaman sıkıştırılarak bol miktarda küresel bilgiye ışık hızında erişim ve anlık bilgi alışverişi imkanı sağlanmıştır. Ancak karşılıklı bağlantılardaki bu genişlik, bir yerdeki sorunun başka bir yerdeki bilgisayarları etkileme potansiyelinin de olduğu ve teknolojik gelişmenin dinamizmiyle birlikte siber güvenlik endişelerini de beraberinde getirdiği anlamına gelmektedir.

---

[1] *Karadeniz Bölgesi'nde İletişimin Geliştirilmesi hakkında Rapor ve 45/2000 sayılı Tavsiye Kararı; KEİPA Üye Devletlerinde Küreselleşme Sorunları ve Beklentileri hakkında Rapor ve 60/2002 sayılı Tavsiye Kararı; Bilgi Toplumu, Yeni Teknolojilerin Rolü hakkında Rapor ve 66/2002 sayılı Tavsiye Kararı; Karadeniz Bilgi İttifakı hakkında Rapor ve 71/2003 sayılı Tavsiye Kararı; KEİ Üye Devletleri Arasında Yüksek Teknolojiler Alanında İşbirliği hakkında Rapor ve 95/2007 sayılı Tavsiye Kararı; Parlamentoların Bilimsel ve Teknolojik İlerlemenin Arttırılması Amacıyla Yasama Desteği Sağlamadaki Rolü hakkında Rapor ve 121/2011 sayılı Tavsiye Kararı.*

2. Toplumlar ve bireyler, hiçbir zaman bugün olduğu kadar birbirine bağlanmamıştır. Elektronik bilgi akışı ağları, neredeyse yaşamın her alanında kök salmıştır. Küresel düzeyde birbirine bağlanmış bulunan ve siber alan olarak bilinen dijital bilgi ve iletişim altyapısı, günümüz faaliyetlerinin neredeyse hepsinde yer bulmakta ve ekonomi, sivil altyapı, kamu güvenliği ve ulusal güvenlik için kritik destek sağlamaktadır. Siber alan; birbirine bağlı yüzbinlerce bilgisayar, tarım, gıda, su, kamu sağlığı, acil durum hizmetleri, kamu, bilişim ve telekomünikasyon, enerji, ulaştırma, bankacılık ve finans ve posta hizmetleri, v.s. sektörlerindeki sistemlerin işleyişini idare eden servis sağlayıcı, 'router', anahtar ve fiber optik kablolardan oluşmaktadır. Günümüzde siber alan, inovasyon ve refah platformu olmanın yanısıra kritik altyapıların belkemiğini ve kumanda sistemini de oluşturmaktadır.

3. Diğer yandan bilgisayar ve iletişim alanındaki gelişmeler, en karmaşık siber güvenlik sorunlarından bazılarını öne çıkarır olmuştur. Daha gevşek düzenlenmiş dijital altyapının daha çok kişiye ulaşmasıyla birlikte birtakım açıklar daha fazla risk oluşturmaktadır. Sağlıklı işleyen bir siber alan, kalkınma ve ilerleme için yararlı olsa da siber saldırılar, maruz kalınan açıkları yıkıcı niteliklere dönüştürebilmekte ve ciddi sonuçlara yol açabilmektedir. Bu gibi saldırılara karşı konulması ve aynı zamanda her bir vatandaşın ve daha geniş anlamda da halkların bilgi teknolojisi devriminin tam potansiyelini kavraması için zayıflıklara yönelik güçlü bir kapasite geliştirilmesi gerekmektedir. Bu itibarla siber tehditlerle ve açıklarla ilgili uzun vadeli tehditleri ele almak için siber tehdit analizinin geliştirilmesi bir zorunluluktur.

4. Siber alan güvenliği, ulusal güvenliğin en önemli unsurlarından biridir. Siber alanın güvenli ve emniyetli hale getirilmesi, bütün bir toplumun – devlet, özel sektör ve vatandaşlar dahil - eşgüdümlü ve yoğunluklu çabasını gerektiren, zorlu bir stratejik sorundur. Siber güvenlik politikaları, siber alan güvenliğiyle ve bu alandaki faaliyetlerle ilgili stratejileri, politikaları ve standartları içermeli; ve tehditleri hafifletmenin, açıkları azaltmanın, uluslararası katılımın, hızlı tepkinin, direncin ve bilgisayar ağı işlemleri, bilgi güvenliği, hukuki yaptırımları ve istihbarat misyonları dahil düzeltme politikalarının ve faaliyetlerinin bütün bir yelpazesini kapsamalıdır, zira bu konular küresel bilgi ve iletişim altyapısının güvenliğiyle ve istikrarıyla ilişkilidir.

5. Uzun bir listeye sahip siber güvenlik önceliklerini ele alırken yenilikçi bir yaklaşım geliştirmek önemlidir. Başka bir sorun da internet üzerindeki çeşitli kanallarda dolaşan verilerin güvenliğinin sağlanmasıdır. Güvenliğin sağlanmasına yönelik bütün mühendislik yaklaşımlarına, her türlü güvenlik açığının takip edilmesine ve hızla tespit edilmesine dair yöntemler eşlik etmelidir. Siber güvenlik sisteminin başarısı, unsurlardan bazılarının değil bütün bir sistemin güvenliğinin kavranmasına bağlıdır. Sonuç olarak siber suçlara ve siber terörizme karşı dijital cephenin yanısıra kişisel, toplumsal ve siyasi cephelerde de savaşılmalıdır.

6. Siber alandaki kırılganlıkları ele almak ve bilgi teknolojisi devriminin tam potansiyelinin küresel topluluk tarafından fark edilmesini sağlamak, hükümetlerin temel sorumluluğudur. Bu sistemlerin güvenliğinde önemli bir ilerleme kaydedilmeden veya yapılandırılma veya uygulanma biçimlerinde ciddi bir değişikliğe gidilmeden sözkonusu devletlerin kendilerini siber suçların ve müdahelelerin artan tehdidine karşı koruyabilmesi şüphe götürür. Hükümetler, bir yandan ekonomik gereksinimleri ve ulusal güvenlik gerekliliklerini karşılarken diğer yandan da siber güvenlik açıklarıyla mücadeleye yardımcı olacak araştırmalara daha fazla yatırım yapmalıdırlar.

7. Hükümetlerin, ülkelerinin karşılaştığı siber güvenlik sorunlarıyla mücadele etmeye yönelik bütüncül bir bakış ve plan oluşturmaları için birbiriyle çelişen menfaatleri bütünleştirmeleri gerekmektedir. Siber güvenlikle ilgili riskleri hafifletecek politikalar geliştirilmesi önem teşkil etmektedir. Tehditler ve riskler hakkında daha fazla toplumsal bilinç oluşturmak ve siber alan güvenliğine yönelik bütünleşik bir yaklaşım geliştirmek de önemlidir.

8. KEİPA üye devletleri, siber güvenlik sorunlarıyla mücadelelerinde diğer birçok ülkede olduğu gibi kapsamlı tedbirler almıştır. Bir yandan güvenliği, emniyeti ve gizlilik haklarını desteklerken diğer yandan da inovasyonu ve teknolojik gelişmeyi teşvik eden bir ortamı koruma paradoksuyla karşı karşıyadırlar.

9. Örneğin Romanya'da Parlamento, 2008 yılında bilgi suçlarıyla mücadele hakkında 298 sayılı Yasa'yı kabul etmiş, ancak bu yasa 2009 yılında Anayasa Mahkemesi tarafından reddedilmiştir. Yasa, tekrar kamuoyunun görüşüne sunulmuş fakat 2011 yılında bu kez Senato tarafından reddedilmiştir. Yasanın, 2012 yılında Temsilciler Meclisi Hukuk Komisyonu'nun yaptığı iki değişiklikle geçmesinin ardından, Yasa Cumhurbaşkanı tarafından ilan edilmiştir. Genel ve işlenmiş verilerin kamusal telefon ve internet ağı tedarikçileri tarafından korunması hakkında 298/2012 sayılı Yasa'nın yeni versiyonunda bütün telekomünikasyon ve İnternet hizmeti tedarikçilerinin bütün veri trafiğini (telefon görüşmelerinin ve mesajların içeriği hariç) altı ay süreyle kayıtlı tutmasına ve bu verilerin ulusal güvenlik kurumlarına gönderilmesi için resmi talepte bulunulmasına vurgu yapılmaktadır.

10. Rusya'da bilgi güvenliğinin artırılmasıyla ilgili sorumlulukların yerine getirilmesi amacıyla *Rusya Federasyonu'nun Bilgi Güvenliği Doktrini* Rusya Federasyonu Devlet Başkanı tarafından onaylanmıştır. Doktrin'in birinci bendine göre Rusya Federasyonu'nun bilgi güvenliği kavramı, bilgi alanındaki ulusal çıkarların devlet tarafından korunması ve aynı zamanda birey, toplum ve devlet menfatleri arasında bir denge kurulması anlamına gelmektedir. Bilgi güvenliği, Rusya'nın ulusal güvenliğinin bütünleşik bir parçasıdır. 2008 yılında Rusya Federasyonu Devlet Başkanı, *Bilgi Toplumunun Geliştirilmesi için Strateji*'yi kabul etmiştir. Bilgi alanında ulusal güvenliğin sağlanması, ülkenin önceliklerinden biridir. Ulusal güvenlik alanındaki yönetimin kapsamını şu hukuki düzenlemeler belirlemektedir: "Rusya Federasyonu Hükümeti hakkında" Federal Anayasa Yasası (md. 23); "Rusya Federasyonu'nun Adli Sistemi hakkında" Federal Anayasa Yasası; "Rusya Federasyonu'nda İnsan Hakları Komiserliği hakkında" Federal Anayasa Yasası (md. 24); "Federal Güvenlik Hizmetleri hakkında" Federal Yasa, "Güvenlik hakkında" Federal Yasa, "Rusya Federasyonu'nda Kamu Kovuşturması hakkında" Federal Yasa, "Polis hakkında" Federal Yasa, "Rusya Federasyonu Sayıştayı hakkında" Federal Yasa, v.s. "Devlet Sırrı Olarak Sınıflandırılan Bilgiler Listesinin Onaylanması hakkında" 30.11.1995 tarihli ve 1203 sayılı (21.09.2012 tarihli değişik) Rusya Federasyonu Devlet Başkanlığı Kararnamesi, devletin Rusya güvenliğini etkileyebilecek olan askeri politika, dış politika, ekonomi, istihbarat, karşı istihbarat ve operasyonel araştırma faaliyetleri alanındaki çalışma listesini ortaya koymaktadır. Bilgi alanında insan haklarını ve özgürlüklerini, örgütlenme haklarını teşvik edecek tedbirler, "Kişisel Veriler hakkında" Yasa, "Kitlesel Medya hakkında" Yasa, "Çocukların, sağlıkları ve gelişimleri için zararlı bilgilerden korunması hakkında" Yasa, "İletişim hakkında" Yasa, "Bazı türlerde faaliyetlere ruhsat verilmesi hakkında" Yasa, Rusya Federasyonu Medeni Kanunu, v.s. ile tespit edilmiştir.

11. Sırbistan'da bilgi güvenliği alanındaki mevcut hukuki düzenlemeler, Veri Gizliliği Yasası ("Sırbistan Cumhuriyeti Resmi Gazetesi", Sayı No. 104/09), Kişisel Verilerin Korunması hakkında Yasa ("Sırbistan Cumhuriyeti Resmi Gazetesi", Sayı No. 97/08 ve 104/09), Elektronik İmza hakkında Yasa ("Sırbistan Cumhuriyeti Resmi Gazetesi", Sayı No. 135/04), İleri Teknoloji Suçlarıyla Mücadelede Devlet Kurumlarının Örgütlenmesi ve Yetkileri hakkında Yasa ("Sırbistan Cumhuriyeti Resmi Gazetesi", Sayı No. 61/05, 104/09) ve Ceza Kanunu'nu ("Sırbistan Cumhuriyeti Resmi Gazetesi", Sayı No. 85/05, 88/05, 107/05, 72/09 ve 111/09) içermektedir. Hukuki çerçeve ise Elektronik İletişim Yasası ("Sırbistan Cumhuriyeti Resmi Gazetesi", Sayı No. 44/10) ile Savunma hakkında Yasa'dan ("Sırbistan Cumhuriyeti Resmi Gazetesi", Sayı No. 116/07, 88/09, 104/09) oluşmaktadır. Verilerin Gizliliği hakkında Yasa ile, Sırbistan'ın ulusal ve kamu güvenliğine, savunmasına, iç ve dış ilişkilerine, yabancı kaynaklı gizli verilerin korunmasına, gizli verilere erişim ve gizlilik taahhüdüne son verilmesine, kurumların yetkilerine ve Yasa'nın icrasını denetlemelerine, Yasa ile getirilen yükümlülüklerin yerine getirilmemesi sorumluluğuna ve veri gizliliğinin korunmasının önemiyle ilgili diğer konulara yönelik bir sistem düzenlenmektedir. Sırbistan Cumhuriyeti'nin 2009-2013 Döneminde E-Devletin Geliştirilmesi Stratejisi ile birlikte Sırbistan Cumhuriyeti'nde ilgili Strateji ile bu dönemde yükümlülük altına alınan faaliyetlerin uygulanmasına yönelik Eylem Planı (Sırbistan Cumhuriyeti Resmi Gazetesi Sayı No. 83/09 ve 5/10), e-devlet geliştirilmesinin ilkelerinden biri olarak bilgi güvenliği ilkesini öngörmekte ve Strateji'nin uygulanmasına dair Eylem Planı da Bilgi Güvenliği Hakkında Yasa Taslağı geliştirilmesini öngörmektedir.

12. Avrupa Konseyi Siber Suçlar Konvansiyonu'nu 10.11.2010 tarihinde imzalamış olan Türkiye'de konuyla ilgili olarak Ulaştırma, Denizcilik ve Haberleşme Bakanlığınca "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" taslağı hazırlanmıştır. Bilgi Teknolojileri ve İletişim Kurumu ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ve TÜBİTAK'ın işbirliğinde diğer Bakanlıkların da katılımıyla her yıl Ulusal Siber Güvenlik Tatbikatları yapılmaktadır. 2012 Temmuz ayında TÜBİTAK-BİLGEM bünyesinde "Siber Güvenlik Enstitüsü" kurulmuştur.

13. Siber güvenlik hakkında kalıcı yasaların ve yönetmeliklerin kabul edilmesi ve bunların gerektiği yerlerde ve zamanlarda tadil edilmesi gerekmektedir. Ancak günümüzün siber güvenlik sorunlarıyla mücadelede sadece ulusal yasaların kabul edilmesi ve uygulanması yetersiz kalmaktadır. Bilgi ve iletişim ağları, hem ulusal hem de uluslararası düzeyde büyük ölçüde özel sektörün mülkiyetindedir ve yine özel sektör tarafından işletilmektedir. Dolayısıyla siber güvenlik sorunlarının ele alınmasında, siber alanı güvence altına almaya katkıda bulunacak kamu – özel sektör ortaklığıyla birlikte uluslararası işbirliği ve normlar, geliştirilecek stratejilerin kilit unsuru olacaktır. Siber alanın dinamikleri, zaman içerisinde stratejilere yönelik uyarlamalar ve değişiklikler yapılmasını gerektirecektir.

14. Gürcistan'ın Ulusal Siber Güvenlik Stratejisi (2012-2015) taslak olarak hazırlanmış ve kesin olarak kabul edilmeyi beklemektedir. Sözkonusu Strateji'yle devletin, özel sektör şirketlerinin, kurumlarının ve şahıs olarak vatandaşların kolektif siber güvenliğini geliştirme yolunda atabilecekleri adımlar belirlenmekte ve kritik bilgi altyapılarına yönelik saldırı risklerini azaltmaya katkıda bulunulmaktadır. Bu Strateji, siber saldırıların önlenmesi ve adli takibinin yapılması hususunda hukuki yaptırım kapasitesinin artırılmasına; tehditlerin ve risklerin sonuçlarının daha iyi anlaşılması maksadıyla ulusal risk değerlendirmelerine yönelik bir süreç oluşturulmasına; internet protokollerinin ve routing sistemlerinin geliştirilmesi suretiyle internet mekanizmalarının güvence altına

alınmasına; güvenilir dijital kontrol sistemlerinin / gözetim ve veri edinimi sistemlerinin kullanılmasına; yazılım açıklarının azaltılmasına ve düzeltilmesine; siber sistemlerin ve telekomünikasyonun fiziksel güvenliğinin geliştirilmesine; siber güvenlik araştırmalarına ve güvenli sistemler geliştirmeye öncelik verilmesine atıfta bulunmaktadır. Strateji, aynı zamanda bilgi paylaşımını kolaylaştırmak, açıkları azaltmak, araştırmaları koordine ederek yeniden yönlendirmek ve siber alanda düşmanca veya kötü niyetli faaliyetleri caydırmaya yönelik stratejiler belirlemek ve geliştirmek için farkındalık, öğretim, eğitim ve uluslararası siber alan güvenliğinde işbirliği konularına özel bir vurguda bulunmaktadır. Siber alanla ilgili karşı istihbarat çabalarının yoğunlaştırılması, siber saldırılara cevap verme eşgüdümünün geliştirilmesi, bilgi altyapılarının korunmasına ve küresel güvenlik kültürü geliştirilmesine yoğunlaşan uluslararası kamu ve özel sektörleri arasında diyalog ve ortaklığın kolaylaştırılması, siber saldırıları ortaya çıkarken tespit edecek ve önleyecek ulusal ve uluslararası takip ve uyarı ağları kurulmasının desteklenmesi veya yasaların ve prosedürlerin en azından kapsayıcı olmasının temin edilmesi ve Avrupa Konseyi Siber Suçlar Konvansiyonu'nun imzalanması da önem taşımaktadır.

15. Ukrayna Ulusal Güvenlik Stratejisi "Değişen Dünyada Ukrayna", bilgi güvenliğini güvence altına almakta ve ulusal siber güvenlik sistemi oluşturulmasına işaret etmektedir. Bilgi güvenliği, Ukrayna "Bilgi" Yasası dahilindeki öncelikli politika konularından biridir. Bilgi ve telekomünikasyon sistemlerinde güvenliğin sağlanması alanındaki faaliyetler, 2005 yılında kabul edilen Ukrayna "Bilgi ve telekomünikasyon sistemlerinde bilginin korunması" Yasası ile düzenlenmektedir. "Ukrayna'da Özel İletişim ve Bilgilerinin Korunması Alanındaki Kamu Hizmetleri" Yasası, 23 Şubat 2006 tarihinde kabul edilmiştir. Bu kuruma Bağımsız Devletler Topluluğu üye devletleri arasında bilgisayar suçlarına karşı mücadelede İşbirliği Sözleşmesi'nin yanısıra informatik ve bilgi hakkında Model Yasa'nın hükümleri kılavuzluk etmektedir. Ukrayna aynı zamanda Avrupa Konseyi Siber Suç Konvansiyonu'nu da imzalamıştır.

16. Sırbistan Cumhuriyeti'nde Bilgi Toplumunun 2020 itibarıyla Geliştirilmesi Stratejisi'ndeki (Sırbistan Cumhuriyeti Resmi Gazetesi, No.51/10) altı öncelikten biri bilgi güvenliğidir. ISD Stratejisi, bilgi ve iletişim teknolojisi uygulamalarının bütün formlarında uygun düzeyde bilgi güvenliğinin, sürdürülebilir bilgi toplumu oluşturulmasının ön gerekliliklerinden biri olduğunu vurgulamaktadır. Bilgi güvenliği alanındaki birinci öncelik, bilgi güvenliğine yönelik hukuki ve kurumsal çerçevenin geliştirilmesidir. Veri Gizliliği Yasası, bilgi ve telekomünikasyon sistemlerini koruma tedbirlerini daha sıkı düzenleyen bir yönetmelik kabul edilmesini öngörmektedir ancak yine de bu konunun bir yasayla düzenlenmesine gerek vardır çünkü birtakım kurumlar için gizli verilerin manipüle edilmesi, kriptolu ürünler için yetki tanınması ve bilgi güvenliği alanında inceleme denetimi amacıyla ICT sistemlerinin akreditasyonu gibi kurumsal bir çerçeve ve yetkinlik oluşturmak gerekir. Gizli verilerin manipülasyonuna yönelik ICT sistemlerinin karşılaması gereken şartlar, tatminkar bir düzeyde uygulama sağlamak için şartların öngörüldüğü gibi kontrol edilebilmesine yönelik bir sistem kurulması gereğidir. Kültür, Bilgi ve Bilgi Toplumu Bakanlığı tarafından oluşturulan özel bir çalışma grubu, bilgi güvenliğinin geliştirilmesini ve bütün bir bilgi güvenliği alanının, özellikle de gizli veri manipülasyonuna (ICT sistemlerinin gizli veri manipülasyonuna yönelik akreditasyonu, gizli verilerin korunması amacıyla kriptografik ürünlerin kullanımı, bilgilerin ve iletişim sistemlerinin elektromanyetik radyasyon açıklarına karşı korunması ve yukarıda bahsedilen alanlarda uzmanlık isteyen görevlerin Ulusal Güvenlik Konseyi Dairesi'ne ve Savunma Bakanlığı'na aktarılması); kamu kurumlarındaki diğer

ICT sistemlerinde bilgi güvenliğine; Sırbistan Cumhuriyeti'nde bilgi ve iletişim sistemlerindeki risklere karşı önleme ve koruma faaliyetlerinde koordinasyona; ulusal iletişim ağlarına (Sırbistan Akademik Ağı'nın konumu ve işleyişi ve Ulusal İletişim Ağının konumu ve işleyişi); Bilgi Güvenliği İncelemesine yönelik ICT sistemlerinde bilgi güvenliğinin düzenlenmesini amaçlayan Bilgi Güvenliği Taslak Yasası'nı geliştirmiştir. Yasayla düzenlenen konuları da kapsamında tutan kamu kurumları, halen Taslak Yasayı uyumlu hale getirilmektedirler. Kamu kurumlarının bilgi sistemlerinin güvenliği ve korunması hakkında Yönetmelik (Sırbistan Cumhuriyeti Resmi Gazetesi No.41/90), kamu kurumlarının bilgi sistemlerinin bilgisayar uygulamasına dayalı olarak güvence altına alınmasına ve korunmasına dair örgütsel ve teknik tedbirleri ortaya koymaktadır.

17. Rusya'da ulusal düzeyde, bilgi toplumu oluşturulması ve geliştirilmesi sorununun çözümüne yönelik bütünleşik bir yaklaşım eksikliğinden ötürü bilgi güvenliği alanındaki güvenlik tehditlerinin kademeli olarak arttığını belirten "Bilgi Toplumu (2011-2020)" Ulusal Programı kabul edilmiştir. "2015 yılına kadar Bilgi Toplumunda güvenlik" 5inci alt-programın öncelikleri arasında şu tedbirler bulunmaktadır: bilgi toplumunun terörizme karşı korunma seviyesinin tespitine ve gözetimine yönelik bir sistem oluşturulması; büyük miktarlarda yapılandırılmamış verilerin depolanmasını ve işleme alınmasını sağlayan korumalı işlevsel yurtiçi hizmetler ve süreç bileşenleri dahil büyük miktarlarda yapılandırılmamış verilerin depolanmasına ve işlenmesine yönelik güvenli yurtiçi teknolojileri oluşturulması ve desteklenmesi, ve aynı zamanda yapılandırılmamış veri işleme miktarının artırılmasına imkan verecek şekilde sürekli destek ve gelişim sağlanması; terörizmle mücadele konularıyla ilgili olarak ortak veri bankasının diğer bölüm ve kurum-içi bilgi kontrol sistemlerinin geliştirilmesi ve bunların entegre edilmesi; ulusal bir yazılım platformu (karmaşık yurtiçi yazılım çözümleri - hazır modüllerin düzeniyle ve konfigürasyonuyla yeni ürünler geliştirilmesine imkan veren ve ortak teknoloji esasında geliştirilen modüller) oluşturulması, süper bilişim ve ağ teknolojileri geliştirilmesi. Rusya Federasyonu Devlet Başkanlığı'nın, süper bilgisayarlar ve ağ teknolojileri kullanımıyla oluşturulan bilgi sistemleri dahilinde bilgi güvenliğinin güvenceye alınması alanından sorumlu federal idari güç yapıları hakkında 8 Şubat 2012 tarihli 146 Sayılı Kararnamesi ile süper bilgisayarların ve ağ teknolojilerinin kullanımıyla bağlantılı bilgi sistemlerinde bilgi güvenliğini güvence altına alacak federal kurumlar - Rusya Federasyonu Federal Güvenlik Hizmetleri ile Teknik ve İhracat Denetimi Federal Hizmetleri (FSTEC Rusya) - oluşturulmuştur. "FSTEC Rusya"ya atfedilen yetkiler kapsamında, bilgi alanında ulusal güvenlik için elzem olan bilgi ve telekomünikasyon altyapısı dahilindeki bilgi güvenliğini güvence altına alma işlevi de bulunmaktadır.

18. Siber alan güvenliği yaklaşımlarındaki önemli sorumluluklar arasında şunlar bulunur: kilit kaynakların ve kritik altyapının güvence altına alınmasına yönelik kapsamlı bir ulusal plan geliştirilmesi; kritik bilgi sistemlerini hedef alan saldırılara tepki olarak kriz yönetimi sağlanması; kritik bilgi sistemlerindeki arızalarda acil durum düzeltme planlarıyla ilgili olarak özel sektöre ve diğer resmi kurumlara teknik yardım sağlanması; özel sektör, akademi organları ve kamu kurumları da dahil olmak üzere devlet, yerel ve hükümet-dışı örgütlere uygun koruma tedbirleri ve karşı tedbirler hakkında özel uyarı bilgileri ve önerileri sağlayan diğer resmi kurumlarla koordinasyon sağlanması; ve diğer kurumlarla birlikte güvenliğe destek olacak yeni bir bilimsel anlayışın ve teknolojilerin yolunu açacak araştırma - geliştirme faaliyetleri yürütülmesi. Özel sektör, akademi ve kamu da dahil olmak üzere devlet, yerel ve hükümet-dışı örgütler arasında koordinasyon sağlanması da çok önem taşır.

19. Siber alanın geniş dağılımlı varlıklarının korunması, birçok ülkenin ve bu ülke vatandaşlarının çaba göstermesini gerektirir. Hükümetler, siber alanı tek başlarına yeterince savunamazlar. Birçok kritik altyapı ve bunların dayandığı siber alan, özel mülkiyetin elindedir ve yine özel sektör tarafından işletilmektedir. Siber alanı oluşturan ve destekleyen teknolojiler, özel sektörden ve akademik yenilenmeden başlayarak hızla gelişmektedir. Teknolojiler ilerledikçe, tehditler ve zayıflıklar değiştikçe ve siber güvenlik konularındaki anlayış değiştikçe ortak eylemler gerekmektedir. En ciddi siber alan zayıflıklarını, olumlu uygulamaların paylaşılması ve yeni teknolojilerin değerlendirilerek uygulanması gibi ortak faaliyetler üzerinden tanımlamak ve düzeltmek için koordineli çabalara gerek vardır.

20. Siber alan güvenliğine yapılan yatırımlar, ileri düzeyde bilgi güvenliği teknolojilerinin tedarik edilmesi yoluyla daha güvenli teknolojiler için bir piyasa oluşturulmasına katkıda bulunacaktır. Aynı zamanda bilgisayar sistemlerinin ve ağlarının güvenli hale gelmesini de sağlayacaktır. Ülkeler, kritik sistemlerini koruma ve savunma yeterliliğine sahip olmalıdır.

21. Ekonomiler ve ulusal güvenlik, bilgi teknolojisine ve bilgi altyapısına daha fazla bağımlı hale gelmektedir. Ağlardan oluşan bir ağ, ekonominin bütün sektörlerinin, başka bir deyişle enerji (elektrik gücü, petrol ve gaz), ulaştırma (demiryolu, havayolu, denizyolu), finans ve bankacılık, bilgi ve telekomünikasyon, kamu sağlığı, acil durum hizmetleri, su, kimya, savunma, sanayi, gıda, tarım ve posta hizmetlerinin işleyişine destek olacaktır. Aynı zamanda elektrik transformatörlerini, boru hattı pompaları, kimyasal tekneleri, radarları, v.s. de kontrol etmektedir.

22. Dolayısıyla bilgi ağlarına yapılan siber saldırılar, kritik faaliyetler üzerinde ciddi sonuçlara yol açabilmektedir. Bu gibi saldırılara karşı koymak, açıkları azaltmak için entegre kabiliyet geliştirilmesini gerektirmektedir. Zayıflık değerlendirmeleri ve düzeltme faaliyetleri, eğitimli profesyonellerin daimi güvenlik denetimlerini yürütmeleri ve en ciddi zayıflıkları giderecek çok katmanlı bir savunma oluşturmak maksadıyla her zaman gerçekleştirilmelidir. Siber alanda tehditlerin yönetilmesi ve zayıflıkların azaltılması, bilhassa karmaşık bir sorundur. Siber alan güvenliği, farklı bir aktörler grubunun çoklu düzeyde harekete geçmesini gerektirmektedir.

23. Siber güvenliğin önemi konusundaki artan bilince ve kabiliyetleri artırmak için alınan tedbirlere rağmen siber riskler, bilgi ağlarının ve sistemlerinin arkasında yer almaya devam etmektedir. Maalesef tek başına hiçbir strateji, siber alandaki zayıflıkları ve ilgili tehditleri tamamen ortadan kaldıramamaktadır. Siber alanın güvenli hale getirilmesi, devam eden bir süreçtir zira yeni teknolojiler ortaya çıkmakta ve yeni zayıflıklar tespit edilmektedir.

Ulusal parlamentoların rolü

24. Ulusal parlamentoların, siber alanı güvence altına alma kaygıları karşısında seslerini duyurmaları ve KEİ üye devletlerinde sürdürülebilir kalkınmanın önemli bir vasıtası olarak bilgi güvenliğini sağlamaya yönelik tedbirlerin artırılmasına daha fazla katkı yapmaları gerekmektedir.

25. Muhtemel siber saldırıları önlemek için bilgi teknolojisi ve telekomünikasyon sistemleri de dahil olmak üzere kilit kaynakların ve kritik altyapıların güvence altına alınmasına yönelik kapsamlı bir ulusal plan geliştirilmesi hususunda hükümetlerin eylemlerini gözetlemek ulusal parlamentoların önemli bir görevidir.

26. Siber güvenlik alanındaki yasaların uluslararası standartlarla hukuken uyumlu hale getirilmeye devam edilmesi de önem arzetmektedir.

27. Parlamentoların, siber güvenlik alanındaki ulusal önceliklere ve stratejik hedeflere dönük araştırmaları teşvik etmek, harekete geçirmek ve geliştirmek için bilim, teknoloji ve inovasyon alanında finansman önceliklerini dikkatle belirlemeleri gerekmektedir.

28. Parlamentoların bir yandan muhtemel siber saldırılardan kaynaklanan zararları en aza indirirken ve hafifletirken diğer yandan da teknolojik kalkınmanın faydalarının yaygın bir biçimde anlaşılmasını ve desteklenmesini sağlamak amacıyla siber güvenlik alanında kapsamlı bir ulusal farkındalık oluşturacak şekilde mevcut hukuki mekanizmaları en yüksek düzeyde kullanmaları gerekmektedir.

29. Bilgi kaynaklarını korumaya ve yetkisiz bilgi erişimini önlemeye yönelik tedbirler kullanılarak çok katmanlı güvenlik sistemlerinden oluşan "derin savunma" sistemi oluşturulmasını desteklemek de gerekir.

30. Siber güvenlik alanında bilgi ve tecrübe alışverişine yönelik kalıcı mekanizmalar geliştirmek amacıyla siber saldırıların önlenmesi ve karşı tedbirler alınması için uluslararası merkezlerden oluşan bir ağın karşılıklı kabul edilebilir şartlarını hazırlamaya yönelik çalışmaların desteklenmesi de bir gerekliliktir.

31. Siber saldırılara ve müdahelelere karşı mücadelede ilgili kurumlara yeterince destek olabilmek için emniyet kurumları, istihbarat kurumları ve adli sistem arasında karşılıklı etkileşimin ve koordinasyonun geliştirilmesine de özel bir önem verilmelidir.

32. Parlamentoların, siber tehditlere karşı bütünleşik bir karşı eyleme geçilmesi için uluslararası bir strateji geliştirilmesine öncülük etmeleri ve bu itibarla ulusal ceza yasalarının uyumlu hale getirilmesi için ortak uluslararası hukuki mekanizmalar geliştirmeleri gerekir.

33. En ileri teknolojilerin oluşturulması ve uygulanması suretiyle bilgi güvenliğinin güvence altına alınmasına yönelik pratik tedbirlerin eşgüdümlü bir biçimde uygulanması için özel sektörü desteklemek amacıyla mevzuat geliştirilmesini desteklemek, parlamentoların görevidir.

34. Parlamentolar ayrıca siber alandaki zayıflıkları azaltmak ve tehditlere karşı eyleme geçmek amacıyla öngörü, erken ve zamanında teşhis, bilimsel ve teknolojik uzmanlık, zamanında tespit için bilgi güvenliği alanında uluslararası standartlar geliştirilmesinin katkı çerçevesini oluşturmaya da gayret etmelidirler.

35. Parlamentoların, bilimsel ve teknolojik ilerleme temelinde sürdürülebilir kalkınmayla ilgili uluslararası akitlerin onaylanmasında da etkin bir rol üstlenmeleri ve bu hükümleri ulusal mevzuata aktarmaları gerekir.

36. Karadeniz Ekonomik İşbirliği Parlamenter Asamblesi, bilim ve teknoloji alanında çok taraflı işbirliğinin geliştirilmesi ve KEİ Bilim ve Teknoloji Çalışma Grubu'yla daha sıkı temas oluşturulması hususunda KEİ'nin giriştiği eylemlere destek vermelidir.

Uluslararası işbirliği

37. Uluslararası siber güvenliğin geliştirilmesinde başlıca enstrümanlardan biri 2001 Avrupa Konseyi Siber Suçlar Konvansiyonu'dur. Bu Konvansiyon, siber suçlarla mücadelede ulusal hukuki çerçevelerin nasıl uyumlu hale getirileceği ve uluslararası işbirliğinin

unsurları hususunda rehberlik etmektedir. Bu hukuki akdin önemi, hem uygulamaya dönük hem de siyasidir. Konvansiyon, siber suçlara karşı ulusal hukuki çerçeve geliştirilmesinin ana hatlarını ortaya koyduğu için bu konudaki Avrupa normlarının ihracında önemli bir araçtır. Bunun yanısıra Konvansiyon'un imzalanması, siber suçluların sınırdışı edilmesi dahil operasyonel konularda uluslararası işbirliğini kolaylaştırmaktadır. Konvansiyon'un siyasi önemi, siber güvenlik konusundaki tek bağlayıcı uluslararası sözleşme olmasıdır ve Konvansiyon'un imzalanması da sözkonusu ülkenin kendi ulusal yasalarını siber suçlarla ciddi ölçüde mücadele edecek şekilde uyumlu hale getirmeye hazır olduğunu göstermektedir. Avrupa Konseyi, tüm dünyada Konvansiyon'u desteklemek için özel sektörle ve üye devletlerle birlikte bir Küresel Proje başlatmıştır. Konvansiyon'a daha çok sayıda ülkenin katılıyor olması, kendi alanlarında sağladıkları kolaylıklarla siber saldırılara sponsorluk yapan suç grupları ve hükümetler için ciddi bir caydırıcılık unsuru oluşturmaktadır.

38. Avrupa Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) Bilgi Güvenliği ve Gizlilik Hükümetler Arası Çalışma Grubu (WPISP), bilgi toplumu ve direnç geliştirme politikaları hususunda tavsiye kararları ve raporlar hazırlamaktadır. Hükümet, iş dünyası ve sivil toplumdan uzmanlardan oluşan bir ağ üzerinden eğilimleri denetlemekte ve bilgi alışverişini kolaylaştırmaktadır. OECD, teknolojinin bilgi güvenliği ve gizlilik üzerindeki etkilerini analiz eden düzenli raporlar yayınlamaktadır. OECD'nin kendi üye devletlerindeki CIIP uygulamaları hakkındaki raporu, bu alandaki en iyi karşılaştırmalı dokümanlardan biridir ve en ileri ekonomilerin olumlu uygulamaları, örgütsel yapıları ve mevzuatı hakkında analizler içermektedir. OECD, "Sistematik Siber Güvenlik Risklerinin Azaltılması" raporuyla "Küresel Şoklar" hakkında bir dizi araştırma başlatmıştır. OECD bağlamında siber güvenlik, büyük ölçüde ekonomi ve teknoloji politikasının bir alt-kategorisi olduğu için bir ulusal güvenlik konusu olarak siber güvenliğin yükselişi, OECD'nin gündemindeki önemini bir şekilde geriye atmıştır. OECD'nin, ulusal bilgi altyapısının dirençli hale getirilmesi hususundaki en olumlu uygulamaları toplama ve değiş tokuş etme konusundaki katkısı, kendi ulusal siber güvenlik kurumları için doğru modeli arayan ülkelere fayda sağlayabilir.

39. Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT), siber güvenlik konusundaki görüşmelere 2008 yılında başlamıştır. O zamandan bu yana AGİT katılımcı devletleri, temel konular olarak siber güvenlik bilincinin artırılmasının, ülkelerin siber suçlarla ve terörizmle mücadele kabiliyetlerinin geliştirilmesi ihtiyacının ve siber alanda sorumlu devlet tavrının belirlenmesinin ele alındığı birkaç üst düzey toplantı yapmışlardır. AGİT ülkelerinin, siber güvenlik konusuna yaklaşımlarında çok farklı ilgi alanları ve bakış açıları bulunmaktadır ve AGİT'in bu tartışmadaki tam rolünün ne olacağı hususunda tam bir uzlaşı oluşmamıştır. Haziran 2010'da yapılan AGİT Güvenlik İşbirliği Forumu ile AGİT Daimi Konseyi Ortak Toplantısı, stratejik siber güvenlik konularında görüşmelere devam edilmesine karar vermiştir.

40. BM Güvenlik Kurulu, siber güvenlikle ilgili kararları kabul etmiştir. BM Sosyal ve Ekonomik Komisyonu çerçevesinde 56/121 sayılı "Bilgi Teknolojisinin Suç Amaçlı Suistimaliyle Mücadele" ve 57/239 sayılı "Küresel Siber Güvenlik Kültürü Oluşturulması" kararları kabul edilmiştir. Her iki karar da uluslararası işbirliğinin önemini, siber suçlular için güvenli sığınakların ortadan kaldırılması, emniyet uygulamalarında işbirliği ve siber güvenlik konularında genel farkındalığın artırılması ihtiyacını vurgulamaktadır. "Küreselleşme ve karşılıklı bağımlılık: kalkınma için bilim ve teknoloji" hakkında 64/422 sayılı Karar, aynı zamanda BM ülkelerinin kendi siber

güvenliklerini korumaya yönelik CIIP değerlendirme incelemesini de içermektedir. Bu girişimler, siber tehditler konusunda artan kaygılara dikkat çekmiş, küresel bir farkındalık oluşturmaya yardımcı olmuş ve BM ülkelerini siber güvenlik konusunda kendi ulusal mekanizmalarını ileriye taşımaları için gerekli tedbirleri almaya yöneltmiştir. 2009 yılında kabul edilen "Uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler" hakkında 64/386 sayılı BM Kararı, uluslararası güvenlik bağlamında siber güvenlik konusunda görüşmelere devam edilmesini, tavsiye kararları sunmak üzere bir grup uzmanın toplanmasını teklif etmektedir. 2010 yılında BM Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanında Gelişmeler Konusunda Kamu Uzmanları Grubu, ülkelere bilgi güvenliğini ve uluslararası işbirliğini artırmaları çağrısında bulunan bir rapor yayınlamıştır. Rapor, riskin azaltılması ve kritik ulusal ve uluslararası altyapıların korunması hususunda devletler arasında daha ileri düzeyde diyalog için tavsiyelerde bulunmaktadır. 12 Eylül 2011'de BM Çin, Rusya, Tacikistan ve Özbekistan Daimi Temsilcilerinin BM Genel Sekreteri'ne, "Uluslararası Bilgi Güvenliği Uygulamaları Yasası" taslağını üyelere dağıtmalarını talep eden ortak bir mektup gönderdiği de not edilmelidir. Yönetmelik'in ana işlevi, askeriye, siyaset, suç ve terörizm sorunları ve tehditleriyle ilgili uluslararası bilgi güvenliği konusunda devletlerin sorumlu davranış biçimlerinin geliştirilmesidir. Sözkonusu doküman, uluslararası istikrarın, barışın ve güvenliğin oluşturulması maksadıyla bilgi ve iletişim teknolojilerinin kullanımına yönelik karşı eyleme atıfta bulunmaktadır. İnternetin düzenlenmesine yönelik çok taraflı, şeffaf ve demokratik bir uluslararası mekanizma oluşturulmasının yanısıra bütün devletlerin bilgi alanı, egemenliğine saygı, toprak bütünlüğü ve siyasi bağımsızlığı hususlarında insan haklarına ve temel özgürlüklere bağlı kalınmasını da öngörmektedir. Rusya Federasyonu, projeyi geliştirenlerden biri olma vasfıyla bütün ilgili taraflara bu konudaki görüşmelerde aktif olarak yer almaları çağrısında bulunmaktadır. Bu girişim, evrensel bir BM dokümanı olarak küresel topluluğun menfaatlerine mümkün olan en geniş ölçüde hitap edecek kapsamlı bir uluslararası bilgi güvenliği ağı sağlanmasına odaklanacak bir Konvansiyon geliştirilmesi yolunda ilk adımı oluşturabilecektir.

41. NATO, 2007 yılında bu alandaki diğer stratejik dokümanların ve faaliyetlerin temelini oluşturan ilk Siber Savunma Politikası'nı geliştirmiştir. NATO, yeni stratejik ortama uyum sağlayan ilk uluslararası örgüt olmuş ve geleneksel olmayan güvenlik tehditlerinin Müttefiklerin ulusal güvenliğinde merkezi bir önem teşkil ettiğini kabul etmiştir. NATO'nun 2007 Siber Savunma Politikası, NATO'nun kendi ağlarının siber savunma kabiliyetinin geliştirilmesine yönelik hedefler koymuş ve üye devletlerle siber savunma konularında görüş alışverişi için başlangıç mekanizmaları oluşturmuştur. NATO Anlık Bilgisayar Tepkisi Kabiliyeti Teknik Merkezi, operasyonel siber savunma konularında merkezi bir teknik kurum görevi görmektedir. Siber savunma alanındaki Mutabakat Zabıtları, düzenli görüş alışverişini, bilgi paylaşımını kolaylaştırmakta ve NATO Ani Müdahale Ekiplerinin siber kriz durumunda her bir Müttefike nasıl destek olabileceğini tarif etmektedir. Kasım 2010'da Lizbon Zirvesi'nde kabul edilen yeni NATO Strateji Konsepti'yle, NATO'nun siber saldırı tehditlerine tepki çabalarını hızlandırmasının gerektiği vurgulanmaktadır. Lizbon Zirvesi, NATO'yu ve Müttefikleri yeni güvenlik sorunlarıyla mücadeleye yöneltmekte ve diğer hedeflerle birlikte İttifak'ın siber gündemi için çok gayretli bir yol haritası çıkarmaktadır. Bütün NATO askeri ve sivil organlarının merkezi bir koruma altına alınmasını, savunma planlaması sürecinin siber bileşeninin hayata geçirilmesini ve bilgi paylaşımı ile erken uyarı kapasitesinin artırılmasını içermektedir. Haziran 2011'de NATO Savunma Bakanları, siber güvenlik alanındaki çabalar için bir vizyon belirleyen NATO Siber Savunma Politikası'nı ve ilgili Eylem

Planı'nı onaylamıştır. Mayıs 2012'de Şikago'da Devlet ve Hükümet Başkanları, bütün NATO ağlarını NATO Bilgisayar Anlık Tepki Kabiliyeti (NCIRC) bünyesinde merkezi bir koruma altına almaya karar vermişlerdir.

42. AB siber güvenlik konusuna bölünmüş bir biçimde yaklaşmış, birbiriyle örtüşen farklı temalarla paralel politikalar uygulamaya konulmuştur. Bu girişimlerin birçoğu, AB üyelerinin ciddi siber saldırılara karşı koymaya hazır olması konusuyla doğrudan ya da dolaylı olarak ilgilidir zira bu stratejiler hem bu saldırıların sonuçlarıyla hem de siber saldırı araçlarıyla ve yöntemleriyle ilgilidir. 2007 yılında Avrupa Komisyonu, operasyonel emniyet alanında işbirliğinin, siyasi işbirliğinin ve üye devletler arasında işbirliğinin geliştirilmesini öngören "Siber suçlarla mücadelede genel bir politikaya doğru" Tebliği'ni yayınlamıştır. Bununla birlikte muhtemel bir hukuki harekete yönelik olarak sektörde bilincin artırılması, eğitim, araştırma ve daha güçlü diyalogun yanısıra üçüncü ülkelerle siyasi ve hukuki işbirliğini de teşvik etmektedir. "Karşı köktenleşme" yani şiddet içeren ideolojik materyalleri denetleme kabiliyeti, uzun zamandır AB karşı terörizm stratejilerinin odak noktası olmuştur. Aralık 2009'da, Avrupa Birliği'nin "dahili güvenlik" gündeminde ciddi bir adım oluşturan "Stokholm Programı" kabul edilmiştir. Program, Avrupa Dahili Güvenlik Stratejisi çağrısında bulunmanın yanısıra daha iyi ve daha dirençli ağ bilgisi güvenlik tedbirleri geliştirme gereği, siber saldırılarla daha iyi mücadele kabiliyeti, bütün üyelerin Siber Suç Konvansiyonu'nu onaylamasının önemi ve hem hükümetler arasında hem de özel sektörle bilgi alışverişinin önemi dahil olmak üzere siber güvenliğe dair birtakım referanslarda bulunmaktadır. Ekim 2010'da kabul edilen yeni AB İnternet Güvenliği Stratejisi, Siber Alanda vatandaşların ve işletmelerin güvenlik seviyesini yükseltmeyi amaçlamakta ve siber suçlarla mücadeleyi hedeflemektedir. Stratejideki üç özel öneri arasında 2013 yılı itibarıyla AB Siber Suçlarla Mücadele Merkezi kurulması, 2012 yılı itibarıyla bütün AB kuruluşlarında Bilgisayar Acil Durum Tepki Ekipleri (CERTS) Ağı kurulması (ve aynı zamanda bu kuruluşların emniyet güçleriyle işbirliği içine girmesi) ve 2013 yılı itibarıyla Avrupa Bilgi Paylaşımı ve Uyarı Sisteminin (EISAS) hayata geçirilmesi yer almaktadır. Konsey, emniyet güçlerine daha iyi sınır-ötesi eğitim sağlanması ve uluslararası düzeyde daha iyi koordinasyon için 2010 yılında Europol'un Avrupa Siber Suçlar Platformu'nun (ECCP) güçlendirilmesi çağrısında bulunan Siber Suçlar Eylem Planı'nı kabul etmiştir. Europol birçok zaman yeni Konsey kararının ve tavsiye kararının odak noktası olarak görülmüş ve ECCP de yakın bir geçmişte birtakım bağlı girişimlerle birlikte tam-zamanlı girişim statüsüne yükseltilmiştir. Önemli bir örgütsel girişim olan Avrupa Siber Suç Merkezi, ilk defa tartışmaya açıldığı 2007 yılından bu yana birçok defa teklif edilmiş ve üzerinde mutabık kalınmıştır. Merkez'in fiilen açılışının öncüsü bir örgüt olarak Avrupa Birliği Siber Suçlar Görev Kuvveti kurulması için Haziran 2010'da mutabakata varılmıştır.

III. SONUÇLAR

43. Son birkaç yılda siber alandaki tehditler çarpıcı bir biçimde artmıştır. Ülkeler ve uluslararası örgütler, yaşamın neredeyse her alanında siber alana daha fazla bağlı olunması nedeniyle, bilgi sistemlerinin kesintiye uğramasını önlemek ve siber alan güvenlik tepkisini sağlamak üzere tasarlanmış politikalar geliştirmeye başlamışlardır.

44. Dünyamız, hızla, İnternete bağımlı hale geldikçe daha güvenli bir siber ortam geliştirilmesi hususunda kararlılık taşımak da zorunlu hale gelmektedir. Dünya Çapında Ağ, özel ve mesleki ortamlarda sonsuz fırsatların kapısını önümüze açmaktadır. İnternet teknolojisi iletişim, araştırma, ticaret ve iş için kullanılmaktadır. Ayrıca ekonominin

hayati sektörlerinde kullanılan endüstriyel denetim sistemleri de internetle bağlantılıdır. Bu da, internet bağımlılığına güvenlik ve emniyet boyutunu katmaktadır.

45. Güvenli internet sistemi, ekonomiler ve toplumlar için büyük önem taşır. Bilgi sürekli olarak akar. Siber alanı oluşturan altyapı, tasarımıyla ve gelişimiyle küreseldir. Siber alanda, ulusal sınırlar çok az anlam taşır. Siber alanın küresel niteliğinden ötürü mevcut zayıflıklar, dünyanın gözü önünde cereyan eder ve istismar etmek için yeterli kabiliyeti olan herkes tarafından heryerde ulaşılabilir.
46. Ülkeler bir yandan güvenliği, emniyeti ve gizlilik haklarını desteklerken diğer yandan da inovasyonu ve teknolojik gelişmeyi teşvik eden bir ortamı koruma paradoksuyla karşı karşıyadırlar. Siber güvenliğin emniyet altına alınması, hem ulusal hem de uluslararası düzeyde devletler, işletmeler ve toplum için temel bir sorundur.
47. Her ülkenin bilgi güvenliği alanında çalışan kişilerin kapasitesini artırmak ve kamu, özel sektör ve akademi çevreleri arasında işbirliğini güvence altına almak için siber alandaki kendi devlet davranışını belirlemesi, beceri geliştirmeye ve eğitime yatırım yapması gerekir. Siber alan güvenliği farkındalığı ve eğitim programlarının yanısıra siber güvenlik tehdidini ve zayıflığını azaltma programlarının uygulanması zorunludur.
48. İnterneti ve diğer ICT ağlarını tehditlerden ve zayıflıklardan korumak ve hem ulusal hem de uluslararası düzeyde daha fazla işbirliği için ulusal parlamentoların, bilgi teknolojilerinin suç amaçlı suistimaliyle mücadele alanında devletler arasında daha fazla koordinasyon ve işbirliği gereksinimini öne çıkarmaları ve bu bağlamda uluslararası ve bölgesel örgütlerin oynayabileceği rolü vurgulamaları gerekir.
49. Siber ağlara yönelik olarak daha çok sayıda saldırı yapılıyor olması, sivil ağları güvenli ve siber alanı emniyetli tutmayı zorlaştıran güvenlik tehditlerinden biri halini almıştır. Bu da güvenli, emniyetli ve dirençli bir siber ortam oluşturulması ve siber güvenlik bilgisinin ve yeniliklerin desteklenmesi gereksinimi öne çıkarmaktadır.
50. Kamu - özel sektör katılımı, güvenli bir siber alanın kilit unsurudur. Kamu - özel sektör katılımı farkındalık, eğitim, teknolojik gelişim, zayıflıkların giderilmesi ve yenilenme faaliyetleri ele alınırken çeşitli biçimler alabilir. Yürütülen faaliyetlerle aynı zamanda ağların ve sistemlerin, belirtilerin ve uyarıların korunmasını, organize saldırılara karşı korunmayı mümkün kılacak araştırmaların ve teknolojilerin geliştirilmesi hususları da desteklenmelidir.
51. Bilgi toplumunun ana dayanaklarını oluşturan bilgi ve iletişim teknolojilerinin kullanımında güvenilirliği ve güvenceyi sağlamak zorunludur. Küresel düzeyde siber güvenlik kültürünün teşvik edilmesi, desteklenmesi, geliştirilmesi ve kuvvetle uygulanması gerekir.
52. KEİ üye devletleri, siber suç ile mücadele için bir ortak yasal çerçevenin yanı sıra ayrıca bilgi ağlarının korunması için müşterek bir faaliyetin geliştirilmesi adına yakın işbirliği yapmalı ve AB üyesi olmayan KEİ üye devletleri de AB üyesi olan KEİ üye devletleri ile ortak bir yasayı kabul etmelidirler.
53. Ülkeler, günümüzün dijital sorunlarıyla baş edebilecek yenilikler ve buluşlar için son teknolojiyle uyumlu araştırma ve geliştirme faaliyetlerine; orantısal olarak ağ güvenliğine, teknik eğitime, siber güvenlik farkındalığına ve dijital okuryazarlığa yatırım yapmalıdırlar.
54. Gereksiz mesajlar, veri hırsızlığı ve diğer çevrim-içi zayıflıklar gibi siber güvenlik tehditlerinin artan hacmi ve sürekli daha karmaşık bir hal alması, kullanıcıların kendi sistemlerini ve bilgilerini güvencede tutmaları için uyanık kalmalarını gerektirmektedir.

Her bir kullanıcının, bilgi ağlarını ve siber sistemleri korumaya yardımcı olacak eylemleri ve riskleri anlaması önemlidir.

55. Bilgisayar, akıllı telefon, tablet bilgisayar gibi çok sayıda cihazı içinde barındıran, iç içe geçmiş bir dünyada herkes, aynı iletişim kanallarını paylaşmaktadır ve her bir tüketicinin siber alanın kendisine ait bölümünü güvencede tutmak için üstleneceği bir rol bulunmaktadır. İnternetin ve diğer dijital varlıkların korunması, her türden her bir kullanıcının paylaştığı bir sorumluluktur. Siber güvenliğin, insanlar İnternetten keyif aldıkça ve yaşamlarına kattığı faydaları takdirle karşıladıkça, her bireysel kullanıcının siber dünyada sorumlu davranmasıyla başladığını hatırlamak gerekmektedir.