SİBER GÜVENLİK ve MİLLİ KAPASİTE OLUŞTURMA

Mustafa AFYONLUOĞLU
afyonluoglu@gmail.com

20.11.2017

Giriş

Siber güvenlik alanında artık telaffuzu dahi güç hacimlerin bir çığ gibi dünya gündeminde ilerlediğini ve bu alanda nitelikli insan kaynağı kapasitesi yetiştirme konusunda ciddi problemler olduğunu yakınen izlemekteyiz. Türkiye olarak, bu alanda farkındalığın her kesimde arttırılması, uzman yetiştirilmesi, özel sektör ve kamu kurumlarında ihtiyaç duyulan kapasitenin yaratılması için ne gibi adımlar atılabileceğini ele almadan önce, 2 yıl gibi kısa bir süre içerisinde bizleri ve tüm dünyayı bu alanda bekleyen ihtiyaçlara kısaca bir göz atalım:

Dünyada Siber Güvenlik'teki Hacimler ve Kapasite İhtiyaçları

Gartner Raporlarına[1] göre siber güvenlik alanında 2015'de **75.4 Milyar $** olan marketin 2020 yılında 170 milyar dolara[2] çıkacağı düşünülmektedir. *Markets & Markets*'e göre bu hacim 2022 yılında **232 milyar $**'a çıkacaktır[3]. *Stanford Üniversitesi*'nce yapılan bir proje çerçevesinde yayınlanan İşgücü İstatistiklerine[4] göre, 2015 yılında sadece ABD'de, siber güvenlik uzmanı arayan **209.000 iş ilanı**, ihtiyaç duyulan uzmanı bulamamıştır ve son 5 yılda bu ilanlar %74 artmıştır. *Cisco* tarafından yayınlanan siber güvenlik raporuna[5] göre, 2016 yılında yaklaşık bir milyon olan siber güvenlik uzman talebi yayınlamıştır. *Symantec* CEO'sunun açıklamalarına göre 2019 yılında siber güvenlik uzmanı talebinin **6 milyon**a ulaşması ve **1.5 milyon uzman açığı**nın karşılanamayacağı beklenmektedir[6].

[1] https://www.gartner.com/newsroom/id/3135617
[2] https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity-market-reaches-75-billion-in-2015-expected-to-reach-170-billion-by-2020/
[3] https://www.marketsandmarkets.com/PressReleases/cyber-security.asp
[4] http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/
[5] http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf
[6] https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#66233f8227ea

IDC'ye[7] göre en yüksek gelişim beklenen alanlar güvenlik analitiği (%10), saldırı istihbaratı (+%10), mobil güvenlik (%18) ve bulut güvenliğidir (%50). Nesnelerin interneti alanındaki güvenlik pazarının 2020 yılındaki büyüklüğünün **29 milyar $** olması beklenmektedir[8]. Market araştırma firması *ABI*'ye göre 2020'de **20 milyon**dan fazla internet bağlantılı araç yazılım tabanlı güvenlik teknolojisine sahip olacak ve (ticari ve bireysel) araçlar için HSM satış hacmi **2.3 milyar adede** yükselecektir[9].

PwC 2016 Güvenlik Raporu'na göre, *Siber Sigorta*, sigortacılık alanında en hızlı büyüyen alan olmuştur ve şu anda yıllık **2.5 milyar $** olan siber sigorta pazarı 2020'de **7.5 milyar $**'a ulaşacaktır[10].

Finans dünyasında *HSRC* (Homeland Security Research Corp.) tarafından yayınlanan "Bankacılık ve Finansal Hizmetlerde Siber Güvenlik: ABD Pazarı 2015-2020 Raporu"na göre, ABD'deki finansal servislerin siber güvenlik pazar hacmi 2016'da **9.5 milyar $** iken 2016-2020 yılları arasında toplam hacmin **68 milyar $**'ı aşması beklenmektedir[11]. Nitekim sadece 4 büyük finansal kuruluşun siber güvenlik harcaması 2016 yılında **1.5 milyar $** *olmuştur (J.P. Morgan: 500 Milyon $, Bank of America: 400 Milyon $, CitiGroup: 300 Milyon $ ve Wells Fargo: 250 Milyon $).*

Ülke ekonomileri açısından bakıldığında siber güvenliğin ciddi bir pay olduğu da dikkati çekmektedir. Örneğin İsrail Siber Bürosu (*NCB*) tarafından yapılan açıklamaya göre, İsrail'in 2015 yılında siber güvenlik alanındaki ürün satışları **6 milyar $** olmuştur ve bu küresel marketin %10'una karşılık gelmektedir. Çin'de bu hacim 2015'de **1 milyar $** iken Asya-Pasifik ülkelerinde mobil siber güvenlik pazarının 2020 yılında **7.5 milyar $**'a ulaşması beklenmektedir[12].

Türkiye ve Siber Güvenlik'te Kapasite Geliştirme

Ülkemizde 2017 itibarı ile yaklaşık 150.000 siber güvenlik uzmanına ihtiyaç olduğu farklı yetkililer tarafından farklı platformlarda dile getirilmektedir. 2013-2014 Siber Güvenlik Stratejisi ve Eylem Planı[13] kapsamında üniversitelerde açılan lisans ve yüksek lisansları programlarının kontenjanlarına bakıldığında bu kapasiteyi karşılamak için yaklaşık 60 yıl gerektiği, 29 Ekim 2017 tarihinde "Sayısal Devlet" teması ile düzenlenen 19. Kamu Bilişim Platformu'nda Prof. Dr. İbrahim Soğukpınar[14] tarafından dile getirilmiştir[15]. Dolayısıyla tüm dünyada olduğu gibi ülkemizde de siber güvenlik alanında nitelikli kapasite geliştirilmesine yönelik ciddi bir ihtiyaç olduğu açıktır. Bunula birlikte, bu

[7] https://www.idc.com/
[8] https://www.csoonline.com/article/2984193/cyber-attacks-espionage/new-cybercrime-wave-drives-iot-security-spending.html
[9] https://www.abiresearch.com/press/abi-research-forecasts-global-hardware-security-mo/
[10] http://press.pwc.com/News-releases/cyber-insurance-market-set-to-reach--7.5-billion-by-2020/s/5CC3FA21-221C-43DF-A133-05435E365342
[11] http://homelandsecurityresearch.com/2014/10/u-s-banking-financial-services-retail-payment-cybersecurity-market-2015-2020/
[12] http://www.apacmarket.com/blog/apac-mobile-security-18
[13] http://www.udhb.gov.tr/doc/siberg/SOME_2013-2014_EylemPlani.pdf
[14] http://www.gtu.edu.tr/personel/1040/1041/ibrahim--soukpnar.aspx
[15] http://www.kamu-bib.org.tr/kamubib-19/program

ihtiyacın sadece üniversitelerde program açılarak karşılanmasını beklemek çok da yeterli bir çözüm olmayacaktır.

Kapasite ihtiyacının muhatabı olarak özel sektör, kamu kurumları ve üniversiteler ilk sırada karşımıza çıkarken ayrıca toplumu da bu konuda bilinçlendirmek, farkındalık ve eğitim çizgisini ilkokula kadar indirmek, daha kapsayıcı ve sürdürülebilir bir politikadır.

Bu kapsamda, milli kapasite geliştirme programlarının 3 seviyede oluşturulması önerilmektedir:

1. Okul öncesinden itibaren farkındalık programları ile başlayan ve ilköğretim, ortaöğretim, lise ve yükseköğretim (lisans ve yüksek lisans ayrı ayrı olmak üzere) seviyelerine yayılmış kapsamlı eğitim-öğretim planları ile genç neslin bilinçlendirilmesi, bilgilendirilmesi, yetkinlik ve beceri kazandırılması
2. Özel sektör için kapasite oluşturma yaklaşımları ve iş birliği önerileri
3. Kamu kurumlarında kapasite oluşturmaya ilişkin öneriler

1. Yeni Nesil'de Kapasite Oluşturma

Bilgi toplumu süreci ile birlikte hayatımıza giren ve zamanla günlük yaşantının ayrılmaz bir parçası olan cep telefonu, tablet, bilgisayar gibi bilişim ve iletişim araçları, sayısal yakınsama ile fonksiyonları artan ve iç içe geçen fotoğraf makinası, yazıcı, fotokopi makinası gibi cihazlar, internet bağlantıları sayesinde hayatımızı kolaylaştıran kamera, klima, buzdolabı gibi yeni nesil IoT [16] cihazları, güvenliği ve sağladığı konforu giderek yazılım endüstrisine emanet eden araba endüstrisi günlük hayatımıza siber güvenliğin girmesine sebep olmuştur. Bu teknik enstrümanlar hayatımızı kolaylaştırırken bir yandan da üzerlerinde barındırdığı yazılımlarda yer alan olası açıklıklar ile mahremiyet dahil birçok alanda riskleri de beraberinde getirmiştir.

Dikkat çekmesi gereken husus şudur ki, bu gelişmelerden yararlanan kesim sadece yetişkinler değildir. Nitekim 3-4 yaşından itibaren tablet ve cep telefonu ile tanışan yeni nesil, 6-7 yaşından itibaren artık doğrudan birçok işini bu cihazlarla yapmaktadır. İlk aşamalarda oyun oynama ile başlayan bu ilgi sonrasında yerini eğitsel programlara bırakabilmektedir. Ancak yeni neslin bu iletişim araçları ile etkileşiminde bazı tehditlere maruz kaldığı görülmektedir. Çocukların ve gençlerin bu tehditlerden olumsuz etkilenmemeleri için bu konuda bilinçlendirilmeleri ve bazı temel becerileri kazanması gerekmektedir.

[16] IoT: Internet of Things (Nesnelerin İnterneti)

Nitekim, Dünya Ekonomik Forumu (WEF) tarafından 2016 Eylül'de yayınlanan raporda[17], temel zeka katsayıları olan IQ[18] ve EQ[19] ölçütlerine ilaveten, sosyal, duygusal ve bilişsel zeka bileşenleri ile ortaya konulan DQ[20] kavramı ele alınmış ve bunu "dijital vatandaşlık", "dijital yaratıcılık" ve "dijital girişimcilik" olarak kategorilendirilip dijital hayat içerisinde çocuklara kazandırılması gereken temel beceriler 8 ana başlıkta ele alınmıştır. Bu beceriler hem günümüz dünyasında "sayısal vatandaş" olmanın gerekleri olarak karşımıza çıkmakta, hem de teknolojinin sağladığı nimetlerden faydalanırken buradaki risklerden korunabilmek için bir gereklilik olarak gündeme gelmektedir.

Sayısal Vatandaş Kimliği: Çevrimiçi ve çevrim dışı sağlıklı ve tutarlı bir sayısal kimlik geliştirmek ve bunu yönetebilmek, dijital ortamda sahte sanal kimliklerin gerçek hayattaki zararları hakkında farkındalık yaratmaktır. Özellikle çevrimiçi sağlıklı bir kimlik geliştiremeyen gençler, burada sahte ve gerçek kimlikleri ile örtüşmeyen bir kimliğe bürünmekte ve gerçek olmayan bir alemde yaşayarak gündelik hayatından kopmaktadır. Özellikle toplumdan gördüğü ilgiyi yetersiz bulan ve zaman içerisinde toplumdan umudunu kesen, kendisini toplumda değersiz görmeye başlayan gençler bu sanal kimliklere daha sıkı bağlanmakta ve sağlıksız bir kişilik gelişim sürecine girmekte, hatta zaman zaman kendilerine zarar vermektedirler. Bu olumsuz sürecin en dikkat çekici örneği, 2015 yılından bu yana dünya gündeminde yer alan Rusya kökenli *Mavi Balina Oyunu*'dur. Bu oyun, kendisine güveni zayıf olan veya topluma küserek kendisini sanal dünyadaki kimliklerine hapseden gençleri hedef almaktadır.

[17] https://www.weforum.org/agenda/2016/09/8-digital-life-skills-all-children-need-and-a-plan-for-teaching-them
[18] IQ: Intelligence Quotient (Kişisel Zeka)
[19] EQ: Emotional Quotient (Duygusal Zeka)
[20] DQ: Digital Quotient (Dijital Zeka)

Daha çok 14-22 yaş aralığında bu oyuna çekilen gençler, oyunu yöneten yönetici tarafından kendilerine verilen talimatlarla gerçek hayatta belli işleri gerçekleştirmekte, böylece kendisini daha değerli ve işe yarar görmektedir. Son aşamada ise yönetici tarafından kendisine hayatına son verme talimatı verilmektedir. Türkiye'de 142 gencin intiharı ile bağlantılı olduğu düşünülen[21] bu oyun ayrıca tüm kişisel ve özel bilgileri de ele geçirmekte, oyundan ayrılmak isteyen kişiye bu bilgiler ile şantaj yapmaktadır.

Bu kritik örnekte öne çıkan sanal dünya problemleri şunlardır:

- Sanal kimlik yönetimi zafiyeti
- Kişisel verilere erişim
- Siber zorbalık
- Sanal ortama bağımlılık
- Kişilik bozukluğuna yol açabilecek ortamın oluşturulması

Ekran Zaman Yönetimi: Bireyin ekran karşısında geçirdiği zamanı yönetebilmesine, özellikle sosyal ağlarda ve oyunlarda kendi kontrolünü sağlamasına yönelik becerileri geliştirmektir. Önce oyunlar ile başlayan sonra sosyal ağlara uzanan bu süreç kontrollü olarak takip edilmediğinde, "teknoloji" veya "internet" bağımlılığı olarak da bilinen aşamaya erişebilmektedir. Psikolojik, sağlık ve sosyal problemleri beraberinde getiren bu bağımlılık, birçok ülkede, gençleri tehdit eden ciddi problemler arasında üst sıralarda yer almakta ve buna özgü tedavi merkezleri kurulmaktadır. Özellikle okul çağındaki çocuklar ve gençlerde en yoğun olarak izlenen bu durum, "*İnterneti aşırı kullanım isteğinin önüne geçilememesi, İnternete bağlı olmadan geçen zamanın önemini yitirmesi, yoksun kalındığında ise aşırı sinirlilik hali ve saldırgan olunması*" şeklinde tarif edilmektedir. Bu çerçevede sadece psikoloji alanında 50'den fazla akademik çalışma[22] yapılmış olup, Avrupa Birliği tarafından yayınlanan araştırma raporuna göre, günde 4 saatten fazla sanal alemde sörf yapan kişilerde tıpkı kumar bağımlılarında olduğu gibi, beyinde insanın kendisini iyi hissetmesini sağlayan adrenalin benzeri bir kimyasal olan dopamin birikmesi meydana geldiği tespit edilmiştir. Bu bağımlılık neticesinde en sık rastlanılan sonuçların depresyon, sosyal fobiler, uyarı kontrol bozuklukları, dikkat bozukluğu ve aile ilişkilerinde bozulmalar olduğu görülmektedir. Beden sağlığı açısından ise gözlerde yanma, sırt ve boyunda ağrı ve sertleşme, ellerde uyuşma, bileklerde el bileği sendromu, genel yorgunluk ve verim düşmesine bağlı başarısızlık şeklinde kendisini göstermektedir.

Özellikle internete yeni bilgi ve eğitim fırsatları olarak bakan ebeveynlerin, süreci takip etmemesi halinde bu kullanımın zaman içinde sosyal ağa yönelmesi ve sosyal ilişkilerin buradan (ve zaman zaman özlem duyulan özelliklere sahip olarak tariflenmiş sahte kimliklerle) sürdürülmeye çalışılması bu bozuklukları başlatmakta ve akabinde bağımlılığı beraberinde getirmektedir. Hem psikolojik hem de bedensel gelişimi olumsuz etkileyen bu durum, ayrıca

[21] http://www.bbc.com/turkce/41281200
[22] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4804263/

çocuğun yabancılarla bu ortamlarda korunaksız olarak iletişim kurmasının ve siber zorbalığa maruz kalmasının önünü açmaktadır.

Özellikle çocukların ve genç yaştaki bireylerin aşırı ve uygunsuz derecede bilgisayar ve Internet kullanımına karşı bilgilendirilmesi, bu konuda ekran karşısında geçen zamanı kontrol altına almalarının sağlanması, oluşması muhtemel sorunları azaltacaktır[23].

Siber Zorbalık Yönetimi: Başta sosyal ağlar kanalı ile olmak üzere siber zorbalık olaylarını fark edebilme, kendini bunlardan koruyabilme ve gerekli tedbirleri alabilme becerisi kazandırmaktır. Siber zorbalık, bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarıdır. Siber zorbalık teknik yönü daha yoğun olan elektronik zorbalık (şifreleri ele geçirmek, web sitelerini hack'lemek, spam içeren e-posta mesajları göndermek, bir elektronik hizmetin servis dışı kalmasını sağlayıcı faaliyetler yapmak gibi) ve elektronik iletişim zorbalığı olarak iki alanda ele alınabilir. Yapılan araştırmalarda, siber zorbalığa maruz kalan gençlerin %90'ının bu durumu yetkili bir merkeze ya da yetişkinlere söylemediği, kız çocukların siber zorbalığa 2 kat daha çok maruz kaldığı görülmüştür. İngiltere'de yüksek okul öğrencilerinin %40'ı, Amerika'da 10-yaş grubu çocukların %16'sı siber zorbalığa maruz kalmaktadır. *Amerikan Pediatri Akademisi* (APA), siber zorbalığı tüm 10-yaş grubu çocuklar için en yaygın çevrimiçi risk olarak değerlendirmektedir. Siber zorbalık, depresyona, düşük benlik duygusuna, düşük özgüvene ve sosyal izolasyona sebep olmakta ağır şartlarda kişiyi intihara kadar sürükleyebilmektedir[24].

Siber Güvenlik Yönetimi: Başta kişisel veriler ve aileye yönelik veriler olmak üzere, verilerin korunmasına ve bu verilere yönelik yapılan siber saldırılara ilişkin bilgilendirilmektir. Buradaki tehdit iki açıdan ele alınmalıdır. Temelde kişisel verileri korumaya yönelik tedbirler öne çıkarılmalıdır. Bunun yanısıra karşımıza çıkacak diğer önemli tehditler şöyle sıralanabilir: Cep telefonu, tablet, bilgisayar gibi kişisel cihazlara çocuklar tarafından bilinçsizce yüklenen oyun vb. programlar vasıtası ile cihazdaki bilgilerin ele geçirilmesi, zararlı yazılımların yüklenerek uzaktan cihazın kontrol edilmesi ve izlenmesi, bu cihazlar üzerinden yasal bakımdan suç sayılacak sitelere uzaktan girilmesi veya suç unsuru olan elektronik materyallere erişilmesi, bu cihaz üzerinden yapılan bankacılık işlemleri gibi güvenli ortam gerektiren işlemlerin bilgilerinin ele geçirilmesi, bu cihazların bir zombi cihaz haline getirilip başka cihazlara saldırılması veya yasadışı elektronik faaliyetlere alet edilmesi ciddi siber güvenlik zafiyetleri arasındadır. Bu risklerin farkına varmak ve tedbirleri almak için, çocuklara ve yetişme çağındaki gençlere, cihazlardaki hangi işlemler sonucunda bu risklerin oluşacağı, bunlardan nasıl korunmak gerektiği konusunda yeterli bilgi verilmelidir.

[23] http://www.ustunzekalilarmerkezi.org/cocuklarda-ve-genclerde-internet-bagimliligi-ve-cozum-onerileri/
[24] https://www.cybersmile.org/advice-help/category/what-is-cyberbullying

Mahremiyet Yönetimi: Mahremiyeti korumak üzere, elektronik ortamda paylaşılan tüm kişisel verilerin kontrolünü geliştirmektir. İnternet ortamında özellikle küçük yaştaki çocuklardan bireyin kendisi, ailesi, evi vb. hakkında kişisel bilgi almak ve sonra bunları kötü amaçlı olarak kullanmak isteyenlere karşı geliştirilmesi gereken bir bilinçlendirme yaklaşımı olarak karşımıza çıkmaktadır. Daha önceden, yetişkin bireylerin sosyal medyada paylaştıkları kişisel verileri (konum, statü vb.) kullanarak sosyal mühendislik yöntemleri ile yapılan dolandırıcılık, hırsızlık vb. faaliyetler için, yetişkinlerin bu konuda daha bilinçlenmesi ve paylaşımlarına özen göstermesi sebebiyle hedef kitle olarak çocuklara yönelinmiştir. Küçük yaştaki kesimi aldatarak, yanıltıcı yönlendirme yaparak kendisi, ailesi, evleri vb. hakkında bilgi almak hem kişisel bilgileri ele geçirmek hem de siber zorbalık ve siber şantaj için daha kolay ve ideal yöntem haline gelmiştir. Hedef araçlar olarak da genelde oyunlar ve sosyal medya tercih edilmektedir.

Kritik Düşünme: Dijital ortamda doğru/faydalı ve yanlış/zararlı bilgiyi ayırt edebilme, çevrimiçinde karşılaşılan güvenilir ve şüpheli kişileri/davranışları anlayabilme becerisini geliştirmektir.

Manipülasyon ve yanlış haber yaymak yeni kavramlar olmamakla birlikte, bu faaliyetlerin internet ve sosyal medya üzerinden, üstelik oldukça hızlı ve büyük hacimlerde yapılmaya başlaması siber tehdit olarak karşımıza çıkmaktadır. Avrupa Birliği tarafından kurulan "Çocuklar için Daha İyi İnternet" insiyatifi çerçevesinde gerçekleştirilen "Daha Güvenli İnternet" Forumunda, bu konudaki sorunlar aşağıdaki şekilde belirlenmiştir[25]:

- **Yanlış Bilgilendirme:** Yanlış (anlatılan olayla ilgisiz) fotoğraf ve video gibi materyaller kullanılarak internet üzerinde oldukça kaliteli bir içerik hazırlamak mümkündür. Bazı sahte haberler ve siteler o kadar inandırıcıdır ki gerçek gazetecileri dahi yanıltabilmektedir.
- **Bulaşıcı Eğilimler:** Sansasyonel haberler özellikle sosyal medya kanalları ile oldukça hızlı yayılabilmektedir. Okuyucuyu "tıklamaya" özendiren ilgi çekici başlıkların yönlendirdiği sayfada genelde beklenen içerik yer almamakta, ancak bu hareket, haber sahibini çok takip edilen/tıklanan kişi haline getirmektedir.
- **Bilgi Bombardımanı:** Ciddi manada büyük hacimlerde bilginin var olması, gerçek ve istenilen kalitedeki asıl bilgiye ulaşmayı zorlaştırmaktadır.
- **Hedefleme ve Profil Oluşturma:** Sosyal medyada yer alan içerik genelde okuyucu kitlelerinin belli gruplarda profillenmesini ve bu profillerin ilgi alanlarını belirlemeyi hedeflemektedir.
- **Sahte Haber ile Para Kazanma:** Sahte haberlere ilgi sağlanması ve okuyucunun belli sayfalara yönlendirilmesi, bu sayfalarda verilen reklamlar sayesinde para kazanmanın bir yöntemi olarak karşımıza çıkmaktadır.

Tüm bu problemler, başta yetişkinler ama özellikle çocuklar ve gençler için, internet ortamında doğru bilgiye erişmenin önemini ortaya koymaktadır. İngiltere'de yapılan araştırmada, internet üzerinden elde edilen bilgilerde özellikle gençlerin içerik konusunda kritik değerlendirme yapmadığını

[25] https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=1987589

göstermiştir. Ofcom tarafından yayınlanan "Çocuklar ve Ebeveynler: Medya Kullanımı ve Tutumlar 2016 Raporu"nda[26], 8-11 yaş aralığındaki çocukların %28'inin, 12-15 yaş aralığındakilerin %27'sinin, "*bir web sayfası Google tarafından arama sonucunda listeleniyor ise, bu sayfanın güvenilir olduğuna inandıklarını*", bu yaş gruplarının %10'unun ise buna hiç dikkat etmediklerini göstermiştir. Bununla birlikte 8-17 yaş aralığındaki kesimin yaklaşık yarısının, hangi sayfaların güvenilir olup olmadığı konusunda içerik hakkında kritik bir değerlendirme sürecine girdiğini göstermektedir.

Dijital Ayak izleri: Sayısal dünyada bırakılan izler ve bunların gerçek hayata etkilerini anlama ve bu çerçevede sorumlulukları yönetebilme becerisini kazandırmaktır.

Sayısal dünyada gerçekleştirilen faaliyetler (bir siteyi ziyaret etmek, bir dosya indirmek, bir çoklu ortam içeriği izlemek, bir yazışma yapmak, sesli görüşme gerçekleştirmek, dosya göndermek, sosyal medyayı kullanmak vb.), gerçek ortamdakinden çok daha fazla iz bırakmakta, yani sayısal olarak detaylı şekilde kayıt altına alınmaktadır. Özellikle bazı katalog suçları engellemek, terörle mücadele, yasadışı faaliyetlerin tespiti, kumar ve benzeri faaliyetlerin belirlenmesi ve önlenmesi gibi toplumu koruyucu sebeplerle yapılan takip ve kayıtların yanısıra ayrıca teknik sistemlerin işleyebilmek için tutmak durumunda olduğu kayıtlar da bunların bir bölümünü oluşturmaktadır. Bu kayıtların bir kısmı (blog yazıları, sosyal medya faaliyetleri gibi) herkese açık olduğundan, bu içeriğin başkalarına zarar verici veya hukuk dışı içerikte olması, gerçek hayatta kullanıcıya doğrudan yansıyacak sonuçlar doğurabilecektir. Bu sebeple internet ortamındaki hareketlerde bu bilinçle yol alınması gerektiği bilincinin aşılanması önem kazanmaktadır.

Dijital Empati: Çevrimiçi ortamda başkalarının ihtiyaç ve duygularına karşı empati yapabilme kabiliyetini kazandırmaktır.

Değerlendirme:

Tüm bu beceriler dikkate alındığında, siber güvenlik ve sayısal vatandaşlık konusundaki eğitimin, çocukların teknoloji ile buluşmaya başladıkları erken dönemlerden itibaren ele alınması gerektiği açıktır. Bu çerçevede aşağıdaki kademelerde eğitim, bilgilendirme ve bilinçlendirme çalışmalarını planlanması gerekmektedir:

- **Okul öncesi dönem**: genel farkındalık yaratma faaliyetleri, temel riskleri ve kaçınma yöntemlerini tanıtma

[26] Ofcom: Children and Parents: Media Use and Attitudes Report 2016: https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf

- **İlk ve orta öğretim**:
    - **Kodlama**: Yazılım Mantığına Giriş, Ortaöğretimde Robotik (NXT, Ardunio gibi kitler ile temel yazılım geliştirme mantığının yerleştirilmesi)
    - **Siber Eğitim**: Siber zorbalık yönetimi, Ekran-zaman yönetimi, mahremiyet yönetimi, Sayısal Ayak İzleri farkındalığı, Sayısal vatandaş kimliği, temel siber güvenlik yönetimi, kişisel verilerin korunması
- **Lise**:
    - **Kodlama**: Güvenli Kodlama Teknikleri, Robotik (İleri seviye Ardunio ve Raspberry PI gibi kitlerle yazılım geliştirme), Gamification (Eğitim hedefli oyun geliştirme)
    - **Siber Eğitim**: Bilgi güvenliği, kritik düşünme, dijital empati
- **Üniversite** – **Lisans Seviyesi**nde standart olarak verilmesi önerilen temel başlıklar:
    - **Kodlama:** İleri seviye kodlama, gömülü kodlama
    - **Siber Eğitim:** Kriptografi ve Yazılım Güvenliği, Bilgisayar ağları, Telekomünikasyon, sayısal medya, web teknolojileri, siber hukuk ve etik, yönetişim ve liderlik, siber soruşturma
- **Üniversite – Yüksek Lisans Seviyesi:**
    - Siber güvenliğin ulusal önceliklendirilmiş tüm dallarında uzman yetiştirme programları