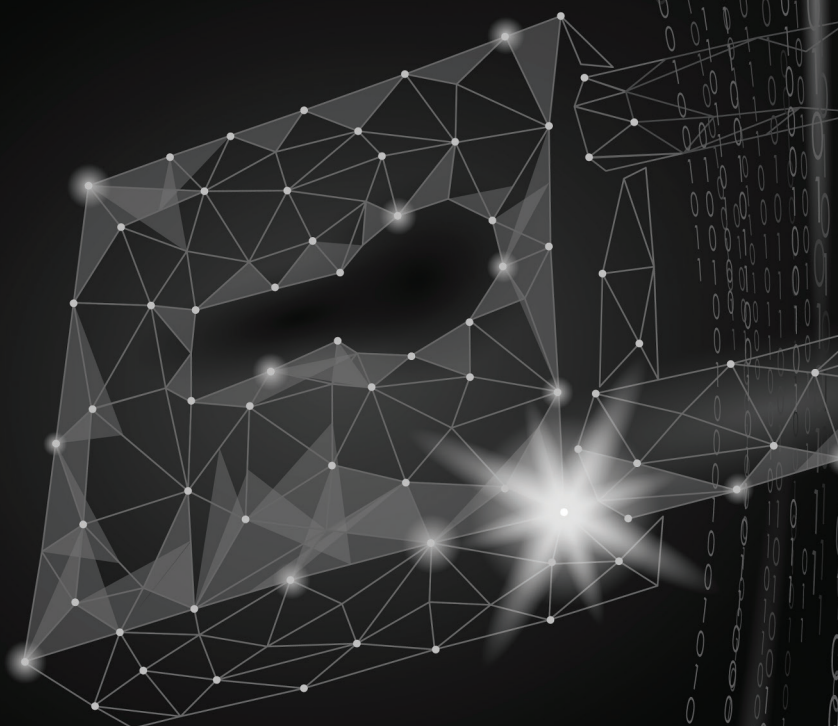
SETA Gelişen Askeri Teknolojiler Serisi .2.

Siber Güvenlik:

Küresel Trendler ve Türkiye'nin Kabiliyetleri

Ahmet Naci Ünal



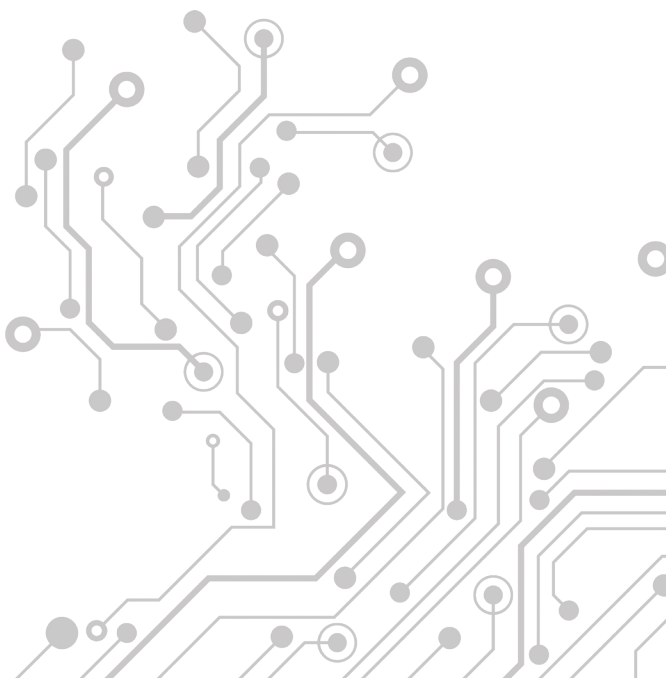
SETA

SETA Gelişen Askeri Teknolojiler Serisi .2.

Siber Güvenlik:

Küresel Trendler ve Türkiye'nin Kabiliyetleri

Ahmet Naci Ünal



SETA

AHMET NACİ ÜNAL

Dr. Ahmet Naci Ünal, Bahçeşehir Üniversitesi (BAÜ) Mühendislik ve Doğa Bilimleri Fakültesi'nde öğretim üyesidir. Elektronik tabanlı savunma teknolojileri, siber güvenlik konseptleri ve karar destek sistemleri konularında akademik çalışmaları bulunan Ünal; BAÜ bünyesindeki Siber Güvenlik Uygulama ve Araştırma Merkezi'nin müdürlüğü ile yine BAÜ Lisansüstü Eğitim Enstitüsü bünyesindeki Siber Güvenlik ve Bilişim Hukuku yüksek lisans programlarının akademik koordinatörlüklerini yürütmektedir. Ünal'ın uzmanlık alanlarıyla ilgili yayımlanmış makaleleri ve kitapları bulunmaktadır.

Gelişen Askeri Teknolojiler Serisi, yeni ve gelişmekte olan askeri teknolojilerin en önemli yönlerine küresel trendler ve Türkiye'nin kabiliyetlerine odaklanarak ışık tutan bir SETA projesidir. Proje, STM (Savunma Teknolojileri, Mühendislik ve Ticaret A.Ş.) tarafından desteklenmektedir.

SETA Yayınları 203
I. Baskı: 2022
ISBN: 978-625-8322-15-6

Kapak Tasarımı: Sema Türk Bayazit
Uygulama: Said Demirtaş
Baskı: Turkuvaz Haberleşme ve Yayıncılık A.Ş., İstanbul

SETA | SİYASET, EKONOMİ VE TOPLUM ARAŞTIRMALARI VAKFI
Nenehatun Cd. No: 66 GOP Çankaya 06700 Ankara TÜRKİYE
Tel: +90 312 551 21 00 | Faks: +90 312 551 21 90
www.setav.org | info@setav.org | @setavakfi

SETA | İstanbul
Defterdar Mh. Savaklar Cd. Ayvansaray Kavşağı No: 41-43
Eyüpsultan İstanbul TÜRKİYE
Tel: +90 212 395 11 00 | Faks: +90 212 395 11 11

SETA | Washington D.C.
1025 Connecticut Avenue, N.W., Suite 1106
Washington D.C., 20036 USA
Tel: 202 223 9885 | Faks: 202 223 6099
www.setadc.org | info@setadc.org | @setadc

SETA | Berlin
Kronenstraße 1, 10117 Berlin GERMANY
berlin@setav.org

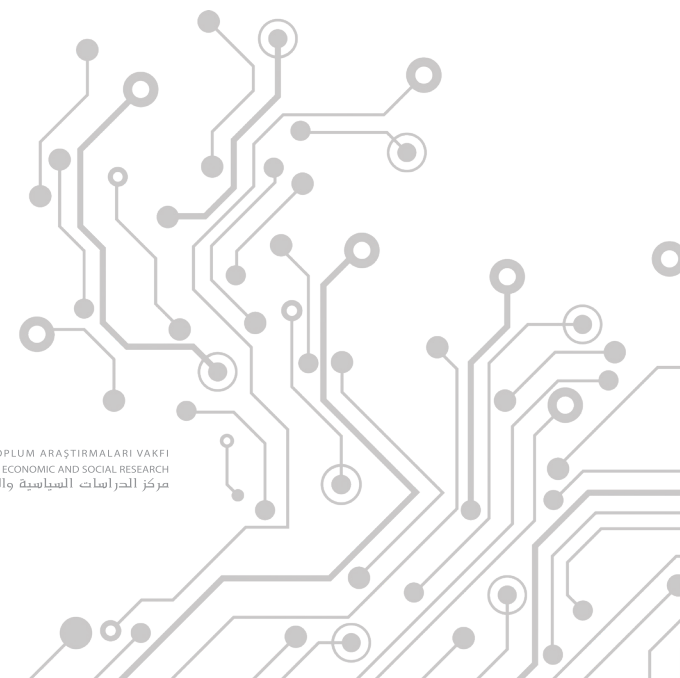
SETA | Brüksel
Avenue des Arts 27, 1000 Bruxelles BELGIUM
Tel: +322 652 0486

SETA Gelişen Askeri Teknolojiler Serisi .2.

Siber Güvenlik:

Küresel Trendler ve Türkiye'nin Kabiliyetleri

Ahmet Naci Ünal



SETA
SİYASET, EKONOMİ VE TOPLUM ARAŞTIRMALARI VAKFI
FOUNDATION FOR POLITICAL, ECONOMIC AND SOCIAL RESEARCH
مركز الدراسات السياسية والاقتصادية والاجتماعية

İçindekiler

Giriş

"Olgu, kavram veya komutların iletişim, yorum ve işlem için elverişli biçimde gösterimi"[1] şeklinde tanımlanan "veri" günümüzün sayısallaşan dünyasındaki en önemli yapı taşlarından birini oluştururken hayatın tüm alanlarını kapsayan önemli bir varlık olarak da değerlendirilmektedir. Yeryüzünde bulunan tüm canlılar ile teknoloji tabanlı sistemlerin tamamı birer veri kaynağı olarak faaliyet göstermektedir. Bu veriler bilişim sistemleri tarafından işlenerek özel, genel ya da disiplinlerarası alanlarda kullanılmak üzere bilgiye dönüştürülmekte; insanların yaşam kalitesinin artırılması ve mevcut kaynakların verimli kullanılması amacıyla sürekli bir veri akışı şeklinde kullanılmaktadır. Bu veri akışının etkinlikle gerçekleştirilmesinde akıllı sensörlerden oluşan ağ yapılarından, hızlı ve kesintisiz iletişimi sağlayan haberleşme teknolojilerinden ve çevik karar vermek için karar destek sistemlerinden yararlanılmaktadır. Bu akıllı ağlar tarafından üretilen tüm bilgilerin oluşturulmasında sistemlerin birbirleriyle haberleşmelerinde standartları oluşturabilmek için etkili bir ara yüz yazılımına, makine öğrenmesi tekniklerine, örgüsel ağ yapılarına ve bulut bilişim teknolojilerine ihtiyaç duyulmaktadır. Bu disiplinlerarası teknolojiler sayesinde anlık veri değişimleri etkili bir şekilde takip edilebilmekte ve çevik karar verme süreçleri gerçekleştirilebilmektedir. Bu çevikliğin sağlanmasında oldukça dinamik bir ortam olan siber uzay kullanılmaktadır.

Siber uzay; "internet, iletişim ağları, bilgisayar sistemleri, gömülü işlemciler ve denetleyiciler de dahil olmak üzere bilgi teknolojisi altyapılarının birbirlerine bağlı olduğu ağdan oluşan küresel bir ortam"[2] olarak ifade edilmektedir. Bu tanım dikkate alındığında siber uzay sadece internet tabanlı değil değişik ağ yapıları aracılığıyla birbirleriyle haberleşebilen sistemlerin de bulunduğu sı-

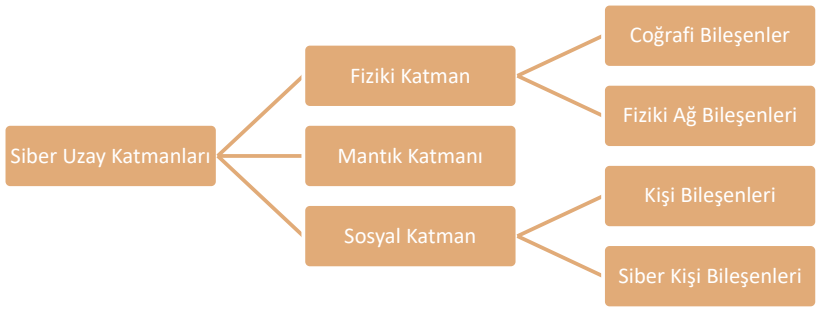
1 "Veri", Türk Dil Kurumu Güncel Türkçe Sözlüğü, https://sozluk.gov.tr, (Erişim tarihi: 20 Aralık 2021).

2 "Department of Defense Dictionary of Military and Associated Terms", Joint Publications, 8 Kasım 2010, https://irp.fas.org/doddir/dod/jp1_02.pdf, (Erişim tarihi: 20 Aralık 2021), s. 58.

nırsız bir bütünleşik fiziksel/sanal ortamı temsil etmektedir. Başka bir ifadeyle siber uzay; verinin/bilginin elde edilmesi, kullanılması ve saklanması süreçlerinin gerçekleştiği, kendisi sanal olmasına rağmen etkilerinin fiziksel olduğu bir ortamdır.

Siber uzay kavramı hakkındaki yaklaşımlar sadece tanımlamayla sınırlı kalmamakta kavramın konumunu da belirlemektedir. Bu kapsamda siber uzay; kara, deniz, hava ve uzaydan oluşan dört boyuta ilave beşinci boyut olarak konumlandırılmaktadır. Bu beş boyutun her birinin birbirlerinden bağımsız konumlar olarak kabul edildiği, sınırlı alanlarda kesişim noktalarının bulunduğu üzerinde durulurken siber uzay düğümlerinin (bağlantı noktalarının) her bir boyutla irtibatlı olduğu da ayrıca belirtilmektedir. Siber uzay fiziki katman, mantık katmanı ve sosyal katman olmak üzere üç ana bölümde incelenmektedir. Bu üç katmandan fiziki ve sosyal katmanlar ayrıca ikişer alt bileşene ayrılmaktadır (Şekil 1).[3]

Şekil 1. Siber Uzay Katmanları



Bu katmanlar ile alt bileşenlerine ait bilgiler şu şekilde özetlenebilir:

- **Fiziki Katman**: Coğrafi ve fiziki ağ bileşenlerinden oluşmaktadır. Coğrafi bileşenler mevcut ağlara bağlı olarak çalışan bilgi sistemlerinin bulunduğu ortamlardır. Fiziki ağ bileşenleri ise kablolu/kablosuz/optik altyapılar ile bu altyapılara erişimi sağlayan her tür teknik bileşendir.

- **Mantık Katmanı**: Mevcut ağların bağlı bulundukları düğüm noktalarını belirtmektedir. Bu noktalar bilgisayar, akıllı telefon ve sensör gibi her tür bilişim sistemleridir.

3 "Cyberspace Operations Concept Capability Plan 2016-2028", The United States Army's, 22 Şubat 2010, https://irp.fas.org/doddir/army/pam525-7-8.pdf, (Erişim tarihi: 20 Aralık 2021), s. 8-9.

- **Sosyal Katman**: Hem gerçek hem de siber/sanal bireylerden oluşmaktadır. Kişi bileşenleri fiziksel olarak var olan tek kişiyi belirtirken siber kişi bileşenleri fiziki kişi bileşenlerine göre daha fazla sayıda olabilmektedir.

Kullanılan teknolojiler düşünüldüğünde siber uzay katmanlarının etkin olarak hayatın bir parçası olduğu görülmektedir. Bu ortamlar; eğitim, haberleşme, enerji üretim kaynakları, sağlık, finans, güvenlik, bankacılık, kimya, savunma, hukuk, ulaşım, tedarik zinciri, havacılık ve uzay gibi disiplinlerarası teknolojilerle donatılmış alanlardan oluşmaktadır.

Bu şartlar altında siber uzayda faaliyet göstermek kadar siber uzayla iletişim halindeki sistemlerin güvenliklerinin sağlanması da önem kazanmaktadır. Bu koruma ise verinin üretilmesi, depolanması ve iletilmesi aşamalarını kapsamaktadır. Koruma altına alınmak istenen veriler sadece sayısal değil aynı zamanda fiziki değerleri de içermektedir. Örnek vermek gerekirse fiziksel ortamlar elle yazılan ya da bilgi sisteminden alınan kağıt çıktılar, bu kağıtların muhafaza edildiği dosyalar, resmi ya da özel mektuplar/raporlar, faks çıktıları ve toplantı yapılan mahaller şeklinde özetlenebilir.

Sayısal ortamlar ise veri bankaları, bulut bilişim sistemleri, bilgi sistemleri ya da harici belleklerde bulunan çeşitli dosyalar, e-postalar ve sosyal medya verileri şeklinde özetlenebilir. Bunların arasında belki de en önemli bilgi kaynağı insanın kendisidir. Sayılan tüm bu bileşenler bir mekan içerisinde faaliyet gösterdiği için bulunulan ortamların fiziki güvenliğinin sağlanması da önem arz etmektedir. Bu aşamada "bilginin bir varlık olarak tehdit veya tehlikelerden korunması için doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilgi varlıklarının her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme girişimi"[4] şeklinde aktarılan "bilgi güvenliği" kavramı ön plana çıkmaktadır. Bilgi güvenliği bileşenlerini erişilebilirlik, bütünlük ve gizlilik olmak üzere üç ana başlıkta incelemek mümkündür (Şekil 2).[5]

4 Şeref Sağıroğlu, "Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemleri", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, ed. Şeref Sağıroğlu ve Mustafa Alkan, (Grafiker Yayınları, Ankara: 2018), s. 26.

5 "Security 101", Carnegie Mellon University Computing Services Information Security Office, https://www.cmu.edu/iso/aware/presentation/security101-v2.pdf, (Erişim tarihi: 20 Haziran 2021).

Şekil 2. Bilgi Güvenliği Bileşenleri

Erişilebilirlik: Bilgi ve bilgi sistemlerinin yetkisiz erişimlerle bozulmalarına karşı korunmasıdır. Bilgi ve bilgi sistemlerine zamanında ve güvenilir bir şekilde erişilmesidir.

Bütünlük: Bilgilerin yetkisiz düzenlenmesinin veya silinmesinin önlenmesidir. Bilgi ve bilgi sistemlerinin doğru, tam ve bozulmamış olmasının sağlanmasıdır.

Gizlilik: Bilginin yetkisiz erişime veya açıklanmaya karşı korunması anlamına gelir. Bilgiye erişim hakkına sahip olanların bunu yapabilmelerini sağlarken yetkilendirilmemiş kişilerin bunu yapmalarının engellenmesidir.[6]

Bu kısa tanımlama ve bilgi güvenliği bileşenleri incelendiğinde bilgi güvenliği kavramının kurum, yerleşke, ev ya da iş yerinin giriş kapısından başlayıp aynı ortamı paylaşan tüm kişi ve cihazları kapsayacak genişlikte olduğu söylenebilir. Oysa günümüzde bu sayılan unsurlarla ilişkili olan teknolojilerin neredeyse tamamı siber uzayla bağlantılı bir şekilde faaliyetlerini sürdürmektedir. Özellikle koronavirüs (Covid-19) salgını sürecinde gerçekleştirilen çevrim içi faaliyetler günlük yaşam alanlarını resmi bir çalışma ortamına ya da sınıf haline getirmiştir. Dolayısıyla güvenlik kavramı sadece fiziki ortamı, çıktıları ya da üretilen verileri değil tüm bu faktörlerin paylaşıldığı siber uzay boyutunun güvenliğini sağlamak şeklinde gerçekleşmektedir. Bu güvenlik anlayışı da bilgi güvenliğinin ötesinde "siber güvenlik" kavramını ön plana çıkarmaktadır.

6 Sağıroğlu ve Alkan, *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, s. 3-5.

Siber Güvenlik

Uluslararası Telekomünikasyon Birliği (International Telecommunication Union, ITU) siber güvenliği "siber çevre, organizasyon ve kullanıcı varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin bütünü"[7] şeklinde tanımlamaktadır. Kullanıcı varlıkları ile sisteme bağlı bilgi işlem cihazları, personel, altyapı, uygulamalar, hizmetler, iletişim sistemleri ve siber uzay imkanlarıyla şahıslar ya da kurumlar tarafından üretilen ve/veya depolanan bilgilerin tamamını içermektedir.

Bu tanımlama incelendiğinde siber güvenlik kavramının sanal ve fiziksel tüm ortamları kapsadığı görülmektedir. Elbette bu ortamlar sadece bilişim sistemlerine ait donanım ve yazılımları değil siber uzayı kullanan tüm sistemler ve bu sistemlerin iletişimini sağlayan haberleşme teknolojilerini de kapsamaktadır.

Bu sebeple herhangi bir nesne, canlı ya da verinin korunabilmesi için ne tür tehditlerle karşılaşılabileceğinin bilinmesi başka bir ifadeyle tehdit tanımlamasının yapılması gerekmektedir. Konu siber güvenlik olunca bu tehdit kaynakları ve tehditlerin etkin olarak kullandıkları yöntemleri incelemek faydalı olacaktır.

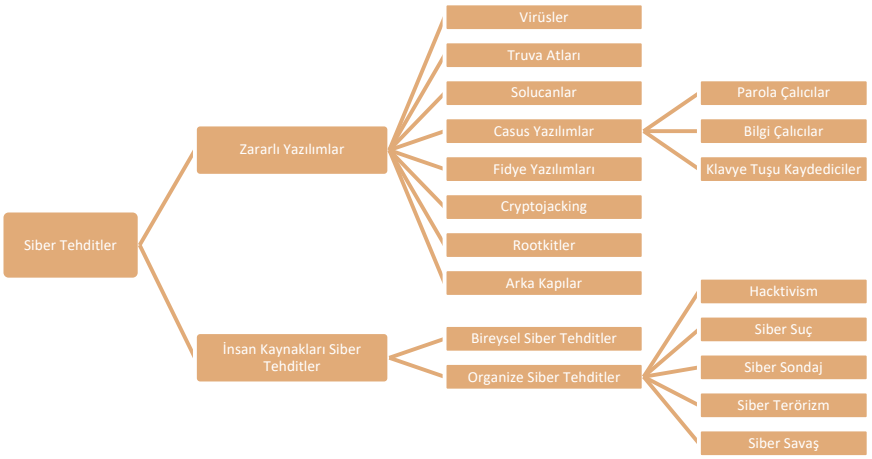
Siber Tehditler

Siber tehditler; siber uzay ortamını kullanan donanım, yazılım ve fiziksel ortam benzeri paydaşların faaliyetlerine zarar verilmesi ve sistemlerin belirlilik hallerinin zafiyete uğratılması olarak tarif edilebilir. Siber uzayda faaliyet gösteren tüm sistemler için siber tehditler en önemli güvenlik sorununu oluşturmaktadır. Bu nedenle siber uzay faaliyetlerinin etkili bir şekilde gerçekleştirilmesi etkin bir

7 "Definition of Cybersecurity", ITU, https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx, (Erişim tarihi: 20 Aralık 2021).

siber tehdit tanımlamasına, tespitine, analizine ve tehdit seviyesinin/zarar riskinin düşürülmesine bağlıdır. Bu kapsamda yapılması gereken temel tanımlama faaliyeti için Şekil 3'ten yararlanılabilir.[8]

Şekil 3. Siber Tehditler



Şekil 3 incelendiğinde siber tehditlerin öncelikle insan kaynaklı mı yoksa yazılım kaynaklı mı olduğunun saptanmasına ihtiyaç vardır. Yapılan bu tasnifle zararlı yazılımların neler olduğu ve kötü amaçlı insanların bu yazılımları hangi stratejilerle geliştirdiklerinin öğrenilmesi amaçlanmaktadır.

Zararlı Yazılımlar

Zararlı yazılım, siber uzayda faaliyet gösteren ya da siber uzay faaliyetlerinden yararlanan her tür sistemi zafiyete uğratmak için tasarlanan tüm yazılımların ortak adıdır. En temel zararlı yazılım kaynakları olarak virüsler, truva atları, solucanlar, casus yazılımlar, fidye yazılımları, *cryptojacking* ve *rootkit*ler sayılabilir. Bu zararlı yazılım kaynakları hakkında şu kısa tanımlamalar yapılmıştır:

- **Virüsler:** En eski zararlı yazılım türüdür. İletilen her tür dosyada saklanabilirler. Mevcut programları değiştirebilirler, uygun ortam oluşturulduğunda başka bilgi sistemlerine kendilerini kopyalarlar.

8 Şekil 3 oluşturulurken yararlanılan kaynaklar için bkz. Erdal Özkaya, *Siber Güvenlik: Saldırı ve Savunma Stratejileri*, (Buzdağı Yayınevi, Ankara: 2020); Refik Samet ve Ömer Aslan, "Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemleri", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, ed. Şeref Sağıroğlu ve Mustafa Alkan, (Grafiker Yayınları, Ankara: 2018), s. 228-232.

- **Truva Atları:** Zararsız bir programmış gibi gözüküp kullanıcının bilgisi olmadan bulaşan, bu zararlı yazılımı yapan kişi ya da kişilerce aktif hale getirildiklerinde dosyalarınızın paylaşılmasına, değiştirilmesine, izlenmesine ve silinmesine sebep olabilen zararlı yazılımlardır. Truva atları, kendi başlarına başka bir sisteme bulaşamazlar ve aktif hale geçemezler.

- **Solucanlar:** Tıpkı virüsler gibi bilgi sistemleri arasında çoğalarak bulaşabilirler. Bu çoğalma hem bulunduğu hem de bulaştığı sistemde çok büyük hacimlerde olur. Bu sebeple bilgi sistemlerinin ağ trafiklerinde büyük yoğunluklara sebep olurlar ve ağ bağlantı erişimini yavaşlatırlar.

- **Casus Yazılımlar:** Bilgi sisteminde bulunan verilerle sistem kullanıcılarına ait bilgileri toplayarak casus yazılımı bulaştıran kişi ya da kişilerle paylaşırlar. Paylaşılan bu veriler; e-ticaret, bankacılık ve kredi kartı şifresi gibi her türlü finansal bilgilerin yanı sıra bilgi sisteminki tüm veri ve dosyalar da olabilir.

- **Fidye Yazılımları:** Bulaştıkları bilgi sisteminde kullanıcı tarafından oluşturulmuş dosyaları ya da bilgi sisteminin tamamını şifreleyerek kullanılamaz hale getirilen zararlı yazılım türüdür. Bilgi sisteminin tekrar erişilebilir olması için kullanıcıdan belli miktarda fidye istenmektedir.

- ***Cryptojacking*:** Bilgi sistemine kullanıcının haberi olmadan yerleşir. Ardından kripto para madenciliği yapmak için bulaştığı bilgi sisteminin işlem gücünü kullanır.

- ***Rootkit*ler:** Kötü amaçlı kişilerin hedef bilgi sistemine erişerek o sistemi kontrol etmesini sağlayan zararlı yazılım türüdür. Bilgi sistemi *rootkit* bulaşının ardından tamamen zombi bilgi sistemi haline gelir.

- **Arka Kapılar:** Geleneksel güvenlik kurulumlarını devre dışı bırakarak kullanıcının haberi olmadan bilgi sistemini uzaktan erişime açabilen yazılımlardır. Arka kapıların oluşturulmasında genellikle truva atlarından yararlanılır. Daha çok karmaşık saldırılar öncesinde bilgi sistemine yüklenirler ve aktifleşmek için saldırı gününü beklerler.

İnsan Kaynaklı Siber Tehditler

Siber güvenlik zafiyetleri kapsamında insan önemli bir yer tutmaktadır. Bazı insanlar bilinçli/bilinçsiz ya da kasıtlı/kasıtsız olarak yaptıkları çeşitli davranışlarla bilgi sistemlerinin güvenliğini sarsabilmekte, hatta siber güvenlik ihlallerine dahi sebep olabilmektedir. Farkında olmama ya da bilinçsiz bir şekilde zarar verme faaliyetlerinin çoğu eğitimsizlikle alakalı olarak değerlendirilebilir. Bu tür faaliyetlerde verilen zarar kasıtlı ve organize olmadığı için sistematik bir süreci de kapsamayabilir. Ancak bazı siber güvenlik olayları doğrudan insanlar tarafından ve kötü amaçlı şekilde gerçekleştirilebilmektedir.

İnsan kaynaklı olan bu siber tehditler ister bireysel isterse organize olsun genellikle şu dört tür faaliyeti içermektedir:

- **Dolandırıcılık:** Kuruma ait verilerin kişisel kazanç için kullanılmasıdır.
- **Bilgi Teknolojilerini Sabote Etmek:** Kuruma karşı büyük ve öngörülemeyen bir eylem olup genel altyapının kullanılabilirliğini engellemeye yönelik faaliyetlerdir.
- **Fikri Mülkiyet Hırsızlığı:** Kuruma ait telif hakları, patentler, ticari markalar ve ticari sırların izinsiz olarak sızdırılmasıdır.
- **Casusluk:** Sanayi veya devlet kuruluşlarından her tür verinin yasa dışı yollarla elde edilmesidir.

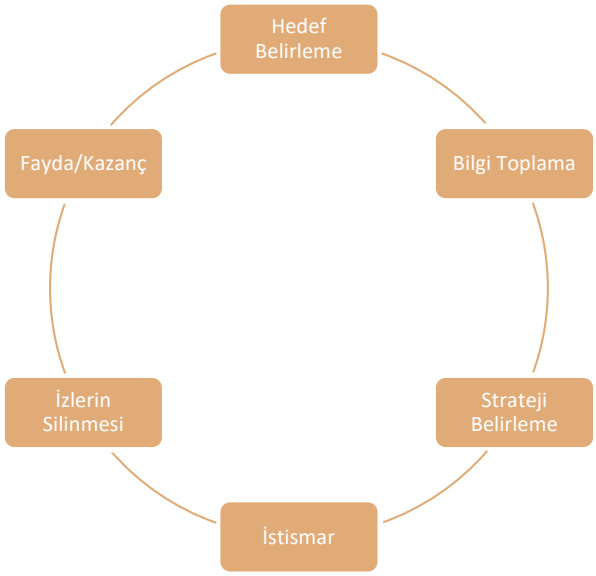
Bu süreç bütünsel bakış açısıyla incelendiğinde zararlı yazılımlar kapsamında belirtilen faktörler ile insan kaynaklı faktörlerin belirli kombinasyonlarla birlikte kullanılabileceği de unutulmamalıdır. Bu durum hem zararlı yazılımların hem de insan kaynaklı tehditlerin gelişen teknolojiyle birlikte hızlı bir dönüşüm sürecine gireceğinin de habercisi olmaktadır. Bu dönüşen tehditler karşısında siber güvenlik araştırmacıları tarafından geliştirilen ve etkili olarak kullanılan “siber saldırı yaşam döngüsü” kavramı önem kazanmaktadır.

Siber Saldırı Yaşam Döngüsü

Siber uzayda faaliyet gösteren ya da siber uzay imkanlarından yararlanan tüm sistemlerde yüzde 100 güvenli ortamdan bahsetmek mümkün değildir. Bunun sebebi bilişim teknolojilerindeki sürekli gelişimin siber tehdit kaynaklarını da dönüştürmesidir. Siber tehdit etkilerini minimize edebilmenin yolu detaylı ve

güncel tutulacak risk analizlerinin yapılmasıyla ilişkilidir. Bu analizin sağlıklı yapılabilmesi için güvenilir veriye ihtiyaç vardır. Bu nedenle tehdidi saptamak, saptanan bu tehdit verilerinin analizini gerçekleştirerek tanımlamak ve bu faaliyetlerin sonrasında tehdidin türünü ve saldırı aşamasını belirlemek gerekmektedir. Başka bir ifadeyle tehdide yönelik "nedir?", "nerededir?" ve "ne yapmaktadır?" gibi soruların cevapları aranmaktadır. Ancak tehdit; siber uzaydan gelince bu sorulara cevap bulunması hem güçleşmekte hem de tehdit belirlemesi için geçen süre uzamaktadır. Bu kapsamda yapılabilecek şey "siber tehdit kaynağı merkezli düşünce" geliştirebilmektir. Bu düşüncenin geliştirilmesinde yardımcı olan en önemli faktör "siber saldırı yaşam döngüsü" olarak tanımlanan süreçtir (Şekil 4).[9]

Şekil 4. Siber Saldırı Yaşam Döngüsü



Siber saldırı yaşam döngüsü, siber saldırganların saldırı süreçlerinin faaliyet basamaklarını göstermektedir. Bu süreçte öncelikle siber saldırının yapılacağı hedef belirlenir. Hedefin belirlenmesi aşamasında ya da hedef belirlendikten sonra hedef sistem hakkında port taraması, sosyal mühendislik, ağa sızılarak trafiğin izlenmesi gibi yöntemler kullanılarak bilgi toplanmasına başlanır.

9 Salih Erdem Erol ve Şevket Sağıroğlu, "Siber Güvenlik Farkındalığı, Farkındalık Ölçüm Yöntem ve Modelleri", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, ed. Şeref Sağıroğlu ve Mustafa Alkan, (Grafiker Yayınları, Ankara: 2018).

Bu işlemin gerçekleştirilmesiyle saldırı yapılacak sisteme ait zafiyet alanları araştırılır. Belirlenen bu zafiyet alanlarının tespitinden sonra hedef sistemin nasıl ele geçirileceğine yönelik strateji üzerinde çalışılmaya başlanır. Bu aşamada hedef bilgi sistemine nasıl saldırılacağı, kullanılacak saldırı tekniği ve zararlı yazılım tipi gibi hangi siber saldırı araçlarından yararlanılacağına karar verilir. Bu kararla birlikte hedef sisteme saldırı işlemi gerçekleştirilerek sisteme sızılır. Bu sızmanın ardından bilgi çalma, bilgi değiştirme, veri ya da bilgi sisteminin şifrelenmesi ve veri silme gibi hedefe yönelik belirlenen amaçlar gerçekleştirilir. Bilgi sisteminde amaçlanan saldırı faaliyeti sonuçlandırıldıktan sonra mevcut izler silinir. Burada saldırganın bilgi ve teknoloji altyapısı ne kadar güçlüyse iz silme faaliyeti de o kadar başarılı olacaktır. Çünkü iz bırakılması bilgi sisteminde oluşturulan anomalinin tespit edilmesini kolaylaştırmak/çabuklaştırmak demektir. Bu sebeple siber izler olabildiğince etkili bir şekilde yok edilmeye çalışılır. Son aşama ise bu saldırı sonucu elde edilen faydanın/kazancın değerlendirilmesidir. Döngünün bu şekilde tamamlanmasının ardından yeni hedef arayışına başlanır. Yani süreç başka hedeflerle ya da aynı hedefin farklı bileşenleriyle devam eder.

Bu döngünün saldırıya uğrayan birimler tarafından düzgün değerlendirilmesi siber saldırganın; tespit edilmesi, tanımlanması ve izinin sürülmesi aşamalarında önemli ipuçlarının elde edilmesinde yararlı olacaktır. Burada belki de dikkate alınması gereken en önemli husus fayda/kazanç ifadesiyle kısaca betimlenen siber saldırıda kullanılan tehdit kaynağının saldırılan sistem üzerinde oluşturduğu etkidir. Bu etkinin doğru tespit edilerek tanımlanması, siber saldırganların amaçlarına ulaşamadan caydırılmaları için bir fırsat olabilir.

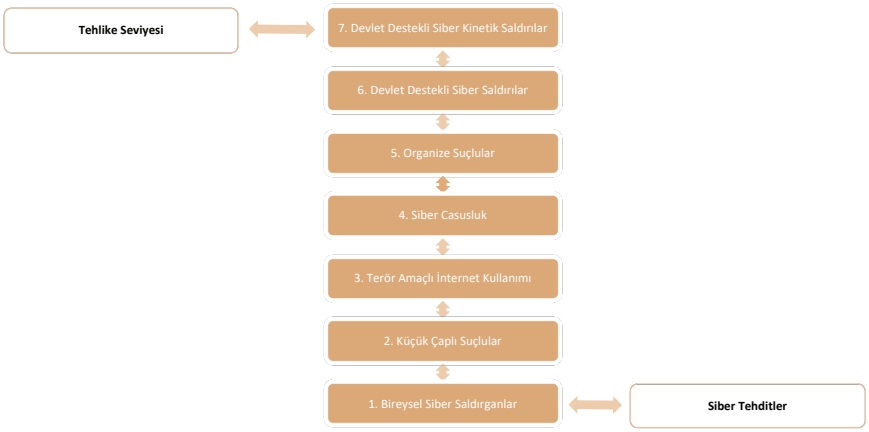
Siber Tehdit Etki Değerlendirmesi ve Caydırıcılık

Herhangi bir sorun ya da problemi çözebilmenin ilk adımı o sorun ya da problemin bütünsel bakış açısıyla doğru tanımlanması ve bizimle ilgisinin ortaya konmasıdır. Bu kapsamda sorunu ya da problemi analiz edebilmek için o sorun ya da problemin kök nedenlerine inerek parçadan bütüne doğru bilimsel analiz yöntemleriyle ilerlenmelidir. Yani kök neden ile problem arasındaki sürecin doğru modellenmesi ya da sınıflandırılması gerekmektedir. Bu sınıflandırma sayesinde asıl yoğunlaşılması gereken alan diğer alanlardan ayrıştırılacağı için hem dikkat olay üzerine yoğunlaştırılacak hem de enerji verimli ve etkili kullanılabilecektir.

Siber Tehdit Etki Değerlendirmesi

Siber tehdit etki değerlendirmesi kapsamında bir sonuca ulaşabilmek için tehdit kaynakları ile tehlike seviyelerinin kıyaslanması gerekmektedir. Bazı akademik kaynaklarda "siber tehdit spektrumu"[10] veya "siber tehdit seviyeleri"[11] olarak adlandırılan çalışmalarda göz ardı edilmemesi gereken en önemli husus; sınıflandırılan/değerlendirilen bu tehditlerin her birinin bireyleri, kurumları ya da devletleri hedef olarak seçebilecek olmasıdır. "Siber tehdit spektrumu" olarak adlandırılan ve siber tehditler ile bu siber tehditlerin tehlike seviyelerinin birbirleriyle kıyaslanması şeklinde ifade edilen çalışmaya ait grafik gösterim Şekil 5'te bulunmaktadır. Aslında tasnif amaçlı gerçekleştirilen bu yapı, bu raporda siber tehdit etki değerlendirmesi bakış açısıyla incelenmektedir.

Şekil 5. Siber Tehdit Spektrumu



Şekil 5'e göre siber tehditler; bireysel siber saldırganlar, küçük çaplı suçlular, terör amaçlı internet kullanıcıları, siber casusluk, organize suçlular, devlet destekli siber saldırılar ve devlet destekli siber kinetik saldırılar olmak üzere yedi basamaktan oluşmaktadır. Bu basamaklar "siber tehditler" ile "tehlike seviyeleri"nden oluşan iki boyutlu evrende kıyaslanmakta ve siber tehditlerin tehlike seviyelerinin düşük ve yüksek olarak sınıflandırılmasına göre ölçeklendirilmektedir.

10 Steven Bucci, "The Confluence of Cyber Crime and Terrorism", The Heritage Foundation, 12 Haziran 2009, https://www.heritage.org/defense/report/the-confluence-cyber-crime-and-terrorism, (Erişim tarihi: 18 Ağustos 2022).

11 Deb Bodeau, Richard Graubar ve Jennifer Fabius-Greene, "Improving Cyber Security and Mission Assurance Via Cyber Preparedness (Cyber Prep) Levels", *2010 IEEE Second International Conference on Social Computing*, (Ağustos 2010), s. 1147-1152; Jenna Ahokas ve Tuomas Kiiski, *Cybersecurity in Ports*, Cilt 3, (Turku School of Economics University, Turku: 2017) s. 14-15.

Bu kapsamda "bireysel siber saldırganlar" hem tehdit hem de tehlike seviyesi açılarından en az siber tehdit etki değerine sahipken "devlet destekli siber kinetik saldırılar" ise en yüksek değerli siber tehdit etki değerine sahiptir. Burada "devlet destekli siber kinetik saldırılar" ile tanımlanmak istenen yapılan siber saldırının sonucunda örneğin elektrik üretim tesislerinin herhangi bir fiziksel saldırı olmaksızın çalışamaz duruma getirilmesidir.

"Siber tehdit seviyeleri"[12] olarak adlandırılan çalışmaların ilkinde seviyeler siber vandalizm, siber dolandırıcılık, siber gözetim, siber casusluk ve siber savaş olmak üzere beş bölüme ayrılmaktadır (Tablo 1).

Tablo 1. Siber Tehdit Seviyeleri

Seviyeler	Siber Saldırgan Tipleri	Saldırganların Amaç ve Hedefleri
Seviye 1 (Siber Vandalizm)	Küçük saldırgan gruplar	Organizasyon yapısını bozmak
Seviye 2 (Siber Dolandırıcılık)	Bireysel veya küçük saldırı grupları	Politik-ideolojik amaçlar Dolaylı casusluk
Seviye 3 (Siber Gözetim)	Büyük saldırı grupları Terör örgütleri Organize suç örgütleri	Genel altyapı bilgisine sahip olmak Büyük ölçekli saldırılar için temel verileri elde etmek
Seviye 4 (Siber Casusluk)	Profesyonel istihbarat kuruluşları	Ülkelerin özel görev ve programları
Seviye 5 (Siber Savaş)	Askeri birlikler	Hedefin bilgi altyapısını yok etmek

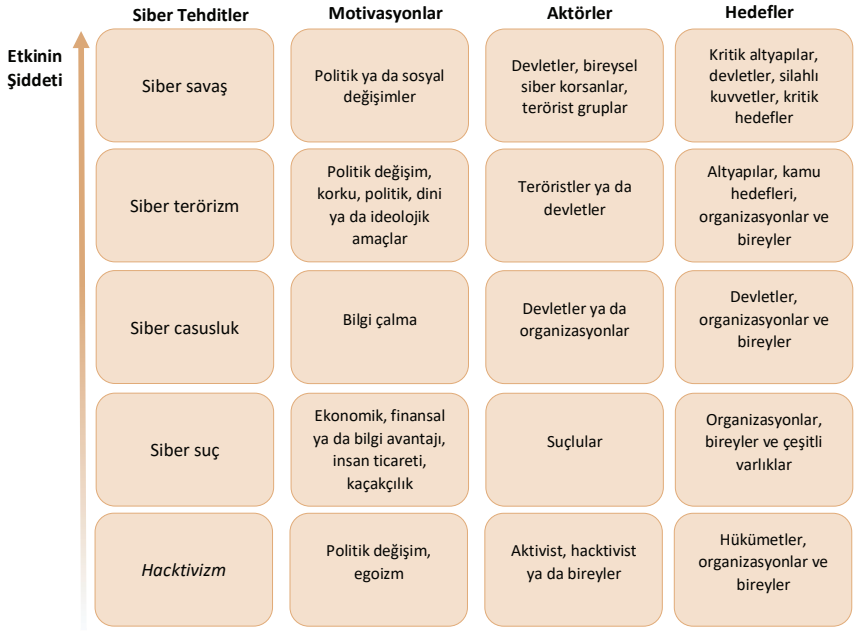
Bu beş tehdit seviyesi "siber saldırgan tipleri" ve "siber saldırganların amaç ve hedefleri" olarak iki ana bölümde incelenmiştir. Bu siber tehdit sınıflamasında siber vandalizm ile küçük saldırgan gruplar etki değeri en düşük seviyeyi temsil ederken siber savaş ile askeri birlikler ise etki değeri en yüksek seviye olarak tanımlanmıştır.

Siber tehdit seviyeleri[13] kapsamında yapılan diğer bir çalışmada siber tehditler *hacktivizm*, siber suç, siber casusluk, siber terörizm ve siber savaş olmak üzere beş bölümde incelenmiştir. Bu dağılım motivasyon, aktörler ve hedefler olmak üzere üç etki değeri olarak birbirleriyle kıyaslanmıştır (Şekil).

12 Bodeau, Graubar ve Fabius-Greene, "Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels", s. 1147-1152.

13 Ahokas ve Kiiski, *Cybersecurity in Ports*, s. 14-15.

Şekil 6. Siber Tehdit Seviyeleri



Burada siber tehdit etki değeri/şiddeti *hacktivizm*den siber savaşa doğru artarken her bir siber tehdidin içerdikleri hususlar yatay eksende motivasyonları, faaliyetlerde rol alan aktörler ve hedefleri yönüyle incelenmektedir. Bu kapsamda incelenen üç çalışma yazarlarının adlarıyla Tablo 2'de toplu halde gösterilmektedir:

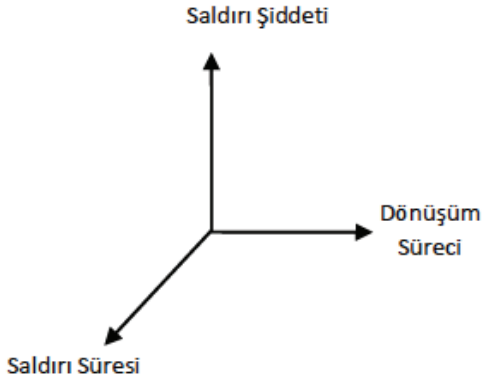
Tablo 2. Toplu Halde Siber Tehdit Değerlendirmesi

Bucci (2009)	Bodreu vd. (2010)	Ahokas ve Kiiski (2017)
Bireysel siber saldırganlar	Seviye 1 (Siber vandalizm)	*Hacktivizm*
Küçük çaplı suçlular	Seviye 2 (Siber dolandırıcılık)	Siber suç
Terör amaçlı internet kullanıcıları	Seviye 3 (Siber gözetim)	Siber casusluk
Siber casusluk	Seviye 4 (Siber casusluk)	Siber terörizm
Organize suçlular	Seviye 5 (Siber savaş)	Siber savaş
Devlet destekli siber saldırılar		
Devlet destekli siber kinetik saldırılar		

Hem içerik hem de yayın tarihleri açısından farklı olan bu üç çalışmada da en alt tehdit seviyesi insan temelli tehditlere ayrılırken en üst seviye tehdit değerlendirmesi ise siber savaş olarak belirtilmektedir. Ancak siber tehdit değerlendirmesi bir sonuç değil siber saldırıların etkinliğinin belirlenmesinde temel oluşturacak bir sürecin başlangıcıdır. Bu kapsamda yapılacak süreç modellemesinde insan beyninin fonksiyonel yapısından yararlanılmaktadır.

İnsan beyni çevresindeki olguları üç boyutlu olarak değerlendirmekte ve herhangi bir problemi analiz ederken de çözüm kümesini üç boyutlu bir ortamda şekillendirmektedir. Bu kısımda anlatılan üç çalışmaya ek olarak yapılan bir diğer çalışmada üç boyutlu siber saldırı uzayı tasarlanmakta ve siber saldırı etki derecesine odaklanılmaktadır (Şekil 7).[14]

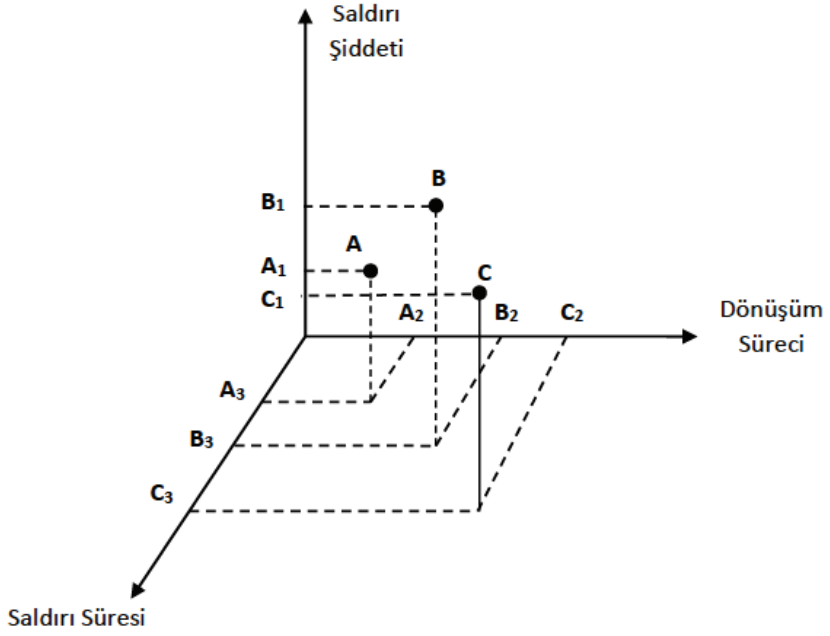
Şekil 7. Siber Saldırı Etkinliğinin Üç Boyutlu Ortamda Modellenmesi



Siber saldırı uzayı; saldırı şiddeti, dönüşüm süreci ve saldırı süresi olmak üzere üç boyuttan oluşturulmaktadır. Dolayısıyla bu uzayda gerçekleştirilecek saldırıların etkililikleri üç eksen üzerinde birbirlerinden farklı ve bütünleşik olarak değerlendirilmektedir (Şekil 7).

14 Martin C. Libicki, "Cyberdeterrence and Cyberwar", Rand Corp, (2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf, (Erişim tarihi: 18 Ağustos 2022).

Şekil 8. Siber Saldırıların Etkinliğinin Üç Boyutunun Örnek Gösterimi



Örneğin Şekil 8'de gösterilen A, B ve C harfleri birbirinden farklı üç siber saldırıyı temsil etsin: A, B ve C siber tehditlerinin her üç boyuttaki iz düşümlerine bakıldığında etki değerlerinin birbirlerinden farklı olduğu görülmektedir. Örneğin saldırı şiddeti ekseninde $B_1>A_1>C_1$ olurken dönüşüm süreci ekseninde $C_2>B_2>A_2$ ve saldırı süresi boyutunda da $C_3>B_3>A_3$ olduğu görülmektedir. Başka bir ifadeyle B siber saldırı kaynağı saldırı şiddeti ekseninde en önemli etkiye sahipken C siber saldırı kaynağı dönüşüm süreci ve saldırı süresi eksenlerinde en büyük etkiye sahiptir. Dolayısıyla tehdit değerlendirmesi aşamasında farklılıkların tasnif edilmesi büyük önem taşımaktadır. Bu tehdit değerlendirmesinin yapılması ve cevap verme süresi ne kadar hızlı gerçekleştirilirse caydırıcılık seviyesi de aynı oranda başarılı olacaktır.

Siber Caydırıcılık

Caydırıcılık "bir saldırganlığı önlemek ve engellemek için önlem alma işi"[15] olarak tanımlanmaktadır. Başka bir ifadeyle "mevcut imkanlarla herhangi

15 "Caydırıcılık", Türk Dil Kurumu Güncel Türkçe Sözlüğü, https://sozluk.gov.tr, (Erişim tarihi: 21 Aralık 2021).

bir saldırıda bulunmadan, karşı tarafı etkisizleştirebilme yeteneği"dir. Bu kavram daha çok askeri yazında kullanılsa da özellikle 2010'lardan itibaren siber uzayın da bir tehdit kaynağı olarak algılanması ve siber tehditlerin siber fiziksel ortamlarda da etkili olmasıyla birlikte akademik yazındaki yerini almıştır.

Özellikle siber savaş kavramını geliştirmeye yönelik çalışmalarda siber caydırıcılık üzerinde durulmakta ve bu kavram Şekil 9'da gösterildiği gibi ifade edilebilmektedir:[16]

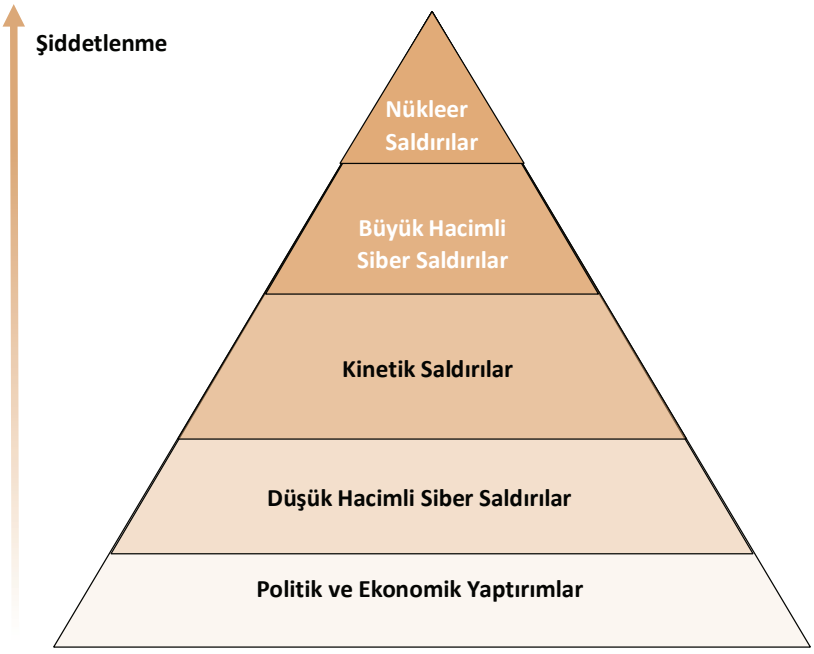
Şekil 9. Siber Caydırıcılık

Bu sınıflandırmada ülkelerin savaşma kabiliyetleri ve etkileri, dolayısıyla caydırıcılık göstergeleri; (tüm şartlar önemli olmasına rağmen) diplomasi ve ekonomik şartları, siber kabiliyetleri, fiziki güç seviyeleri ve nükleer güçlerine göre derecelendirilmiştir. Bu kapsamda yapılan sıralamada diplomasi ve ekonomik şartlar caydırıcılık seviyesi en düşük bileşen olarak değerlendirilirken nükleer güç kapasitesi ise en önemli güç çarpanı yani caydırıcılık faktörü en yüksek bileşen olarak değerlendirilmektedir. Dolayısıyla bu derecelendirmeye göre sadece nükleer güce sahip olmak bile en üst seviyede caydırıcılık sağlayabilmektedir. 2009'da yapılan bu çalışmadan altı yıl sonra yapılan farklı bir çalışmada ise şu şartlara dikkat çekilmiştir (Şekil 10).[17]

16 Libicki, *Cyberdeterrence and Cyberwar*, s. 29.

17 Annegret Bendiek ve Tobias Metzger, "Deterrence Theory in the Cybercentury: Lessons from a State-of-the-art Literature Review", SWP-Berlin, 2 Mayıs 2015, https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf, (Erişim tarihi: 18 Ağustos 2022).

Şekil 10. Olası Bir Gerginlik Modeli



Şekil 10 incelendiğinde yine nükleer güç en tepedeki yerini doğal olarak korurken siber saldırılar boyutlarına/hacimsel durumlarına göre kinetik vuruşun altında ve üstünde yer almaktadır. Bu durum ise günümüz dünyasında büyük boyutlu bir siber saldırının neredeyse nükleer güce denk bir hale geldiğini göstermektedir. Hatta nükleer silahlar kullanıldıkları takdirde oluşturacakları uzun süreli sağlıksız (radyoaktif) etkiden dolayı sadece caydırıcı rollerini sürdürürken büyük çaplı bir siber saldırı pek çok alanda etkili olabilmektedir. Ayrıca devletlerin denetiminde olduğu için nükleer gücün kontrolü de daha kolay olabilmektedir. Oysa siber saldırılar değişik seviyelerdeki siber saldırganlar tarafından rahatlıkla gerçekleştirilebilmektedir (Şekil 5 ve 6 ile Tablo 1 ve 2).

Siber saldırıların bu kadar etkili olması ve neredeyse nükleer silahların etki derecesine gelmiş olması akla "Bu saldırıların bu kadar etkili olmasında sadece stratejiler mi etkilidir?" sorusunu getirmektedir. Bu saldırıların etkili olmasında elbette belirlenen stratejilerin önemli bir yeri olmakla birlikte bu stratejilerin gerçekleştirilmesinde en önemli faktör ise siber silahlar olarak adlandırılan zararlı yazılım türleridir.

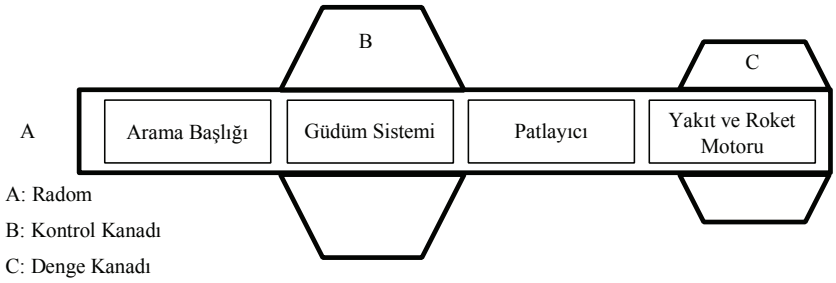
Siber Silahlar

Silah sistemleri yakın geçmişte ve günümüzde sahip olunan etki faktörüne göre "klasik (konvansiyonel) silahlar" ve "kitle imha silahları" olarak adlandırılırken "biyolojik silahlar", "kimyasal silahlar", "nükleer silahlar" ve "siber silahlar" gibi kullandıkları teknolojilerin adlarıyla da anılmaktadır.

Siber silahlar dışında kalan bütün silahlar fiziksel olarak çeşitli platformlar tarafından hedeflerine gönderilmekte, bu silahların oluşturduğu fiziksel tahrip dereceleri tespit edilmekte ve sonuçlar yine fiziksel olarak değerlendirilebilmektedir. Siber silahlar ise herhangi bir harici platform tarafından taşınmamakta, herhangi bir sistem tarafından yönlendirilmemekte ve tahrip dereceleri klasik keşif araçlarıyla tespit edilememektedir. Ancak en az diğer silah sistemleri kadar fiziksel etkiye sebep olmaktadır.

Siber silahlar dışında kalan tüm harp başlıkları için kullanılabilen en gelişmiş silah sistemi olarak güdümlü füzeler incelenebilir. Güdümlü füzeler itki sistemi, arama başlığı, güdüm sistemi ve harp başlığı (mühimmatı) olmak üzere dört temel bölümden oluşmaktadır (Şekil 11).[18]

Şekil 11. Güdümlü Füzenin Temel Bölümleri



Kaynak: Bendiek ve Metzger, "Deterrence Theory in the Cybercentury: Lessons from a State-of-the-art Literature Review".

18 Filippo Neri, *Introduction to Electronic Defense Systems*, (Artech House, Londra: 1991), s. 231.

Bu bölümler arasından güdüm sistemi; aktif, pasif ya da yarı aktif güdüm yöntemleriyle tasarlanmış, kızılötesi (*infrared*, IR), radyo frekans (RF) ya da kullanılacağı ortama göre çeşitli detektörlerle donatılmış bir arama başlığından ve insanlı bir hava platformuna göre[19] çok daha üstün bir manevra sisteminden; füzenin hızını ve menzilini belirleyecek itki sistemi olarak roket motorundan, etki ve tahrip derecesine göre hazırlanmış patlayıcıdan oluşur.

Siber silahlarda ise hem siber hedeflere yönlendirecek güdüm sistemi hem itkiyi sağlayacak motor sistemi hem de tahrip derecesine etki edecek harp başlığının tamamı zararlı yazılımlardan oluşmaktadır. Dolayısıyla siber silahın geliştirilmesi, kullanılması ve etkisinin belirlenmesi faaliyetlerinin tamamı siber uzay şartlarında gerçekleşmektedir. Ancak siber silah saldırısının sonuçları çoğunlukla belli bir süre sonra fiziksel tahrip olarak da kendisini gösterebilmektedir. Ayrıca güçlü bir siber savunma sistemine sahip olunmadığında uzun bir süre saldırı yapıldığı bile kavranamayacaktır.

Siber Silahlar ve Tasarım Aşamaları

Siber silahların tanımlanması ya da düzenlenmesi, uluslararası boyutta sadece uluslararası hukuk araştırmacıları arasında değil bilgi teknolojisi, uluslararası siyaset ve güvenlik araştırmacıları arasında da net biçimde çözülmemiş bir konu olarak kabul edilmektedir. Başka bir ifadeyle siber silahlar teriminin çeşitli teknik, yasal, politik ve güvenlikle ilgili yönleri göz önüne alındığında evrensel olarak kabul edilmiş bir tanıma ulaşılması da pek olası değildir.[20] Bu belirsizlik terörizmin de uluslararası geçerlilikte kabul görmüş bir tanımının olmamasına benzemektedir. Ancak bu belirsizlik sadece tanımlamada kendini gösterirken siber silahlar üzerindeki çalışmalar sürmektedir. Siber silahlar hakkında farklı boyutlara odaklanan diğer bir çalışmadan[21] yararlanarak gösterim açısından yapılan bazı eklemelerle birlikte oluşturulan kavramsal gösterim Şekil 12'de sunulmuş ve süreçle ilgili değerlendirmeler aynı kaynak kapsamında özetlenmiştir.

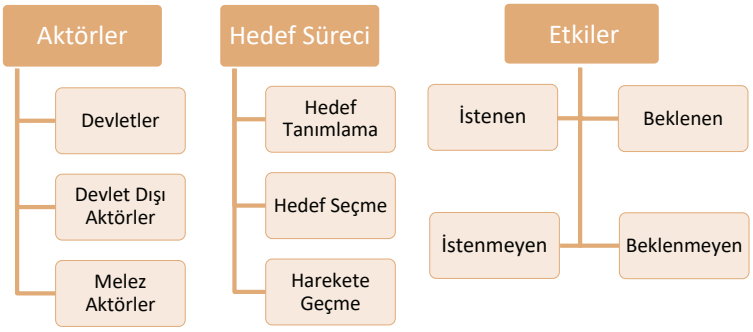
---

19 İnsanlı sistemler için bir insanın dayanabileceği maksimum G miktarının 9 olması sebebiyle manevra yeteneği sınırlanmışken güdümlü füzelerde bu miktar çok daha fazladır.

20 Ivana Kudlácková, David Wallace ve Jakub Harasta, "Cyber Weapons Review in Situations Below the Threshold of Armed Conflict", 2020 12th International Conference on Cyber Conflict (CyCon), https://ieeexplore.ieee.org/document/9131728, (Erişim tarihi: 21 Aralık 2021), s. 97-112.

21 Clara Maathuis Wolter Pieters ve Jan van den Berg, "Cyber Weapons: A Profiling Framework", 2016 International Conference on Cyber Conflict (CyCon), https://d1rkab7tlqy5f1.cloudfront.net/TBM/Over%20faculteit/Afdelingen/Engineering%20Systems%20and%20Services/People/Professors%20emeriti/Jan%20van%20den%20Berg/Research/Clara_Maathuis_Cyber_Weapons_a_Profiling_Framework.pdf, (Erişim tarihi: 4 Ocak 2022), s. 1-8.

Şekil 12. Siber Silah Kullanım Konseptinin Kavramsal Gösterimi



Burada aktörler; devletleri, devlet dışı oluşumları ve bu iki faktörün ortak olarak kullanıldığı melez (hibrit) alanları belirtmektedir. Devletler ifadesi bir yapı olarak devletleri, devletleri yöneten hükümetleri ve bu devletlere ait resmi kurumları işaret etmektedir. Bu üst düzey oluşum ekonomik, politik, teknik ve askeri imkanlara sahip olarak belirli bir süreç dahilinde stratejiler oluşturmakta, bu stratejilere uygun tasarımlar yapmakta/yaptırmakta, bu tasarımları test etmekte/ettirmekte ve gerekli olduğunu değerlendirdiği anda da kullanılabilmektedir. Ancak devlet organları gibi büyük bir yapının harekete geçmesi ve süreç kapsamında çevik davranabilmesi çoğunlukla mümkün olamamaktadır.

Devlet dışı aktörler ise devlet bileşenleri ile irtibat kurmadan, bireysel, ideolojik, ekonomik veya etik değerler sebebiyle harekete geçebilmektedir. Bilgisayar korsanları, siber profesyoneller, güvenlik araştırmacıları, özel kuruluşlar veya kurumlar şeklinde ifade edilebilen bu yapıların çoğu daha esnek ve hızlı hareket ederek siber silah geliştirme sürecini daha çabuk sonuçlandırabilmektedir. Devletler özellikle ekonomik sebepler göz önüne alındığında konvansiyonel silahlar konusunda daha tecrübeli ve üretken olurken devlet dışı aktörler daha kısıtlı ekonomik kaynaklara sahip olmalarının da etkisiyle siber silahları geliştirme konusunda daha hızlı davranabilmektedir.

Melez aktörler ise devletler ile devlet dışı aktörlerin ya da devlet dışı aktörler ile kötü niyetli birey veya organizasyonların ortak hareket ettikleri durumları temsil etmektedir. Üretilen bu siber silahlar ekonomik ya da sosyal birtakım kaygılarla devletlerin kullanımına sunulabileceği gibi bazı kötü niyetli oluşumlar tarafından siber terör, siber suç ve siber savaş saldırıları gibi alanlarda kullanılabilmektedir.

İkinci basamak ise siber uzayın içinde ya da dışında bulunan aktörün/aktörlerin belirlediği amaç/amaçlar doğrultusunda hedeflerin tanımlaması ve tanımlanan

hedefler içerisinden amaca uygun olanın/olanların seçilmesi işlemidir. Hedeflerin seçildiği ve önceliklendirildiği bu süreç kısaca "hedefleme süreci" olarak adlandırılabilir. Bu raporda değinilmese de bu süreç kapsamında hedefe yönelik kullanılacak siber silahın tasarlanması ya da temin edilmesi gerekmektedir. Harekete geçme kapsamında aktörün amacına göre tanımlanan hedefe belirlenen siber silahla saldırılmalıdır. Tüm bu süreçler gerçekleştirildikten sonra kullanılan siber silahın hedef üzerindeki etkisi incelenir. Tıpkı fiziksel saldırılarda olduğu gibi hem istenen hem de istenmeyen etkilerle karşılaşılması mümkündür. Her iki şart altında da bu etkiler beklenen ya da beklenmeyen sonuçlar üzerinden değerlendirilmektedir. Siber silah kontrollerinin olasılığının araştırıldığı bir çalışmada[22] siber silahlar üç bölümde incelenmektedir:

- Yalnızca saldırı veya zarar verme amacıyla kullanılan saldırı silahları[23]
- Yalnızca saldırı veya zarar verme amacıyla kullanılan siber saldırı silahları
- Siber saldırı silahıyla/silahlarıyla yapılan saldırılara karşı korunmak için kullanılan siber savunma silahları

Siber Silah Geliştirme Süreci

Belirtildiği gibi siber silah kavramındaki belirsizliklere rağmen bu konu hakkında belki de en detaylı çalışma Maathuis vd.[24] tarafından yapılmıştır. Bu çalışmada siber silah geliştirme süreci; tanımlama, keşif, tasarım, geliştirme, test etme, doğrulama, izinsiz giriş ve kontrol, saldırı, bakım ve sızma şeklinde belirlenmiştir.

22 Dorothy Denning, "Reflections on Cyberweapons Controls", *Computer Security Journal*, Cilt: 16, Sayı: 4, (2000), s. 43-53.

23 Bu incelemede yazar tarafından "zarar veren bir silah", varlığı caydırıcı amaçlı veya bir saldırgana karşı kullanılsa bile saldırı silahı olarak kabul edilmiştir.

24 Maathuis, Pieters ve Berg, "Cyber Weapons: A Profiling Framework", s. 1-8.

Siber Silahların Fiziksel Silah Sistemleri ve Platformlar Üzerindeki Etkileri

20. yüzyılın sonlarına doğru geliştirilmeye başlanan "elektronik savaş düzeni", "elektronik harp", "bilgi savaşı", "ağ merkezli harekat" gibi kavramlarla cephelerin sayısallaştırılması gündeme gelmiştir. Günümüzde ise modern silahlı kuvvetlerin neredeyse tüm bileşenlerinin yazılım ve donanım destekli sistemlerle donatıldığı görülmektedir. Çoğu askeri sistem, siber uzay ortamından yalıtılarak faaliyet göstermesine rağmen yakın gelecekte "askeri nesnelerin interneti" (*internet of battlefield things*, IoBT) altyapılarını oluşturma yolunda projeler geliştirilmektedir. Günümüz için somut örnek verecek gelişmelere rastlanılmamakla beraber akademik dünyada çeşitli bilimsel ortamlarda sunulan bildiriler aracılığıyla gelişmelerin hangi alanlarda gerçekleştiği üzerinde fikir edinilebilmektedir. Bu kapsamda olması planlanan ya da öngörülen ortam mevcut akıllı sensörlere ilave olarak üç boyutlu radarlar ve "lazer görüntü algılama ve ölçme" (*laser imaging detection and ranging*, LiDar) sensörlerini de içerecek şekilde askeri (dost ve tehdit) ve sivil sensör düğümlerinden oluşmaktadır. Bu ağ yapıları küçük yerleşik bilgi işlem cihazlarından güçlü uç bulutlara kadar oldukça geniş bir siber coğrafyayı kapsayacak hacimde planlanmaktadır. Donanım yönüyle gerçekleştirilen bu ortam zaman, performans/işlevsellik, güvenlik ve güvenilirlik bileşenleriyle de desteklenmek zorundadır. Bu kapsamda yan kanal yayılımlarını kullanarak sivil ve tehdit düğümlerin keşfi ve göreve özgü askeri nesnelerin internet işlevlerinin yukarıdan aşağıya hızlı sentezi için algoritmalara ve risk değerlendirmelerine ihtiyaç duymaktadır. Aynı zamanda veri kirliliği karşısında güvenli ve esnek durum tahmini ve kontrolünün sağlanması için sensör gözlemlerinin fiziksel dinamiklerin-

den yararlanmaya yönelik algoritmalarla da desteklenmesine ihtiyaç duyulduğu belirtilmektedir.[25]

Siber Savaş Prensipleri[26]

Siber savaş prensipleri; "fiziksel sınırlamaların olmaması", "fiziksel (kinetik) etkiler", "gizlilik", "değişkenlik ve tutarsızlık", "kimlik ve ayrıcalıklar", "çift kullanım", "altyapı kontrolü" ve "operasyonel ortam olarak bilgi" şeklinde sekiz alt başlıkta incelenmektedir.[27]

Fiziksel Sınırlamaların Olmaması

Fiziksel dünyada her bir platform kendisine tanımlanmış coğrafyada ve belirlenen zaman diliminde faaliyet göstermektedir. Mesafe ve uzayın fiziksel sınırlamaları siber uzayda geçerli değildir. Siber uzayda fiziksel mesafe, saldırıların gerçekleştirilmesi için ne bir engel ne de bir kolaylaştırıcıdır. Bir siber saldırı dünyanın diğer tarafından ya da yan odadan eşit etkinlikle gerçekleştirilebilir. Kinetik dünyada hedefe ulaşmanın fiziksel sınırlamaları varken siber uzayda hedefin tespiti ve ele geçirilmesinde benzer sınırlamalar bulunmamaktadır. Hatta siber saldırganlar çok fazla zaman ve/veya malzeme tüketimi olmadan bir siber silah oluşturup birden çok kopyasını çıkarabilmektedir.

Fiziksel (Kinetik) Etkiler

Siber savaşın amacı fiziksel etkiler oluşturmaktır. Bu, fiziksel hasarı ya da sadece hedef alınan aktörün karar verme sürecini etkilemeyi içerir. En güncel sorulardan biri hangi siber olayların siber savaş olarak değerlendirilmesi gerektiğidir. Fiziksel savaş genel olarak ülkelerin silahlı kuvvetlerinin kullanılması şeklinde gerçekleşmektedir. Bu durum Birleşmiş Milletler mevzuatında da net olarak belirtilmektedir. Ancak siber savaş konusunda uluslararası boyutta net bir tanımlama bulunmamaktadır. Bu konuda yapılan en önemli çalışma Cambridge Üniversitesi tarafından ya-

25 Tarek Abdelzaher, Nora Ayanian ve Tamer Basar, "Will Distributed Computing Revolutionize Peace? The Emergence of Battlefield IoT", 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), https://files.stample.co/browserUpload/01a250b2-b112-43b7-ad70-0f3ce011ea51, (Erişim tarihi: 5 Nisan 2022), s. 1129-1138.

26 Raymond C. Parks ve David P. Duggan, "Principles of Cyberwarfare", *IEEE Security & Privacy*, Cilt: 9, Sayı: 5, (Eylül-Ekim 2011), s. 30-35.

27 Parks ve Duggan, "Principles of Cyberwarfare".

yımlanan ve bilgisayar terimi olarak birinci ve ikinci sürümünün yayımlandığı *Tallinn* el kitabıdır.[28]

Siber savaş kavramı diğer bir yaklaşıma göre kritik altyapıların hedef alındığı siber saldırılar olarak değerlendirilmektedir. "Kritik altyapılar; işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları" içermektedir.[29]

Bu kapsamda ilk siber savaşın İran'ın Natanz Nükleer Tesisi'ne düzenlenen siber saldırı olduğu değerlendirilmektedir. Özetle nükleer kirlenmeye sebep olabilecek bir fiziksel saldırı yerine siber saldırı ile bu tesisin merkezinde yer alan reaktörün devre dışı bırakılması amaçlanmıştır. Bunu yapabilmek için de reaktörün önemli bir bileşeni olan santrifüj sistemlerinin hızlandırılarak/yavaşlatılarak istikrarsızlaştırılması hedeflenmiştir. Bu hedefe ulaşmak için de anılan sistemleri kontrol eden SCADA[30] sistemlerine yönelik siber saldırı yapılması gündeme gelmiştir. Bu kapsamda oluşturulan zararlı yazılımın İran'a gönderilmesi, tesis bilgi sistemlerine transferi, kullanılan mikro kontrolörlere üretim aşamasında (üretici firmanın haberi olmadan) yüklenmesi ve saldırı günü bu zararlı yazılımın aktifleştirilmesi şeklinde gerçekleştirilmiştir. Bu saldırının ortaya çıkması ise diğer mikro kontrolörleri alan ülkelerin tesislerinde de bu zararlı yazılımların aktifleşerek benzer hasarın oluşması sonucu bu zararın kök nedenlerinin araştırılmasıyla gerçekleştirilmiştir.[31] Bu saldırı "Stuxnet" adıyla siber savaş tarihini başlatmıştır.

Gizlilik

Siber uzayda saklanmak için aktif adımlar atılabilir ancak yapılan her şey görünür durumdadır. Tamamen gizlenmiş olmak diye bir kavram yoktur. Sadece daha az tespit edilebilir izler yani mevcut veri akışlarındaki aykırılıkları saklamaya çalışmak vardır. Bu nedenle siber uzayda fiziksel dünyadaki radar enerjisini daha az yansıtmaya veya kızılötesi işaretleri soğutarak gizlemeye benzer adımlar atılamaz. Bunun yerine mevcut veri akışlarındaki kanıtlar saklanmaya çalışılır.

---

28 Michael N. Schmitt, "Introduction", *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (Cambridge University Press, Cambridge: 2017).

29 "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, (Ocak 2013), https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a-3412cf8f45a.pdf, (Erişim tarihi: 8 Nisan 2022).

30 Supervisory control and data acquisition (SCADA), merkezi denetim ve veri toplama sistemi olarak tanımlanabilir. Bu sistemler geniş bir alana yayılmış ve pek çok kontrol biriminden oluşan sistemlerin tek merkezden bilgi sistemleri tarafından kontrol edilip izlendiği bir elektronik mikro kontrolördür.

31 Daniel P. Hughes, "Archer's Stakes in Cyber Space: Methods to Analyze Force Advantage", *Cyber Weaponry Issues and Implications of Digital Arms*, ed. Henry Prunckun, (Springer, Berlin: 2018), s. 71-85.

Değişkenlik ve Tutarsızlık

Siber savaşta tutarsızlık her zaman aynı şekilde davranmayan saldırılara, saldırıyı değiştiren ortamlara ve saldırı performansındaki dalgalanmalara dönüşebilir. Siber uzayın değişmeyen tarafı fiziksel dünyada değişiklik gerektirenlerdir. Örneğin fiziksel dünyadaki bir kişi daha hızlı bir işlemciyi kullanmadıkça, yazılım performansı bir bilgisayarın işlem gücü kapasitesini aşamayacaktır. İletişim bant genişliği de haberleşme altyapısı ile sınırlı kalacaktır.

Bu ilkenin bir etkisi, bir saldırıdaki belirli bir adımın işe yarayacağından asla emin olunamamasıdır. İlk tehdit erişiminden hedefe ulaşma noktasına kadar bir sistemin durumundaki değişikliği gösteren veri yolları kullanılarak saldırılar planlanır. Bu süreçteki her yol bir saldırı senaryosu seti veya belirli bir saldırganın ulaşabileceği saldırı senaryoları setidir.

Kimlik ve Ayrıcalıklar

Siber uzaydaki bazı kişiler bir saldırganın gerçekleştirmek istediği herhangi bir eylemi gerçekleştirme yetkisi, erişimi veya yeteneğine sahip olabilir. Saldırganın amacı kendi kimliğini gizleyebilmek için o kişinin kimliğini ele geçirmeye çalışmaktır.

Çift Kullanım

Siber savaş araçları –tıpkı fiziksel savaş araçları gibi– çift kullanımlıdır. Güncel teknolojiyi kullanan savaş uçakları (örneğin F-16'lar) hem yer hedeflerine taarruz hem de havadan gelen rakip hava araçlarına karşı savunma amaçlı olarak kullanılabilmektedir. Bu kullanım tipini belirleyen en önemli unsur kullanılan mühimmattır. Siber savaştaysa saldırı ve savunmada hem donanım hem de yazılım olarak aynı araçlar kullanılır. Örneğin saldırı yapılırken güvenlik açığı tarayıcıları kullanılırken savunma yapılırken de benzer tarayıcılar kendi sistemlerindeki zayıflıkların bulunup onarılması için kullanılmaktadır. Benzer şekilde ağ yöneticilerinin, ağ sorunlarını teşhis etmek için kullandıkları ekipman saldırganlar tarafından da keşif için kullanılmaktadır.

Altyapı Kontrolü

Hem savunucular hem de saldırganlar kullandıkları siber uzayın çok küçük bir bölümünü kontrol ederler. Rakibin kullandığı siber uzayın bir bölümünü kim kontrol altına alabilirse rakibini kontrol edebilir. Bu sebeple sızma testleri benzeri

metotlar kendi ağlarına önceden saldırı benzetimi yaparak tehdide açıklık derecesinin tespit edilmesine dayanmaktadır.

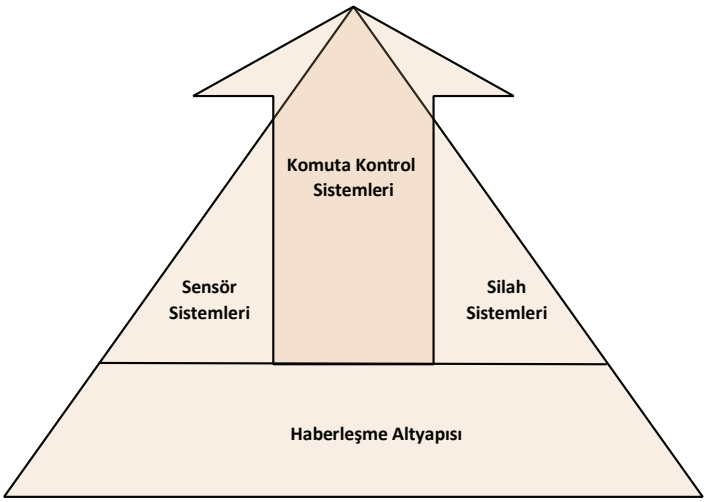
Operasyonel Ortam Olarak Bilgi

Fiziksel savaşlarda arazi şartları, hava durumu ve tehdit birliklerinin pozisyonu gibi unsurların hepsi operasyonel ortamı etkilerken siber uzay ortamında bu süreç mevcut ağlara bağlı olarak çalışan bilgi sistemleri, kablolu/kablosuz/optik altyapılar ile bu altyapılara erişimi sağlayan her tür teknik bileşenden oluşmaktadır. Dolayısıyla hem fiziksel hem de siber savaş ortamında bilgi en önemli güç çarpanı olarak değerlendirilmektedir.

Siber Harekat Sahasına Bütüncül Bakış

Fiziksel silahlı kuvvetlerin kuruluşunda bulunması gereken en önemli bileşenler; personel, istihbarat, lojistik ve harekat gibi alanlardır. Bu alanların hepsi güçlü bir komuta, kontrol, muhabere, bilgisayar, istihbarat, gözetleme ve keşif (*command, control, computing, communications, intelligence, reconnaissance, surveillance*, C4ISR) yapısıyla birlikte önemli bir askeri güç unsurunu oluşturmaktadır. Siber savaş söz konusu olduğunda ise benzer yapılanma siber uzay ortamını kullanırken Şekil 13'te özetlenerek gösterilen yapı önem kazanmaktadır.[32]

Şekil 13. Siber Harekat Sahasına Bütüncül Bakış



32 Nuri Mutlu, "Komuta Kontrole Bütüncül Bakış", *Aselsan Dergi*, Sayı: 109, (Haziran 2021), s. 21.

Burada sensör sistemleri ile kinetik ve siber silah sistemleri ön plana çıkarken kesintisiz ve güvenli bir haberleşme ağı devreye girmektedir.

Siber Komuta ve Kontrol Sistemleri

Siber komuta ve kontrol sistemleri; verilen görevin başarılması için planlayan kişi/kişilerle yönlendirme, koordine ve kontrol etme gibi faaliyetlerin, personelin, teçhizatın, ağ altyapılarının ve güvenlik yazılımlarının çeşitli yöntem ve teknolojilerle düzenli bir şekilde kontrol edilmesi ya da kullanılması sürecidir.

Bu sürecin etkin yönetilebilmesi için tespit edilen verinin zararlı olup olmadığının belirlenerek tehdit analizinin yapılması gerekmektedir. Tehdit olduğu hakkında kesinlik ya da yoğun şüphe varsa tehdit derecelendirilmesine göre uygulanacak tedbirin belirlenmesi elzemdir.

Bu kapsamda tehdit olan ya da olabilecek unsurlar; insan kaynaklı tehditler, zararlı yazılım içeren web sayfaları/uygulamaları, web sayfalarının zararlı propaganda amaçlı kullanılması, bilgi sistemlerinin ele geçirilmesi/işlevsiz bırakılması/zombi (*botnet*) bilgi sistemi haline getirilmesi, akıllı ağ yapılarında bulunan sensörlerin ele geçirilerek oluşturulan sahte verilerin güvenli sistemlere iletilmesi, kritik altyapı tesislerine ve eş zamanlı olarak farklı hedeflere saldırılar düzenlenmesi olarak sayılabilir.

Sensör Sistemleri

Çeşitli kaynaklar tarafından üretilen ses, ışık, basınç, elektromanyetik saçılım ve frekans gibi işaretler; özel cihazlar tarafından tanımlandıktan sonra yine bu cihazlar tarafından elektrik işaretlerine dönüştürülerek bir bilgi sistemine ya da diğer akıllı ağ sistemlerine aktarılır. Bu tanımlama ve dönüşüm işlemini yapan cihazlara akıllı sensörler denir.

Şekil 14. Akıllı Sensörlerin Çalışma Prensibi

Şekil 14'te[33] çalışma prensibi modellenen akıllı sensörler bulundukları çevrede bulunan ve tanımlayabildikleri işaretleri algılama elemanı ile tespit ederek elektrik işaretine dönüştürürler. Sonra işlem yapılacak formata işaret koşullandırma katında dönüştürülen işaret doğrudan mikroişlemciye aktarılır. Mikroişlemci tarafından kullanıma hazır hale getirilen işaret ya değerlendirme merkezine ya da diğer akıllı ağ düğümlerine aktarılır. Akıllı sensörlerin en önemli özellikleri küçük boyutları, enerji ihtiyaçlarının düşük olması, yüksek hassasiyetleri, hızlı veri işleyebilmeleri ve etkin kullanılmalarıdır. Bu sürecin etkili bir şekilde oluşturulması çok çeşitli kaynaklardan elde edilen verilerin etkin bir şekilde yönetilmesi ve merkezi sunucuya kesintisiz aktarılmasına bağlıdır.

Daha çok nesnelerin interneti tabanlı oluşturulan "siber fiziksel ortamlar"[34] sivil ortamlarda olduğu gibi askeri harekat ortamlarında da kullanılmakta ve askeri nesnelerin interneti olarak adlandırılmaktadır. Ancak bu alan 21. yüzyılın başlarından itibaren askeri literatürde "ağ merkezli harekat" ya da "ağ merkezli savaş" olarak adlandırılmaktadır.

Silah Sistemleri

Silah sistemleri incelendiğinde kuvvet komutanlığı farkı gözetmeksizin pek çok silah sistemi ve platformun yazılım destekli ve gömülü sistem tabanlı olduğu görülmektedir. Bu kapsamda en ileri teknolojiye sahip olacak silah sistemi/platformu –geliştirilme çalışmaları büyük bir gizlilik içinde devam eden– altıncı nesil savaş uçaklarıdır. Açıklanan projeler ışığında bir öngörü çalışması yapan STM Thinktech[35] kullanılabilecek olası teknolojiler hakkında bir bilgi görseli hazırlamıştır. Bu görselde yer alan teknolojiler şu şekilde özetlenmektedir:

- Yapay zeka (YZ): insansız hava aracı (İHA) sürüleriyle eş güdüm
- Kara, hava, deniz ve uzay platformlarıyla müttefiklerle güçlü sensör bağlantısı
- Daha büyük uçak gövdesi ve daha verimli motorlar

33 Billie F. Spencer, Manuel Euripides Ruiz Sandoval ve Narito Kurata, "Smart Sensing Technology: Opportunities and Challenges", *Structural Control and Health Monitoring*, Cilt: 11, Sayı: 4, (2004), s. 349-368.

34 Amerika Birleşik Devletleri Ulusal Bilim Kurulu (The National Science Foundation, NSF) "siber fiziksel sistemleri" hesaplama ve fiziksel bileşenlerin sorunsuz etkileşimiyle oluşturulan ve buna bağlı olarak tasarlanmış sistemler olarak tarif etmektedir.

35 "Altıncı Nesil Savaş Uçaklarının Öngörülen Özellikleri", STM Thinktech, 10 Kasım 2020, https://thinktech.stm.com.tr/tr/altinci-nesil-savas-ucaklarinin-ongorulen-ozellikleri, (Erişim tarihi: 4 Ocak 2022).

- Sensör bilgileri ve görüntülerini birleştirerek kullanabilen pilot kaskları
- Tam anlamıyla ağ merkezli harekat
- Siber savaş ve siber güvenlik kabiliyetleri
- Yönlendirilmiş enerji silahlarını kullanabilme
- Elektronik karıştırma, elektronik harp sistemleri ve kızılötesi karartma ile artırılmış görünmezlik
- Opsiyonel olarak pilotlu hava platformları

Altıncı nesil savaş uçaklarının da –tıpkı beşinci nesil savaş uçaklarında olduğu gibi– sabit donanım üzerine yerleştirilen yazılımlar aracılığıyla harekat fonksiyonelliği kazanacağı düşünülmektedir. Bu kapsamda tüm sistemler siber savaş bileşeni haline gelmektedir. Ancak akıllı sensörler sayesinde harekat sahasının neredeyse sınırsız olması bu platformların adeta bir komuta kontrol merkezi gibi faaliyet göstermesine de sebep olabilecektir. Buna binaen özellikle ağ merkezli harekat/savaş ve elektronik harp bu süreçte kilit rol oynamaktadır.

Ağ Merkezli Harekat/Savaş

"Ağ merkezli savaş kavramı, geniş bir şekilde ağ bağlantılı bir gücün belirleyici bir savaş avantajı oluşturmak için kullanabileceği yeni ortaya çıkan taktik, teknik ve prosedürlerin kombinasyonunu" tanımlamaktadır.[36] Harekat ortamını kara, deniz, hava ve uzay boyutlarıyla modellemekte ve bu boyutları kullanan platformları (kullandıkları teçhizatla birlikte) bir arada kullanmaktadır. Bu konsept öncesinde üç boyutlu olarak gösterilen "elektronik harekat sahası" (*electronic order of battle*, EOB) kavramını geliştirerek anlık görüntüleme ve operasyon imkanlarını geliştirmektedir.

Elektronik Harp

Elektromanyetik tayfı;[37] izlemek, bilgi toplamak, kontrol etmek ya da düşmana saldırmak ve gerektiğinde elektromanyetik tayfın kullanımını engelle-

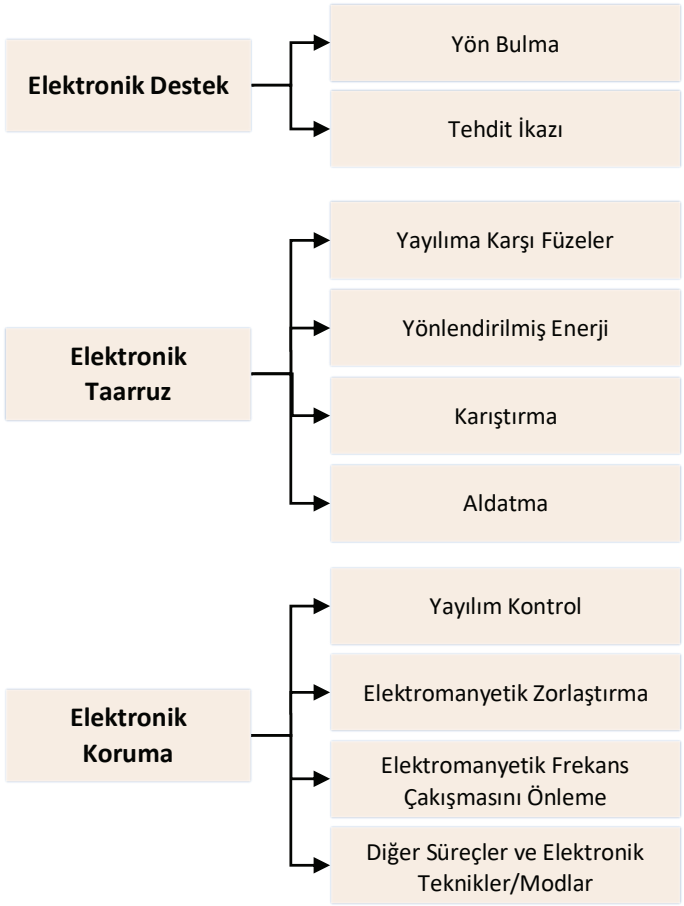
36 John J. Garstka, "Network-Centric Warfare Offers Warfighting Advantage", Signal, 1 Mayıs 2003, https://www.afcea.org/content/network-centric-warfare-offers-warfighting-advantage/#:~:text=Data-links%20are%20the%20new%20weapon,create%20a%20decisive%20warfighting%20advantage, (Erişim tarihi: 16 Aralık 2021).

37 Tayf (spektrum): Elektromanyetik dalgaların sahip oldukları frekans ve dalga boylarına göre sınıflandırılmasıdır.

mek için elektromanyetik sistemler ve yönlendirilmiş enerjinin askeri amaçlar için kullanımıdır.[38]

Elektronik harp; elektronik destek, elektronik taarruz ve elektronik koruma olmak üzere üç ana bölümden oluşur. Bu bölümlerin temel alt bileşenleri Şekil 15'te gösterilmektedir.[39]

Şekil 15. Elektronik Harbin Bölümleri



38 D. Curtis Schleher, *Electronic Warfare in the Information Age*, (Artech House, Londra: 1999), s. 2; David B. Hoisington, *Electronic Warfare Volume I*, (Lynx Publishing, Auburn: 1994), s. 1a-1, 1a-16, 1a-17.

39 Hoisington, *Electronic Warfare Volume I*.

Elektronik Destek: Acil tehdit belirlemesi için yapılan ve bilinçli/bilinçsiz elektromanyetik enerji yayın kaynaklarının aranması, tespit edilmesi ve tanımlanması etkinliklerini içeren elektronik harp bölümüdür. Yön bulma ve tehdit ikazı alt bileşenlerinden oluşur.

Elektronik Taarruz: Tehdit elektromanyetik sistemlerin muharebe yeteneklerinin azaltılması, etkisiz kılınması veya ortadan kaldırılması için elektromanyetik sistemler ya da yönlendirilmiş enerji silahları ile taarruz edilmesini kapsayan elektronik harp dalıdır. Yayılıma karşı füzeler, yönlendirilmiş enerji, karıştırma ve aldatma alt bileşenlerinden oluşur.

Elektronik Koruma: Uygulanmakta olan dost ya da düşman elektronik harp etkinliklerinin, dost muharebe yeteneğini azaltan, etkisiz kılan ya da yok eden etkilerinden, personel, tesis ve donanımların korunması faaliyetlerini kapsayan elektronik harp bölümüdür. Bu bölüm yayılım kontrol, elektromanyetik zorlaştırma, elektromanyetik frekans çakışmasını önleme ve diğer süreçler/tedbirler alt bileşenlerinden oluşmaktadır.

Siber Savunma Sisteminin Oluşturulması

Kişinin birey olarak kendini savunmak, saldırıları anlamak, tespit etmek ve savunma yöntemi hakkında karar vermek için bilgiye ve çeşitli bilgi erişim ya da bilgi üretim araçlarına ihtiyacı vardır. Kısaca belirtmek gerekirse savunma, saldırılara karşı sistemi koruma eylemidir. Bu nedenle siber savunma, yürütülmekte olan kritik işlemleri saldırılara karşı güvenli hale getiren aktif bir süreci ifade etmektedir.

Siber savunma siber altyapının korunmasına yönelik olsa da gerektiğinde karşı siber saldırı yapılmasına yönelik strateji geliştirilmesinde de etkin bir rol oynamaktadır. Bu kapsamda öncelikle siber varlıkları kullanan/yöneten insanların bireysel farkındalığı kadar uzmanların da görev ve diğer faaliyetlere yönelik sonuçları yorumlayarak ve algılanan tehdit verilerini kullanarak süreci karar destek sistemi girdisi haline getirmeleri bir dönüşüme uğrayacaktır. Elbette bu sürece yönelik kullanılacak verilerin tespitinde sensörlerin kullanılması büyük önem taşımaktadır. Bu sensörler aracılığıyla saldırının kapasitesi ve stratejisi gibi unsurlar dinamik bir şekilde gerçekleşebilecektir. Durumsal farkındalık süreciyle oluşturulan verilere dayanarak savunma sisteminin aktif hale getirilmesi gerekmektedir. Bu gereklilik kısaca siber komuta ve kontrol olarak ifade edilebilir. Bu kapsamda komuta, karar verme kapsamında duruma bağlı olarak seçeneklerin anlaşılması ve bunların hızlı bir şekilde değerlendirilmesinin yollarını araştırırken kontrol ise kararların iletilmesi ve bunların sistem genelinde güvenilir bir şekilde uygulanması için kurulu bir sistem olarak karşımıza çıkmaktadır.[40]

40 O. Sami Saydjari, "Cyber Defense: Art to Science", *Communication of the ACM*, Cilt: 47, Sayı: 3, (Mart 2004), s. 52-57.

Buraya kadar belirtilen hususlar siber savunmanın kapsamlı bir görünümü olup bu katmanlara ek bir faktör olarak "siber istihbarat"ın eklenmesi gerektiği de belirtilmektedir.[41] Bu sayede geçmiş saldırılardan öğrenilen derslerin belirtilen süreçlere dahil edilmesiyle siber savunma faaliyeti güçlendirilebilir.

41 Michael Robinson, Kevin Jones ve Helge Janicke, "Cyber Warfare: Issues and Challenges", *Computers & Security*, Sayı: 49, (2015), s. 70-94.

Türkiye'de ve Dünyada Siber Güvenlik Faaliyetleri

Siber güvenlik faaliyetlerinin geldiği boyut değerlendirildiğinde hem bireylerin güvenliğinin etkinleştirilmesi hem de ülkelerin milli güvenlikleriyle doğrudan alakalı olarak geliştiği görülmektedir. Hatta bireysel faktörlerde yapılacak basit hataların doğrudan ülke güvenliğine etki edebildiğine de şahit olunabilmektedir. Bu sebeple yüksek seviyeli önlemlerin geliştirilmesi gerekmektedir.

Bu kapsamda 20 Ekim 2012'deki 28447 sayılı *Resmi Gazete*'de "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu ile ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarının hazırlanması ve koordinasyon görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığının (Ulaştırma ve Altyapı Bakanlığı) sorumluluğuna verilirken aynı kanunla Türkiye'de "Siber Güvenlik Kurulu" da teşkil edilmiştir.

Siber güvenlik alanında teknoloji üreten ve dünya ile rekabet edebilen Türkiye'nin ana hedefleri doğrultusunda T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı öncülüğünde ve ilgili tüm kamu kurum/kuruluşları, özel sektör ve akademi temsilcilerinin katkılarıyla temelleri atılan ve siber güvenlik ekosisteminin geliştirilmesini amaçlayan Türkiye Siber Güvenlik Kümelenmesi adlı bir platform kurulmuştur. Platformun faaliyetleri Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığının da desteği ve koordinasyonu ile yürütülmektedir.[42]

Türkiye'nin 2023 vizyonu çerçevesinde belirlenen ulusal siber güvenlik hedefleri ise şöyle aktarılmaktadır:[43]

---

42 "Türkiye Siber Güvenlik Kümelenmesi", Siber Küme, https://www.siberkume.org.tr/Index, (Erişim tarihi: 11 Nisan 2022).

43 Arife Yıldız Ünal, "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı Siber Güvenlikte 2023 Vizyonunu Gerçeğe Dönüştürecek", Anadolu Ajansı, 29 Aralık 2020.

- Kritik altyapıların siber güvenliğinin 7/24 korunması. Ulusal seviyede siber güvenlik alanında en son teknolojik imkanlara sahip olunması; operasyonel ihtiyaçlar çerçevesinde yerli ve milli teknolojik imkanların geliştirilmesi

- Siber olaylara müdahalenin olay öncesini, esnasını ve sonrasını kapsayan bir bütün olmasından hareketle proaktif siber savunma anlayışının geliştirilmeye devam edilmesi; siber olaylara müdahale ekiplerinin yetkinlik seviyelerinin ölçülmesi ve izlenmesi; siber olaylara müdahale ekiplerinin yetkinliklerinin artırılması

- Kurumsal, sektörel ve ulusal bazda siber olaylara hazırlık seviyelerinin risk temelli analizler ve planlamalara dayalı yaklaşımlarla artırılması; kurum ve kuruluşlar arası veri paylaşımının güvenli biçimde sağlanması

- Kaynağı ve hedefi yurt içi olan veri trafiğinin yurt içinde kalması; kritik altyapı sektörlerinde düzenleme ve denetlemeye dayalı siber güvenlik yaklaşımının geliştirilmesi

- Kritik altyapı sektörlerinde, bilişim teknoloji ürünlerinde üretici bağımlılığının önüne geçilmesi; yeni nesil teknolojilerin güvenliğinin sağlanmasına yönelik gereksinimlerin belirlenmesi; yenilikçi fikirlerin ve Ar-Ge faaliyetlerinin desteklenerek yerli ve milli ürün ve hizmetlere dönüşümünün gerçekleştirilmesi

- Toplumun tüm kesimleri tarafından siber uzayın güvenle kullanılması; siber güvenlik farkındalığının tüm toplumda üst seviyede tutulmasına yönelik etkinliklerin sürdürülmesi

- Kurum ve kuruluşlarda kurumsal bilgi güvenliği kültürünün yerleşmesi; çocukların siber ortamda korunmasının sağlanması; siber güvenliğe ilgi duyan veya uzmanlaşmak isteyen bireylere yönelik projelerle insan kaynağının güçlendirilmesi

- Örgün ve yaygın eğitimde siber güvenlik eğitiminin yaygınlaştırılması ve eğitim içeriklerinin zenginleştirilmesi; ulusal ve uluslararası düzeydeki paydaşlarla bilgi paylaşımı ve iş birliğini sağlayacak mekanizmaların geliştirilmesi

- Siber suçların en aza indirgenmesi ve caydırıcılığın artırılması; internet ve sosyal medyada doğru ve güncel bilgi paylaşımının sağlanmasına yönelik mekanizmaların geliştirilmesi

Türkiye'de olduğu gibi teknolojiyi etkin olarak kullanan diğer ülkelerde de siber güvenlik stratejileri geliştirilmektedir. Bu kapsamda Amerika Birleşik Devletleri (ABD), Rusya, Çin, İngiltere, İsrail ve İran tarafından belirlenen politika ve stratejiler aşağıda aktarılmıştır:[44]

ABD

- Kritik altyapıların korunması için Amerikan kamu ve özel sektörünün birlikte hareket etmesi

- Siber uzay alanından gelebilecek saldırılara karşı kamu ve özel sektörün birlikte hareket etmesinin yanı sıra bu ortak hareket kabiliyetinin geliştirilmesi konusunda taktik ve planların ortaya konulması; özel sektörün siber uzay alanındaki görevlerini yerine getirme konusunda teşvik edilerek desteklenmesi ve tüm bu amaçlar kapsamında federal bir sistemin geliştirilmesi

- ABD işçi ve işveren kesimleri ile tüm toplumun siber saldırılar karşısındaki farkındalığının artırılması; bu konudaki eğitim ve oryantasyon faaliyetlerine federal düzeyde önem verilmesi

- Rusya'nın artan siber gücü ve siber meydan okumalarının ABD'nin güvenliği açısından ciddi tehdit oluşturması nedeniyle bu tehditlerin ortadan kaldırılması doğrultusunda planlar geliştirilmesi

- Çin'in özellikle siber casusluk faaliyetleri alanında tehdit oluşturması nedeniyle ABD'nin teknolojik yeniliklerini ve özel sektörünün ticari çıkarlarını korumak için gerekli tedbirleri alması

- Tarım ve gıda sektörlerindeki; içme suyu ve kamu sağlığı ve acil müdahale sistemlerindeki; sosyal güvenlik, bilgi ve telekomünikasyon altyapılarındaki; enerji, ulaşım, bankacılık ve finans ve kimya sektörlerindeki; posta ve gemicilik sistemlerindeki tüm resmi bilgisayar, yazılım ve ağ teknolojilerinin ulusal kritik altyapılar olarak tanımlanarak siber saldırılara karşı korunması

- Siber uzayın küresel düzeyde ortak kullanım alanı olduğu; bu alanın mal ve hizmetlerin, fikirlerin, girişimcilerin ve sermayenin serbest dolaşımı-

44 Ali Burak Darıcılı, "Devletlerin Güncel Siber Güvenlik Stratejileri", Anadolu Ajansı, 2 Aralık 2020.

nın sağlanması için güvenli ve özgür olması gerektiği; bu kapsamda da ABD'nin söz konusu serbestlik imkanlarını sağlamak için her türlü tedbiri alması; bu kapsamda "internetin parçalanması"na (*fragmentation of internet*) yönelik Rusya ve Çin kaynaklı teknik ve idari tedbirlerle küresel düzeyde mücadele edilmesi

- ABD'nin müttefik ülkelerin istikrarını bozmayı hedefleyen siber saldırılara karşı bu ülkelere tam destek vermesi

Rusya

Gerasimov Doktrini ile ortaya konulan prensipler dahilinde Rusya, askeri niteliğe sahip olmayan yöntemleri askeri kapasitesine dahil ederek daha az konvansiyonel güçle –dolayısıyla daha az insan kaybı ve maliyetle– sıcak çatışma süreçlerini yönlendirmeyi ve yönetmeyi amaçlamıştır. Bu bağlamda askeri bir müdahale öncesinde hedef bölge, ülke, topluluk ya da devlete yönelik siber saldırılarla avantaj sağlanması, hedefin yıpratılması, psikolojik savaş yöntemleriyle baskı altına alınması, moralinin bozulması, savunma direncinin kırılması ve kritik altyapılarına zarar verilerek ekonomisinin zarara uğratılması varılmak istenen hedefler arasındadır.

Çin

- Ekonomik büyüme ve istikrarın sağlanabilmesi için önemli etkiye sahip yeni nesil teknolojilerin siber espiyonaj operasyonları kapsamında temin edilmesi
- Çin Komünist Partisi'nin ülke yönetimindeki etkinliğinin sürdürülmesi için internetin denetlenmesi ve böylelikle yerel muhalif hareketlerin, ayrılıkçı odakların ve olası toplumsal kalkışmaların kontrol edilmesi
- Ağ teknolojileri merkezli hasım enformasyon savaşı planlarına karşı tedbirlerin geliştirilmesi
- Ülkenin iç işlerine müdahaleye yönelik faaliyetlere karşı konulması
- Yabancı istihbarat servislerinin Çin aleyhine planladığı siber espiyonaj faaliyetlerine karşı etkili bir kontrespiyonaj yapısının tesis edilmesi
- Siber uzay alanı kaynaklı yeni nesil teknolojilerin verdiği imkanlar dahilinde askeri kapasitenin desteklenmesi ve aynı zamanda potansiyel hasım askeri güçlerin kritik altyapılarına karşı planların hazırlanması

- Hedef bölge ve yönetimlere karşı ağ teknolojileri merkezli enformasyon savaşı stratejileri ve siber saldırı faaliyetlerinin organize edilebilmesi

İngiltere

Savunma: İngiliz hükümetleri ulusal bilişim altyapısının savunmasını güçlendirmeyi ve İngiltere'nin kritik verilerini ve sistemlerini hedef alan siber tehditlere karşı korunmayı sağlamalıdır. Bu hedefe ulaşılması konusunda ise kamu ve özel sektör birlikte hareket etmelidir.

Caydırıcılık: İngiltere siber tehditlere karşı mevcut aktif ve pasif mukavemet unsurlarını güçlendirerek etkin bir caydırıcılık algısı oluşturmalıdır.

Kalkınma: İngiliz hükümetleri siber tehditlere karşı İngiltere'nin siber kapasitesini geliştirmelidir. Bu kapsamda ülkenin büyüyen siber güvenlik endüstrisinin kalkınmasına destek verilmelidir.

İsrail

İsrail söz konusu stratejik planlarıyla küresel siber güvenlik ekonomisinde dikkat çeken bir ülkedir. Ülkedeki kamu otoritesi, siber güvenlik alanında özel sektörü ülkenin güvenliği ve ticari menfaatleri doğrultusunda somut ekonomik programlarla teşvik etmektedir. Bu teşvikle uyumlu bir şekilde ülkenin çeşitli üniversiteleri ve araştırma merkezleri siber güvenlik alanında Ar-Ge çalışmalarına ağırlık vererek bu alanda yeni ürünler ortaya koymaktadır.

Bu kapsamda Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) verilerine göre İsrail bilimsel Ar-Ge harcamalarına gayrisafi milli hasılanın yüzde 4'ü civarında (10 milyar avro) bir pay ayırarak bu konuda dünyanın önde gelen devletlerinden biri konumuna ulaşmıştır. Dahası İsrail'in bilgi, komünikasyon ve teknoloji sektörü hızla büyümektedir. Ülkenin 2014'te küresel siber güvenlik sektöründeki payı yüzde 8 büyüyerek 6 milyar dolara ulaşmıştır. Öte yandan 2016 için İsrail'de siber güvenlik endüstrisinde 350'den fazla irili ufaklı firmanın ticari faaliyet yürüttüğü bilinmektedir. Bahse konu sayı 2017'de hızla artarak 420 aktif firmaya ulaşmıştır. Söz konusu siber güvenlik firmalarının 26'sı 2017'de dünyanın en aktif ve hızla büyüyen ilk 500 siber güvenlik şirketi arasında yer almıştır.

İran

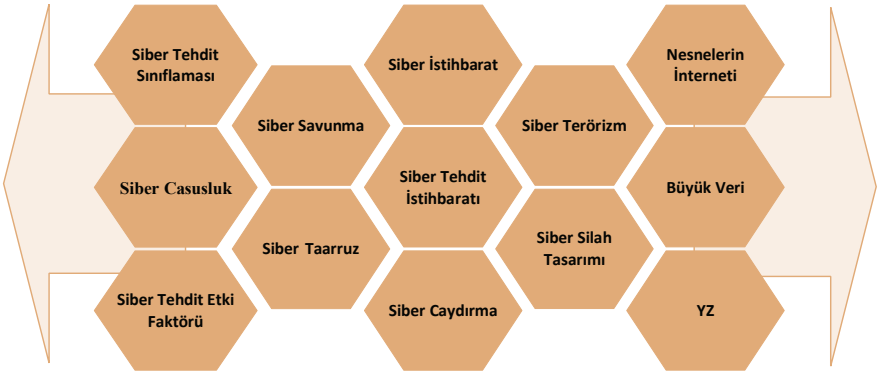
İran, nükleer tesislerini hedef alan Stuxnet saldırısı sonrasında bir misilleme refleksiyle siber güvenlik çalışmalarına hız kazandırmıştır. İlk etapta misilleme motivasyonuyla hızlanan İran'ın siber saldırı kapasitesini geliştirmeye yönelik gayretleri ilerleyen dönemlerde alınan tedbirlerle ülkeyi siber uzayda etkili bir aktör haline getirme hedefine dönüşmüştür. Bu kapsamda Tahran yönetimi güçlü bir siber saldırı kapasitesine sahip olmayı ulusal amaç edinmiştir. Söz konusu hedefin arka planında ise küresel bir güç olmayan İran'ın Ortadoğu'da ABD, Suudi Arabistan ve İsrail'e karşı verdiği güç mücadelesinde siber uzayın sağladığı asimetrik avantajlardan yararlanmak istemesi yatmaktadır.

İran'ın siber saldırı kapasitesinde siber politikaların belirlenmesinde çatı organizasyon olan Siber Güvenlik Yüksek Konseyi, Devrim Muhafızları, İran İstihbarat Bakanlığı, Siber Komutanlık ve bu kurumlarla irtibatlı vekil (*proxy*) bir yapılanma olan İran Siber Ordusunun önemli rolü bulunmaktadır. İran'ın siber saldırı hedeflerinin ülkenin geleneksel iç ve dış savunma öncelikleriyle uyumlu bir şekilde belirlendiği görülmektedir.

Genel Değerlendirme

Siber güvenlik kavramı –günümüz teknolojisinin geldiği boyut da dikkate alındığında– vazgeçilemeyecek bir alan olarak kendini göstermektedir. Bu kavram sadece kişileri değil sektörleri, kuruluşları, kurumları ve elbette devletleri yakından ilgilendiren bir alan olarak değerlendirilmektedir. Sadece iki kelimeden (siber ve güvenlik kelimelerinden) oluştuğu görülse de bu, buz dağının sadece görünen yüzüdür. "Siber güvenliği oluşturan bileşenler nelerdir?" diye sorulduğunda ilk başta ne kadar derinlikli bir konudan bahsedildiği fark edilmeyebilir. Ancak Şekil 16'daki seçkide de görüldüğü gibi siber güvenlik çok çeşitli bileşenlerden oluşmaktadır.[45]

Şekil 16. Siber Güvenlik Bileşenlerinden Seçmeler



Şekil 16'da yer alan siber güvenlik bileşenlerinden yapılan seçki incelendiğinde bu bileşenlerin hem sivil hem de askeri anlamda kullanılabilir bileşenler olduğu-

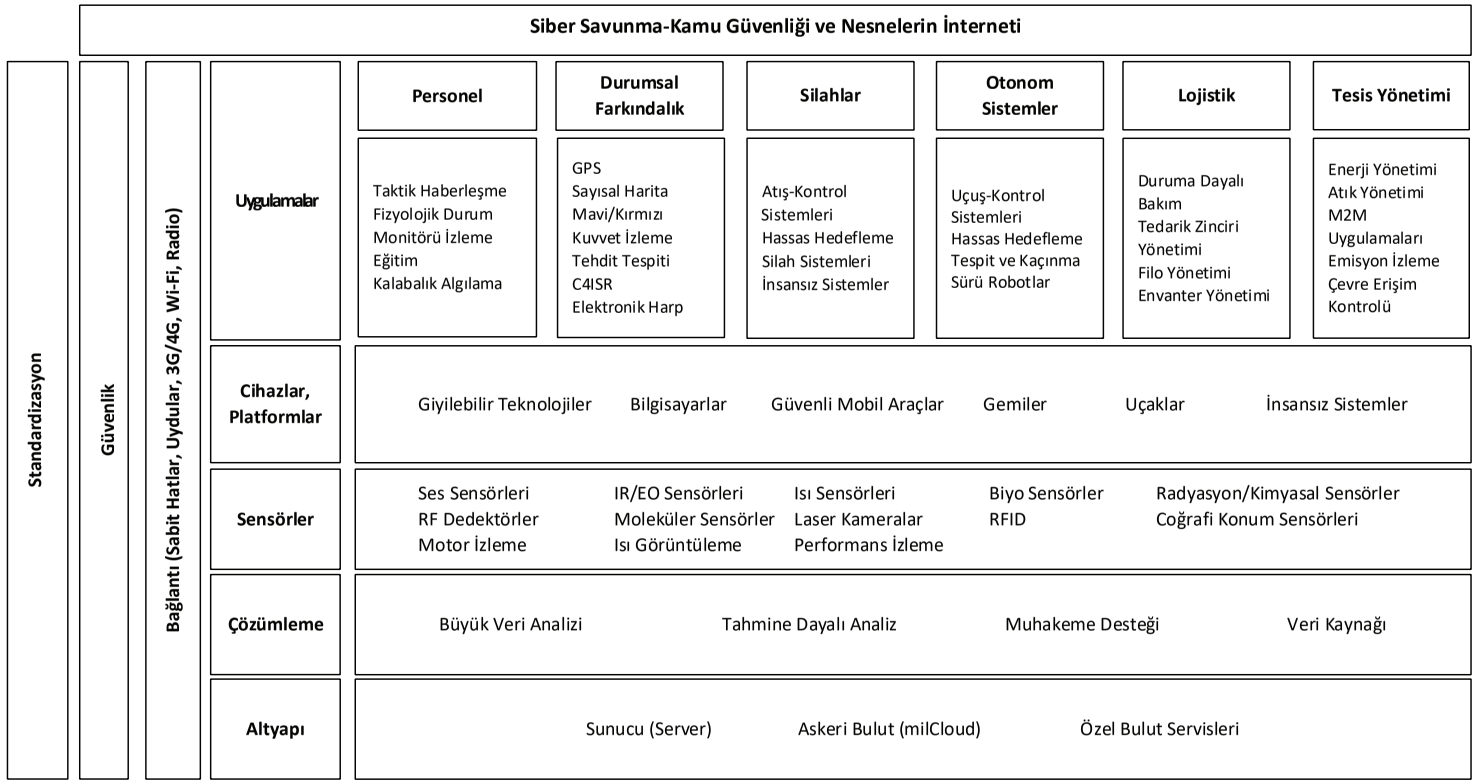
45 Bu gösterimde yatay yöndeki oklarla alanın daha geniş bileşenlerden oluştuğu ve şeklin sadece bu rapor kapsamındaki konularla sınırlandırıldığı ifade edilmeye çalışılmıştır.

nu görmek mümkündür. Buna binaen siber güvenlik kapsamındaki olguların pek çoğu –tıpkı siber silahların hem siber savunma hem de siber taarruz amaçlı kullanılabilmeleri gibi– çift kullanım alanına sahiptir. Dolayısıyla siber savaş gibi siber güvenliğin en üst katmanı düşünüldüğünde bu kavram sadece silahlı kuvvetlerle sınırlı kalmamakta aynı zamanda milli güç unsurlarını oluşturan tüm katmanların sorumluluk sahalarını da kapsamaktadır. Özellikle Şekil 16'da en sağ sütunda gösterilen YZ, büyük veri ve nesnelerin interneti bileşenleri bu sürecin daha da karmaşıklaşmasına ve tehdit türlerinin çevikleşmesine sebep olabilecek teknolojiler olarak görülmektedir.

Özellikle askeri sistemlerin oluşturduğu ortamlara odaklanıldığında fiziksel savaş alanlarında kullanılan tüm silah sistemleri ve platformların oluşturduğu boyutun; toplanan, üretilen, paylaşılan ve kullanılan veriler kapsamında siber fiziksel ortamlar haline geldiği görülmektedir. Bu sebeple askeri bir büyük veri ortamından bahsedilmesi mümkündür. Bu kapsamda harekat verileri belli ortamlarda şifrelense ya da anonimleştirilse bile her gün neredeyse *petabyte*larca verinin üretilmesi, paylaşılması ve depolanması şeklinde kullanıma sunulması bu alanın siber faaliyetlere (siber casusluk, terörizm ve taarruz vb.) açık olduğunu göstermektedir. Tüm bu gelişmeler kapsamında "ağ merkezli harekat" ya da "ağ merkezli savaş" kavramları yerine "askeri nesnelerin interneti" kavramını kullanmak uygun olacaktır. Buraya kadar sayılan özellikleri destekler nitelikte askeri nesnelerin interneti yapısının siber savunma-kamu güvenliği kapsamındaki önemi toplu halde Şekil 17 yardımıyla özetlenebilir.[46] Bu yapı özellikle askeri harekat ortamında kurulup kullanılacak sistemin ne derece karmaşık ve bir o kadar siber güvenlik kalkanına sahip olması gerektiğinin de bir göstergesi olarak değerlendirilebilir.

46 Paula Fraga-Lamas, Tiago M. Fernandez-Carames, Manuel Suarez-Albela ve Luis Castedo, "A Review on Internet of Things for Defense and Public Safety", *Sensors*, Cilt: 16, Sayı: 10, (2016).

*Şekil 17. Siber Savunma-Kamu Güvenliği ve Askeri Nesnelerin İnterneti**



* Fraga-Lamas, Fernandez-Carames, Suarez-Albela ve Castedo, "A Review on Internet of Things for Defense and Public Safety".

Ayrıca hem hasım hem de dost kuvvetlerin etkin bir YZ platformuyla birlikte hareket ettikleri düşünüldüğünde sistem üzerinde bulunan zararlı yazılımların oluşturduğu anomalilerin tespit edilmesi, tanımlanması ve müdahale edilmesi de bir o kadar güçleşecektir.

Bu kapsamda büyük veri, askeri nesnelerin interneti ve YZ teknolojileri bir arada ve siber güvenlik şemsiyesi altında bütünleşik bir yapıda değerlendirildiğinde yine sürecin savunma/taarruz, dost/düşman gibi ikilemelerle çift yönlü hareket ettiği söylenebilir.

Sayılan bu bileşenlerin sivil/resmi tüm güvenlik katmanlarını etkisi altına alabildiği de göz önüne alındığında "işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar" olarak tanımlanan "kritik altyapılar"ın[47] korunması büyük önem taşımaktadır. Çünkü kritik altyapıları oluşturan bileşenlerin zarar görmesi doğrudan milli güvenlik zafiyeti olarak ortaya çıkabilmektedir. Bu sebeple sivil/asker tüm katmanlarda etkili bir siber güvenliğin sağlanması en öncelikli süreç olarak değerlendirilmelidir. Etkili siber güvenlik sürecinin belirlenmesinde ise "siber güvenlik yaşam döngüsü"[48] önemli bir yol gösterici olarak kullanılabilir (Şekil 18).

Şekil 18. Siber Güvenlik Yaşam Döngüsü

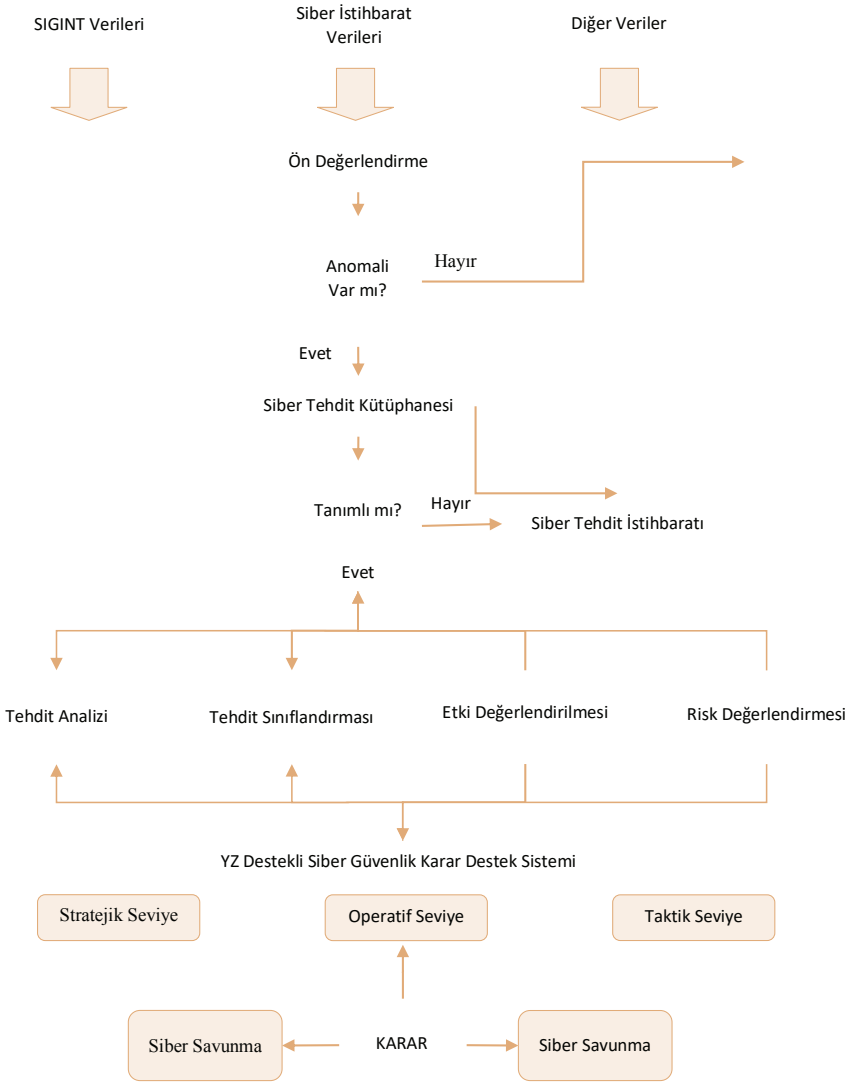
47 Kritik altyapı tanımlaması 20 Haziran 2013'teki 28683 sayılı *Resmi Gazete*'de yayımlanarak yürürlüğe giren "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nda yer almaktadır.

48 "Framework for Improving Critical Infrastructure Cybersecurity", NIST, (2018), https://www.nist.gov/cyberframework, (Erişim tarihi: 20 Mayıs 2019).

Bu döngünün etkinliğinin artırılabilmesi için "YZ destekli siber güvenlik karar destek sistemi"[49] tasarlanabilir (Şekil 19). Söz konusu temel tasarımda her tür kaynaktan gelen veriler ön değerlendirmeye tabi tutularak verilerin içerisinde anomali olup olmadığı araştırılır. Eğer anomali yoksa normal faaliyetlere devam edilirken anomali olması halinde ise bu veri siber tehdit kütüphanesine gönderilerek mevcut tehdit verileriyle karşılaştırılır. Eğer tanımlanamıyorsa siber tehdit istihbaratı yönüyle araştırılır ve tehdit tanımlaması yapılır. Ardından siber tehdit kütüphanesine işlenir. Anomali olarak tanımlanan veriler; tehdit analizi, tehdit sınıflandırması, etki değerlendirmesi ve risk değerlendirmesinin ardından YZ destekli karar destek sistemine aktarılır. Burada siber tehdidin siber tehdit katmanı (stratejik, operasyonel ya da taktik) belirlenir ve ilgili karar vericiye (seviyesine uygun olarak) yapılmasının uygun olacağı değerlendirilen seçenekler sunulur. Karar verici tarafından bu seçenekler yardımıyla ve mevcut mevzuat kapsamında etkin karar alınır.

49 Bu raporda belirtilen hususlar dikkate alınarak temel tasarım basit bir algoritma süreci şeklinde yapılmıştır.

Şekil 19. YZ Destekli Siber Güvenlik Karar Destek Sistemi



Siber güvenlik kavramının etkilerinin çok yönlü olmasındaki en temel sebeplerden biri de toplumun tüm katmanlarını kapsamasıdır. Günümüzde siber uzaya girme yaşı özellikle ebeveynlerin çocuklarını oyalamak adına kullanmalarına izin verdikleri akıllı telefonlar nedeniyle okul öncesi yaşlara kadar inmiştir. Buna binaen okul öncesi çağdan başlayıp ölünceye kadar olan tüm süreçte insanlık siber uzayda faaliyet göstermektedir. Dolayısıyla bütünleşik bir yapıya sahip olan siber güvenlik süreçlerindeki en zayıf halkayı siber güvenlik bilincine sahip olmayan bireyler oluşturmaktadır. Bu nedenle şu temel hususların dikkate alınmasının gerekliliği değerlendirilmektedir:

- Siber güvenlik konusunda farkındalık oluşturulması ve önlemler alınmasına yönelik bilinç seviyesini güçlendirecek planlı ve güncel tehditleri de barındıran eğitimlerin –bireylerin eğitim düzeyleri ve yaş farkları da gözetilerek– toplumun tüm katmanlarını kuşatacak şekilde planlanması

- Toplumun en küçük birimi aileden başlamak üzere tüm kurum, kuruluş ve sektörleri içerecek şekilde siber güvenlik stratejileri ile siber güvenlik uygulama politikalarının oluşturulması, bu politikaların güncel tutulması ve gerçekçi uygulamaların yapılması

- Kurumsal bazda özellikle kritik altyapı sistemleri başta olmak üzere hassas teknoloji için gerekli tüm yazılımların üretilmesinde milli kaynak kodlamalarının özendirilmesi ve bunların güvenli yazılım oluşturma standartlarına uygun bir şekilde oluşturulması

- Siber tehdit belirlemesi, siber tehdit analizi, siber tehdit sınıflandırılması, siber tehdit etki değerlendirilmesi, siber caydırıcılık ve siber saldırgan profillerinin belirlenmesi gibi alanlarda tüm ilgili bilim dallarının (psikoloji, sosyoloji, yönetim organizasyon, davranış bilimleri, stratejik yönetim, mühendislik vb.) disiplinlerarası konularda özgün projeler gerçekleştirmesinin özendirilmesi

SETA Gelişen Askeri
Teknolojiler Serisi .2.

Siber Güvenlik:

Küresel Trendler ve Türkiye'nin Kabiliyetleri

20. yüzyılın sonlarına doğru geliştirilmeye başlanan "elektronik savaş düzeni", "elektronik harp", "bilgi savaşı" ve "ağ merkezli harekat" gibi kavramlarla cephelerin sayısallaştırılması gündeme gelmiştir. Günümüzde ise modern silahlı kuvvetlerin neredeyse tüm bileşenlerinin yazılım ve donanım destekli sistemlerle donatıldığı görülmektedir. Çoğu askeri sistem siber uzay ortamından yalıtılarak faaliyet göstermesine rağmen yakın gelecekte askeri nesnelerin interneti altyapılarının oluşturulması üzerine projeler geliştirilmektedir.

Siber uzayda faaliyet gösteren tüm sistemler için siber tehditler en önemli güvenlik sorununu oluşturmaktadır. Bu nedenle siber uzay faaliyetlerinin etkili bir şekilde gerçekleştirilmesi etkin bir siber tehdit tanımlamasına, tespitine, analizine ve tehdit seviyesinin/zarar riskinin düşürülmesine bağlıdır. Diğer taraftan siber güvenlik kapsamındaki olguların pek çoğu –tıpkı siber silahların hem siber savunma hem de siber taarruz amaçlı kullanılabilmeleri gibi– çift kullanım alanına sahiptir. Dolayısıyla kritik altyapıları oluşturan bileşenlerin zarar görmesi doğrudan milli güvenlik zafiyeti olarak ortaya çıkabilmektedir. Bu sebeple sivil/asker tüm katmanlarda etkili bir siber güvenliğin sağlanması en öncelikli süreç olarak değerlendirilmelidir.

SETA

9 786258 322156