TEKNOLOJİNİN CASUSLUKTA KULLANILMASI VE KARŞI ÖNLEMLER

Samet OĞUZ, Eyüp Burak CEYHAN, Şeref SAĞIROĞLU*

***Özet*—Günümüzde teknoloji ile beraber istihbarat ve casusluk sınır tanımaz hale gelmiştir. Kurum ve kuruluşların özellikle de devletlerin siber uzaya bağımlı hale geldiği günümüzde siber istihbarat ve siber casusluk önemini arttırmıştır. Bu çalışmada siber istihbarat/casusluk faaliyetlerinin nerelerde yoğunlaştığı ve nasıl kullanıldığına değinilerek, bu faaliyetlere karşı alınması gereken önlemlerin neler olduğu ortaya konmaya çalışılmış, özellikle de kişi ve kurumların yapması gerekenler ortaya konulmuştur.**

***Anahtar Kelimeler*—Siber istihbarat, Siber Casusluk, Sosyal Mühendislik, Sosyal Ağlar, Casus Yazılımlar, Arama Motoru.**

***Abstract*— Today, through the technology, intelligence and espionage does not recognize borders. The characteristics of institutions and organizations, especially states, have become dependent on the cyberspace therefore importance of cyber intelligence and cyber espionage has increased. In this study, where the focus of cyber intelligence/espionage activities and how to use these activities are mentioned. Also what measures need to be taken against these activities, particularly the measures to be taken by the individuals and organizations are presented.**

***Index Terms*— Cyber intelligence, Cyber espionage, Social Engineering, Social Networks, Spyware, Search Engine**

I. GİRİŞ

Faydalı bilgiler toplayıp, değerlendirmeler yaparak karar vericilerin yoluna ışık tutmak anlamına gelen istihbarat ve casusluk, aynı zamanda karar vericilerin tespit ettiği uygulamalar doğrultusunda psikolojik eylem ve propaganda gibi vasıtalarla toplumların algılarına yön vermek anlamını da ihtiva etmektedir. Ortalama olarak yarım asrı geride bırakan, askeri açıdan bir disiplin haline gelen istihbarat ve casusluğun yönetimi, hedefleri, çalışma metotları ve kullandığı araçlar teknolojinin değişim ve gelişimi ile beraber sürekli aşama kaydetmiştir [1].

Bilişim dünyasındaki gelişimin ivmesi, bize önümüzdeki zaman dilimlerinde siber istihbarat ve siber casusluk faaliyetlerinin ulusların güvenliğinin temel taşı haline geleceğini göstermektedir. Öyle ki günümüzde sanal hamleler sonucu çok fazla iş gücünün atıl bırakılması ile büyük kayıplara sebep olunabilmektedir. Bilişim sistemlerinin ve sanal âlemin toplumun bütün birimlerinde kullanılıyor olmasına ve birçok kamu kurumunda bu teknolojilerin yaygınlaşmasına paralel olarak, istihbarat birimleri de bu bilişim teknolojisinden yoğun olarak faydalanmaktadırlar. Ülkeler teknolojik ilerlemeler doğrultusunda uygulamalarını siber uzaya transfer etmek durumunda kalmışlardır. Bu durumun doğal sonucu olarak ülkelerin sahip oldukları tüm faydalı bilgiler, veriler siber uzayın bir parçasını oluşturmaktadır. Ne yazık ki bu eksende ülkelerin ulusal güvenlikle ilgili risk unsuru olabilecek bilgileri de sanal dünyada yer edinmektedir. Yarış içerisinde olan veya birbirlerine düşmanlık yapan devletler, değişik topluluklar bu bilgilere ulaşmak maksadıyla siber istihbarat ve casusluk çalışmaları yapmaktadırlar.

Bu çalışmada; siber istihbarat ve siber casusluğun ne olduğu ve hangi yöntemleri kullandığına değinilmiştir. Ayrıca kamu kurum ve kuruluşlarının gelişen teknolojiye bağlı olarak maruz kalabilecekleri siber casusluk faaliyetlerine nasıl önlemler alması gerektiği ortaya koyulmuştur.

II. SİBER İSTİHBARAT KAVRAMI VE YÖNTEMLERİ

A. *Siber İstihbarat*

İstihbarat, Arapça kökenli bir kelime olup; Türk Dil Kurumu tarafından yeni öğrenilen ve elde edilen bilgi olarak ifade edilmektedir [2]. İşlevsel olarak istihbarat olanak ve araçlar vasıtasıyla ulaşılması gereken bir konuda bilgi edinimi ve edinilen bilgilerin sadelikten çıkarılarak işlenmesi, anlamlandırılması ve çeşitli boyutlar kazandırılarak buradan bir sonuç çıkarılmasıyla ilgili işlevsel çabalar bütünüdür [3].

Arapça kökenli "tecessüs" kelimesinin karşılığı olan casusluk, bilgisi dışındaki işlemleri öğrenme arzusu gizli şeyleri merak etme anlamına gelmektedir. Casusluk faaliyeti ve espiyonaj kelimeleri aynı doğrultuda kullanılmak üzere yabancı dillerden alınarak casusluk manasında kullanılmaktadır [3].

Toplumların yaşamlarını devam ettirdikleri her yerde, her zaman varlığını sürdürmüş olan casusluk faaliyetleri dünyanın en eski iş sahalarından biridir. İstihbarat ve casusluk, yıllardan beri süre gelen devletlerin bekalarını sağlamak ve üstünlük yarışlarında ön sıralarda yer alabilmek için yürüttükleri faaliyetlerdir. Bu iki terim ehemmiyetlerini hiç kaybetmemiştir [4].

* Samet OĞUZ, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara, (soguz@kho.edu.tr).

E.Burak CEYHAN , Gazi Üniversitesi Bilgisayar Mühendisliği, Ankara, (eyupburak@gmail.com).

Prof. Dr.Şeref SAĞIROĞLU, Gazi Üniversitesi Bilgisayar Mühendisliği, Ankara , (ss@gazi.edu.tr).

İnternet alt yapılı bilişim teknolojilerinin neredeyse bütün endüstri dallarında temel taşı oluşturduğu görülmektedir. İnternette veri iletimi için kullanılagelen e-postanın ardından, e-reklam, e-ticaret, e-devlet, e-oylama vb. pek çok terim yeni teknoloji ile birlikte her geçen gün daha fazla gündelik yaşamımızın birer parçası haline gelmektedir. Bunun yanında internet bağlantılı cep telefonları, diz üstü, kişisel ve tablet bilgisayarlar gibi üretilen her yeni sistem de bilgisayar tanımının sınırlarını zorlamaktadır [5].

Yeniliklerle büyüyen teknolojinin, ulusların güvenliğini ve özgürlüğünü doğrudan etkilediği, dünyada gücü tayin eden en önemli ilke haline geldiği çağımızda, teknolojik ve ekonomik istihbarat çok daha ehemmiyetli duruma gelmiştir. Casusluk faaliyetlerinin eski zamanlarda sadece askeri ve siyasi alanlara yönelirken, günümüzde telekomünikasyondan bilgisayar teknolojisine, taşımacılıktan tekstil endüstrisine, nano teknoloji ile optik alanındaki araştırmalara kadar her alanda etkisini hissettirerek dünyayı kocaman bir şehir haline getirmeye devam etmektedir. Teknolojik yenileşmeler bilgi birikimini ve bilgiye ulaşmayı kolaylaştırırken aynı zamanda casusluk faaliyetlerini de kolaylaştırmaktadır [6].

Teknolojik yeniliklerin bilgiye ulaşımı kolaylaştırmasından ziyade asıl olarak istihbarat faaliyetlerini kolaylaştırdığı ortaya çıkmıştır . Hayatın olağan akışı içinde etkilerini çoğu zaman unuttuğumuz internet üzerinden kişilerin şahsi bilgilerinin, özel şirketlere ve kamu kurumlarına ait verilerin, kullanıcı hesaplarının ele geçirilerek kötü amaçlı kullanılması gibi olaylar sıkça yaşanmaktadır. İstihbaratın çalışma alanı; devletin kontrol görevini yerine getirebilmesi için, tehdit unsuru olabilecek konularda önem seviyesine göre karar mercilerine gerekli olan bilgi hakkında gerekli desteği sağlamak ve ayrıca propaganda, psikolojik eylemler gibi faaliyetler ile düşman istihbarat ve diğer faaliyetlerini engellemek olduğu dikkate alındığında, siber uzayda bu gayeyi taşıyan çalışmaların tamamı "siber istihbarat" olarak kavramsallaştırılabilir [1].

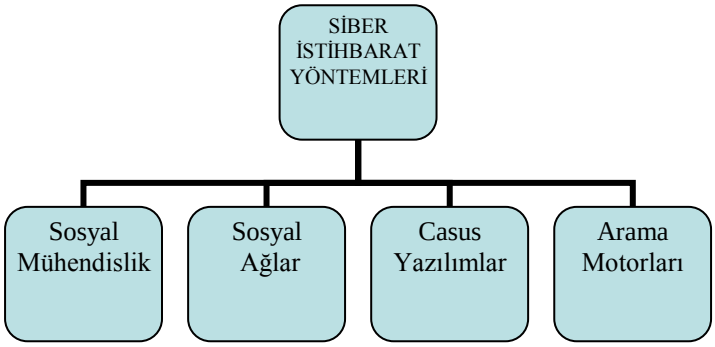
İstihbarat alanında ağırlıklı olarak bilişim teknolojisinin kullanımını kapsayan ve ayrıca içerisinde uzay araçları, uydular ve hava araçları ile icra edilen istihbarat faaliyeti olarak düşünülen siber istihbarat [7]; şahsi, sosyal, siyasal veya askeri avantaj sağlamak için, bilişim sistemlerine veya bilgisayarlara kanunsuz bir şeklide sızarak, kişilerden, rakiplerden, şirketlerden, devlet kurumlarından veya bankalardan, onların izni olmadan sırlarını elde etme eylemidir [2]. Ayrıca bilişim ortamındaki tehlike ve kötü amaçlı faaliyetlerin izlenmesi, değerlendirilmesi ve tedbirlerin alınması sürecidir. Siber istihbarat, bilişim teknolojisinin ve casusluk faaliyetlerinin birlikte kullanılarak savunmanın güçlendirilmiş halidir. Siber istihbarat faaliyetleri elektronik ortamda özellikle de sanal âlemde riskli verilerin siber teröristler tarafından ele geçirilmesini önlemek için en etkili yöntemleri kapsamaktadır [7].

Siber istihbaratı diğer istihbarat yöntemlerinden ayıran ve onlardan daha avantajlı konuma getiren şey kullanılan araçlardır. Bu materyaller ileri seviyede teknolojik ürünlerdir; faydalı ve nitelikli stratejik verilere sahip olurken, zaman ve ekonomik tasarruf sağlarlar. Bunun yanı sıra, bu araçlar daha az iş gücü ve sermaye ile daha kesin bilgi sağladığından dolayı alışılagelmiş istihbarat düşüncesini geliştirmektedir. Birçok uzmana göre siber istihbarat; düşmanın bizim hakkımızda bilgi sahibi olmasını engellerken, onun hakkındaki her şeyi öğrenmektir [5].

Bilişim sistemlerine karşı gerçekleştirilecek saldırılar, büyük tehditler ancak gelişmiş bir siber istihbarat alt yapısı ile fark edilip, önüne geçilebilir. Kişisel veya kurumsal güvenlik alanı ne kadar önemli olsa da ülke çapındaki güvenliğin önemi ile kıyaslandığı zaman kişilerin güvenliği bir parça daha geri planda kalmaktadır. Çünkü burada mevzu bahis olan, kişisel bir banka hesabı veya küçük çaplı bir bilişim sistemi değildir. Burada büyük bir devletin; istihbaratının, gizli servislerinin, sırlarının, ekonomisinin, vatandaş bilgilerinin, teknolojisinin vb. şeylerinin ele geçirilebilmesi gibi bir tehlike söz konusudur. Siber savaşların her geçen gün fazlalaşması, devletlerin bilinçli ve yoğun bir şekilde siber istihbarata yatırımda bulunmalarını gerektirmektedir [8].

B. Siber İstihbarat Yöntemleri

Sanal dünyada işe yarayan veya yaramayan birçok veri mevcuttur. Bu verileri ele geçirip istihbarat oluşturmak için çok çeşitli yöntemlerden yararlanılmaktadır. Bu yöntemleri Şekil 1'deki gibi sınıflandırmak mümkündür.



Şekil 1. Siber istihbarat yöntemleri.

Sosyal Mühendislik (Sosyal Ağlara Dayalı Siber İstihbarat)

Güvenliğin en zayıf halkasının insan olduğu varsayımına dayanan sosyal mühendislik, ilk olarak insanların birbirleri ile olan iletişim ve ilişkilerini veya kişilerin farkında olmadan yaptıkları hataları kullanarak hedef kişi, kurum veya kuruluş hakkında bilgi toplamak olarak açıklanabilir. Sosyal mühendislik, bilgiye ulaşmak için kişilerden yararlanılması, etkileme ve ikna yöntemlerinin kullanılmasıdır. Sosyal mühendislik, normal şartlarda insanların tanımadıkları kimseler için yapmayı göze almayacakları şeylerin yapılabilirliğini arttırma becerisi olarak ifade edilebilir [5].

İnsan ilişkilerinden, dikkatsizliklerinden veya eğilimlerinden faydalanarak gizli bilgilere erişme çabası sosyal mühendislik olarak adlandırılmıştır [1]. Amaç; hedef alınan şahıs veya şirket yapısı, kurumsal ağ yapısı, iş verenler ya da işçilerin kendilerine ait bilgileri, şifreleri ve saldırıda kullanılabilecek her türlü materyalin toplanmasıdır [9]. Bu teknikte uzman analizci kişiler, sanal alemde paylaşılan herkesin kullanımına açık kişiye ait verileri, herhangi bir gizliliğe sahip olmamalarına rağmen, diğer kaynaklardan temin edilen başka

bilgilerle uzmanlık gerektirecek bir biçimde birleştirmekte ve gizliliğe sahip veya önem arz eden bilgi haline getirmektedir [1].

Sosyal mühendisliğin faaliyet gösterdiği alanlardan biri de herkesin kullanabileceği karşılıklı iletişim imkânı sunan sosyal ağlardır. En çok kullanılan sosyal ağ sitelerinden biri olan Facebook'un farklı insanlar tanımak, kendi düşüncelerini anlatmak ve diğer insanların hangi fikir ve düşüncelere sahip olduklarını anlamak üzere üç temel fonksiyonu bulunmaktadır. Facebook sosyal ağ sitesinin global eksende bir milyara yakın internet kullanıcısı bulunmaktadır. Bu durum söz konusu sosyal ağ sitelerinin dünya çapında ne kadar yaygın olarak kullanıldığının ve ne kadar etkili olduğunun bir ispatıdır [10].

Sosyal mühendisliğe iyi bir örnek olması açısından Thomas Ryan tarafından yapılan Robin Sage testini gösterebiliriz. Robin Sage adını kullanarak Facebook, Twitter, Linkedln gibi sosyal ağlarda birçok profil oluşturulmuştur. 2 aylık test sonucunda hayali bir kişilik olmasına rağmen Google ve Lockheed Martin gibi firmalardan iş teklifi almış, erkeklerden akşam yemeği teklifi almış, FBI ve CIA hariç birçok istihbaratçı ve askeri personel kendisi ile arkadaş olmuş ve böylelikle bir çok ulaşılması zor olan bilgiye ulaşılmıştır [6].

Sosyal Ağlar

Kurum ve kuruluşlar, gruplar ve kişiler arasında eş zamanlı bilgi paylaşımı imkânı sağlayan, internet üzerinde birbirleriyle yaptığı diyaloglar ve paylaşımların bütünüdür [4]. İnternet blogları, internet günlükleri, video, resim gibi veri paylaşım siteleri, kişisel forumlar, arkadaşlık siteleri, haber paylaşım siteleri vb. internet hizmetleri sosyal ağ grubunda sayılabilir. Facebook, twitter, youtube, flickr, mylife, myspace, raptr ve linkedln örnek olarak verilebilir. Sosyal ağlar, istihbarat toplayan birimler ve istihbarat örgütleri için büyük fırsatlar sunmaktadır. Sosyal ağları kullanarak şahıslar, devletler, kamu kurumları hakkında bilgi sahibi olunabilir [5].

Wikileaks'i yapan Julian Assange, Russia Today'e verdiği demeçte Facebook'un kişilerin ad ve şahsi bilgileri hakkında büyük bir havuz olduğunu ve kullanıcıları tarafından isteyerek kullanılsa da, ABD istihbaratının kullanması için geliştirildiğini iddia etti. Facebook'u şu ana kadar yapılmış en korkutucu "casus makinesi" olarak adlandıran Assange, "Herkes şunu anlamalı ki, arkadaşlarını Facebook'a ekleyerek ABD istihbarat servisleri için bedavaya çalışıyorlar ve onlar için bu veritabanını oluşturuyorlar." demiştir. Assange'ın bu iddiası da sanal iletişim ortamları ile istihbarat örgütlerinin ne kadar çok iç içe geçtiğini göstermektedir. İstihbarat örgütleri sanal iletişim ağlarını kullanarak ulusal güvenliği tehdit edecek konuma gelebilmektedir. Günümüzde bunu en etkin kullanan örgütlerden biri de İŞİD terör örgütüdür. Bu siteler sayesinde bulduğu kişileri sosyal mühendislik metodunu kullanarak ikna etmekte ve kendisine militan yapmaktadır [5].

Rusya, sosyal ağlarda fotoğraf ve bilgi paylaşımı sağlayan (LiveJournal, vkontakte.ru vb.) paylaşım sitelerine askeri personelin üye olmasını yasaklamıştır. Sosyal ağlar istihbarat birimlerinin işine yaradığı gibi, suçluları yakalamada veya personel seçiminde de kullanılabilmektedir [4].

Casus Yazılımlar

Casus yazılım, kişilere ait önemli bilgilerin ve kişilerin yaptığı işlemlerin, kişilerin bilgisi dışında kopyalanmasını ve bu bilgilerin kendi çıkarları için kullanan kişilere transfer edilmesini sağlayan yazılım olarak ifade edilebilir [11]. Casus yazılımlar; Truva atı, rootkit, klavye dinleyici gibi, kullanıcıdan habersiz olarak bilgisayarlarda çalışan ve bilgisayarlardaki verileri belirli sunuculara gönderen yazılımlardır [4].

Casus yazılım veya spyware (İngilizce spy ve software sözcüklerinden türetilmiştir), başlıca kötücül yazılım (malware) türlerinden biridir. Geniş bant kullanan bilgisayarların yaklaşık olarak %90'ına yakınında casus yazılım bulunduğu düşünülmektedir. ABD'de Gartner Group tarafından Eylül 2004'de yapılan bir araştırmada 3 milyon işletme bilgisayarı gözden geçirilmiş ve bilgisayarlar üzerinde 83 milyon casus yazılım tespit edilmiştir [11].

Casus yazılımlar, hedef sisteme entegre olduktan sonra kendi kopyalarını oluşturmazlar. Casus yazılımın amacı önceden belirlenmiş bir sistem üzerinde gizli kalarak ulaşılmak istenen gizli bilgileri toplamaktır. Bu bilgi kimi zaman bir banka şifresi gibi önemli bir bilgi bile olabilir [11]. Bunun dışında, maddi amaç güden kuruluşlar internet üzerindeki kullanıcı alışkanlıklarını saptamak ve kullanıcıların ihtiyaç duyduğu emtiaları tespit ederek bu hizmet veya ürünlere ilişkin markaların reklamlarını kullanıcılara ulaştırmak gibi amaçlarla casus yazılımları internet üzerinde yayabilmektedirler.

Arama Motorları

Arama motoru, veri tabanında bulunan bilgileri aramak için kullanılan bir yazılımdır. Web robotu, arama indeksi ve kullanıcı arabirimi gibi üç bileşenden oluşmaktadır. Ancak arama sonuçları genellikle en çok tıklanan internet sayfalarından oluşan bir liste olarak belirlenmektedir [12]. Arama motorları birkaç yönden önemli istihbarat kaynağı olarak kullanılmaktadır.

Bunlardan bir tanesi, dünya üzerinde bulunan bütün sunuculardaki verileri depolamasıdır. Böylelikle her türlü bilgiye ulaşmış olmaktadır. Bu bilgiler arasından da veri madenciliği ile önemli bilgilere ulaşabilmektedir [4].

Bir diğer istihbarat elde etme yöntemi ise, arama motorunu kullanarak kimlerin neyi aradığı bilgisidir. Arama motoru firmaları (Google, yandex vb.) hangi ülkenin, hangi şehrinin, hangi kişilerin, hangi bilgileri aradığını bilmektedir. Örneğin; google firması hangi IP (internet protocol) adresinden hangi aramaların yapıldığını bilmektedir. Hangi IP adresini hangi şirketin veya devlet kurumunun kullandığını bulmak çok basittir. Bu şekilde hangi firmanın neleri araştırdığı veya hangi devlet kurumunun nelere ilgi duyduğu bilinebilir. Bu bilgiler genellikle ticari firmalar tarafından reklamcılık faaliyetleri için kullanılmaktadır [1].

III. SİBER İSTİHBARATA KARŞI KOYMA YÖNTEM VE TEKNİKLERİ

Siber istihbarat, siber saldırıların ve siber savaşın en önemli ve etkin unsuru yani olmazsa olmazıdır. İstihbaratsız savaş düşünülemeyeceği gibi siber istihbaratsız da siber saldırılar düşünülemez. Zaten incelendiği zaman bu iki terimin iç içe olduğu ve uygulama alanlarının ve karşı koyma yöntemlerinin neredeyse aynı olduğu ortaya çıkmaktadır. Siber istihbaratın önüne geçebilmek için öncelikle tam olarak siber güvenliğin sağlanması zarureti vardır.

Siber güvenlik tam olarak olgunlaşmamış bir disiplindir. Bu hususta güvenlik birimlerinin kabiliyetleri ve yetişmiş kaliteli kişi sayısı oldukça azdır. Buna sanal dünyada olan olaylara karşı gereken faaliyetlerin yapılmasının gerektirdiği uluslararası karakter de eklenince siber güvenlik ve siber savunma hususunda meydana getirilen oluşumların istenildiği kadar yeterli olmadığı anlaşılmaktadır. Siber ağların devletleri aşan sınırları düşünüldüğünde, siber güvenlik alanında faydalı önlem ve durumlar oluşturulabilmesi için uluslararası kurum ve kuruluşların icralarının ve devletlerin kendi aralarında oluşturdukları işbirliğinin önemi ortaya çıkmaktadır. Devletler açısından bakıldığında, internet üzerinden gelecek tehlikeler ve bunlara karşı uygulanacak önlemlerle ilgili farklı yöntemler ve bakış açıları ortaya çıkmaktadır. Siber alemde kendilerine karşı yapılan saldırılara askeri karşılık verilmesi düşüncesine dayanan siber saldırıları savaş sebebi görebilecekleri gibi bir yaklaşımın yanında; siber uzaydan gelen tehditlerin aynı yerde karşılık bulması gerektiğini düşünen ve söyleyen yaklaşımlar da bulunmaktadır. Bu yaklaşımlar saldırıların nerden kaynaklandığı, ne amacı güttüğü ve orantılı güç kullanımı tartışmalarını da beraberinde getirmektedir [13].

Siber istihbarat alanında güvenlik çalışmalarının sonuç alabilmesi için alışılagelmiş tehditler ile siber tehditler arasındaki farklılıkları ortaya koyarak siber ortamın kendine has özelliklerine dikkat edilmesi gerekmektedir. Bu hususta ilgi çeken birinci nokta süreç içerisinde daha az bilgi birikimi ile daha karışık saldırıların gerçekleştirilebilir duruma gelmesidir. Üzerinde durulması gereken ikinci nokta ise siber saldırıları yapan şahısları ve bu saldırıların yapıldığı mekânları bulmaktır. Alışılagelmiş tehditlerin ve bu tehditlerin yapıldığı mekanların bulunması günümüzde göründüğü kadar zor değildir. Bu konuda dikkat edilmesi gereken üçüncü nokta ise siber saldırıların menzilinin ve gücünün artmasıdır. Alışılagelmiş saldırı araçlarının etkinlik alanının belli bir sığası, mesafesi vardır ve araçlar ancak bu mesafe içinde bir tehlike oluşturabilmektedir. Oysaki siber saldırı araçları günümüzde çok cüz'i bilgi ve para ile geliştirilebilmekte ve internet üzerinden dünyanın herhangi bir noktasına bu araçlar kullanılarak siber saldırılar ve siber casusluk faaliyetleri gerçekleştirilebilmektedir [14]. Bu saldırıları ve casusluk faaliyetlerini engelemek için; sistem güvenliğinin arttırılması, askeri ve sivil doktrinin geliştirilmesi, bunlarla ilgili cezaların belirlenmesi ve siber silahların ve sistemlerin uluslar arası düzeyde olacak şekilde kullanımının sınırlanması gerekmektedir [15]. Tabi ki bu önlemleri almak sadece tehlikeleri azaltmaktadır. Dünya'da mevcut olan veya örnek teşkil edebilecek sistemleri de incelememiz gerekmektedir. Örneğin Couldron adındaki yazılım gibi, sistemleri önceden denetleyen, açıkları bulan ve sonra da analiz yaparak bizlere alınması gereken önlemleri gösteren programlara sahip olmamız gerekmektedir. Fakat unutulmaması gereken önemli bir nokta ise bunların milli olması gerekliliğidir [16].

Dünya geneline bakıldığında, siber istihbarat ve siber savunma faaliyetlerine özel kurum ve kuruluşlardan ziyade en çok devletlerin orduları ve güvenlik güçleri tarafından başvurulduğu gözlemlenmektedir. Özellikle de çağı yakalamak amacıyla siber istihbarat faaliyetlerini aktif olarak kullanmaktadırlar.

Nisan 2015'de ABD Güvenlik Sekreteri tarafından açıklanan Yeni Güvenlik Stratejisi'nin (The DoD Cyber Strategy) bilgi paylaşımı ve kurumlar arası koordinasyonu, özel sektör ve müttefikler arasında gerekli irtibatların oluşturulmasını, koalisyon ve andlaşmaların yapılmasını içerdiği ve ayrıca David Kaye'nin (BM Özel Raportörü) 2015'de İnsan Hakları Komisyonu'nda ifade ettiği gibi dijital haberleşmede şifrelemenin kullanılmasının pozitif etkiye sahip olduğu bununla beraber internet güvenliği, bireysel gizlilik, özgür düşünce ve ekonomik büyümeye de etki edebildiği ortaya konulmuştur [17]. Hem ABD'nin Yeni Güvenlik Stratejisi'ne hem de David Kaye'nin açıklamalarına dikkat etmek ve bizlerin de aynı hassasiyetle faaliyetlerimizi (siber güvenlik alanında) yapıp yapmadığımızı tekrar gözden geçirmemiz gerekmektedir.

Dünyada olup biten bu siber casusluk olayları karşısında, siber casusluk ve siber saldırılara karşı koymak ve gücüne güç katmak amacıyla Türk Silahlı Kuvvetleri (TSK) de kendi bünyesinde gerekli önlemleri almaya başlamıştır. TSK yalnız kendi bünyesinde siber güvenlikle ilgili çalışmalar ve faaliyetler gerçekleştirmekle kalmayıp, diğer kamu kurum ve kuruluşları ile siber güvenlik alanında işbirliği yapmaya da başlamıştır. TÜBİTAK UEKAE bünyesinde 2001 yılında Bilişim Sistemleri Güvenliği Bölümü kurulmuştur. Ayrıca ilk çalışmalar TSK bünyesinde yapılmıştır. 2012 yılında TSK bünyesinde Siber Savunma Merkez Başkanlığı kurulmuş ve bu başkanlık diğer kurum ve kuruluşlar ile de koordineli olarak faaliyet göstermektedir. Siber güvenlik alanında yapılan çalışmalar planlanıp gerçekleştirilen sunumlar bu alanda tecrübe paylaşımı, yeni bakış açıları kazanma, ortak bilinç oluşturulması ve iş birliği konusunda çok özel bir yere sahiptir. Yapılmakta olan siber güvenlik tatbikatları kâğıt üzerinde sağlam görünen sistemlerin eksikliklerinin meydana çıkması ve böylelikle gereken önlemlerin alınması açısından çok elzemdir [13].

Özel veya kamu ayrımı yapılmaksızın birçok sektörde kurumların, bilişim teknolojilerine olan bağımlılığı ve ihtiyacı artmasıyla birlikte siber alanda yaşanan tehlikeler de artmaktadır. Siber casuslukta en etkili yöntemlerden biri olarak kullanılan sosyal mühendislik gibi en zayıf halka olan insandan kaynaklanan saldırıların riskini minimize etmek için personele siber güvenlik ile alakalı konularda daha fazla eğitimler verilip bilgilendirmeler yapılması gerekmektedir. Siber saldırıları engellemek için kurum ve kuruluşların dikkat etmesi gereken 10 husus aşağıdaki şekilde özetlenmektedir [18]:

1. Mobil cihazların kullanımında gerekli hassasiyet gösterilmeli: Kurum çalışanlarının her yerden kurum bilgilerine ulaşabilmesi ve herhangi bir önlemin alınmamış olması gözden kaçırılmamalıdır.
2. Kurum içi güvenlik politikası oluşturulmalı: Kurumdaki herkesin her yere erişim izninin olmaması ve yetkilendirilmelerin olması.
3. Sorumluluklar belirlenmeli: Herkesin sorumluluk alanlarının belirlenmiş olması ve işe alınmadan personele sorumlu olacağı alanların neler olacağı hakkında bilgi verilmesi.
4. Çalışanlara eğitim: Kurum çalışanlarına düzenli bir şekilde eğitim verilmeli.
5. IT ekibine eğitim: IT ekibinin de eğitimi aksatılmadan icra edilmeli ve sistemleri nasıl kullanacakları yönünde uzman olmaları sağlanmalı.
6. Güçlü şifreler kullanılmalı: Sistemde güçlü şifrelerin kullanılması sağlanmalı,alfa numerik ve üç ayda bir değiştirilen şifrelerin kullanılması sağlanmalı.
7. Envanter raporu tutulmalı: Envanter raporu düzenli olarak tutulmalı.
8. Yedekleme yapılmalı: Bilgi ve yazılımların yedeklenmesi yapılmalı ve ayrıca yedekler test edilmelidir.
9. İş sürekliliği yönetimi gerekli: Kurumun karşılaşabileceği riskleri, önemli iş süreçleri ile ilgili varlıklarını, bilgi güvenliği zafiyetlerinden dolayı oluşabilecek zararları, ekstra önlemlerin belirlenmesi ve icrasını, bilgi güvenliğini de kapsayan iş sürekliliği planlarının kararlaştırıldığı konuları içermelidir.
10. Güvenlik yazılımı olmalı: Güncel ve aktif olan güvenlik yazılımlarının kullanılması gerekmektedir.

IV. SONUÇ

Yaşadığımız çağ itibariyle ulusal güvenliğin sağlanması çok geniş çerçeveli olarak ele alınmalı ve çalışmalar bu doğrultuda gerçekleştirilmelidir. Sadece sınır güvenliğinin korunması için çaba gösterilmesinin günümüzde ulusal güvenliğin sağlanmasına yetmeyeceği aşikârdır. Teknolojinin eriştiği aşamalar ve teknolojik araçların öncelikle kamu kurumları olmak üzere hayatın her alanında ve aşamasında yer alması, siber güvenliği ve bu doğrultuda siber istihbaratı, ulusal güvenliğin ehemmiyeti yüksek olmazsa olmazı yapmıştır.

Gelecek günlerde ülkeler arasındaki savaşların sonuçlarını klasik cephelerdeki güç yerine daha karmaşık bir etki oluşturan ve savaşa yeni boyutlar kazandıran siber uzayda yaşanan muharebeler belirleyecektir. Siber yetenekler sayesinde, teknolojiye bağımlılığı her geçen gün artan ülkelerin teknolojik alt yapıları önemli hedefler haline gelecektir. Devletlerin ülkelerini koruyabilmek için, teknoloji ile donatılmış her türlü askeri imkanlarının yanında onlar kadar önemli siber saldırı ve siber istihbarat yeteneklerini de geliştirmeleri gerekecektir. Son zamanlarda dünyanın farklı yerlerinde meydana gelen siber saldırılar, devletlerin bu alanda kendi kabiliyetlerini geliştirmelerinin ve teşkilatlanmalarının zaruretini gözler önüne sermiştir. Bu doğrultuda siber tehlikelerin gün geçtikçe şekil değiştirerek kendini geliştirilmesi ve yeni tehdit türlerinin ne olduğunun tam olarak belirlenememesi, siber savunma alanında alınacak karşı önlemleri çıkmaza sokmaktadır. Tüm bu yenilikler, geleceğin muharebe alanında siber savaşların ehemmiyetini göstermekte ve siber savaşların dünya üzerindeki bütün devletlerin özelliklede bilişim teknolojisini her alanda kullanan devletlerin ulusal ve uluslar arası güvenlikleri için tehlike arz ettiğini gün yüzüne çıkarmaktadır.

Devletler ve kurumlar kendi güvenliklerine yönelik siber tehditlerle mücadele ederken, yeni teknolojik gelişmişlik seviyelerine ulaşabilmek açısından siber istihbarat karar vericiler için kilit rol oynamaktadır. Siber istihbarat sayesinde ülkeler hedef olabilecekleri siber tehditlere ve siber casusluk faaliyetlerine karşı gerekli önlemleri alabileceklerdir. Ayrıca devletler ve kurumlar, siber istihbarat sayesinde gelecekte karşılaşabilecekleri saldırı-casusluk-bilgi hırsızlığı gibi faaliyetlere karşı önceden önlem alabileceklerdir. Siber savaşların muhakkak olacağı gelecekte, devletlerin ve kurumların bünyesinde bulunan karar vericiler, siber istihbaratın önemini iyi benimsemeli ve bünyelerinde bulundurdukları istihbarat veya bilgi edinmek için kullandıkları teşkilatları, siber istihbaratı aktif bir biçimde kullanabilecek düzeye getirmelidirler. Bu teşkilatlar kanunların kendilerine verdiği yetki çerçevesinde yeri geldiği her alanda siber istihbarat faaliyetlerini aktif veya pasif bir şekilde kullanabilmelidirler.

Siber saldırılar ve siber casusluk konusundaki gelişmeler ve yöntemler çok hızlı bir şekilde değişmektedir. Siber saldırılar ve bu çerçevede siber casusluk faaliyetleri konusunda yasal düzenlemeler ihtiyaçlar doğrultusunda değiştirilmelidir. Siber savaş alanlarının olmazsa olmazı siber istihbarat yapılanmasının tek bir elden yönetilmesi gerekmektedir. Ayrıca kritik altyapı sistemlerinde kullanılan yazılım ve donanımlar mümkün olduğu kadar milli olmalıdır. Kritik altyapı sistemlerinde kullanılmak üzere yurt dışından alınan yazılım ve donanımlar beraberinde riskleri de getirmektedir. Özellikle yazılımların içerisine yerleştirilme ihtimali bulunan gizli kodlar, arka kapılar vb. yazılımlar, sistemi siber saldırılara açık hale getirmektedir. Bu nedenle, özellikle gelişmiş ülkeler kamu kurumlarındaki bilgisayarlarında kendi işletim sistemlerini kullanmaktadır. Kamu hizmeti ağları ve internet arasında bağlantı olmaması veya sınırlanması gerekmektedir.

Özellikle kritik altyapıların güvenliğinden sorumlu personelin eğitimine gereken önem verilmeli ve bu doğrultuda yeterli mali kaynak ayrılmalıdır. Konu, insan ve olumsuz yönleri, düşkünlükleri ve zayıflıkları olunca çok dikkatli olunması gerekmektedir. Siber istihbarat ve casusluk bakımından en önemli unsur olan insanların, zayıflıklarını tamamen ortadan kaldırmak mümkün görünmediğine göre, siber istihbaratta ve casusluğa karşı başarıyı elde etmenin yolu insan etkeninin çok iyi değerlendirilmesinden yani eğitiminin en üst seviyeye çıkarılması ve durumsal farkındalığının arttırılmasından geçmektedir. Bu çalışmada açıklanan siber istihbarat yöntemlerine baktığımızda hepsinin insan odaklı olduğunu söyleyebiliriz. Ayrıca bir zincir halkasının kuvveti en

zayıf halkası kadardır özdeyişinden yola çıkarak; kurumların insanlardan oluştuğu ve gerekli eğitim-farkındalık seviyesine çıkarılmaları gerektiği akıldan çıkarılmamalıdır. Eğitimli, nitelikli ve farkındalık seviyesi yüksek olan personelin her zaman anahtar role sahip olduğu ve olacağı dikkate alınarak insan faktörü üzerine odaklanmalı ve gerekli çalışmalar yapılmalıdır.

KAYNAKÇA

[1] Bayraktar, G. "Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat", *Güvenlik Stratejileri Dergisi*,120-135, 2014.

[2] "İstihbarat Nedir?", www.tdk.gov.tr , Erişim Tarihi: 30 Mart 2015.

[3] Gültekin, A. "İstihbarat Teknikleri", *Timaş Yayınları*, 32-36, 2004.

[4] Çifci, H. "Her Yönüyle Siber Savaş", *TÜBİTAK Popüler Bilim Kitapları*, 289-302, 2013.

[5] Özçoban, C. "21.Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü", *Harp Akademileri Stratejik Araştırmalar Enstitüsü Yüksek Lisans Tezi*, 75-84, 2014.

[6] Yayla,M. "Hukuki Bir Terim Olarak Siber Savaş", *TBB Dergisi*, 104 : 194-198, 2013.

[7] Çetinkaya, Ş. "Siber Terör ve Siber İstihbarat", http://www.21yyte. org/tr/ arastirma /terorizm-ve-terorizmle-mucadele /2011 /09/23 /6 309 /siber-teror-ve-siber-istihbarat, Erişim Tarihi: 30 Mart 2015

[8] Akçadağ,E. "Sürekli Artan Önemi Işığında Siber Güvenlik", http://www.bilgesam.org/incele/1207/-surekli-artan-onemi-isiginda-siber-guvenlik/#.VUJy7pWJiP8, Erişim Tarihi: 08 Nisan 2015

[9] Şahin,M.Y. "Karşı istihbaratta insan boyutunun irdelenmesi:Gafil muhbirlik örneği", *Harp Akademileri Stratejik Araştırmalar Enstitüsü Yüksek Lisan Tezi*, 48-70, 2013.

[10] Yılmaz, S. "Batı İstihbaratı ve Sosyal Medya", http://usam.aydin.edu.tr/ analiz /guvenlik_isthbrt..pdf, Erişim Tarihi: 08 Nisan 2015.

[11] "Casus Yazılım", http://tr .wikipedia.org/wiki/Casus_yaz %C4%B1l%C4%B1m, Erişim Tarihi: 10 Nisan 2015.

[12] Yurdakul,N.,.Bat,M. "Şirketler İçin Rekabette Sanal Farkındalık: Arama Motoru Pazarlaması", *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 45-60, 2011.

[13] Kaya,A., Öğün, M. "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler" *Güvenlik Stratejileri Dergisi*, 158-170, 2013.

[14] Canbay,C., Ünver,M. "Ulusal ve Uluslararası Boyutta Siber Güvenlik", *Elektrik Mühendisliği Dergisi.(438),* 94-103, 2010.

[15] Geers,K. "Strategic Cyber Security" *CCD COE Publication*, 132-139, 2011.

[16] Jajodia, S., Noel, S., Kalapa, P., Albanese, M., Williams, J. "Cauldron Mission-Centric Cyber Situational Awareness with Defense in Depth", IEEE Military Communications Conference (MILCOM), 1339-1344, 2011.

[17] Serrano, B. "Cyber Security and Cyber Espionage in International Relations", http://diplomacydata.com/cyber-security-and-cyber-espionage-in-international-relations/, Erişim. Tarihi: 23.09.2015.

[18] Ağaç,F. "Siber Güvenliğin Anahtarı Ulusal Çözümler", *Bilişim Dergisi*, 173, 88-91, 2015.