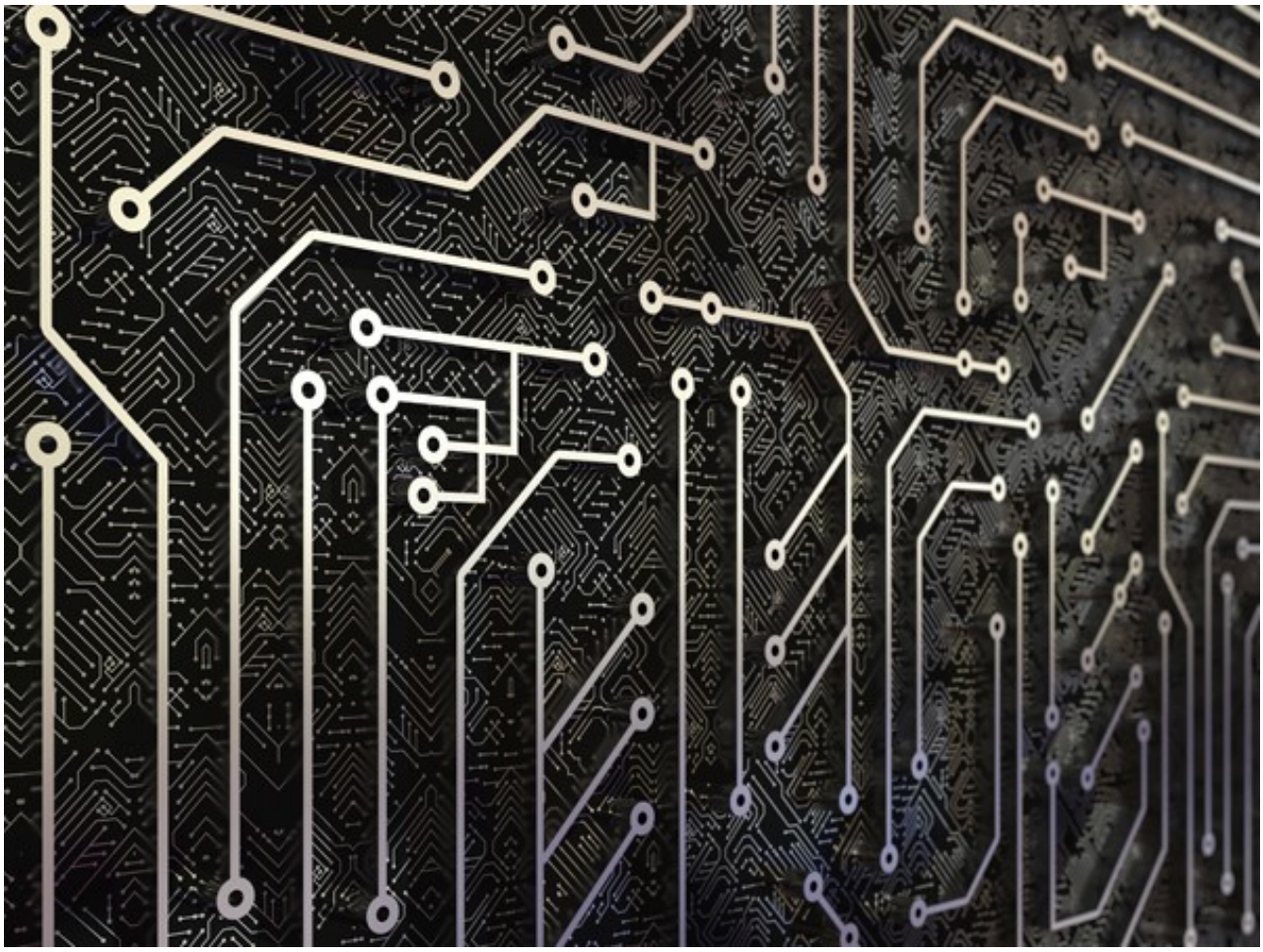


TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİSİNE YÖNELİK DEĞERLENDİRMELER

DİJİTAL TÜRKİYE PLATFORMU

Dijital Türkiye

Şubat 2017

YÖNETİCİ ÖZETİ

Hayatın hemen her alanında merkezi bir rol edinmiş olan bilgi ve iletişim teknolojileri sağladığı geniş imkanlar yanında güvenlik risklerini de beraberinde getirmiştir. Bugün siber güvenlik farklı kurumların sorumluluklarıyla kesişen çok boyutlu ve stratejik olarak ele alınması gereken bir konu haline gelmiştir. Siber alanın ortaya çıkardığı yeni tehditlerle baş etmek ve fırsatları değerlendirmek için devletin diğer aktörler ile birlikte çalışması zorunluluk halini almış, bir yönetişim modelinin üretilmesini gerekli kılmıştır.

Dünyada ve ülkemizde toplumların dijital bağımlılığı tek bir aktör tarafından kontrol edilebilecek boyutların ötesine geçmiştir. Devletler, siber güvenliğin farklı boyutlarında otoritelerini hedef alan meydan okumalara karşı gelebilmek için ulusal ve uluslararası aktörler ile iş birliği geliştirmek zorundadır.

Siber güvenlik yönetişiminde devlet kurumlarının eş güdümünün yanı sıra sivil toplum kuruluşları, üniversiteler ve özel sektörün iş birliğiyle oluşturacağı ekosistem Türkiye'nin **teknoloji ihracatı**, **diplomatik etkinliği**, **istihbarat gücü**, **siber alandaki menfaatlerinin korunması** gibi birçok önemli konuda ilerlemesinin yolunu açacaktır. Ulusal seviyede hazırlanan bir siber güvenlik stratejisinin **küresel bir yaklaşıma** sahip olması, Türkiye'nin ürettiği yönetişim çözümleriyle küresel rolünü artıracak bir fırsat olarak görülmelidir. Bir yandan ulusal anlamda siber güvenlik yönetişimi modelleri geliştirilirken, aynı zamanda uluslararası düzlemde farklı aktörler ile ortak çalışma platformları inşa edilmelidir.

Siber güvenlik algısının tehdit odaklı olması konuyla ilgili bazı fırsatların gözden kaçmasına neden olabilmektedir. Dijital tehlikelerin ulusal güvenlik boyutunda tehditler ortaya çıkardığı yadsınamaz bir gerçek olmakla beraber yeni gelişmekte olan geniş bir pazar oluşturduğu da stratejistlerin gözünden kaçmamalıdır.

Bu raporda Türkiye'nin açıkladığı siber güvenlik stratejisini güçlendirmek adına siber güvenliğin etki alanı içerisinde bulunan **kamu ve özel ağların korunması, kritik altyapı güvenliği, siber diplomasi, siber istihbarat, ekonomi ve eğitim** alanlarında atılması Dijital Türkiye Platformu tarafından önerilen bazı uygulama önerileri sıralanmıştır. Yönetici özetinin devamında her bir konu başlığı altında Türkiye'de atılması gereken somut adımlar sıralanmıştır.

KAMU, ASKERİ VE ÖZEL AĞLARIN KORUNMASI

- Siber güvenliğin milli güvenliğin bir parçası haline gelmiştir. Kamu ve askeri ağların güvenliğinde bütüncül bir yaklaşım sergilenmelidir. Bu ağlarda yaşanacak veri sızıntısı ya da başka bir güvenlik açığının ulusal güvenliğe direkt etkisi olacağı unutulmamalıdır.
- Kamu kurumlarının kullandığı ağların savunması ve düzenli denetimlerinin yapılması için hangi kurum veya kurumların sorumlu olduğu belirli hale gelmelidir. Şüphesi her kurum öncelikli olarak kendi güvenliğinden sorumludur. Fakat kamu kurumlarına yönelik güvenlik denetimlerinin diğer kamu kurumları ve gerekli güvenlik yeterlilikleri sağlayan özel şirketlere yaptırılması olumlu bir adım olacaktır. Bir kurumun kendi imkanlarıyla başa çıkamadığı saldırılara yönelik koordine mekanizması kurulmalı çeşitli senaryolar üzerinde çalışılmalıdır.
- Askeri kurumlar kendi siber güvenlik stratejilerini oluşturup askeri ağların güvenliğini artırmak için gerekli denetim mekanizmalarını tesis etmeli, kendi siber güvenlik stratejilerini hazırlamalıdır.
- Stratejik karar alma seviyesindeki yetkililerin siber alanın 5. Muharebe alanı olarak kabul edilmesinin ortaya çıkardığı tehdit ve fırsatlara yönelik farkındalık eğitimleri düzenlenmeli, taaruzi siber operasyonlar konusunda doktrinel çalışmalar yapılmalıdır.
- Milli Güvenlik Üniversite'sinde siber güvenliğin teknik taraflarıyla birlikte, milli güvenliğe entegrasyonuyla ilgili lisans / yüksek lisans bölümleri açılmalıdır.
- Özel ağların savunmasında saldırı senaryoları oluşturulmalı ve devlet kurumlarının hangi durumlarda müdahil olabileceğine dair yasal çerçeve belirlenmelidir. Şirketler kendi ağlarının güvenliğinden sorumlu tutulsa da özel kurumların yabancı devlet destekli gruplar tarafından hedef alınması uluslararası bir duruma dönüşeceği için devletin müdahil olması gerekecektir.

SİBER İSTİHBARAT

- Sinyal ve elektronik istihbarata yoğunlaşacak, bünyesinde üst düzey teknik uzmanlık bulunduracak yeni bir yapı oluşturulmalı ve özellikle bilimsel, elektronik ve teknik istihbarata karşı koyma faaliyetleri icra etmelidir.
- Uluslararası siber güvenlik firmalarından siber tehdit istihbaratı elde etme yönünde çalışmalar yapılmalıdır.

SİBER DİPLOMASİ

- Türkiye, Birleşmiş Milletler (BM) nezdinde yürütülen ve siber alanda norm geliştirmeyi hedefleyen Governmental Experts on Information Security grubunun çalışmalarına dahil olmalıdır.
- NATO akreditasyonuna sahip, stratejik siber güvenlik çalışmalarına yoğunlaşan Müşterek Siber Güvenlik Mükemmeliyet Merkezi (CCD COE) ile iş birliği sivilleri de kapsayacak şekilde genişletilmelidir.
- Avrupa Konseyi bünyesinde 2001 yılında hazırlanan ve siber suçlarla mücadelede uluslararası iş birliğini sağlamaya yönelik olan Budapeşte Konvansiyonu'nun güncellenmesi önerilmeli ve bu çalışma Türkiye'nin inisiyatifiyle devam etmelidir.

EKONOMİ

- Yerli ürün geliştirmede devlet desteğinin odağı ürünü küresel pazarlarda rekabet edebilecek seviyeye getirmek olmalıdır. Teşvik edilecek ürünlerin üretim sürecinin ardından uluslararası pazarlara açılabilmesi için gerekli ürün yönetimi, pazarlama, satış ve reklam aşamalarında danışmanlık desteği devam etmelidir.
- Ürün geliştirme konusunda yatırımcıların dünyadaki trendleri yakından takip etmesini sağlayacak ve güncel tehditlere karşı özgün çözümler geliştirilmesinin yolunu açacak çalışmalar yapılmalıdır.

- Dünyadaki siber güvenlik uzman açığı fırsat olarak değerlendirilmeli, siber güvenliğe eğilimi olan gençlerin yetiştirilmesine ön ayak olunarak sadece Türkiye'de değil yurt dışında da iş bulma imkanlarının önü açılmalıdır.

EĞİTİM

- Siber güvenlik eğitimi **farkındalık oluşturma** ve **uzman yetiştirme** olarak iki ana amaç altında toplanmalıdır.
    - 'Güveliğin en zayıf halkası insandır' prensibiyle Internet ve İletişim teknolojilerini kullanan vatandaşların temel seviyede siber tehditler ve sonuçları hakkında **farkındalığının sağlanması** için seferberlik düzeyinde ulusal bir program hayata geçirilmelidir.
    - **Uzman yetiştirmek amacıyla** üniversite ve lise aşamasında gerek temel siber güvenlik gerekse de spesifik konular üzerine derinlemesine eğitim ve araştırma olanakları geliştirilmelidir.
    - Örgün eğitim dışında kalan bilgisayar bilimlerine yatkın vatandaşların siber kabiliyetlerinden milli menfaatler adına yararlanmak için özel programlar düzenlenmelidir.

Kamu ve özel sektör arasında bilgi/siber güvenlik birimlerinde operasyonel seviyede çalışan teknik personel arasında **değişim programları** uygulanmaya konularak kurumsal teknik kapasitenin geliştirilmesi amaçlanmalıdır.

GİRİŞ

Dünya bugün küresel, ulusal ve bireysel katmanlarda etkileri görülen baş döndürücü bir dijital dönüşüme sahne olmaktadır. Uluslararası organizasyonlar, hükümetler, şirketler ve sivil toplum örgütleri dijital dönüşümün insanoğlunun önüne serdiği yeni dünyada eski harekât tarzları (*modus operandi*) ile devam edilemeyeceğinin farkında olarak ortaya çıkan tehdit ve fırsatlara ayak uydurmak için yeni yaklaşım ve stratejiler geliştirmektedir.

Siber alandan kaynaklı tehditler çok boyutlu ve üssel şekilde artmaktadır. Siber saldırganlar banka hesaplarını boşaltmakta, elektrik dağıtım şebekelerini devre dışı bırakmakta, su kaynaklarını kontrol edebilmekte ve son ABD seçimlerinde görüldüğü gibi demokratik süreçlere müdahale edebilmektedir. Suçlunun tespit edilmesindeki teknik zorluklar, hukuki yaptırımların yetersiz kalması, siber alanın ulusal sınırları aşan yapısı, uluslararası iş birliğinde karşılaşılan sorunlar, siber suçluların devlet otoritesi karşısında manevra alanını genişletmekte ve siber tehditleri ulusal güvenlik meselesi haline getirmektedir.

Türkiye 1990'lı yıllardan bu yana dijital dönüşüme ayak uydurmaya yönelik çeşitli adımlar atmıştır. Siber güvenliğe yönelik bir stratejiye doğan ihtiyaç nedeniyle de ilk kez 2012 yılında siber güvenlik stratejisini yayınlamış; stratejinin ikincisini 2016'da kamuoyuyla paylaşmıştır. Dünyada 50'den fazla ülke siber güvenlik stratejisi oluşturmuştur. Stratejilerin geliştirme süreçleri, hedefleri ve kapsamı birbirinden farklılık arz etse de sayısı artmakta olan bu ülkelerin benzer bir çalışma içerisine girmesi, siber güvenliğin ancak ulusal bir stratejiyle yönetilebileceğini gösteren en önemli göstergelerin başında gelmektedir.

Türkiye'nin siber güvenlik stratejisi oluşturulurken farklı kesimlerin görüşleri alınmış konuyla ilgili taraflardan ortak akıl çerçevesinde mümkün olduğu kadar katkı sunmaları beklenmiştir. Siber güvenlik meselelerine çözüm üretmek ancak böyle kapsamlı bir yaklaşım ile mümkün olacaktır. İlgili konu hakkında genel bir çerçeve çizen, kapsamını belirleyen ve amaç(lar) koyan strateji belgelerinin nasıl eyleme dökületeceği ciddi önem taşımaktadır. Türkiye'nin siber güvenlik stratejisinde

Birleşmiş Milletler'in Internet ve Telekomünikasyon ajansı ITU'nun yaptığı Global Cyber Security Index (2015) sıralamasında Türkiye yedinciliği üç ülke ile paylaşmıştır. Türkiye, 1 üzerinden verilen notlardan hukuki düzenlemelerin hazırlanması (0.5), teknik dayanıklılık (0.66), organizasyonel yapılanma (0.75), kapasite geliştirme (0.75) ve uluslararası işbirliği (0.5) ile Avrupa bölgesinde de dördüncü sırada yer almıştır.

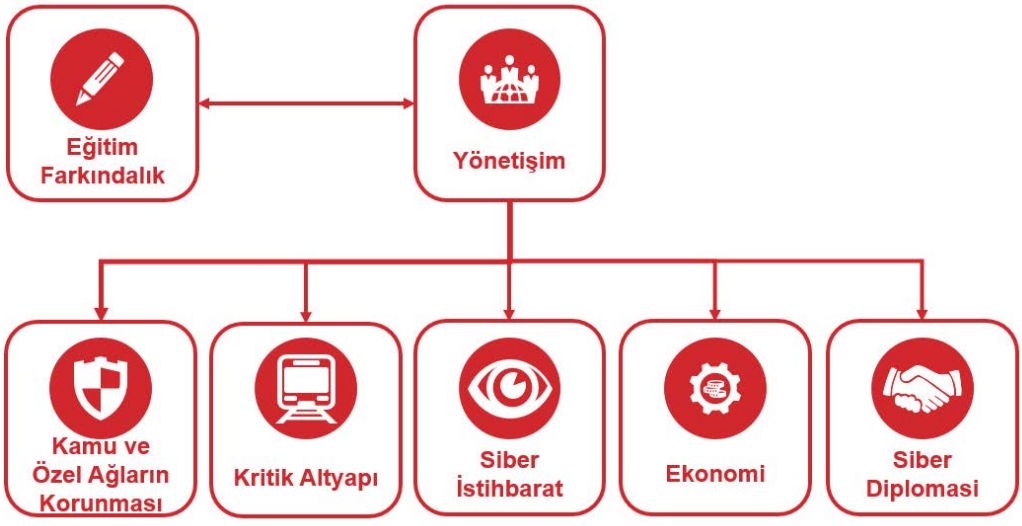
ortaya konulan vizyon ile nasıl yol alınabileceği ülkemizin geleceğini belirleyen önemli faktörlerden biri olacaktır. Bu belgede önümüzdeki dönemde siber güvenlik adına atılacak adımlara yönelik öneriler sunulmaya çalışılmıştır.

Böyle bir çalışma yapılırken iki önemli prensibe dikkat edilmiştir. Siber güvenliğin genel olarak ele alınma biçimi tehdit odaklı olagelmiştir. Siber güvenlikle ilgili herhangi bir rapor ya da strateji belgesi siber tehditlerin küresel ekonomiye verdiği zararlardan bahsetmeden, ülkelerin milli güvenliklerine karşı oluşturduğu ciddi tehditlerin altını çizmeden ve bireysel özgürlüklerimizin hedef alındığı bir dünya ortaya koymadan vazgeçmez. Fakat bu madalyonun sadece bir yüzüdür. Mevcut tehditlerin sürekli olarak arttığı yadsınamaz bir olgudur ve dünyada 'siber kıyamet' senaryolarının yazılması bu gerçeğin inkâr edilemeyecek boyutta olduğunu göstermektedir. Ancak siber güvenliğin kendi ekonomisini ve istihdam pazarını oluşturduğunu da gözden kaçırmadan bu alana yönelik ulusal stratejiler ve politikalar üretilmelidir.

Bu çalışmanın ikinci dayanak unsuru siber güvenliğin kısa ve orta vadede tüm dünyayı ilgilendiren bir sorun haline dönüşeceği, global vizyondan uzak çözüm önerilerinin sürekliliğinin tartışmalı olduğudur. Siber tehditlerin üstesinden gelmek, tıpkı küresel ısınma, sınır aşan suçlar, insanlığı tehdit eden hastalıklar gibi ancak global çözümler üretilerek mümkün olacaktır. Global yaklaşımla hazırlanan politikalar Türkiye'nin ürettiği çözümlerin küresel uygulanabilirliğini ortaya koyduğunda ülkemizin uluslararası arenadaki gücüne de katkı sağlayacaktır.

Raporun ilerleyen bölümlerinde aşağıdaki şekilde anlatılmaya çalışılan siber güvenliğin kapsamının yer aldığı konularda atılması önerilen adımlara detaylarıyla birlikte yer verilmiştir.

Siber Güvenlik Stratejisinin Kapsamı



1. YÖNETİŞİM

Siber güvenlik başlı başına bir çalışma alanı olmanın dışında birçok farklı alanla yapısı itibariyle kesişmektedir. Disiplinler arası bir çalışma alanı haline gelen siber güvenliğin ana ekseni güvenlik olsa da silahlı kuvvetlerin etki ve yetki alanının dışına çıkan boyutları bulunmaktadır. Siber güvenlik sadece kritik altyapıların korunması ve bir istihbarat meselesi olarak ele alınırsa ülkemiz adına başarı getirecek bir yol haritası oluşturulması mümkün gözükmemektedir. **Ekonomi, diplomasi, uluslararası hukuk iç güvenlik**, siber güvenliğin yoğun etkileşimde bulunduğu alanlardan sadece bazılarıdır.

Farklı alanlarla etkileşim uygulama safhasında değişik sorumluluklara sahip birçok kurumun eş güdümünde yürütülmesi gereken çalışmalar ortaya çıkarmaktadır.

Siber güvenliğin milli güvenlik açısından taşıdığı kritik önem, uluslararası güç dengesinde oynayabileceği oyun değiştirici rolü, getirebileceği ekonomik fayda ve bunun gibi nedenlerden dolayı stratejik seviyede ele alınması gerekmektedir. Yürütmenin başına bağlı yeni bir birimin ihdas edilerek gerekli kadro desteğiyle siber güvenlik yönetişimi konusunda bir an önce harekete geçmesi ülkemizin siber gücünü artırmada ve gerek dışarıdan gerekse içerden Türkiye'ye yönelik siber tehditlere karşı dayanıklılığın perçinlenmesi aciliyet arz etmektedir.

Siber güvenlik yönetişimi ile ilgili iki farklı kurumsal yaklaşım sergilenebilir. Yönetişimi sağlayacak ve gerek devlet kurumları arasında gerekse devlet-dışı aktörler ile koordinasyonu sağlayacak bir yapının **müsteşarlık ya da bakanlık** düzeyinde meydana getirilecek bir kurumla yürütülmesi düşüncesi ön plana çıkmıştır. Her iki seçenekte de çeşitli bakanlıklardan ilgili bürokratların toplanması ve yürütmenin başına rapor etmesi büyük önem taşımaktadır. Ülkemizin bekasını yakından ilgilendiren siber güvenlik meselesinin stratejik seviyede ele alınması genelkurmaydan dışişleri bakanlığına, içişleri bakanlığı dış ticaret müsteşarlığına MİT'e kadar uzanan farklı kurumların iş birliği ve uzmanlığı ile ancak alt edilebilecektir.

Dünyanın birçok ülkesinde siber güvenlik yönetişimi icranın en yetkili organına bağlı şekilde yürütülmektedir.

ABD'de siber silah geliştirilmesi ve kullanılması başkanın emriyle yapılmaktayken, İsrail başbakanlık bünyesinde kurduğu Milli Siber Büro ile akademi, bürokrasi ve özel sektörden oluşan bir sacayağı inşa etmiştir.

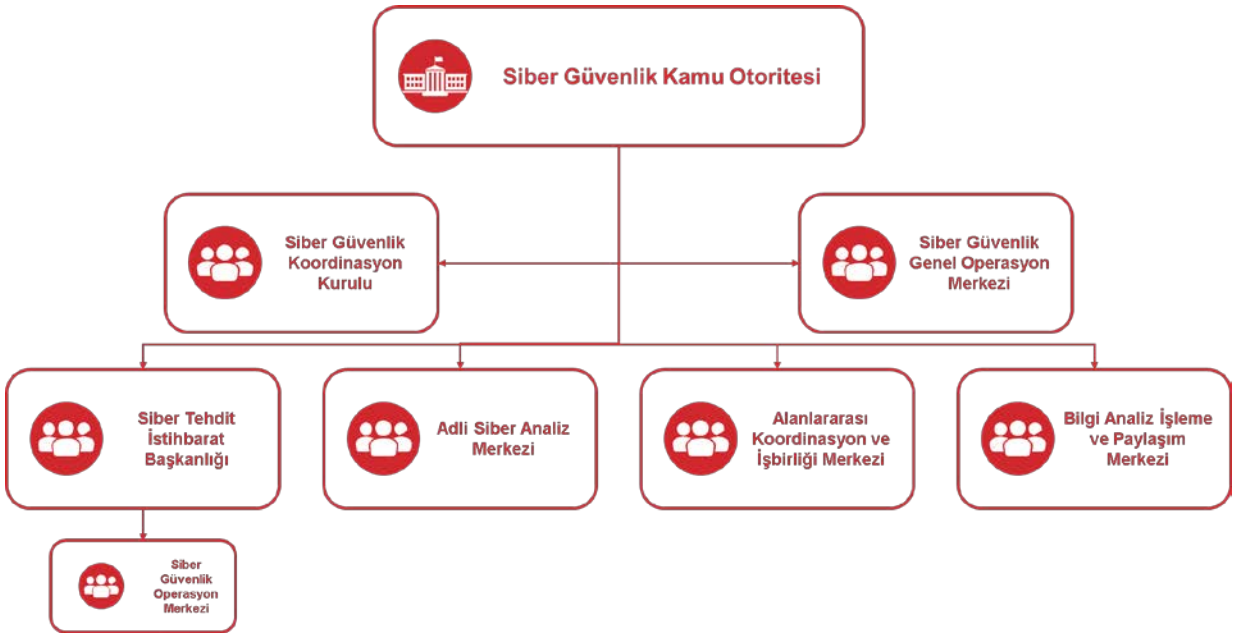
İran'da siber alanla ilgili tüm faaliyetler devlet hiyerarşisinin bir numarasındaki ismin başkanlığındaki Siber Alan Konseyi tarafından yürütülmektedir. Siber güvenlik konusunu cumhurbaşkanlığına bağlayan **Azerbaycan** da sayısı artırılabilecek örneklerden sadece bir başkasıdır.

Ulaştırma Denizcilik ve Haberleşme Bakanlığı bünyesinde devam siber güvenlik eylem planı çalışmalarının sonucu olarak ortaya çıkan SOME ve USOM inisiyatiflerinin ilerlemesi için kademeli ve sıkı takip edilen bir program hayata geçirilmelidir. Bugüne kadar, çeşitli kurumlarda SOME ekipleri kurulmuş ancak etkili altyapılar hazırlanamamıştır. Bunun yanı sıra, SOME'lerin müdahale etmesi gereken saldırıların fark edilmesi için gerekli teknik altyapılar da yetersiz düzeydedir. Saldırıların engellenmesi için pro-aktif metotların benimsenmesi ve bu yaklaşıma sahip teknolojilerin kullanılması gereklidir. Bu kapsamda USOM'un da belli bir vadede bir Güvenlik Operasyonları Merkezi haline dönüştürülmesi ve teknik altyapısı kuvvetli SOME'ler ile entegre çalışması konusu değerlendirilmelidir.

Dikkat çekilmesi gereken önemli bir nokta, sadece devlet kurumlarının çabasının ulusal güvenliğe yönelik siber tehditleri alt etme konusunda yeteri olmayacağıdır. **Sivil toplum, üniversite ve özel sektör** çapında yapılacak çalışmalar ve geliştirilecek iş birlikleri ulusal siber güvenliği güçlendirilmesi ve ülkemizin siber caydırıcılığının arttırılmasında önemli paya sahiptir.

Aşağıda görülen tabloda siber güvenlik ile ilgili stratejimizde kurulması öngörülen kamu otoritesinin alabileceği kurumsal yapının genel şeması verilmiştir.

Siber Güvenlik Yönetişim Modeli



2. KAMU, **ASKERİ VE ÖZEL AĞLAR**IN KORUNMASI

Siber güvenliğin ülke yönetimlerinin gündemine geldiği ilk yıllardan itibaren bir güvenlik meselesi olması nedeniyle askeri kuvvetlerin direkt ilgi alanına girmiştir. Fakat günümüzde siber güvenlik sadece askeri kuvvetlerin çözüm getirebileceğinin ötesinde karmaşık problemler ortaya çıkartmış olmasına rağmen siber güvenliğin askeri boyutu önemini korumaktadır.

Stratejik siber güvenliğin gerilim alanlarından biri siber güvenlikteki asker sivil ilişkileridir. Türkiye'nin hazırladığı siber güvenlik stratejisi başarılı bir şekilde askeri ve sivil siber güvenliği ayırmış; siber güvenlik stratejisinde siber güvenliğin askeri boyutuna değinilmemiştir.

Türkiye'de Genelkurmay Başkanlığı'na bağlı olarak Siber Savunma Komutanlığı kurulmuştur. Askeri sistemlerin güvenliğinden sorumlu olan Komutanlık diğer askeri birimlerin siber güvenliğini güçlendirmek adına olumlu adımlar atmaktadır ve uluslararası siber tatbikatlarda ciddi başarılar elde etmektedir.

Siber güvenliğin savunma alanında, ülkeler komuta kademesi başta olmak üzere, askeri karar alma mekanizmalarındaki kişilerin siber alanın getirdiği fırsat ve tehditlere ilişkin bilinçlendirilmesi için ciddi eğitim yatırımları yapmaktadır. Harp akademileri bünyesinde siber güvenlik laboratuvarları kurulmakta, özel sektör ile etkili iş birlikleri tesis edilmekte ve askeri okul programlarına siber güvenlik dersleri konulmaktadır. Lisans ve yüksek lisans derslerinde devlet ve özel üniversiteler ile ortaklık kurulduğu gözlemlenmektedir. Türkiye'de yeni kurulan Milli Güvenlik Üniversitesi'nde siber güvenliğin farklı seviyelerinde dersler açılmasının siber güvenliğin milli güvenliğe entegrasyonu konusunda kritik öneme sahip olduğu değerlendirilmektedir.

Kamu kurumlarının dijital altyapısında bulunan bilgisayar ve iletişim ağların milli güvenliğin ayrılmaz bir parçası olarak değerlendirilmelidir. Bu bağlamda kamu ağlarının güvenlik denetimi tek bir kurumun sorumluluğunda toplanabilir. Gerekli durumlarda yeterli güvenlik kleransını sağlayan özel şirketlerden destek alınmalıdır. Kamu ağlarının güvenliği için kullanılan yerli/yabancı ürünlerin test aşamalarının sıkı denetim altında yapılması için de siber güvenlikle ilgili kurulması önerilen kamu otoritesi içerisinde ayrı bir birim oluşturulmalıdır.

Kamuya ait sistem ve uygulama envanterinin çıkarılması, merkezi olarak takibinin sağlanması ve kurumların kendi inisiyatifleri doğrultusunda, yetkili merci onayı olmadan servis başlatmamaları bütünsel ve tutarlı bir güvenlik ortamı için gereklidir.

Özel şirket ağlarının korunması her ne kadar firmaların kendi sorumluluklarında olsa da yabancı devlet destekli siber saldırganların koordineli bir şekilde Türk firmalarını hedef alması vakayı uluslararası bir boyuta taşıyacaktır. Böyle durumlarda hangi aşamadan sonra devlet kaynaklarının olaya nasıl müdahil olacağına dair bir yasal çerçeve hazırlığına ihtiyaç duyulmaktadır.

Türkiye'nin stratejisinin askerlerin siber güvenliğe yön verdiği Fransız ekolünden ziyade, sivil ve askeri siber güvenliğin bütünüyle farklılaşmadan ayrıldığı ABD ekolüne yakın olduğu söylenebilir.

ABD Savunma Bakanlığı siber güvenlik stratejisi hazırlayarak bir bölümünü internet üzerinden paylaşmıştır. Bu belgede ABD'nin siber alanı yeni bir muharebe alanı olarak gördüğü ve bu alanda ulusal çıkarlarına yönelen herhangi bir tehdidi yok etmek için elindeki gücü kullanacağını ilan etmiştir**. TSK'nın da kendine has siber güvenlik stratejisi geliştirmesi** ve kamuoyu ile kısmen de olsa paylaşması tavsiye edilebilir.

Ülkeler siber güç geliştirmek için sivil hackerlardan faydalanmaya çalışmaktadır. İngiltere'de hüküm giymiş hackerlar Merkez Bankası tarafından istihdam edilebilmektedir. **Çin'de** ulusal çapta düzenlenen hacker yarışmalarında başarılı olan gençler -18 yaşının altında bile olsa- Çin ordusu tarafından işe alınabilmektedir**. Rusya'nın**, Russian Business Network (RBN) adlı hacker grubunun Kremlin'den destek alarak Rus çıkarlarına hizmet eden siber operasyonlarda kullandığı ortaya çıkmıştır.

3. SİBER İSTİHBARAT

Siber istihbarat kavramı ili şekilde ele alınmalıdır. İlki siber yollardan istihbarat toplama ve istihbarata karşı koyma faaliyetleri, ikincisi ise siber tehdit istihbaratıdır.

Dijital yollardan elde edilen istihbarat bugün gizli servisler için vazgeçilmez bir hal almıştır. MİT çatısı altında yer alan 'Sinyal ve Elektronik ve Teknik İstihbarat' yapısının, ABD deki benzeri 'National Security Agency' veya 'Ulusal Güvenlik Müsteşarlığı' adı ile MİT, Asker, Jandarma ve Polis istihbarat birimleri dışında, bağımsız olarak, Başbakanlığa Bağlı bir Müsteşarlık olarak yapılandırılması değerlendirilmiştir.

Bilimsel-Elektronik ve Teknik İstihbarat üst düzeyde bilişsel ve teknik uzmanlık bilgi birikimi gerektirmektedir. Kadrosunda, bir çok bilim insanı, üst düzey uzman, matematikçi çalıştırması gerekir. İnsan istihbaratı ile uğraşan birimlerden yapısal olarak çok farklıdır. Bilimsel ve Teknik İstihbaratçıların aynı çatı altında olması durumunda çok anlamsız ve olumsuz rekabet ortamı oluştuğu tecrübe edilmiştir.

Her türlü elektronik ve bilişim ortamında gönderilen bilginin toplanması, toplanan bilginin bilimsel yöntemlerle değerlendirilmesi, değerlendirme sonuçlarının istihbarat raporları olarak yayınlanması faaliyetleri ile, teknik istihbarata karşı koyma faaliyetlerini icra etmesi öngörülmektedir.

Siber tehdit istihbaratı konusunda ise uluslararası güvenlik şirketleri ile verimli bilgi paylaşım sistemi kurulması Türkiye açısından kaçınılmazdır. Siber suçlular için bir 'cennet' haline gelmekte olan ülkemizde siber güvenlik şirketleriyle kazan-kazan anlayışıyla yapılacak ortak çalışmalar Türkiye'nin siber suçlarla mücadelede işini kolaylaştıracaktır.

4. KRİTİK ALTYAPI GÜVENLİĞİ

Kritik altyapılar vatandaşların yaşamsal faaliyetlerini devam ettirebilmesi için gerekli olarak tanımlanan kritik altyapıların işlevine kısmen ya da tamamen yerine getiremediği takdirde, toplumsal düzen ve kamu otoritesi olumsuz etkilenmektedir.

Temel olarak kritik altyapılar, ulaşım, haberleşme, enerji finans sektörlerinde bulunan ağ, varlık ve sistemleri kapsarken **üzerinde uzlaşma sağlanmış bir kritik altyapı tanımı olmadığının altı**

çizilmelidir. Ülkeler açısından kritik altyapıların tanımlanması ve sınıflandırılması siber güvenliğin bu alt başlığında atılacak adımların başında gelmektedir. Temel olarak günlük yaşamın devamını sağlayan sistemler olarak adlandırılsa da ülkelerin özel durumlarına göre kritik altyapı listesinde bazı farklılaşmalar gözlemlenmektedir. Milli sembol olarak tanınan anıtlar ve devlet yetkililerinin kullandığı ulaşım araçları kritik altyapılar arasında sayılabilirken, coğrafi konumdan dolayı bazı kritik altyapıların öncelik sırası da değişebilmektedir. 15 Temmuz kalkışmasında da görüldüğü üzere Cumhurbaşkanı Tayyip Erdoğan'ın uçağının güvenliği ülkemizin geleceğini etkileyebilecek önem seviyesine sıçramıştır. Bu itibarla ivedilikle kritik altyapıların belirlenmesi çalışması sonuçlandırılıp öncelik sıralaması yapılaması gerekmektedir.

Kritik altyapılarının belirlenmesinin yanı sıra, kullanılan sistemlerin güvenlik süreçlerinin benzer şekilde yürütülmesi ve **farklı aktörler arasında bilgi paylaşımı sağlanması** ulusal siber dayanıklılık adına önemlidir. Dünyada olduğu gibi Türkiye'de de kritik altyapıların ciddi bir kısmı özel sektör tarafından yönetilmektedir. Özel sektörü hedef alan bir siber saldırının gün yüzüne çıkması ve gerekli paydaşlarca bilinmesi kurumun/şirketin itibari göz önüne alındığında tercih edilen bir yol değildir. Bundan dolayı siber saldırının hedefindeki özel kurum saldırıyı saklamayı tercih edebilmektedir. Böyle bir durum ise diğer kritik altyapı işletmecilerinin aynı siber saldırıya karşı savunmasız bırakmaktadır. Kritik altyapı işletmecileri arasında kendilerinin itibarını zedelemeyecek şekilde bir bilgi paylaşım mekanizması kurulması gereklidir.

Kritik altyapıların korunmasında özel sektör ve kamu arasında çizilmesi gereken sınırlar ve oluşturulması elzem olan düzenlemeler bulunsa da bir diğer çekişme alanı sivil ve askeri kurumlar arasındaki yetki paylaşımıdır. Güvenlikten sorumlu olan TSK'nın hangi durumlarda sivil alanlara müdahil olacağı konusu bir soru işaretidir.

Dijital bir sistemle yönetilen bir barajın kapakları yabancı devlet destekli hackerlar tarafından kontrolü ele geçirilerek etrafındaki yaşam alanlarına bir güvenlik tehdidi oluşturduğunda barajın idare eden özel sektör temsilcisi bu tehdide karşılık vermede yetersiz kalabilir. Böyle bir durumda devletin hangi kurumunun devreye gireceği, hangi seviyeden sonra askerin işin içine dahil olacağı süreçlerin hazırlığı bir an önce tamamlanmalıdır. Fiziksel dünyada toplumsal olaylara askerin

Kritik altyapıların toplumsal hayatın sağlıklı bir şekilde devamı açısından taşıdığı önem, kritik altyapıları terör örgütlerinin ve kitlesel karışıklık çıkartmak isteyen grupların başlıca hedefleri arasına sokmuştur. IŞİD'in gerçekleştirdiği Paris saldırılarının arkasından **İngiltere'de** resmi yetkililer IŞİD'in siber saldırılar ile kritik altyapıları hedef alabileceğine dair basına açıklama yapma gereği duymaları bu endişenin bariz göstergelerinden biridir. Aynı şekilde **Belçika hükümeti** nükleer tesislerin siber teröristler tarafından hedef alınacağına dair rapor yayınlamıştır.

müdahalesine izin veren EMASYA protokolü bulunmaktadır. Buna benzer bir protokol sivil-asker, kamu-özel sektör yetki ve müdahale alanını belirlemek için faydalı olabilir.

Kritik altyapı güvenliğini sağlamak için, satın alma dahil her türlü süreçte regülasyonlar ve standartlar olmalı. Örneğin bir ihaleye çıkılırken en çok hangi oranda ithal ürün müsaadesi olacağı ve kaynak ülkelerin sınırlandırılması gibi konular tanımlanmalı.

5. SİBER DİPLOMASİ

Siber diplomasi tanımının yıllar içerisinde farklı şekilde kullanıldığı görülmüştür. Devletlerin konvansiyonel diplomatik kanalların ötesine geçerek sosyal medyayı halklara mesaj gönderme yöntemi olarak benimsemesi siber diplomasi olarak adlandırılmıştır. Fakat bugün siber diplomasi kavramı bir devletin siber güvenlikle ilgili uluslararası platformlarda izlediği politika ve İnternet yönetişimi konusundaki stratejisinin bir bütünü olarak kullanılmaktadır.

Türkiye'nin siber güvenlik stratejisinde siber diplomasi ayrı bir başlık olarak ele alınmasa da çeşitli konularda uluslararası iş birliğinin önemine dikkat çekilmiştir. Siber diplomasi çalışmalarının yoğunlaşması gelen alanlar arasında siber norm oluşturma çabaları, siber suçlarla mücadelede iş birliği ve İnternet yönetişimi gelmektedir.

BM NEZDİNDE YAPILABİLECEK ÇALIŞMALAR

Siber alanın yeni bir operasyonel mecra olarak uluslararası ilişkilerin bir parçası haline gelmesi, hem uluslararası savaş hukuku hem de uluslararası ilişkileri düzenleyen Birleşmiş Milletler (BM) gibi kurumları değişime zorlamaktadır.

BM nezdinde bilgi ve siber güvenlik ile ilgili devam eden çalışmaların başında **Group of Governmental Experts on Information Security (GGE)** gelmektedir. Siber alanda istikrar ve anlaşmazlıkların önlenmesi için gereken adımları belirlemeyi amaçlayan çalışma grubunun uluslararası normlar oluşturma öncelikli hedefleri arasında yer almaktadır. Devletlerin siber alanda izledikleri politikaları sınırlayan norm, kural ve prensipler ile sorumlu devlet davranışlarının belirlenmesi konusunda rapor yayınlamaktadır. 2004'den bu yana faaliyet gösteren 20 üyeli grubun çalışmalarına Türkiye'nin bu zamana kadar katılmaması dikkat çekicidir. BM nezdindeki Türkiye temsilciliğinin bu konuda adım atması yeni bir dünya kurulurken Türkiye'nin de o dünyada yerini alması konusunda belirleyici olacaktır.

NATO NEZDİNDE YAPILABİLECEK ÇALIŞMALAR

Türkiye'nin önemli üyeleri arasında bulunduğu NATO siber alanı bir muharebe alanı olarak kabul edip, 2016 Temmuz ayında düzenlediği zirvede tıpkı kara, hava ve denizde olduğu gibi siber alanda da müttefiklerini etkin şekilde savunma kararı almıştır.

İttifak'ın siber güvenlik alanında yürüttüğü iki önemli proje bir düşünce kuruluşu olarak çalışan Mükemmeliyet Merkezi ve uluslararası hukuk alanında yapılan çalışmalardır. Estonya'nın başkenti Tallinn'de kurulan **Müşterek Siber Savunma Mükemmeliyet Merkezi** (CCD COE) her geçen sene

etkinliğini artıran önemli bir kuruluş haline gelmiştir. Türkiye'nin de üye olduğu Merkez'de ülkemiz sivil ve asker olmak üzere her dönem iki devlet personel bulunmaktadır. Türkiye'nin Merkez'deki etkinliğinin artması için sivillere yönelik iş birliği imkanlarının geliştirilmesi gerekmektedir. Almanya ve İngiltere'nin bu konuda attığı adımlarla üniversitelerinde çalışan araştırma görevlilerinin Merkez'le ortak proje yürütmesinin yolu açılmıştır. Benzer bir fırsat Türk araştırmacılar için de oluşturulabilir.

Siber alanın bir muharebe alanı olarak kabul edilmesi siber savaş hukuku çalışmalarının da gerekliliğini ortaya çıkarmıştır. Bu konuyla ilgili NATO bünyesinde dünyanın birçok yerinden uzmanların katılımıyla Tallinn Manuell kitabı yazılmıştır. Daha sonra güncellenerek Tallinn Manuel 2.0 yayınlayacaktır. İlk kitap için yapılan çalışmada 20 uluslararası hukuk uzmanı katılırken, ikincisinde 50'ye yakın ülkeden uzman katkı sunmuştur. Siber alanda devletlerarası anlaşmazlıklarda temel metin olarak kabul edilebilecek bu metnin yazılmasında Türkiye'nin önceliklerinin yansıtılması adına aktif katkı sunulması belirleyici bir etki oluşturması beklenmektedir.

NATO'nun her kademesine ciddi katkılar sağlayan ülkemizin siber güvenlik alanında İttifak'ın çalışmalarına vermekte olduğu/vereceği katkı ulusal siber güvenliğin güçlendirilmesinde önemli rol oynayabileceği düşünülmektedir. Dünya'da da örnekleri görüldüğü üzere, kamu ve özel sektör siber tehditlere karşı yetenekleri paylaşarak mücadele yöntemine başvurmaktadır. Bu açıdan bakıldığında NATO'nun siber güvenlik çalışmaları içerisinde yer alan sivil/asker personelin görev sürelerinin sonunda kazandıkları tecrübeyi sadece bağlı bulundukları kurumla değil, diğer kamu kuruluşlarıyla hatta özel sektör ile paylaşabileceği bir bilgi paylaşımı mekanizması ulusal siber güvenlikte dünya standartlarına yaklaşabilmek için kritik öneme sahiptir.

AVRUPA KONSEYİ BÜNYESİNDE YAPILABİLECEK ÇALIŞMALAR

Avrupa Konseyi 2001 yılında siber suçlarla mücadele konusundaki ilk uluslararası dokümanı yazarak üye devletlerin imzasına sunmuştur. İçerisinde Türkiye'nin de bulunduğu 50 kadar devlet telif hakları, bilgisayar suçları ve çocuk pornografisine kadar geniş kapsamlı suçlarda ulusal kanunlar arasında uyum sağlanmasını hedeflemektedir. Türkiye'nin 2015 yılında yürürlüğe koyduğu Konvansiyonun önemli eksikliklerinin başında güncelliğini kaybetmesi gelmektedir. Siber suçlarla mücadele Türkiye'nin siber güvenlik stratejisinde de bulunan uluslararası iş birliğinin en çok ihtiyaç hissedildiği alandır. Bu sebeple Türkiye'nin siber suçlarla mücadelede Budapeşte Konvansiyonu'nun güncellenmesi sürecinde aktif rol alması, ikili iş birliklerin oluşturulmasında önemli rol alacaktır.

6. EKONOMİ

Siber güvenlik pazarı hem ürün hem de istihdam açısından siber güvenlik stratejisinde yer alması gereken bir konudur. Güvenlik uzmanı istihdamındaki açık tüm dünyada giderek artmaktadır. 2016 yılında dünya çapında 1 milyon pozisyon açığı doldurulamamıştır ve bu rakamın 2019'da 6 milyona ulaşması beklenmektedir. Ülkelerin ve şirketlerin siber güvenlik bütçeleri her geçen yıl artmaktadır.

Siber güvenlik pazarında ekonomik anlamda avantaj kazanılması **için ürün geliştirme, istihdam üretme ve yönetişim danışmanlığı** olarak üç farklı alana odaklanılması bir öneri olarak değerlendirilebilir. Küresel çözüm getirmeyen bir ürünün yerel markette de uzun vadeli ayakta kalamayacağı gerçeğinden hareketle ürün geliştirmede güvenlik piyasasının temel ihtiyaçları ve öne çıkan trendler takip edilmelidir.

Yerli ürünün geliştirilmesi için devlet desteğinin fark yaratan bir faktör olduğu göz ardı edilemez. Fakat güvenlik gibi bir konuda oluşacak küçük bir zafiyetin ortaya çıkaracağı kayıp ciddi boyutlara ulaşabileceğinden **desteklenecek ürünlerin uluslararası muadillerinden geri kalmaması kritik öneme sahiptir**. Hedef yurtdışında rekabet edebilir bir ürün geliştirmek olursa, uzun süreli, teknolojik yönelimlerin düzgün şekilde takip edildiği ve teknoloji üreten bir altyapıya kavuşulmuş olur. Bunu yapabilmek için tamamen kapalı yazılımlar yerine, açık kaynaklı, ''crowd sourcing'' (işin kalabalık topluluklara yaptırıldığı) modellerin kullanıldığı yazılımlar teşvik edilmelidir.

Finans sektöründeki ihtiyaçları karşılamaya yönelik kurulan startup firmaların oluşturduğu FINTECH ekosistemi, sağlam ürün ve firmaların yeşermesine olanak sağlayacak bir sektörel girişim örneğidir. Bunun bir benzeri siber güvenlik dünyası için de oluşturulabilir.

Yerli ürünlerde kötü niyetli güvenlik açıklıklarının bulunmaması güvenli kullanım için önemli olsa da yeterli değildir. Yerli ürün teşviki dikkatli şekilde dizayn edilmeli ve ürünün global pazarlara hazırlanmasına yardımcı olmalıdır. Kamu kurumlarında kullanılmak üzere alınan güvenlik ürünlerinin

Türkiye'nin yakın bölgesi siber güvenlik açısından ciddi fırsatlar barındırmaktadır. Irak'ın kuzeyinde petrol ihracatının artmasıyla birlikte kritik altyapı hizmetlerinde siber güvenliğe duyulacak ihtiyaçtan, siber alanda önemli tehditlere hedef olan Gürcistan'a kadar birçok ülke gerek ürün, gerek uzman yetiştirme gerekse de yönetişim konularında verilecek desteğe ihtiyaç duymaktadır. Türkiye'nin arkasında durduğu siber güvenlik firmalarının çevre ülkelerde faaliyet göstermesi sadece ticari değil aynı zamanda diplomatik ve jeopolitik olarak da stratejik seviyede ele alınmalıdır.

satın alımında gerek yerli gerek yabancı ürünlerin aynı test süreçlerinden geçmesi gereklidir. Yerli ürün teşviki üretim sürecinde olduğu gibi üretim sonrası satış sürecinde de devam etmelidir.

Türkiye'de siber güvenlik alanında çalışan ve uzmanlık geliştiren pek çok firma bulunmaktadır. AR-GE destekleri ve bu konudaki akademik birikim de göz önünde bulundurulduğunda, bunları ulusal bir hedef etrafında çalıştırabilmek için bir koordinasyon sağlamak ve her parçanın kendi işlevini en iyi şekilde yerine getireceği bir yapılanma dahilinde bütünü oluşturmak en önemli hedef olmalıdır.

7. EĞİTİM

Siber güvenlik eğitiminin iki ana başlık altında ele alınması ulusal siber dayanıklılığı artırmada etkili olduğu değerlendirilmiştir. Ülkenin ulusal siber gücüne katkı yapacak ve kamu ve özel sektörün **siber uzman ihtiyacına cevap verecek iş gücünü geliştirmek** için gereken eğitim programlarının yanında, **her yaştan internet kullanıcısının farkındalığını artırmak** için düzenlenecek eğitim programları da siber güvenlik için vazgeçilmez adımlar arasında yer almalıdır.

Uzman yetiştirme konusunda hedef odaklı ve stratejik hareket etmek verimli sonuçların ortaya çıkmasına yardımcı olacaktır. Değişim yapısı gereği siber alanın kaçınılmaz bir unsurudur. Bu yüzden **uzman yetiştirilirken yeni gelişmekte olan alanlara öncelik verilmelidir.** Ülkenin elindeki insan kaynağından mümkün olan faydanın kazanılması için uluslararası güvenlik piyasası yakından takip edilmeli eğitim programları ona göre güncellenmelidir.

Uzman yetiştirmede kilit rolü üniversiteler oynamaktadır. Dünyada siber güvenlik lisans programlarının bir parçası haline gelmekte iken, Türkiye'de açılan yüksek lisans programlarının sayısı bile sınırlı sayıda kalmaktadır. Siber güvenliğin lisans eğitiminde nasıl yer alacağı konusunda akademisyenlerin yapacağı bir çalışma yol gösterici olacaktır. Güvenlik piyasası işverenleri adayların sahip olduğu güvenlik programlarına ait sertifikalara en az diploma kadar önem vermektedir. Lisan ve yüksek lisans eğitiminde öğrencilere sertifika kazandırmaya yönelik programların düzenlenmesinin önemli olacağı ifade edilmektedir.

Ulusal bir kurum tarafından üniversitelerde açılan bölüm ve programların yetkinlik derecesine göre sınıflandırma yapılması ve bu kurumdan sertifika alınması gibi bir seçenek açılan programların yeterliliğini artırmada yardımcı olacaktır**. NSA ve GCHQ'nun** yeni başlattıkları uygulama bu konuda örnek teşkil edebilir. Bu iki kurum ABD ve İngiltere'de siber güvenlik programı başlatan üniversiteler eğer isterlerse denetleyip gerekli kriterleri taşımaları durumunda sertifika vermektedir ki bu belge ile okullarda sunulan siber güvenlik eğitiminin yetkinliği tescil edilmiş olmaktadır. Böyle bir uygulamanın Türkiye'de olması gereklilik arz etmektedir.

Hem uzman yetiştirme hem de farkındalık eğitimleri konusunda adım atılması gereken önemli mecralardan biri de liselerdir. Bilgisayar bilimlerine eğilimi olan gençlerin eğitimine üniversiteye girmeden destek olmak ve yol göstermek birçok gelişmiş ülkede sıradan bir uygulama halini almıştır.

Siber güvenlik ile ilgili sadece üniversite değil aynı zamanda lise öğrencilerini de kapsayacak yaz ve kış kampları düzenlenmelidir. Düzenlenecek kamplar ile yatkınlığı bulunan gençler tespit edilerek kendilerine gerekli imkânın verilmesinin yolu açılacaktır. Çin ülkedeki yetenekli hackerları bu sayede bulmakta ve sonrasında milli çıkarlarına uygun şekilde istihdam edebilmek için donanımlı bir eğitim programından geçirmektedir. Dünyada özel şirketlerin de düzenlediği siber güvenlik yarışmaları bulunmaktadır.

Yukarıda sayılan adımların dışında siber yeteneklerin keşfedilmesi ve desteklenmesi açısından üzerinden çalışılması gereken başka bir alanda örgün eğitim dışında kalan ve/veya bilgisayar bilimleriyle ilgisiz alanlarda bulunan öğrencilerdir. Sivil toplum kuruluşlarının ve meslek örgütlerinin bu kişilerin siber alanın karanlık tarafından legal kısmına geçmede önemli bir rol oynayabileceği değerlendirilmektedir.

Farkındalık eğitimi ise uzman yetiştirmeden daha kapsamlı ve tüm internet kullanıcılarını içine alan bir konudur. 1980'lerde başlatılan ve okuma yazmayı yaygınlaştırması amaçlanan ülke çapındaki kampanyalar gibi güvenli internet kullanımı için benzer bir seferberlik düzenlenmesi ulusal güvelik meselesi olarak görülmelidir. Çeşitli konularda hazırlanan **kamu spotlarına** internet güvenliğinin eklenmesi gibi medya yollarının kullanılmasından, kamusal alanlardaki kısa ve etkili bilinçlendirme faaliyetlerine kadar geniş kampanyaların düzenlenmesi ulusal siber dayanıklılığın artırılmasında öncelikli adımlar arasında yer almaktadır. ABD'de düzenlenen **'Ulusal Siber Güvenlik Ayı'** benzer bir kampanya için örnek teşkil edebilir.

Farkındalık eğitiminin bir başka boyutu bugün yönetici pozisyonunda olan fakat internet ile yetişmeyen kadroların yaşanan siber değişime uyum sağlamaları konusunda destek verilmesidir. Siber alanın yeni bir mücadele alanı olduğunun kavranması, çeşitli fırsat ve tehditlerin farkındalığının kazandırılması hem kamu hem de özel sektör için siber güvenlik adına çok önemli bir engeli ortadan kaldıracaktır. Teknoloji ile iç içe çalışan sektörlerde dahi yöneticilerin dijital dünyanın güvenlik boyutunu benimsemesi zaman alan ve bazen başarısızlıkla sonuçlanan bir süreç olduğu tecrübe edilmiştir. Bu nedenle üst yönetimlere yönelik geniş kapsamlı farkındalık eğitimleri siber güvenlik konusunda ulusal boyutta ciddi bir sıçramaya neden olabilir.

İstihdam edilen personelin seviyesinin artırılması ve güncel tehditlere karşı kendilerini geliştirmeleri ulusal siber dayanıklılığın temel unsurlarından biridir. Bunun yanında kamu ve özel sektörde bulunan ve siber güvenlikten sorumlu personel ve yöneticileri arasında bilgi paylaşımı ve birlikte çalışma tecrübesi geliştirilmelidir. Özellikle ulusal ve sektöre Siber Olaylara Müdahale Ekipleri (SOME) ile kritik altyapı yöneticilerinin bir araya getirildiği platformların varlığı kısa vadede dahi olumlu sonuçlar doğuracaktır.

Kamu ve özel sektördeki siber güvenlik ekiplerinin bir değişim programına tabi tutulmasının ulusal siber güvenliğin geliştirilmesinde gözle görülür fayda sağlayacağı değerlendirilmiştir.

DİJİTAL TÜRİYE

PLATFORMU

Dijital Türkiye Platformuna Ait Bilgiler

Dijital Türkiye Platformu İletişim Bilgileri

Kemankeş Karamustafa Paşa Mah. Alipaşa Değirmeni Sok. No:3 34560 Karaköy / İstanbul

Tel: +90 (212) 244 11 69

e-mail: info@tbv.org.tr

“Digital Europe” yapılanması paralelinde kurulan **“Dijital Türkiye Platformu”,** AB'de bir çatı kuruluş olarak ortaya çıkan “Digital Europe”un Avrupa Birliği Dijital Ajanda 2020 vizyonu ile Türkiye'nin 2023 hedeflerinin aynı doğrultuda yürütülmesi amacıyla biraraya gelmiş ortak bir sivil toplum çalışma grubudur.

Türkiye’de bilgi, iletişim ve elektronik alanında faal dört sivil toplum örgütü TBV, TÜBİSAD, TBD, TESİD olarak bizler,Türkiye’nin AB üyelik adaylığının ulusal bir hedef olduğu inancı ile AB’nin yol haritalarını, ülkemiz için yol haritası olarak benimsiyor, AB’nin 2020 hedeflerini, ülkemizin ekonomik ve sosyal büyüme hedefleri olarak kabul ediyoruz.