Siber İstihbarat ve Güvenlik Politikaları

Yavuz ÖZALP – Sakarya Üniversitesi (Lisans)

"Yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır."
(Rex Hughes – NATO Güvenlik Danışmanı)

Haber ya da yeni öğrenilen bilgi anlamına gelen istihbarat kelimesi anlamı itibari ile Arapça kökenli olup "istihbar" kelimesinin çoğuludur. Fakat istihbarat kelimesi anlamı itibari ile haberin çok ötesinde işlenmiş bilgiyi içerir. Haber ile arasındaki fark; haberler ham olan bilgiyi ifade ederken, istihbarat ise ham bilginin işlenmesini, analiz edilerek yorumlanmasını ve kıymetlendirilmesini gerektirmesidir. Ve insanların fıtri bir melekesi olan tecessüs (merak, öğrenme arzusu) ile doğmuştur.[i]

Bu bağlamda istihbarat, insanlar arasında ki ilk ilişkinin kurulmasından itibaren var olan bir kavram olduğunu söyleyebiliriz. İnsanların ilişkide olduğu ya da her ne sebeple olursa olsun iletişim kurmak istediği veya iletişimde bulunduğu kişiler hakkında bilgi edinerek (ekonomik, siyasi, insani vb.), önceden hazırlanılması işi de bir evi istihbarat çalışmasıdır. Devletler için ise istihbarat "hayatta kalmak" anlamını taşır. Bu nedenle etkin olmayan bir istihbarat servisine sahip olan devletler kör, sağır ve dilsizdir demek mümkündür.

Teknolojinin hızlı gelişimi istihbarat servislerinin gereksinimlerini de değiştirmiş ve istihbarat dünyasında yeni kavramlar ortaya çıkarmıştır.
Bunlar başlıca; Açık Kaynak İstihbarat, Siber istihbarat ve Siber Güvenlik olarak sıralanabilir.

Açık Kaynak İstihbarat

Bilgi Teknolojilerinin gelişmesine paralel olarak istihbarat anlayışında da değişim olmuştur. Günümüzde artık istihbarat sahadan masa başına doğru hızla bir yol alarak gelmiş ve bilgi toplama ve istihbarat elde etme işi %80' ler oranında masa başından sağlanır olmuştur. İstihbarat servisleri teknolojiden daha fazla ve etkin yararlanarak açık kaynakları kullanma yönünde büyük ölçüde insan gücü, para ve çaba sarf etmişler ve bu durum istihbaratta yeni bir kavram geliştirmiştir ; "Açık Kaynak İstihbarat" .

Açık Kaynak İstihbarat; her kesimin kolay elde edebildiği, işlenerek kıymetlendirilmesi sonucunda *istihbarat değeri olan* haber ya da bilgiye açık kaynak istihbarat denir. Başka bir deyişle Açık Kaynak İstihbarat; istihbarat analistlerinin yararlandığı kaynakların her hangi bir kişinin de rahatlıkla ulaşabildiği kaynaklardan elde edilen istihbari bilgi olmalarıdır. İstihbaratta Açık Kaynakların kullanılması ve ortaya çıkarılan istihbari bilgi basit gibi görünse de aslında hayati önem taşımaktadır. Özellikle Soğuk Savaş döneminde İstihbarat servislerinin dünyanın bir ucundan diğer ucuna haber iletmek için kullandıkları başlıca yöntemler açık kaynaklardandır. Günümüzde Üniversiteler, sivil toplum örgütleri ve düşünce kuruluşları (Think Tank) ise bu açık kaynakların önemli olanlarının

ayıklandığı ve devşirildiği merkezlerdir. Özellikle gelişmiş ülkelerdeki düşünce kuruluşları açık kaynakları kullanarak istihbarat analizi için çok önemli olan stratejik bilgiyi üretmektedirler.[ii] Bu nedenle istihbarat servislerinin Açık Kaynakları kullanmaları saha elemanlarından gelen istihbarat raporlarından daha değerli hale gelmiştir. 2010 yılında Mavi Marmara baskınına katılan İsrail komandolarının fotoğraflarının MİT (Milli İstihbarat Teşkilatı) tarafından sosyal medyadan elde edildiği de açık kaynakların ne denli önemli olduğunu ortaya koymaktadır. Bu nedenle günümüzde Açık Kaynak İstihbaratın en önemli kaynağı internet olmuştur.

Soğuk Savaş yıllarının başlarından itibaren Sovyetler Birliği'nin direktörlükler altında tüm istihbarat faaliyetlerini (askeri istihbarat hariç) yürüten KGB (Devlet Güvenlik Komitesi), akademik yayınlar, yazılı ve işitsel medyayı kullanarak şifreli mesajlarla sahadaki elemanları ile iletişime geçmesi (Operasyon emirleri gönderilmesi vb.) diğer istihbarat servislerini harekete geçirmişti. Princeton Üniversitesi'nde başlayan "Yabancı Yayın İstihbarat Servisi" nin (Foreign Broadcasting Intelligence Service) kurulması ile İkinci Dünya Savaşı radyonun ana istihbarat kaynağı olduğu bir savaş haline geldi.[iii] Uluslararası Yayınları Tedarik Komitesi ise küresel olarak dış dünyada ki tüm yazılı akademik ve medya yayınlarını toplamaya başladı ve soğuk savaş ile birlikte bu iki yapı CIA bünyesinde farklı isimlerle yer aldı.[iv]

Soğuk Savaş döneminde ABD'de yaklaşık olarak iki bin civarında şifre çözücü eleman çalışıyordu. Bunlar özellikle Sovyetler Birliği yazılı medya ve akademik yayınlarında ki metinlerin içine yerleştirilmiş şifreli mesajları çözmekle görevliydiler. Açık Kaynak İstihbaratı etkin bir şekilde kullanmaya başlayan ABD istihbaratta birçok başarısızlık yaşadıktan sonra bu yolla soğuk savaş döneminde birçok saldırıyı ve karşı istihbaratı bertaraf etmişti. Günümüzde bilgisayar teknolojilerinin geldiği noktada Açık Kaynakların, karmaşık, çok sayıda ve zor analiz edilebilir olsa da bir istihbari bilgi havuzu olduğunu söyleyebiliriz.

Siber İstihbarat

Günümüzde İnternetin sosyal ve ekonomik yaşantının ayrılmaz bir parçası haline gelmesi, hükümetlerin de iletişim ve bilgi alanında ki bu büyük değişime kayıtsız kalamamasına, kurum ve hizmetlerini siber uzaya taşımalarına yol açmıştır.[v] Bu sayede kamu ve özel sektör tarafından verilen hizmetlerin kalitesinin ve hızının artması sağlanmıştır. Bununla birlikte kamu ve özel sektörde şeffaf (açık) yönetim anlayışı benimsenmiş fakat bu durum işletmeler için bilgi ve sistem güvenliği sorununu doğurmuştur. Tüm dünyayı saran internet ağı sayesinde bilgiye ulaşmayı kolaylaştırması bu dönemde toplumların da birbirine internet ağı üzerinden iletişim ve etkileşimleri kolaylaşmış ve artış göstermiştir.

Bilişim teknolojilerinin gelişmesi ve yaygınlaşması ile birlikte devletlerin istihbaratta insan kaynağından çok bilişim teknolojilerine yatırım yapma yoluna gittiğinden bahsetmiştik. Bilgi ve iletişim sistemlerinin bu amaçla yaygın olarak kullanılmaya başlanması İstihbarat teşkilatlarının istihbarat organizasyon şemalarında ve bilgi toplama anlayışlarında değişiklik yapmayı zorunlu hale getirmiştir. Yapılan değişiklikler sonucunda "Siber Birimler/Emniyet Şubeleri/kuvvetler" ortaya çıkmıştır.

Siber İstihbarat, elektronik ortamda saldırı, bilgi toplama (sızma), tehdit ve saldırıların izlenmesi ve analiz edilerek yorumlanmasını da içeren bir süreçtir. Bu süreçte siber saldırı ve sızma girişimlerinin başarı derecesi kullanılan teknolojinin ve kalifiye insan gücünün niteliği ile doğru orantılıdır.

İstihbarat ve siber uzayda üstünlük sağlamak adına uydu ve bilgisayar istihbarat sistemlerinin geliştirilmesi ve bunların modern çağın istihbarat aracı olarak kullanılması daha da önemli hale gelmiştir. Nitekim Türkiye'de 2012 yılında MİT'e devredilen Türkiye'deki en gelişmiş elektronik istihbarat birimi olan eski Genelkurmay Elektronik Sistemler (GES) Komutanlığı MİT'te devredilerek Elektronik ve Teknik İstihbarat (ETİ) birimi altında görev yapmaya başlamıştır. Birimin doğrudan MİT Müsteşarı Hakan Fidana bağlı olması siber istihbaratın sadece dar anlamda askeri ve güvenlik meselesi olmadığını ortaya koymakta ve Türkiye'nin Siber İstihbarata verdiği önemi göstermektedir. Ayrıca Türkiye gibi bir çok ülkede görevi olası siber saldırılara hızla cevap vermek ve düşman kuvvetlerinin haberleşme ve koordinasyonunu sağlayacak bilgi teknolojilerini saf dışı bırakmak olan "siber kuvvetler" de kurmaya başlamışlardır.[vi]

Siber İstihbarat'ın en önemli unsuru olan yüksek

hızla veri işleyebilme, hızlı karar alabilme ve davranış geliştirebilmenin yanında ses, fotoğraf, görüntü ve yazışmaların stenografi analizi ile gizli metinler, şifreler tespit edebilmek, siber saldırıları sezmek için çeşitli karar destek algoritmaları kullanabilmek de önemlidir. Bu nedenle bu alanda teknoloji kadar yetişmiş nitelikli insan gücüde büyük önem arz etmektedir. Siber güvenlik alanında yetişmiş nitelikli eleman sıkıntısı yaşandığından açığı kapatmak amacıyla üniversiteler ve özel eğitim merkezleri Siber Güvenlik uzmanlığı eğitim programları açarak ihtiyaç duyulan elemanları yetiştirilmeye başlanmıştır.

Haziran 2013' te Hong Kong'da basına açıklamalar yapan ABD Merkezi Haber alma Teşkilatı (CIA) elemanı olan Edward Snowden, ABD Ulusal Güvenlik Teşkilatı'nın (NSA) "Prizma" isimli dinleme ve izleme sistemini ortaya çıkardı. Snowden' in verdiği raporlarda NSA, kullanıcı sayısı 1 milyarı aşan üç GSM şirketine siber saldırılar düzenleyerek SMS veri tabanına sızmaya çalışmış ve SMS takibi yaparak istihbari veri elde etmeyi amaçladığı ortaya çıkmıştı. Aynı zamanda Çin'de saygın ve büyük bir akademik enstitü olan Çin Eğitim ve Araştırma Enstitüsü'ne network altyapısı sağlayan Tsinghua Üniversitesine sızma girişiminde bulunmaları ve benzer şekilde Hong Kong merkezli deniz altı fiber kablo altyapısı Pacnet'e de müdahale edildiği ve teknik takip yapıldığını gösterdi. Ayrıca aralarında Türkiye'nin Washington Büyük Elçiliğinin de bulunduğu yabancı temsilciliklerin dinlenildiği ortaya çıktı.

Snowden olayına benzer bir olayda soğuk savaş döneminde yaşanmış ve hala dünyada en gelişmiş sistem olduğu bilinen "ECHELON" ifşaa edilmişti. Siber istihbaratın ve kullanılan teknolojinin geldiği noktaya örnek olarak; ABD Ulusal Güvenlik Teşkilatı'nın (NSA) kullandığı kod adı "ECHELON" olan sistem verilebilir.

Siber âlemde bir diğer konuda bağımsız (olduğu sanılan) Hacker gruplarının düzenledikleri siber saldırılardır. Çoğu zaman devletlerarasında sorunlara neden olan Hackerlerin saldırıları ve sızma girişimleri ile gizli bilgilerin ortaya çıkarılması, stratejik devlet kurumlarının internet sitelerine ve ağ sistemlerine yapılan sanal saldırılar ile internet sitelerinin ve ağ sistemlerinin kullanılamaz hale gelmesi, saldırıların gayri resmi olarak devlet destekli gerçekleştirdiklerini akıllara getiriyor. ABC televizyonunun araştırma programı Four Corners tarafından Programda, geçen yıl bitmiş olması planlanan ancak geciken, Avustralya'nın yeni istihbarat karargâhına ilişkin planların, bir siber saldırı ile Çin'de bir sunucuya bağlı kişiler tarafından çalındığı iddia edildi. İddiaya göre, planlarda iletişim kablolama ve sunucu yerleri, kat planları ve güvenlik sistemleri detaylı biçimde gösteriliyor.[vii] Siber saldırılara çokça maruz kalan ABD bu yüzden sürekli olarak Çin'i suçlarken, sanal saldırıları düzenleyen Hackerlerin Çin ordusu tarafından desteklendiğini iddia etmesi Hacker gruplarının devlet destekli olduğunu ispatlar niteliktedir.

Geliştirilen elektronik istihbarat sistemlerinin devletler tarafından kullanımının yaygınlaşması ile savaşlar, sıcak çatışmalardan yerini çok büyük ekonomik zararlar verebilecek ve olumsuz psikolojik etki yaratacak olan "Siber Savaşlara" bırakmıştır. Öyle ki 2010 yılında İran'ı, Buşehr'de ki Nükleer Santraline faaliyete geçmesinden kısa süre sonra yapılan siber saldırılar sonucu yaklaşık olarak 800 milyon $ zarara uğratmıştı. İran'ın Nükleer santral sistemlerinin çökertilerek kullanılamaz hale gelmesinde ABD ve İsrail istihbarat servisleri tarafından geliştirilen bir virüsün neden olduğu iddia edildi.

Bu örnekler siber savaşların boyutlarını gözler önüne sererken devletlerin bir siber yarış içinde olduklarını söyleyebiliriz. Bu nedenle ulusal güvenliğin sağlanması ve rekabet gücünün korunması adına siber güvenliğin Milli Güvenlik Politikaları içinde yer alması zaruri hale gelmiştir.

-Echelon

1960 yılında Sovyetler Birliğine iltica etmiş iki ABD Ulusal Güvenlik Teşkilatı (NSA) elemanı Moskova'da düzenledikleri basın toplantısında Dünya'nın ilk defa duyacağı "Küresel Bilişim Teknolojileri Dinleme ve İzleme Sistemi olan "ECHELON'u" ifşa etmişlerdi. Kod adı "Echelon" olan bu sistem Soğuk Savaş Döneminin bitimine kadar telefon ve telgrafları, uydu, yer altı ve okyanus dibi uluslararası iletişim kablolarından dinleme yapmayı amaçlayan bir sitemdi. Öncelikle İngiltere ve ABD'nin istihbarat paylaşımını içeren sisteme daha sonradan üç ülke daha dâhil olunca Echelon

sistemi küresel bir ağa ulaştı.

ABD, İngiltere, Avustralya, Kanada ve Yeni Zelanda'nın içinde olduğu bu sistem günümüzde küresel olarak Dünya üzerinde ki her hangi bir noktada uydu, telefon ve internet gibi küresel iletişim araçlarının dinleme ve izlemesini yapabilen ve filtreleme sağlayan bir sistemdir. 1950'ler den bu tarafa şartlara ve ihtiyaçlara göre geliştirilen Echelon ortak ülkelerin girdiği "anahtar kelimeler" ile dünya üzerinde gerek telefon konuşması gerekse internet üzerinden yapılan görüşmelerde anahtar kelimelerden herhangi birinin kullanılması ile "Dictionary"(Sözlük) adı verilen filtreleme sistemi ile kayıt işlemine başlamaktadır. Echelon sistemi sadece dinleme ve izleme yapmamakta siber istihbaratta dünyanın en ileri teknolojisini kullanmaktadır. Bir kişinin ses frekanslarından telefon dinlemesi yapmasından anahtar kelimelerden birin kullanılması halinde tüm görüşmeyi kayıt altına alması ve uydu sistemlerine ve ya internet ağına bağlı her bilişim teknolojisi cihaza sızarak veri elde etme işine kadar yapabilmektedir. Bu şekilde günde yaklaşık olarak 1 milyon veririn analiz edildiği NSA dünya üzerinde 37 merkezde, içerisinde 2 bin dil bilimci ve analistin, toplamda ise 55 bin kişinin çalıştığı söylenmektedir.

Siber Güvenlik Politikaları

Siber birliklerin kurulması ile ekonomik, siyasi ve askeri nedenli siber savaşların gündeme geldiği ve devlet destekli siber terör eylemlerinin yaşandığı bu yüz yılda devletler, siber güvenlik politikaları oluşturarak ölümün olmadığı bu sanal saldırıları en az ekonomik zararla bertaraf etmeye çalışmaktadır.

Hâlihazırda küresel iletişim ağlarından yararlanan İstihbarat Servisleri neredeyse istedikleri bütün kapalı veri bankalarına girerek gizli ve özel bilgilere ulaşabilmektedirler.[viii] Fakat siber saldırı ve sızma girişimlerinin başarı derecesi, kullanılan teknolojinin ve kalifiye insan gücünün niteliği karşısında, karşı tarafın aldığı siber güvenlik önlemleri göz ardı edilmeden değerlendirilmelidir. Bu yüzden devletler, istihbarat savaşlarının en yoğun olarak yaşandığı bu çağda konvansiyonel silahlar kadar siber güvenliğe de önem vermektedirler. Türkiye ilk adım olarak Ulaştırma, Denizcilik ve Haberleşme bakanlığı bünyesinde BTK (Bilgi Teknolojileri Kurumu) ve Emniyet bünyesinde Siber Suçlarla Mücadele Şubesi ile önlem alırken, ABD aldığı önlemleri genişleterek 2009 yılında siber saldırılara karşı "Siber Savaş Komutanlığı" kurmuş ve başına bir Orgeneral atayarak 30 bin Hava Kuvvetleri askerini yeni komutanlığında görevlendirmiştir.

Siber saldırılar, askeri ve siyasi amaçlı üstünlük göstergesi olabileceği gibi *ekonomik zarar verme, tahrip etme amaçlı ve endüstriyel hırsızlıkta* olabilir. ABD'nin Çin'i suçlamasının en önemli nedenlerinden bir tanesi de internet siteleri ve ağ sistemlerine yapılan saldırıların yanı sıra endüstriyel hırsızlıktır. Bazı uzmanların Çinli Hackerler tarafından ABD'nin gelişmiş silahlarına ait bilgilerin çalınmış ve hala çalınıyor olması ihtimalini gündeme getirmeleri Haziran 2013 'te ABD Başkanı Barack Obama ve Çin Halk Cumhuriyeti Devler Başkanı Şi Cinping görüşmelerinin önemli konularından biri olmuştu. Hatta Çin'in yeni insansız hava araçlarının geliştirilmesinde ABD'den çalınan bilgilerin kullanıldığı iddiaları da vardı. Bu iddiaların önemli noktası tehditlerin boyutu ve siber güvenliğin önemidir. Bu nedenle Dünya'da özellikle askeri projelerin özel sektör konsorsiyum ile geliştiriliyor olması, proje bilgilerinin ve çalışanlarının can güvenliğinin korunması adına özel sektörün de devletler kadar ciddi siber güvenlik önlemleri almalarını gerektirmektedir.

AB üyesi devletlerin ciddi siber tehditlere maruz kalması AB'yi harekete geçirmiş ve AB bünyesinde ortak bir Siber Güvenlik Stratejisi oluşturulması kararlaştırılmıştır. Bu bağlamda siber suçlar tanımlanmış ve stratejik öneme sahip özel sektör şirketlerinden (enerji, ulaşım, bankacılık ve finans) zorunlu olarak güvenlik önlemleri almaları istenmiştir. AB Siber Güvenlik Stratejisi çerçevesinde

• Siber dayanıklılığın sağlanması
• Sanal âlemde işlenen suçların ciddi oranda azaltılması
• Siber savunma politikası ile Ortak Güvenlik ve Savunma Politikasına (CSDP) ilişkin becerilerin geliştirilmesi
• Siber güvenlik için gerekli olan sınaî ve teknolojik kaynakların geliştirilmesi
• Avrupa Birliği için tutarlı bir uluslararası sanal alem politikasının oluşturulması ve temel AB değerlerinin desteklenmesi [ix]

Kararlaştırılmıştır.

NATO ise, 2007 yılında üyesi Estonya'nın ağ sistemine yapılan kitlesel siber saldırıların ardından 2008 Bükreş Zirvesinde Siber tehditlere karşı önlem alınması ve siber güvenlik alanında işbirliği için güvenlik merkezleri kurulması kararlaştırılmıştır. 2012 yılında NATO üyesi ülkelerin katılımıyla "NATO Siber Güvenlik Tatbikatı" düzenlendi. Tatbikatta gerçekleştirilen senaryoların kapsamını, siber saldırılar sonucu tatbikata katılan üye ülkelerin mevcut durumlarının değerlendirilmesi, koordinasyon ve yeterliliklerinin test edilmesi ve alınacak önlemler oluşturmuştur. Türkiye'nin Genelkurmay Başkanlığı ve TÜBİTAK'ın temsil ettiği tatbikatta yeterlilikleri de test edilmiş oldu. Haziran 2013'te NATO Siber Güvenlik konusunda Savunma Bakanları düzeyinde ilk defa düzenlenen "Siber Güvenlik Zirvesinde" kapasite sıkıntıları, eksiklikler ve üye ülkeler arasında oluşan dengesizlikler masaya yatırıldı. Siber Güvenlik alanında zayıf kalan üye ülkelere saldırı olması halinde NATO olarak yardımcı olabilecek yöntemler oluşturulması kararlaştırıldı.

-Türkiye'de Siber Güvenlik

Türkiye, Dünya'da siber saldırılara en çok maruz kalan 4. Ülke olması ve Milli Askeri Projeler geliştiriyor olması sebebiyle siber güvenliğe ağırlık vermektedir. Nitekim Bakanlar Kurulu kararı ile "Siber Güvenlik Kurulu" kuruldu. Bu kurulda Başta Milli İstihbarat Teşkilatı, Dışişleri Bakanlığı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ve TÜBİTAK olmak üzere birçok devlet kurumu bulunuyor. Siber Güvenlik Kurulu'nun hazırladığı "Ulusal Siber Güvenlik Stratejisi 2013 -2014" eylem planı resmi gazetede yayınlanarak yürürlüğe girdi. Rapor halinde sunulan eylem planında Siber Saldırı ve Sızma girişimlerine karşı 2013 ve sonrasında nasıl bir stratejik yol izleneceği belirlendi. Ulusal Siber Güvenlik Stratejisi eylem planı çerçevesinde yasal düzenlemeler yapılacak, adli süreçte yardımcı olacak çalışmalar yürütülecek, ulusal siber güvenlik altyapısı güçlendirilecek, Siber olaylara müdahale merkezleri kurulacak ve siber güvenlik alanında nitelikli insan kaynağı yetiştirilip bilinçlendirme faaliyetleri yürütülecek.

Kurulacak olan "Siber Olaylara Müdahale Merkezleri, 7/24 müdahale esasına göre çalışacak "USOM" (Ulusal Siber Olaylara Müdahale Merkezi) kurularak, USOM'un koordinasyonunda çalışacak sektörel "SOME" (Siber Olaylara Müdahale Ekipleri) oluşturulacak. Sektörel SOME'ler siber olaylara müdahalenin yanı sıra kendisine bağlı SOME'lere ve ilgili olduğu sektöre özel bilgilendirme ve bilinçlendirme faaliyetleri yürütecek. Kurum ve kuruluşlar bünyesinde de sektörel SOME' lerin koordinasyonunda çalışacak SOME'ler kurulacak. USOM ve SOME'ler olaylara müdahale ederken suç soruşturmasına destek sağlayacak verilerin sağlanması için adli makam ve kolluk birimleri ile koordineli hareket edecekler. USOM ulusal temas noktası olarak diğer ülkelerin eşdeğer makamlarıyla ve uluslararası kuruluşlarla yakın işbirliği yapacaktır.[x]

Siber Güvenlik önlemleri tatbikatlarla desteklenerek Ocak 2011 ve Aralık 2013 yılında "Ulusal Siber Güvenlik Tatbikatı" ve Mayıs 2012 "Siber Kalkan Tatbikatı" gerçekleştirildi. Tatbikatlar ile Siber saldırılara karşı önlem alınması, kurumların bilgi ve iletişim sistemlerinin güçlendirilmesi, kurumlar arası koordinasyonun artırılması amaçlanmaktadır. Tatbikatta sonra yayınlanan sonuç bildirgelerinde başarılı sonuçlar alındığı anlaşılmaktadır.[xi]

---

[i] Gültekin Avcı, İstihbarat Teknikleri, Timaş Yayınları, Mayıs 2004
[ii] Öğün, İstihbarat 'ta Açık Kaynakların Önemi, 21.Yüzyıl Türkiye Enstitüsü, Temmuz 2011
[iii] Broadcast Intelligence Service.
[iv] Sait Yılmaz, Kamu Diplomasisi, Kum Saati Yayınları, 2012
[v] Akçadağ, BİLGESAM ANALİZ, Sürekli Artan Önemi Işığında Siber Güvenlik, Temmuz 2012
[vi] Krekel, Adams, George Bakos, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage, Createspace Independent Publishing Platform, 2012 October

[vii] Bkz. : http://www.bbc.co.uk/turkce/haberler/2013/05/130528_avustralya_cin.shtml
[viii] Yılmaz, S. ve Salcan, Siber Uzayda Güvenlik ve Türkiye, Milenyum Yayıncılık, Ocak 2008
[ix] Avrupa Komisyonu Basın Bildirisi, Brüksel, Şubat 2013 - http://www.avrupa.info.tr
[x] Ulusal Siber Güvenlik Stratejisi – Resmi Gazete, 20 Haziran 2013
[xi] Ulusal Siber Güvenlik Tatbikatlar için Bkz. : http://www.tk.gov.tr/etkinlikler/ulusal_etkinlikler/index.php