SİBER VATAN VE SİBER GÜVENLİK

Siber Tehditlerle Mücadele Örgütlenmesinde Türkiye Örneği

Dr. Alper BİLGİÇ
Jandarma ve Sahil Güvenlik Akademisi

Türk Dil Kurumunun Güncel Türkçe Sözlüğünde "siber" kelimesinin bir karşılığı bulunmamakta ancak bir ön ek olarak eklendiği kelimenin bilgisayarla ve uygulayım bilimiyle (teknolojiyle) ilgili olduğunu ifade etmek için günlük kullanımda kendine yer bulduğu görülmektedir.[1] Ayrıca terimin, anılan sözlükte "güdüm bilimi" olarak tanımlanan "sibernetik" kelimesinin köküne dayandığı ileri sürülebilir. Norbert Wiener tarafından "hayvanlarda ve makinelerde kontrol ve iletişim işlemleri" olarak tanımlanan "sibernetik", en genel anlamda, örgütlü sistemlerde haberleşme ve kontrol mekanizmalarını inceleyen sevk ve idare bilimi olarak ifade edilebilir.[2] Bu bağlamda, siber alanın gelişimi örgütlü bir sistem ve bunun üzerinde gerçekleşen iletişim olarak yaşamın birçok alanına tesir etmektedir. 1950'lere dayanan bilgisayar ağı üzerinden etkileşim ve iletişim sürecinin başlangıcında bilgisayar ağlarına yetkisiz erişim yasak değildi.[3] Giderek artan sayıda bilgisayarın birbirine bağlı hale geldiği bir ortamda bilgisayar sistemlerinin istismarının yaygınlaşması buna bakış

1 Türk Dil Kurumu, 2019

2 Tortop, İsbir, Aykaç, Yayman ve Özer, 2012

3 Warf, 2018, s.128

açısını da değişmiştir.[4] Bir yandan bilişim teknolojilerinin artan kapasitesi toplum olarak çalışma ve işleyiş biçimini dönüştürmek açısından benzersiz etkiler yaparken, diğer yandan teknolojik ilerlemeler aynı zamanda kötüye kullanım ve zarar verme için de imkân yaratmaktadır.[5] Günümüzde bilgisayar kullanıcıları genel ağ üzerinde küresel anlamda etkileşimde bulunmaktadır. Bu da, olumlu yönleriyle birlikte, nispeten mesafenin önemsizleştiği ve sınırların bulanıklaştığı artan tehdit ortamının bir işaretçisidir. Bu ortam "doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler" olarak tanımlanan siber uzayda hayat bulmaktadır.[6] Siber uzay, siber alan veya siber dünya olarak da anılmaktadır. "Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğinin ihlal edilmesi" siber olay olarak tanımlanmaktadır.[7] Bu bağlamda, "siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünü" olarak ifade edilen siber güvenlik kavramı güvenlik kavramının çeşitlenmesine katkıda bulunmaktadır.[8]

4 Warf, 2018, s.128

5 McQuade, 2009, s.43

6 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023, s.10

7 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023, s.10

8 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023, s.10

Günümüzde gözlemlenen yeni güvenlik anlayışı çerçevesinde, güvenlik kavramının çeşitlenerek farklı başlıklar altında incelendiği görülmekle birlikte, literatürde yeni güvenlik alanlarının temel olarak: birey güvenliği, ekolojik güvenlik, ekonomi güvenliği, sağlık güvenliği, demografik güvenlik, doğal kaynakların güvenliği, enerji güvenliği, gıda güvenliği ile bilgi, bilişim ve teknoloji güvenliğini içerdiğini ifade edebiliriz.[9] Güvenlik çalışmaları bağlamında "Bölgesel Güvenlik Kompleksi Teorisi" önermesinin dayandığı şey mesafenin etkisidir.[10] Ancak, siber uzayın gelişimini de içeren birçok diğer teknik ve teknolojik gelişim ve yenileşimler ile birlikte, etkileşim kapasitesindeki devrimin mesafenin önemini aşındırdığı ve değişen süreçte küresel karşılıklı bağımlılık döneminin deneyimlendiği[11] ve örneğin, siber savaş hakkındaki kurguların da mesafenin bu alanda pek önemli olmadığı çatışma biçimlerine işaret ettiği[12] ileri sürülebilir. Küresel ölçekte uluslararası bir sistem içinde görünüşte küçülen dünyanın, teritoryal faktörü siyasî arenadan kaldıracağı beklentisinden de bahsedilmektedir.[13] Ancak, söz konusu genel küresel yapıya rağmen, önemli bölgesel farklılıkların olduğunu da unutmamak gerekmektedir.[14] Gücün ya da barışın türevi olarak güvenlik, devletin devamlılığı bakış açısından ulusal güvenlik mefhumu olarak ele alınmaktadır.[15] Bu durumda konu devlet kavramı bakımından ele alınabilir, fakat güvenlik alanında devlet dışı aktörlerin varlığı da unutulmamalıdır. Ayrıca, savaş kelimesini kullanmanın uluslararası hukukta da net bir karşılığı olmalıdır. Devletler, uluslararası hukukun temel süjesi olarak kabul edilmektedir.[16] Bu bağlamda, taraflar arasında vuku bulduğunu kabul edeceğimiz bir nevi vekâlet savaşında, devlet dışı aktörlerin devlet destekli oldukları ileri sürülse bile, ilgili devletin hedef devlete savaş açtığını kabul etmesi de beklenir. Tecrübe edilen bazı olaylarda malumun ilamı hayat bulmamış, suçlanan taraflar ithamı kabul etmemiştir. Siber alan, anonimlik sağlar ve asimetriktir.[17] En nihayetinde, savaş kelimesinin siber alandaki mücadelede doğru tercih olduğu şüphelidir çünkü savaş kavramında yenen ve yenilen taraflar arasındaki ilişkide galibin mağlup üzerinde iradesinin mutlak tahakkümü beklentisi doğmaktadır. Mevcut durumda, devlet yapılanmasında bu alan saldırılara karşı savunma odaklı bir görünüm sergilemektedir. Diğer taraftan, karşılanamayacak beklentiler yaratmak özellikle siber emniyet bağlamında,

Günümüzde bilgisayar kullanıcıları genel ağ üzerinde küresel anlamda etkileşimde bulunmaktadır. Bu da, olumlu yönleriyle birlikte, nispeten mesafenin önemsizleştiği ve sınırların bulanıklaştığı artan tehdit ortamının bir işaretçisidir.

9 Karabulut, 2009, s.141

10 Buzan, Wæver ve de Wilde, 1998, s.59

11 Buzan, Wæver ve de Wilde, 1998, s.163

12 Buzan, Wæver ve de Wilde, 1998, s.59

13 Buzan, Wæver ve de Wilde, 1998, s.163

14 Buzan, Wæver ve de Wilde, 1998: 164

15 Şahin, 2020, s.875

16 Gökçer, O. ve Gözen Ercan, P., 2020, s.193

17 Gökçer, O. ve Gözen Ercan, P., 2020, s.186

Siber güvenlik kapsamında oluşturulan örgütlenme ve yönetim modelinin anlaşılması bakımından devlet yapılanması içinde görevli birimleri incelemek faydalı olacaktır.

dinamik tehditler karşısında klasik tedbirlerin görece yetersiz kalması durumunda, güvensizlik ortamına ve politika üretiminde sorunsallığa evrilebilir. "Siber vatan"[18] yaklaşımı güvenlik bağlamında ele alındığında, bunun sayısallaşan (dijitalleşen) bir devlet anlayışının beraberinde gelen bir kavram olarak karşımıza çıktığını söyleyebiliriz. Siber vatan, ele alınan konuya da uygun olarak, devletin hak ve menfaatlerinin gözetilmesi gereken kavramsal bir alanı ifade edecek şekilde geniş anlamda düşünülebilir. Devletin önemli unsurlarından biri de onu meydana getiren insan topluluğudur. Modern güvenlik anlayışında insanının güvenliğini sağlamak için oluşturduğu devletin güvenliğini sağlamak bir araçsallık içermektedir. Bu bağlamda, toplumsal hayatta ihtiyaç duyulan düzeni de sağlaması beklenen devlet, kurduğu teşkilatlarla idari faaliyetlerini yürütür.[19]

Sosyal sözleşme teorisi anlatımıyla, özetle ve çalışma bağlamında en genel anlamıyla, kendisini oluşturan insanların güvende olma isteğiyle gücüne rıza gösterilen ve adına "devlet" denen aygıtın varlık amacına uygun olarak, söz konusu topluluğu oluşturan bireylerin, siyasal gücü elinde tutanlar tarafından o topluluğun ulaşmaya çalıştığı bu ortak amaca yönlendirilmesi süreci olarak kamu yönetiminin hem yapısal ve hem işlevsel yönleri bulunmaktadır. Bu bağlamda, devlet aygıtından beklenenin kamu düzenini sağlaması olduğunu söylemek yanlış olmayacaktır. Kamu düzeninin unsurlarından birinin de kamu güvenliği olduğu hatırlanacaktır. Kamu güvenliği, "tehlikelerin önlenmesi ve bu yapıyı meydana getiren unsurların devletle ve birbirleri ile ilişkilerinin ve varlıklarının tehlikelerden korunması durumu ve bu duruma ilişkin toplumda bir inanç oluşmasıyla, toplumsal yaşayışta güvenliğin sağlanmış olması halidir".[20] Bu ortam, iç ve dış güvenlik kavramlarıyla da ilişkilidir. Klasik güvenlik kavramsallaştırmasında bu kavramlar devletin toprak unsurunun sınırlarıyla ilişkilendirilerek tanımlanabilmektedir. Ancak çok yönlü ve karmaşık yeni güvenlik tehditleri bağlamında siber güvenlik alanında tespit ve tanımlamadaki zorluklar da göz önünde bulundurularak farklı düşünme ihtiyacı doğmaktadır. Sınırları aşan küresel bir olgu olarak internetin genel kullanıma açıldığı dönemden bugüne katlanarak gelişimiyle, etkileşimin ve hızının arttığı siber alanda gerçekleştirilen suç davranışları ve bunların failleri fiziksel sınırlardan bağımsız hale gelmiştir.[21] Siber suçların soruşturulması ve kovuşturulmasında yargı yetkisi sınırlarının tayini önemli bir problem sahasıdır.[22] Özellikle kolluk açısından, bu çerçevede karşılaşılan yeni nesil suç ortamında, değil belediye sınırının, ülke sınırının bile ifadesiz kaldığı ve kalacağı görülmektedir.

Siber güvenlik kapsamında oluşturulan örgütlenme ve yönetim modelinin anlaşılması bakımından devlet yapılanması içinde görevli birimleri de incelemek faydalı olacaktır. Türkiye'de "Siber Güvenlik Kurulu", kritik altyapıların belirlenmesine yönelik teklifleri karara bağlamak, siber güvenlikle ilgili politika, strateji ve eylem planlarını onaylanarak ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak, siber güvenlikle ilgili hükümlerden istisna tutulacak kurum ve kuruluşları belirlemek gibi görevleri yerine getirmek üzere 2012 yılında kurulmuştur.[23] O dönem Siber Güvenlik Kurulu'nun "Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden" teşekkül etmesi öngörülmüştür.[24] Anılan bu görevlerin, 2018 yılında yapılan

18 Batı Karadeniz Kalkınma Ajansı tarafından üst düzey Siber Güvenlik Uzmanlarının yetiştirilmesi için hazırlanan "BAKKA Siber Güvenlik Uzmanı Yetiştirme Projesi (Siber Vatan)" kullanılan bir kavram olarak ortaya çıkmıştır.

19 Bilgiç, 2019, s.30

20 Bilgiç, 2019, s.18

21 Marion ve Twede, 2020, s.xiv- xv

22 Warf, 2018, s.134

23 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar

24 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar

değişikliklerle, Cumhurbaşkanınca belirlenecek bir "kurul veya merci" tarafından sürdürüleceği düzenlenmiştir.[25] Genel anlamda, internet ortamının güvenli, serbest, özgür ve faydalı kullanımı ve sağlıklı gelişimine yönelik çalışmalar yapmak üzere 2011 yılında Ulaştırma ve Altyapı Bakanlığı bünyesinde İnternet Geliştirme Kurulu oluşturulmuştur.[26] İnternet Geliştirme Kurulu çatısı altında, sektör paydaşlarının katılımıyla siber güvenlik alanında çalışmalar yürütmek üzere Siber Güvenlik İnisiyatifi kurulmuştur.[27] Türkiye'de "siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak" için Siber Güvenlik Kurulu 2012 yılında kurulmuştur.[28] Sanayi ve Teknoloji Bakanlığı bünyesinde Türkiye'de ulusal siber güvenlik kapasitesinin artırılmasına yönelik çalışmalar yürütmek üzere 2012 yılında Siber Güvenlik Enstitüsü kurulmuştur.[29] Bilgi Teknolojileri ve İletişim Kurumu da siber güvenlik üzerine çalışmalar yürütmektedir.[30] Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığının ortaya koyduğu misyon doğrultusunda Cumhurbaşkanlığı Savunma Sanayii Başkanlığının desteğiyle, Türkiye'de "siber güvenlik ihtiyaçların tespiti ve yenilikçi yöntemlerle karşılanması için en üst düzey iş birliği ve eşgüdümü ve sağlıklı rekabet koşullarını sağlayarak ekosistemi geliştirmek ve bunun sürekliliğini sağlayacak mekanizmaları oluşturmak" için, ilgili tüm kamu kurum/kuruluşları, özel sektör ve akademi temsilcilerinin katılımlarıyla 2017 yılında Türkiye Siber Güvenlik Kümelenmesi oluşturulmuştur.[31]

Türkiye'de siber güvenlik alanında ilk "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" 2013 yılında yayımlanmıştır.[32] Müteakiben 2016-2019 yıllarını kapsayan ikinci strateji ve eylem planı belgesi ve en son olarak da 2020-2023 yılları arasındaki döneme ilişkin strateji ve eylem planı belgesi yayımlanmıştır.[33] Ayrıca, Türkiye'de siber güvenliğe ilişkin genel politika çerçevesinde örgütlenme ihtiyaçlarını karşılamak için, "siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması" maksadıyla; "internet aktörleri, kolluk güçleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişim ve koordinasyonu" temin etmek üzere 2013 yılında Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur.[34] USOM, "siber güvenlik olaylarına yönelik alarm, uyarı, duyuru faaliyetleri yapmakta, kritik sektörlere yönelik siber saldırıların önlenmesinde ulusal ve uluslararası koordinasyonu sağlamaktadır."[35] 2016-2019 strateji belgesi ve eylem planı kapsamında ulusal siber güvenlik kapasite inşası, teknolojik önlemler, tehdit istihbaratı edinimi, üretimi ve paylaşımı ile kritik altyapıların korunması programları yürütülmüş, 2020-2023 belgesi çerçevesinde siber güvenlik alanına yönelik faaliyetler sürdürülmektedir.[36] Bu alandaki yapılanmanın bir alt unsuru olarak Siber Olaylara Müdahale Ekipleri (SOME) teşkil edilmiş, bunlar da sektörel ve kurumsal olarak iki ayrı sınıfta tanımlanmıştır. Özetle, bakanlıklar ve diğer tüm kamu kurumları/kuruluşları ile Sektörel SOME'lerin bulunduğu sektörlerdeki kurumların/kuruluşların bünyelerinde Kurumsal SOME'ler kurulmaktadır. "Kurumsal SOME'ler kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla yükümlüdürler."[37] Kurumsal SOME'ler, bir "siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara" ve USOM'a bildirmekle yükümlü tutulmuşlardır.[38] Sektörel SOME'ler, "siber olayların önlenmesi veya za-

Türkiye'de siber güvenlik alanında ilk "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" 2013 yılında yayımlanmıştır.

25 2/7/2018 tarihli 703 sayılı KHK'nın 205'inci maddesi ile 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'na (Ek md.2) eklenmiştir.

26 Ulaştırma, Denizcilik ve Haberleşme Bakanlığı İnternet Geliştirme Kurulu Yönetmeliği, md.1

27 Siber Güvenlik İnisiyatifi, 2021

28 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı

29 Siber Güvenlik Enstitüsü, 2021

30 Bilgi Teknolojileri ve İletişim Kurumu, 2017a

31 Siber Kümelenme Projesi, 2019

32 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023

33 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023

34 Bilgi Teknolojileri ve İletişim Kurumu, 2017b

35 Bilgi Teknolojileri ve İletişim Kurumu, 2017b

36 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023

37 Bilgi Teknolojileri ve İletişim Kurumu, 2017b

38 Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, md.5

rarlarının azaltılmasına yönelik faaliyetlerini USOM'la koordineli şekilde yürütürler" ve "birlikte çalıştıkları SOME'lerde yaşanan siber olayları gecikmeksizin USOM'a bildirirler."[39] "Sektörel SOME'ler düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerinde (Enerji, bankacılık ve finans, ulaştırma, su yönetimi, elektronik haberleşme vb.) faaliyet gösteren kurum, kuruluş ve işletmeleri kapsayacak şekilde kurulur."[40] Cumhurbaşkanınca belirlenecek kurul tarafından kararlaştırılan kritik sektörlerde Sektörel SOME kurulması zorunlu kılınmıştır.[41] İhtiyaç duyulması durumunda diğer sektörlerde de sektörün ilgili olduğu Bakanlık bünyesinde Sektörel SOME'ler kurulabilmesine olanak tanınmıştır.[42] Bilgi Teknolojileri ve İletişim Kurumu (BTK), Sektörel SOME'lerin koordinesi sorumluluğunu taşımaktadır.[43]

Siber güvenlik kavramının kendisine görünür biçimde yer edinmeye başladığı Türkiye'nin idari yapılanması içinde 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesiyle kendilerine siber güvenliğe ilişkin kurum içi ve ülke geneli görevler tevdi edilen birimler bulunmaktadır. Bu kapsamda, diğer görevlerinin yanında:

- Cumhurbaşkanlığı Politika Kurullarından Güvenlik ve Dış Politikalar Kuruluna "siber güvenlik ile ilgili politika ve strateji önerileri geliştirmek"[44];
- Dışişleri Bakanlığının hizmet birimlerinden Bilgi Teknolojileri Genel Müdürlüğüne "siber güvenlik alanında (Dışişleri Bakanlığının) merkez ve yurtdışı teşkilatında gerekli önlemleri almak, siber güvenlikle ilgili çalışmalar yapmak"[45];
- Hazine ve Maliye Bakanlığının hizmet birimlerinden Bilgi Teknolojileri Genel Müdürlüğüne "(Hazine ve Maliye Bakanlığının) mevcut bilişim altyapısının kurulumu, bakımı, ikmali, geliştirilmesi ve güncellenmesi ile ilgili işleri yürütmek, haberleşme ve siber güvenliğini sağlamak ve bu konularda görev üstlenen personelin bilgi teknolojilerindeki gelişmelere uygun olarak hizmet içi eğitim almalarını sağlamak"[46];
- Kültür ve Turizm Bakanlığının hizmet birimlerinden Bilgi Teknolojileri Genel Müdürlüğüne[47] "(Kültür ve Turizm Bakanlığının) mevcut bilişim altyapısının kurulumu, bakımı, ikmali, geliştirilmesi ve güncellenmesi ile ilgili işleri yürütmek, haberleşme ve siber güvenliğini sağlamak ve bu konularda görev üstlenen personelin bilgi teknolojilerindeki gelişmelere uygun olarak hizmet içi eğitim almalarını sağlamak"[48];
- Milli Savunma Bakanlığının hizmet birimlerinden Muhabere ve Bilgi Sistem Dairesi Başkanlığına "Muhabere ve Bilgi Sistemleri Güvenliği, Kripto Güvenliği, TEMPEST Elektromanyetik Dinleme ve Dinlemeden Korunma Güvenliği, Siber Güvenlik, Elektronik Harp faaliyetlerini yürütmek, onaylamak ve denetimini yapmak"[49];
- Görevleri arasında "Ekonomik etki düzeyi yüksek ve birden çok sektörde gelişimi hızlandırma potansiyeline sahip ileri teknolojiler ile büyük veri, yapay zekâ, siber güvenlik gibi kritik alanlarda bireylerin ve işletmelerin ar-ge ve üretim yetkinliklerinin artırılması amacıyla politika önerileri ve stratejiler oluşturmak, belirlenen politika ve stratejilerin uygulanmasını sağlamak, ilgili alanlarda ar-ge ve yatırım faaliyetlerini ve girişimleri desteklemek, ilgili alanlara ve desteklere dair düzenleme ve denetlemeler yapmak"[50] da sayılan Sanayi ve Teknoloji Bakanlığı Bakanlığının hizmet birimlerinden, Milli Teknoloji Genel Müdürlüğüne "bilişim ve ileri teknoloji ürün ve sistemlerinin siber güvenlik ve bilgi güvenliği düzeyinin yükseltilmesine, siber güvenlik alanında yerli ve milli ürünlerin üretilmesine, yerli ve milli ürünlerin ülke genelinde kullanımının yaygınlaştırılmasına, veri merkezi ve veri işleme altyapısının güçlendirilmesine ve siber güvenlik ekosisteminin geliştirilmesine katkı sağlamak,

39 Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, md.7

40 Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, md.6

41 Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, md.6

42 Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, md.6

43 Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, md.6

44 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, md.26

45 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, md.143/Ç

46 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, md.227/A

47 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, md.287/C

48 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, md.287/C

49 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, md.343

50 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, md.385

destek ve teşvik programları uygulamak" [51];

- Görevleri arasında "bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek" ve "Görev alanına giren konularda politika ve strateji önerilerinde bulunmak"[52] da sayılan Cumhurbaşkanlığı Ofislerinden Dijital Dönüşüm Ofisinin hizmet birimlerinden,
  - Siber Güvenlik Dairesi Başkanlığına "Cumhurbaşkanınca belirlenen politikalar kapsamında kamu kurumları ve kritik altyapılara yönelik siber güvenlik stratejileri geliştirmek", "ulusal siber güvenlik ve bilgi güvenliğini destekleyici projeler geliştirmek", "siber güvenlik ile ilgili politika, strateji ve eylem planlarının ülke çapında etkin şekilde uygulanmasına yönelik gelişmeleri takip etmek", "siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşlar konusunda ilgili kurumlara önerilerde bulunmak", "kamu, özel sektör ve üniversiteler arasındaki işbirliğinin artırılması suretiyle ulusal siber güvenlik ekosisteminin oluşturulmasına katkı sağlamak", "özel sektörün kapasitesinin kritik alanlara yönlendirilmesi ve mükerrer yatırımların önlenmesi için öncelikli siber güvenlik alanlarını belirlemek", "kritik altyapılar başta olmak üzere her alanda, yerli ve milli siber güvenlik ürünlerinin geliştirilmesine ve bu çözümlerin kullanımının kamuda yaygınlaştırılmasına yönelik çalışmalar yapmak"[53] ve
  - Bilgi Teknolojileri Dairesi Başkanlığına da "(Dijital Dönüşüm Ofisinin) bilgi ve iletişim teknolojileri ve siber güvenliğinin sağlanmasıyla ilgili hizmetlerini yürütmek"[54] olarak yüklenen sorumluluklar arasında "siber güvelik" kavramı açıkça telaffuz edilmektedir.

Ayrıca, Milli İstihbarat Teşkilatının görevleri arasında "dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak"[55] hususları ve yetkileri arasında "telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabil(eceği)"[56] ifade edilerek istihbarat açısından siber güvenlik kavramına açıkça yer verildiği görülmektedir. Emniyet Genel Müdürlüğünün teşkilat kanununda "adli süreçlerin hızlandırılması amacıyla, siber suçlarla mücadele birimlerindeki adli bilişim incelemeleri ve siber suç analizlerinde personel yetersizliği nedeniyle ihtiyaç duyulan teknik personeli hizmet alımı yoluyla temin edebil(eceği)"

Siber vatan konseptinde, sayısallaşan bir dünyada meydana gelebilecek siber afetlere karşı da bütünleşik afet yönetimi ilkesine uyum ve bu sistem içerisinde ilgili aktörlerin kapasitesi de düşünülmelidir.

belirtilerek siber kelimesinin siber suçlarla mücadele bakımından kullanıldığı görülmektedir.[57] Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığının Siber Suçlarla Mücadele Daire Başkanlığı adında birimlerinin olduğu da bilinmektedir. Siber suçlarla mücadele kapsamında "Siberay" adında bir toplumsal farkındalık oluşturma projesi başlatıldığı görülmektedir.[58] Ayrıca, Jandarma Genel Komutanlığı bünyesinde MEBS ve Siber Güvenlik Komutanlığı adında ayrı bir birim de bulunmaktadır.

Genel anlamda, siber vatan konseptinde, sayısallaşan bir dünyada meydana gelebilecek siber afetlere karşı da bütünleşik afet yönetimi ilkesine uyum ve bu sistem içerisinde ilgili aktörlerin kapasitesi de düşünülmelidir. Daha özelde ise siber olaylar kapsamında gerçekleşen eylemlerin hem mülki hem de adli boyutu olacağı beklenilmelidir. Bu alanda suçları işlenmeden önleme, önlenemeyip işlenmiş

51 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, md.388/A

52 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, md.527

53 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, md.527/B

54 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, md.527/B

55 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu, md.4

56 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu, md.6

57 3201 sayılı Emniyet Teşkilat Kanunu, Ek md.35

58 Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, 2020

2020-2023 dönemi için stratejik amaçlar arasında da yer alan "siber güvenliğin milli güvenliğe entegrasyonu" büyük önem arz etmektedir.

olanları da aydınlatma kendine has zorlukları barındırmaktır. En önemlisi de suç fiilinin tespit edilmesiyle ilgili yönüdür. Kriminolojik açıdan suçun oluştuğunu önermek için sapma davranışının gerçekleşmesini tanımlayacak normun varlığı ve sapmanın hukuk düzeni içerisinde ceza yaptırımına bağlanmış olması gerekmektedir. Siber alan değişimin çok hızlı yaşandığı bir alandır. Bu alanda genel geçer tanımlama gayreti de kendi içinde belirli zorluklar taşımaktadır. Türkiye'de bu alandaki suç davranışını tanımlamada "bilişim alanında suçlar" ifadesinin tercih edildiği gözlemlenmektedir. Siber alandaki suçlar; genel anlamda, bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme, banka veya kredi kartlarının kötüye kullanılması ile yasak cihaz veya programlar alt başlıklarıyla 5237 sayılı Türk Ceza Kanunu'nda tanımlanmıştır. Bu alandaki eylemlere yönelik diğer temel mevzuat olarak Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi (Council of Europe Convention on Cybercrime), 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 5271 sayılı Ceza Muhakemesi Kanunu (md.134), 5809 Sayılı Elektronik Haberleşme Kanunu, 5846 sayılı Fikir ve Sanat Eserleri Kanunu, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 6102 Sayılı Türk Ticaret Kanunu, 5070 Sayılı Elektronik İmza Kanunu, 5187 sayılı Basın Kanunu, Markaların Korunması Hakkında Kanun Hükmünde Kararname yer almakta ve bunların yanında alt düzey mevzuat da bulunmaktadır. Ancak bu hukuki düzenlemelerin, sürekli değişime tabi bir alanda ihtiyaçlara cevap vermesi bakımından sürekli iyileştirme mantığıyla ele alınması gerekecektir.

Siber tehditlerle mücadele topyekûn bir mücadeledir, toplumdaki tüm kurum/kuruluşların yanında tüm fertlerin de bunun bir parçası haline getirilmesi gerekir.

Siber güvenlik olaylarına yönelik olarak gerçekleştirilecek müdahalelerde nihayetinde diğer unsurların yanında iç güvenliğin önemli bir parçası olarak kolluğun durumundan da bahsetmek gerecektir. Teknoloji her zaman iyi huylu değildir. Teknolojide gelişmeler, kolluğun suçla mücadele kapasitesini artırması için bir fırsatken aynı zamanda, genelde tüm toplumun özelde de bunlarla mücadelenin vasıtalarından biri olan kolluğun hilafına, suçlu düşünen beyinler için de artırılmış suç işleme imkân ve kabiliyeti yaratmaktadır. Bu durum, hem önleyici hem de adli bakımdan kolluğun kapasite inşası ihtiyacını perçinlemektedir. Kolluk örgütleri, yeni teknolojilerin görevlerine ve sorumluluk alanlarına etkisini sürekli takip etmeli, yeni nesil suçlara da karşı hem suçları önleme hem de işlenmiş suçların tespiti ve aydınlatılması için teknik ve idari yapılarını güçlendirmelidirler. Siber alanda gerçekleşen birçok farklı türde suç olduğundan, var olan tüm siber suçları listelemek zordur.[59] Ancak bilgisayar korsanlığı (hacking), çevrimiçi dolandırıcılık (online fraud), hizmet aksatma saldırısı (denial-of-service attacks), ve internette insanları gizlice takip etme (stalking), istenmeyen elektronik posta gönderme (spamming), kimlik hırsızlığı (identity theft), kötücül yazılım (malware), siber zorbalık (cyberbullying) ve taciz (harassment) günümüzde en yaygın görülenleri arasında sayılabilir.[60]

2020-2023 dönemi için stratejik amaçlar arasında da yer alan "siber güvenliğin milli güvenliğe entegrasyonu" büyük önem arz etmektedir. Ancak, bu bütünleştirmede takip, kontrol ve raporlamanın adımlarının ayrıntılı planlamasının yapılması gerektiği aşikârdır. Ayrıca, "ulusal siber olaylara müdahale organizasyonu" ortaya konmuş olsa da koordinasyona dayalı bu sistem içinde önemli rol üstlenen USOM biriminin yaptırım gücünün ne olduğu hususunun da belirlenmesi gerekir. Türkiye'deki çoklu kolluk sisteminde "emniyet ve asayiş işlerinde; il ve ilçelerde jandarma ile polis ve sahil güvenlik teşkilatları arasındaki ilişkiler ile asayiş toplantıları (...) Emniyet ve Asayiş İşlerinde İl, İlçe ve Bucaklardaki Jandarma ve Emniyet Ödevlerinin Yapılması ve Yetkilerinin Kullanılması Suretini ve Aralarındaki Münasebetleri Gösterir Yönetmelik hükümlerine göre yürütülür."[61] Bu münasebetlerin yürütülmesinde, sınır kavramının ortadan kalktığı siber alanda da eş-

59 Marion ve Twede, 2020, s.xii

60 Warf, 2018, s.130

61 Jandarma Teşkilat, Görev ve Yetkileri Yönetmeliği, md.50

güdümü ve yardımlaşmayı sağlamak ön planda tutulmalıdır. Ayrıca, devlet yapılanması içerisinde yöneticilerin seçmenlerine yönelik hizmet anlayışları neticesinde şekillenen siyasi tercihleri, devletin bu alanlara hizmet götürmek maksadıyla yeni birimlere sahip olmasına vesile olmaktadır.[62]

62 Bilgiç, 2019:10

Diğer kolluk faaliyetlerindeki görev konularının kapsamından en temel anlamda yer veya hizmet yönünden ve siber alan bağlamında hedef kitle bakımından farklılaşan; bu alana ilişkin düzenlemeleri uygulamak, bu konularla ilgili koordinasyonu sağlamak için bu özel konuda ve özel alanda görev yapmak üzere özel idari kolluk çerçevesinde genel idari kolluğun özel görev kolluğu olarak siber kolluk geliştirilmelidir. Ancak unutulmamalıdır ki, siber tehditlerle mücadele topyekûn bir mücadeledir, toplumdaki tüm kurum/kuruluşların yanında tüm fertlerin de bunun bir parçası haline getirilmesi gerekir.

KAYNAKÇA

1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi (01 Kasım 1983). T.C. Resmî Gazete (30474). https://www.mevzuat.gov.tr/MevzuatMetin/19.5.1.pdf adresinden 04 Haziran 2021 tarihinde alınmıştır.

2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar (11 Haziran 2012). T.C. Resmî Gazete (28447). https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf adresinden 04 Haziran 2021 tarihinde alınmıştır.

2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu (01 Kasım 1983). T.C. Resmî Gazete (18210). https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2937.pdf adresinden 04 Haziran 2021 tarihinde alınmıştır.

3201 sayılı Emniyet Teşkilat Kanunu (04 Haziran 1937). T.C. Resmî Gazete (3629). https://www.mevzuat.gov.tr/MevzuatMetin/1.3.3201.pdf adresinden 04 Haziran 2021 tarihinde alınmıştır.

5809 sayılı Elektronik Haberleşme Kanunu (5 Kasım 2008) T.C. Resmî Gazete (27050- Mükerrer). https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf adresinden 04 Haziran 2021 tarihinde alınmıştır.

Bilgi Teknolojileri ve İletişim Kurumu (2017b). *USOM ve Kurumsal Siber Olaylara Müdahale Ekibi.* https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi adresinden 05 Haziran 2021 tarihinde alınmıştır.

Bilgi Teknolojileri ve İletişim Kurumu, (2017a). *Siber Güvenlik. https://www.btk.gov.tr/siber-guvenlik-genel-bilgi* adresinden 05 Haziran 2021 tarihinde alınmıştır.

Bilgiç, A. (2019). *Düzenli Karmaşa: İç Güvenlik Yapılanmasında Çoklu Kolluk Sistemi.* Gazi Kitabevi, Ankara.

Buzan, B., Wæver, O. ve de Wilde, J. (1998). Security: A New Framework for Analysis. Lynne Rienner Publishers, Inc., Boulder.

Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı (2020). Siberay. https://www.siberay.com/hakkimizda adresinden 05 Haziran 2021 tarihinde alınmıştır.

Gökçer, O. ve Gözen Ercan, P. (2020). Siber Savaşlarda Jus Ad Bellum ve Jus In Bello. Alternatif Politika, 12 (1), s.172-203. https://alternatifpolitika.com/site/cilt/12/sayi/1/7-Gokcer%26Gozen-Ercan-Siber-Savas-Jus-Ad-Bellum-Jus-In-Bello.pdf adresinden 05 Haziran 2021 tarihinde alınmıştır.

Jandarma Teşkilat, Görev ve Yetkileri Yönetmeliği (12 Aralık 2016). Bakanlar Kurulu Kararı (2016/9741). T.C. Resmî Gazete (29955). https://www.mevzuat.gov.tr/MevzuatMetin/21.5.20169741.pdf adresinden 04 Haziran 2021 tarihinde alınmıştır.

Karabulut, B. (2009). Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek. Yayımlanmamış Doktora Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Marion, N.E. ve Twede, J. (2020). Cybercrime: An Encyclopedia of Digital Crime, ABC-CLIO, LLC., Santa Barbara.

Mcquade III, S.C. (2009). Encyclopedia of Cybercrime. Greenwood Press, Westport.

Siber Güvenlik Enstitüsü (2021). https://sge.bilgem.tubitak.gov.tr/tr/kurumsal/sge-tarihcesi adresinden 05 Haziran 2021 tarihinde alınmıştır.

Siber Güvenlik İnisiyatifi (2021). https://www.btk.gov.tr/siber-guvenlik-inisiyatifi adresinden 05 Haziran 2021 tarihinde alınmıştır.

Siber Kümelenme Projesi (2019). https://www.siberkume.org.tr/Index adresinden 05 Haziran 2021 tarihinde alınmıştır.

Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ (2013). T.C. Resmî Gazete (*28818*). *https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=19004&mevzuatTur=Teblig&mevzuatTertip=5* adresinden 04 Haziran 2021 tarihinde alınmıştır.

Şahin, G. (2020). Bölgesel Güvenlik Kompleksi Teorisi Kapsamında Somali ve Afrika Boynuzu'nun **Güvenliği; Aktörler, Tehditler ve Riskler.** Güvenlik Stratejileri Dergisi, 16(36), s.873-914 https://gsd.msu.edu.tr/Content/sayilar/dokuman/GSD_36/GSD_36_Art_4_122020.pdf adresinden 05 Haziran 2021 tarihinde alınmıştır.

Tortop, N., İsbir, E.G., Aykaç, B., Yayman, H. ve Özer, M.A. (2012). *Yönetim Bilimi.* Nobel Yayıncılık, Ankara.

Türk Dil Kurumu (2019). *Güncel Türkçe Sözlük.* http://www.tdk.gov.tr adresinden ulaşılmıştır.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı İnternet Geliştirme Kurulu Yönetmeliği. (2013). T.C. Resmî Gazete (*28851*). https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=19120&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5 adresinden 04 Haziran 2021 tarihinde alınmıştır.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023. https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf adresinden 05 Haziran 2021 tarihinde alınmıştır.

Warf, B. (2018). The SAGE Encyclopedia of the Internet. SAGE Publications, Inc., Thousand Oaks.