SAVSAD Savunma ve Savaş Araştırmaları Dergisi
The Journal of Defence and War Studies
Haziran /June 2023, Cilt/Volume 33, Sayı/Issue 1, 1-32.
ISSN: 2718-0301 E- ISSN: 2718-0700

SİBER SAVAŞ: BİLGİ KRİZİ Mİ YOKSA GÜVENLİĞİ Mİ?

Aykut ÇALIŞKAN[*]

Öz

Günümüz dünyasında yaşanan riskler oluşum ve sonuçları itibariyle toplumsal yaşamı etkilemekle kalmayıp gerilime sahne olan sosyal çatışma ve sorunlar üzerinden toplumsal değişimi etkilemekte ve de biçimlendirmektedir. Siber saldırıların bilgi sistemlerinin güvenliğini hedeflemesi sadece ulusal güvenliği etkilemekle kalmayıp bilgiyi metalaştırarak metaforik açıdan savaşın aracı haline getirmektedir. Bu yönüyle toplumsalı siber savaş ile buluşturan gerçeklik ise bilgi sistemlerindeki güvenlik beklentilerini açığa çıkarırken, devletlerin bilgi güvenliğine ilişkin oluşan gereksinimleri toplumsal alanda önemli bir temayı ortaya koymakta ve söz konusu bağlam üzerinden sosyolojik tespitlere kapı aralamaktadır. Bu durum diğer toplumsal olgu ve eylemler gibi siber savaşın gelişim süreçlerini incelemeyi gerekli kılmaktadır. Ayrıca bilgi ve iletişim araçları üzerinden oluşan tehdidinin boyutlarını da açımlamaya yönlendirmektedir. Bilgi teknolojilerinde yaşanan gelişmelerin çeşitlilik ve değişkenlik içeren yönünün bulunması ise siber tehlikelerin önlenmesinde risk yönetim sürecini ve çözümlenmesini zorunlu hale getirmektedir. Bu çerçevede araştırma sorunsalı olarak siber savaşların ortaya çıkış gerekçeleri incelenerek sosyolojik açıdan bilgi krizine mi yoksa bilgi güvenliğine mi neden olduğu sorusuna yanıt aranmıştır. Çalışma kapsamında doküman inceleme tekniği üzerinden alana dönük çalışmalar ve kaynaklar incelenmiş, birincil kaynak taraması üzerinden araştırma sorunsalı tartışılmıştır. Çalışmada bu tespitin literatüre sunduğu kavramsal ve kuramsal katkılar ile kısıtları ortaya konulmuştur.

Makalenin Türü: *Araştırma Makalesi*

Anahtar Kelimeler: *Siber Savaş, Bilgi Güvenliği, Siber Güvenlik, Bilgi Toplumu, Sosyal Ağlar.*

Jel Kodu: *N40, H56.*

Yazarın Notu: *Bu çalışma bilimsel araştırma ve etik kurallarına uygun olarak hazırlanmıştır. Bu çalışmada etik kurul izni veya yasal/özel izin gerektirecek bir içerik bulunmamaktadır. Çalışma ile ilgili herhangi bir çıkar çatışmasının bulunmadığı SAVSAD Savunma ve Savaş Araştırmaları Dergisi'ne yazar imzası ile beyan edilmiştir.*

[*] Doç.Dr., Dokuz Eylül Üniversitesi Sosyoloji Bölümü, aykut629aykut@hotmail.com, ORCID: 0000-0002-1886-6991.

Geliş Tarihi/Arrived: 13.10.2022
Kabul Tarihi/Accepted: 10.04.2023

Cyber Warfare: Information Crisis or Information Security?

Abstract

The risks in today's world do not only affect social life in terms of their formation and results. At the same time, it affects and shapes social change through social conflicts that are the scene of tension and problems. Cyber attacks target the security of information systems. It not only affects national security, but cyber warfare also commodifies information in the process of its emergence. This situation makes cyber wars a tool of war metaphorically. In this respect, the reality that brings social processes together with cyber warfare reveals security expectations. The needs of states for information security open the door to sociological determinations in the social field. This makes it necessary to examine the development processes of cyber warfare, like other social phenomena and actions. It also directs the dimensions of the cyber threat to expound. The multidimensionality of developments in information technologies brings forward the solution of risk management in the prevention of cyber dangers. Within the scope of the study, studies and sources related to the field were examined through the document analysis technique. In the study, the conceptual and theoretical contributions, and limitations of these determinations to the literature are revealed.

Article Type: *Research Article*

Keywords: *Cyber Warfare, Information Security, Cyber Security, Information Society, Social Network.*

JEL Code: *N40, H56.*

Author's Note: *This study was prepared in compliance with the scientific search and publication ethics. There is no content necessitating any permission from Ethical Board or any legal/special permission in this study. I, as the author of the article, signed my declaration certifying that there was no conflict of interest within the article preparation process.*

GİRİŞ

Günümüzde bilginin elde edilmesi kadar bilginin nasıl korunacağı konusu öne çıkmakta, sosyolojik tezahürü ise sadece kamusal alanı ilgilendirmemekte aynı zamanda bireylerin ve toplumsal grupların bilinç düzeylerine ve eylem şekillerine göndermede bulunmaktadır. Aktörünü bilginin üretilmesi, amaca dönük kullanılması ve sistemsel eksikliklerinin tespit edilmesi amacıyla toplumsaldan alan siber tehditler, grift yapıları ve özellikle devlet dışı aktörleri bilgi ediniminin parçası haline getirmekte, kamusalın dışına doğru bir alan açarak toplumsal aktörleri bu alana yönlendirmektedir. Siber savaş ise buradaki boşluğu hedefine alarak bireylerin teminat altına alınan özgürlüklerine ve sınırları belli olmayan içeriklere yönelmekte, sonuçları itibariyle devletleri, toplumsal kurumları ve bireyleri etkilemektedir. Sadece siber saldırıların eyleyicisi konumundaki

aktörlerin davranışlarından değil, aynı zamanda siber uzamdaki bilgi sistemlerinin kullanıcısı olan bireylerin ve toplumsal grupların davranış şekillerinden etkilenen siber savaş, toplumsal alanda gerçekleşme ihtimali bulunan iki yönlü risk algısını ortaya koymakta ve siber uzayda gün yüzüne çıkmaktadır.

Bu çalışmanın odağında meşru olmayan yollardan temin edilen bilgilerle şekillenen siber savaş kavramı ve güvenlik sürecine olan etkilerinin tartışılması yer almaktadır. Siber savaş kavramının kurumsal ve bireysel etkilerinin ele alınışı güvenlik beklentilerini açığa çıkarırken, bu durum bilgi sistemlerinin yönetim süreçlerini merkezine yerleştirmektedir. Ayrıca başta toplumsal aktörlerin siber savaş açısından rolleri ve sosyal konumları olmak üzere toplumsal alanda önemli bir temayı ortaya çıkarmakta ve sosyolojik tespitlerle siber savaş kavramını incelemeyi gerekli kılmaktadır.

Bilgi üretimi ve öznenin sorgulandığı postmodern dönemde toplumları bekleyen temel soru ise bilginin üretiminde görülen farklılık ve hangi bilginin kim için nasıl elde edildiği ya da elde edileceği sorusudur. Başka bir anlatımla bilgi sistemlerinin aktörleri açısından bu sorunun makro ölçekte bilgi güvenliğini ne düzeyde etkilediği ve savaş ya da türevleri gibi konseptlere olan yansımalarıdır. Kamu güvenliğini sağlamakla görevli devletin, gereksinim duyulan alanlarla ilgili işlevsel bölünmelere açık olduğu ve eksikliği hissedilen süreçlere uyum sağlama zorunluluğu kamu-birey açmazında bilgi ve iletişim süreçlerinin sistemsel inşasını ve güvenliğini zorunlu hale getirmektedir. Buna mukabil güvenlik taleplerinin özgürlük beklentileriyle nasıl bir ilişki içerisinde değerlendirileceği sorusu ise temel bir sorunsal olarak belirmektedir. Bu çıkarım sadece ulusal güvenlik ölçeğinde değil aynı zamanda genişleyen sosyal ağlar sebebiyle uluslararası toplum düzleminde de ele alınması gereken bir sorunsal olarak ortaya çıkmaktadır. Dijital dünyada üretilen bilgilerin içerik ve kapsamı ulusal güvenlik açısından önem arz edebilirken, şiddet yönetimi olarak akıllara gelen savaş olgusunu da dijital araçlar vasıtasıyla elde edilen bilgiler sayesinde yeni değişimlere açık hale getirebilmektedir. Dolayısıyla kamusal güvenliğinin sağlanmasında önemli sorumluluğu olan devlet, toplumsal kurumlar ve bireylerin bu süreç içerisindeki konumu, ilişkileri ve sorumlulukları siber savaş açısından yeni bir tartışma alanını oluşturmaktadır.

Bu kapsamda çalışma siber savaşların ortaya çıkış süreçlerini inceleyerek sosyolojik açıdan bilgi krizine mi yoksa bilgi güvenliğine mi neden olduğu sorusuna yanıt arayacaktır. Araştırmanın daraltılmış çerçevesini ulusal güvenlik sorunu olarak siber savaşı etkileyen ve harekete

geçiren toplumsal boyutları aramak ve güvenlik bağlamında devlet, devlet dışı aktörlerin etkilerini tartışmak olarak sıralamak mümkündür. Söz konusu sorunsalın çözümlenmesinde çalışma planı ise tarihsel bir izlek üzerinden araştırılmıştır. Öncelikle güvenlik epistemolojisinin tarihsel süreç içerisindeki gelişim süreçlerini ortaya koyan uluslararası ilişkiler teorilerindeki temel tartışmalar aktarılmış, bilgi güvenliğinin parçaları ve bilgi sistemlerine etkileri tartışıldıktan sonra siber savaş olgusunun gelişimi ve gerçekliği sorularına yanıt aranmış, devamında siber savaş kavramındaki aktörlerin faillik süreci ve çeşitli kuramsal arka planları üzerine tartışmalar sürdürülmüştür. Bu yönüyle araştırmanın sınırlılıkları arasında birincil kaynak araştırmalarına bağlı özelliği gösterilebilir.

Araştırmada, doküman inceleme tekniği üzerinden alana dönük çalışmalar ve kaynaklar incelenmiş, birincil kaynak taraması sonucunda elde edilen Türkiye'ye yönelik siber saldırı olayları göz önünde bulundurularak araştırma sorunsalı olarak ileri sürdüğümüz dikotomik kavramsal karşılaştırma çözümlenmiştir. Siber savaşların bilgi krizine mi yoksa bilgi güvenliğine mi neden olduğu sorusuna MAXQDA programında gerçekleştirilen nitel araştırma analizi üzerinden yanıt aranmıştır. Bu çerçevede ilgili sorunsalın çözümüne dair varsayımlar eleştirel paradigma doğrultusunda ilerleme göstermiştir. Yapılan çalışmanın siber savaş olgusunun sosyolojik bağlamının anlaşılması için mevcut gerçekliği sorgulamak, toplumsal ve bireysel davranış süreçlerini anlamak ve resmetmek ile toplumsal gerçekliği ortaya çıkarmak açısından önemli çıktılar sağlayacağı değerlendirilmektedir.

Uluslararası İlişkiler Teorisinde Temel Tartışmalar ve Güvenlik Epistemolojisine Yansımaları

Geleneksel güvenlik anlayışların geçtiğimiz yüzyılda yaşanan gelişmelere bağlı olarak değişim göstermesi şüphesiz güvenlik anlayışlarında epistemolojik değişimi de beraberinde getirmiştir. Toplumların askerî güvenlik alanında yaşadığı sorunlar üzerinden karakterize olan güvenlik kavramı toplumsal değişimin tetiklediği yeni tehditler ve çıkarlar doğrultusunda değişim göstermek zorunda kalmıştır. Güvenlik anlayışını devlet-asker bileşeni olarak algılayan eylemden birey ve toplumlara yönelen tehditlere doğru genişletilmesinin ardında nüfus artışı, küreselleşme, liberalizm ve yeni güvenlik konsepti gibi parametrelerin önemli etkisi bulunmaktadır (Akdemir ve Arslan, 2020). Ancak bu süreci beraberinde getiren parametreler ve değişimler tarihsel süreç içerisinde yaşanan gelişmeler ile anlam kazanmıştır. Uluslararası ilişkiler boyutuyla güvenlik çalışmalarının devletlerin öncül meseleleri arasında yer alması

yeni olmadığı gibi güç ilişkilerinin belirleyiciliği Soğuk Savaş dönemi dâhil etkisini sürdüren bir başlık olarak öne çıkmıştır.

Modern devletlerarası sistemin ortaya çıkmasını sağlayan ve Otuz Yıl Savaşları'na son veren Westphalia Anlaşması (1648) temsili bir görünüm kazanırken, tarihsel süreçte yaşanan savaşlar güç politikasının hâkim unsur olarak öne çıkmasını ve sorunların çözümünde realizm gerçekliğini gözler önüne sermiştir (Kolasi, 2014). 17. yüzyılda bireyin ontolojik ihtiyaçları arasında yer alan güvenlik olgusu iki düşünür tarafından ele alınarak insan doğası üzerinden incelenmiş, doğa ve toplum hali güvenlik kavramıyla ilişkilendirilerek güvenlik ile bireyin hak ve özgürlüklerinin konumu tartışılmıştır (Emekliler, 2011). Thomas Hobbes'a göre güvenlik kavramı güç ve devlet temelinde açıklanırken bireyin devlete karşı toplumsal sözleşme bağlamında ödev ve sorumlulukları öne çıkarılmış, John Locke'a göre ise bireyin hak ve özgürlüklerinin korunması ile güvenlik kavramı özdeş hale getirilmiştir. Bu noktada Hobbes'un toplum sözleşmesi kuramını geliştirerek modern devlet düşüncesini teorik temele kavuşturması söz konusu iken, Locke devlet iktidarının sınırlandırılması konusunu savunmuştur (Arslanel ve Eryücel, 2012). Bu düşünsel açıklamalar ise günümüze kadar güç kullanma yetkisi ve siyasanın kutuplarını düzlemsel açıdan açığa çıkarma açısından başvurulan fikirleri oluşturmuştur. Dolayısıyla kişilerin ve toplumların güvenlik anlayışları, siyasi bakış ve felsefi dünya görüşlerinden türemiştir (Booth, 1997).

Tarihsel süreçte uluslararası güvenlik çalışmalarının üç büyük tartışma ekseninde değerlendirilmesi önem arz etmektedir (Sezgin ve Kaya, 2008). İlki, 1940'lara kadar temel uzlaşının barışın sağlanmasına yönelik ele alındığı ve etik tartışmalar üzerinden yürüyen idealizm-realizm tartışmasıdır. İnsan doğası üzerinden ele alınan bu tartışmada güç ve çıkar çatışmasını öncelleyen realizmin idealizme üstün geldiği savlanmaktadır. İkinci tartışma alanı ise 1960'lara kadar geleneksel realizm ile davranışçılar arasında metodolojik varsayımın öne çıktığı, bilimsel deneyin tarihsel inşaya üstün geldiği ve böylece pozitivizmin hâkim paradigma olduğu süreçtir. Üçüncü tartışma alanı ise 1980'li yıllardan sonra post-pozitivist bir epistemolojinin uluslararası ilişkileri açıklama açısından pozitivizmden daha geçerli olduğu ve uzlaşı yerine farklılığı öne çıkardığı söylemdir. Söylemsel olarak inşa edilen ifadeler bir kenara güvenliğin kavramsal açıdan ne olması gerektiğinden çok ne olmayacağı konusundaki tartışmalar ise Soğuk Savaş döneminden sonra değişime uğramıştır. Paradigma değişimini beraberinde getiren süreç ise 1980'li yıllarda sadece askerî alanda değil, aynı zamanda toplumsal, siyasal, ekonomik ve kültürel alanda yaşanan gelişmeler ile okunmaya başlamıştır. Bu bağlamda Soğuk Savaş öncesi dönem güvenlik

çalışmaları açısından uzun süre klasik realizm altında etkisini sürdürmüş ve stratejik boyutta devam etmiştir (Birdişli, 2014).

Balzacq'ın (2009) aktardığına göre post-pozitivist tartışma sözde üçüncü tartışmayı oluştururken eklektik bir çalışma grubuna göndermede bulunmaktadır. Ayrıca 1970'li yıllarda etkisini belirginleştiren postyapısalcı felsefenin güvenlik çalışmalarına eklemlenmesi Beşerî Bilimlerin aksine daha geç bir sürece denk gelmiş; güç, yapılar ve bilgi üzerinde disipline edici etkisi klasik realist güvenlik çalışmalarına eşlik etmiştir (Hansen, 2017). Soğuk Savaş'ın sona ermesiyle birlikte güvenlik kavramı ise genişlemiş ve derinleşmiştir (Faleg, 2012). Özellikle Soğuk Savaş'ın sonlanmasına yakın ve sonrasında eleştirel güvenlik çalışmaları post-pozitivist meydan okunmanın parçası haline gelmiş tehditlerin inşası, kimlik ve farklılık, insan güvenliği ve özgürleşme gibi kavramlar üzerinden tartışma alanı açmıştır (Fierke, 2017).

Eleştirel güvenlik çalışmaları açısından ilk dalga; güvenliğin öznesinin sadece devlet ile sınırlı tutulamayacağını, öznenin toplum, topluluklar, gruplar ve bireyler şeklinde geliştirilmesini vurgulayarak güvenliğin askerî, siyasi, ekonomik, toplumsal ve çevresel olmak üzere beş sektörde incelenmesini ifade eden Barry Buzan'a ait (1983) *"People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era"* başlıklı çalışmadır (Rumelili ve Karadağ, 2017). Bu tespitle birlikte geleneksel araştırmacılar tarafından güvenlik gündeminin sadece askerî meseleler ile sınırlı tutulamayacağı görüşü sonrasında yeni bir tartışma alanı açılmıştır. Kopenhag Ekolü devlet merkezli, askerî-siyasi konulara odaklanan güvenlik yaklaşımlarını eleştirip güvenlik kavramını askerî, siyasi, ekonomik, toplumsal ve çevresel olmak üzere beş sektör çerçevesinde genişletirken, güvenlikleştirme teorisi bağlamında nesnel bir tehdidin yol açtığı sorunlardan ziyade söz edimleri yoluyla ifade edilen güvenlik söz edimini öne çıkarmıştır (Akgül-Açıkmeşe, 2011). Bu sektörler arasında gösterilen toplumsal sektörün referans nesnesini ise sosyal grupların aidiyet ve sadakat hisleri neticesinde şekillenen biz algısının tehdit edilmesi oluşturmuştur (Buzan, 1998 akt. Baysal ve Lüleci, 2015). İlerleyen süreç dâhilinde güvenliğinin yeniden kavramsallaşmasına imkân tanıyan eğilimleri; güvenliğe yönelik kavramların derinleşmesi, genişlemesi ve sektörleşmesi, güvenliğin devletten insan ya da insan güvenliğine doğru kayması, yeni tehdit, hassasiyet ve risklerin algılanarak güvenlik kaygılarının güvenlikleştirilmesi, yeni beliren güvenlik tehlikeleri ve kaygıları ile savunmasız insanlara *"beka ikilemi"* arz edecek şekilde risk, tehlike ve afetlere yüzleşmesi için askerî olmayan stratejilerin araştırılması olarak ifade edilmiştir (Brauch, 2008).

Eleştirel güvenlik çalışmaları iki akımdan oluşmakla birlikte (Yavuz, 2009) bu akımlardan ilki realizme karşı çıkmaları ve epistemolojik olarak post-pozitivizmi benimsemiş olmaları dışında, söylem ve hedefleri açısından ortaklıkları bulunmayan farklı yaklaşımları barındıran ve bir araya getiren Keith Krause ve Michael Williams'ın 1997'de yayınladıkları *"Critical Security Studies"* başlıklı çalışmadır. İkincisi ise; özgürleştirme *(emancipation)* temelinde yeni bir güvenlik söylemi ve pratiği şekillendirmeyi amaçlayan post-pozitivist çoğulculuğun yerine teorik kesinliğe dayalı Ken Booth ve Richard Wyn Jones'un çalışmalarının temsil ettiği Welsh/Aberystwyth ekolüdür (Yavuz, 2009). Booth (2007) güvenlik söz edimine ilişkin söylem üretmekten yoksun bireylerin Kopenhag Ekolü tarafından ihmal edildiğini dile getirmiştir. Bu açıdan Aberystwyth ekolü bireyleri hem güvenliğin referans nesnesi olarak ele almakta hem de merkez dışı bağlamlarda yaşanan güvensizlikleri anlamada güvenlik alanında farklı aktörlerin etkin olduklarını vurgulamaktadır, aynı zamanda literatürde eleştirel güvenlik çalışmaları açısından bu ekolün dışında feminist, postkolonyal, yeşil teori gibi farklı yaklaşımlara da yer vermektedir (Küçük, 2021).

Bu bağlamda güvenlik kavramı içerik olarak genişle(til)mekle kalmamış toplumsal alanda yeni tartışma konularının parçası olmuştur (Bilgin, 2010). Sorunların niceliksel anlamda artmasından ziyade gündemin genişlediğinin anlaşılması bu tespiti ortaya koyan önemli bir gerçekliktir. Özellikle güvenlik kavramının ulus ötesi ağlar üzerinden sınırlarının belirsizleşmesi ülkeleri yeni tehdit ve risklere de maruz bırakmıştır. Bu riskler ekonomik, toplumsal, çevresel ve teknolojik gerilimlerden kaynaklı olarak ekonomik ve sosyal eşitsizlik, etnik çatışmalar, küresel terör, kitlesel göç, sınır aşan suçlar bağlamında uyuşturucu ticareti, göçmen veya silah kaçakçılığı ile siber saldırılar gibi başlıklarla güvenlik kavramını yeniden inşa etmiş ve etmeye de devam etmektedir.

Bilgi ve Güvenliği

Hızla gelişen bilişim teknolojileri aracılığıyla verinin saklanması, depolanması, paylaşılması ve transferinde sağladığı olanaklar ile günümüzde anlamlandırılan bilgi, en önemli üretim faktörü olarak kabul edilmektedir (Acılar, 2009). Elektronik ortamda kullanılan bilginin genişlemesi ve iletişim imkânlarının artmasıyla birlikte kurumsal ve kişisel düzeyde üretilen bilginin güvenliğinin sağlanması ihtiyacı doğmuştur (Vural ve Sağıroğlu, 2008). Bu sürece teknoloji bağlantılı uzaktan depolamada yararlanılan bulut bilişim alanındaki gelişmeleri ve geliştirilen güvenlik tedbirlerini eklemek mümkündür (Wang vd., 2010; Rao ve Selvamani,

2015). Bilginin erişilebilir olması ise gündelik hayatı kolaylaştırmış, böylelikle bilgi pek çok faaliyetin gerçekleştirilmesi için talep edilen bir konuma kavuşmuştur.

Bilgiyi toplumsal düzlemde tanımlamadan önce geçirdiği süreçleri hiyerarşik bir yapı içerisinde ifade etmekte fayda olup, planlama, karar verme, karşılaştırma, analiz, değerlendirme ve tahmin gibi aşamalar içerisinde bilginin gelişim sürecini ele almak gerekmektedir (Çapar, 2003; Güngör ve Güney, 2017). Bilginin gelişim sürecinde toplumsal değişim dinamiklerinin de önemli bir rolü bulunmaktadır. Geçen yüzyılda fikirlerin ve teknolojinin de etkisiyle bilgi, metalaşan bir konuma kavuşmuştur. Üretim araçları ve inovasyon açısından talep edilen bilgi, internet ve iletişim teknolojileri vasıtasıyla bireysel ve kurumsal açıdan önem kazanmıştır. Bilgi, mecazi anlamda gelişim göstererek insan ediminin önemli bir bileşeni haline gelmesiyle birlikte geçmişte üretilen bilginin içeriği ve oluşma süreci de önemli bir mesafe katetmiştir. Günümüz dünyasında bilginin bireyler, şirketler, kurumlar ve devletler için güç olarak değerlendirilmesi ise güvenlik sorunlarını artırmıştır (Eminağaoğlu ve Gökşen, 2009). Bu bağlamda Wallerstein (2013) bireyin ve kurumların bilgi kaynaklarının denetimi için sürdürülen mücadelede çatışma içerisinde olduğunu vurgulamıştır (Wallerstein, 2013 akt. Özdemirci ve Torunlar, 2018).

Özetle bilgi, veriye dayalı ispat süreciyle bilimsel yöntem ve ölçme sonucu elde edilen ve kavrayışla özbilgiye ulaşılan bir düşünüş olarak tanımlanmaktadır (Canberk ve Sağıroğlu, 2006). Bilgi güvenliği ise; bilgilere izinsiz erişim sağlanması, kullanılması, yok edilmesi ya da ifşa edilmesi ve hasar verilmesi gibi adımlardan korunma işlemi olarak tarif edilmektedir (Baykara vd., 2013). Bilgi güvenliğinin sağlanabilmesi için uyulması gereken bileşenler; gizlilik, bütünlük, kayıt tutma, kimlik tespiti, güvenirlik ve inkâr edememedir (Tekerek, 2008). Sayısal ortamdaki bilginin saklanması ve taşınması esnasında bilgi bütünlüğünün bozulmaması gerekmektedir bu amaçla izinsiz erişimlerden korunması için bilgi saklama ve işleme platformlarının güvenli bir şekilde inşa edilmesi önem arz etmektedir (Güngör, 2015).

Bilgisayarların ve bilgi sistemlerinin artan kötüye kullanımı, veri bankalarında kişisel mahremiyete yönelik tehditler ise veri güvenliği konusuna ilgiyi artırmıştır. Bu bahisle dört farklı koruma tedbirinden bahsedilmektedir (Dennning ve Denning, 1979). Bu tedbirler; hangi kullanıcının sisteme gireceğini belirleyen erişim kontrolleri, kullanıcının erişebileceği veri kümeleri arasında değerlerin yayılmasını izleyen akış kontrolleri, sorgulayıcıların gizli bilgileri çıkarmasını önleyen ve istatistiksel sorgu dizeleriyle oluşturulan çıkarım kontrolleri ile veri

şifreleme, aktarım veya depolama aşamalarındaki gizli bilgilerin yetkisiz ifşasını önlemedir.

Bu çerçevede bilgi güvenliği kavramı, bilgisayar sistemleri üzerinden depolanan ve asıl amacına uygun şekilde kullanılması ve kontrol edilmesi süreçlerinin yanında sisteme yasal ya da yasadışı yollardan erişim sağlayabilen kişilerin amaçlarına göre incelenmesi süreçlerine doğru genişleme göstermiştir. Bilgisayarlara yönelik donanım ve yazılım içerikli tehditlerin ulusal güvenliği etkileyen boyutlara ulaşması bilgi teknolojileri açısından güvenlik önlemlerinin geliştirilmesine neden olmuştur (Topçu, 2021). Bilgi ve güvenliği kavramı bilginin üretimi, depolanması ve işlenmesinin dışında sistemsel bir alanda yer alan kullanıcıların kullanım amaçlarına göre sanal bir sistem inşa etme süreçlerini beraberinde getirmiştir. Dolayısıyla kişilerin verileri ya da toplumsal aktörlere ilişkin üretilen bilgilerin sistem içerisinde nasıl dolaşım gösterdiği ve erişildiği sorusu bilgi güvenliği kavramını şekillendirmiştir.

Siber Savaş, Katmanları ve Toplumsal Alanla İlişkisi

Siber savaşın tanımını yapmak üzere literatürde bir uzlaşı bulunmadığını ve yaygın olarak benimsenen bir tanımın yer almadığını vurgulamak gerekmektedir (Robinson vd., 2015). Ancak siber savaşın kökleri radyo iletişimi ve radar teknolojilerinin gelişimine uzanmakta, elektronik savaş olarak tanımlanan ve siber savaş tarafından kapsanan teknoloji gelişimiyle ilişkilendirilmektedir (Green, 2015). Norbert Wiener'in *"Sibernetik"* isimli kitabında hayvanlarda ve makinelerde kontrol ve iletişim olarak tanımladığı sibernetik kelimesinden türemesiyle birlikte bilişim ve iletişim teknolojilerinde yaşanan gelişmelerin şekillendirdiği uzayı tarif etmek amacıyla kullanılan kavramsal terim ise siber uzay olarak ifade edilmektedir (Yayla, 2013).

Uluslararası doktrinde siber savaşın farklı tanımları olduğunu ifade eden Türkay (2013) siber savaşın dijital veya teknolojik yollarla yürütülen bir savaş yöntemi anlamına geldiğini, siber savaşın altyapıları devre dışı bırakma, istihbarat toplama ve propaganda dağıtımı kavramlarını içerdiğini aktarmıştır. Bir başka tanımda ise siber savaş, herhangi bir devlet tarafından düşman kaynaklarının kesintiye uğraması ya da kontrol edilmesi amacıyla gerçekleştirilen saldırıyı veya askerî savunma kapsamında bilgi ve iletişim teknolojilerindeki fiziksel ya da fiziksel olmayan ortamlarda değişik şiddet düzeylerinin kullanılmasını ifade etmektedir (Taddeo, 2012).

Siber saldırı türlerini derleyen Güntay (2018) karşılaşma sıklığı açısından en yüksek oranlara sahip olanların virüs, solucanlar, trojanlar,

zararlı yazılımlar, web tabanlı saldırılar, oltalama ve sosyal mühendislik, zararlı kodlar, botnetler, servis dışı bırakma olduğunu ifade etmesine karşın verilen zararlar açısından spesifik olay türlerine göre siber saldırı türlerinin değişebileceğini belirtmiştir. Ayrıca söz konusu olaylarda yaşanan maddi kayıplar ve zararların bireyleri, kâr amacı güden unsurlar ile uluslararası aktörleri etkileyebileceğini aktarmıştır (Güntay, 2018).

Alan yazında devletler arasında rekabetin yaşandığı beşinci alan olarak tarif edilen siber uzay, dünyadaki tüm bilgisayarlı ağlarla birlikte bu ağlardan geçen komutlar ile komutları kontrol eden tüm uç noktalardan oluşan bir ağı içermektedir (Tabansky, 2011). Tabansky (2011) siber uzayın üç katmanını; elektrik enerjisi, depolama birimi, iletişim altyapıları, optik fiberler, işlemciler ve entegre devreler gibi yapı taşlarını kapsayan fiziksel katman, insanlar tarafından programlanmış etki ve tepki talimatlarının verildiği yazılım katmanı ile makine tarafından depolanan veri katmanını sonucunda elektronik ortamda üretilen bilgi olarak ifade etmiştir. Siber savaş ise bilgisayar ağlarına yönelik düşmanca eylemlere dikkat çekmektedir (Woods ve Weinkle, 2020). Bu açıdan tasarım aşamasında bilgisayar sistemleri ve alt yapılarına yönelik güvenliğin inşa edilmemesi durumunda siber savaşın kaçınılmaz bir gerçek olduğu belirtilmiştir (McGraw, 2013).

Siber savaşı konvansiyonel savaşlardan ayıran en önemli özellik ise fiziksel bariyerleri kaldırmış olmasıdır. Veri ya da verinin anlamlı hale getirildiği bilginin depolandığı aygıtların işlevini kaybetmesini amaçlayan siber saldırılar, siber uzayda somut hedefleri bulanıklaştırmakta ve tehdit tespitine ilişkin risk algılarını artırmaktadır. Taddeo (2012) siber savaşlar ile geleneksel savaşları şiddet, siviller, fiziki ve insani boyutları bakımından karşılaştırarak farklılıklarını ortaya koyduğu çalışmasında siber savaşların şiddet seviyeleri, faillerin doğası ve ücretlendirme alanı açısından geleneksel savaştan ayrıldığını ifade etmiştir. Ayrıca bilgi teknolojilerinde yaşanan gelişmelerin ulusal savunma başta olmak üzere askerî alanda gerçekleşen teknolojilere entegre edilmesi siber uzayın güvenliği sorunsalını da beraberinde getirmiştir. Siber güvenlik ve bilgi güvenliği kavramları alan yazında birbirleriyle örtüşen anlamlarda kullanılsa dahi, siber güvenlik kavramının siber saldırıların potansiyel hedefi olan insanları da bilmeden siber saldırıya dâhil etmesi nedeniyle kavramsal açıdan ayrıldığı, bilgi sistemlerine ilişkin rollerde görülen farklılaşmanın ise bu ayrıma katkı sağladığı aktarılmıştır (Von Solms ve Van Niekerk, 2013). Bilgi teknolojilerinde görülen ve toplumsal aktörleri ilgilendiren bu durum bireyin sanal ortamda davranışlarını etkileyebilirken bilgi üzerinden gerçekleşen toplumsal güç ilişkilerinde de tayin edici olabilmektedir (Foucault, 1981; Behrent, 2013; Cavelty, 2018).

Bu çerçevede siber uzayda varlık gösteren aktörlerin eylemleri de siber uzayı etkileyen bir parametre olarak öne çıkmaktadır. Sistem olarak inşa edilen ve bilgi üretiminin dışında bilgi akışına imkân tanıyan özellikleri nedeniyle günümüzde bilgi teknolojileri, her türlü bilişim ve iletişim vasıtası aracılığıyla toplumsal açıdan bireyleri birbirine bağlayan bir ağ görevi görmektedir. Dolayısıyla bilgi sistemlerinde yer alan aktörlerin konumları gereği eylemleri, tanımlanan rolleri ve bilinç düzeyleri üzerinden okunan sosyolojik tespitler bilgi sistemlerinin güvenliğini etkilemektedir.

Alan Yazında Siber Savaşın Gerçekliği Üzerine Tartışmalar

Siber savaş(lar)ın geçmişte yaşanıp yaşanmadığı, savaş biçimi olarak adlandırılmayı hak edip etmediği ya da kavramsal olarak casusluk gibi savaşın dışında bir faaliyet ya da ayrı bir suç kategorisinde tartışılıp tartışılamayacağını değerlendiren farklı görüşler bulunmaktadır (Rid 2012; Whetham, 2016). Siber savaşın savaş biçimleri arasında değerlendirilip değerlendirilemeyeceğini tartışmadan önce savaş kavramının terminolojik açıdan Quincy Wright'ın (1942) aktarımıyla incelenmesinin faydalı olacağını ifade etmekte yarar bulunmaktadır. Buna göre savaşın şiddet çatışması olarak değerlendirilmesinin yetersiz olduğu ve savaşın belirleyici özelliklerinden bahsetmenin gerekliliği vurgulanmıştır. Bu durumda savaşın belirgin özellikleri; kuvvet kullanma hali, düşmanca bir tutum veya eylem, hukuki sonuçlar doğurma ve savaşın faili olarak devlet biçiminde sıralanmıştır (Varlık, 2013).

Siber savaş tanım olarak internet veya ileri bilgisayar teknolojilerinin bir siyasi topluluğun temel çıkarlarına zarar vermek amacıyla kullanılması olarak belirtilebilir (Carr, 2010), aynı zamanda siber savaşa şüpheyle bakmak ya da siber savaş satıcısı olmak üzere ikili bir ayrıma gidilebilir (Orend, 2014). Siber savaşın gerçeklik durumuna ilişkin somut gösterimleri açığa çıkaran pek çok hadise ise özellikle 2000'li yıllardan sonra öne çıkmıştır.

Son yirmi yılda kinetik savaşlardan ayrı ya da kinetik savaşlara eklemlenen siber savaşların neler olduğuna dair tartışmalar devam ederken, yüksek düzeyde ağ bağlantılı toplumların kendi doğal güvenlik açıklarından dolayı siber taktikleri kullanma noktasında çekinceleri olabileceği ifade edilmektedir (Libicki ve Geers, 2015). Öte yandan bu süreçte yaşanan siyasi ve askerî gelişmeler ise siber savaş olgusunu etkilemiştir. Özellikle siber savaşın nükleer savaş gibi caydırıcı özelliklerinin olmaması açısından ülkeleri cesaretlendirdiği ve siber savaş fenomeninin Soğuk Savaş'ı açıklık

ve şeffaflık zamanı gibi gösterecek şekilde hükümet gizliliğiyle örtüldüğü değerlendirilmiştir (Clarke ve Knake, 2014).

Alan yazında siber savaş olarak nitelendirebilecek saldırılar ise birkaç örnek olay üzerinden gösterilmektedir. Bunlardan ilki şüpheyle yaklaşılan ve 1982 yılında doğalgaz boru hattını kontrol etmek amacıyla Kanadalı şirketten çalındığı iddia edilen bir yazılımla yerleştirilen virüs sayesinde Rusya Sibirya'daki boru hatlarındaki akışın normalin üstüne çıkması nedeniyle gerçekleşen patlama olarak gösterilmektedir ve bu durumun ABD tarafından sonradan fark edildiği ifade edilmektedir (Lindsay, 2013). Başka bir örnekte ise; NATO'nun Kosova ve Sırbistan'daki Eski Yugoslavya Cumhuriyeti hedeflerini vurması sonrasında siber saldırıların Sırplar tarafından 2001 yılında NATO altyapılarına yöneldiğini belirtmektedir (Vatis, 2001).

2007 yılında meydana gelen ve siber savaşın politika nesnesi olarak değerlendirilen olayda ise Estonya'nın Tallinn kentindeki bir parktan kaldırılan anıt sonrasında başlayan (DoS *"Denial Of Service"* ve Ddos *"Distributed Denial of Service*") saldırılar sonucu hükümet, bankacılık, medya ve siyasi parti web sitelerine karşı gerçekleştirilen siber saldırılar dünya tarafından ilk siber savaş vakası olarak kabul edilmektedir (Kaiser, 2015). Ayrıca "Stuxnet" adlı siber solucanın İran Natanz'da yer alan nükleer tesise çarptığının tespiti, siber suç ve devlet arasındaki eylemi göstermek için kullanılan örnekler arasında gösterilmektedir (Farwell ve Rohozinski, 2011).

Ülkeler arasında yaşanan politik gerilimlerden dolayı gündeme gelen siber savaş, bilgi çağının gereksinimleri arasında gösterilen yazılım kaynakları ve stratejik öneme sahip alt yapıları hedefleyen saldırılar üzerinden yaşanan bir gerçeklik olarak okunmaktadır. Öte yandan bilgi çağı olarak nitelendirdiğimiz günümüzde iletişim alt yapıların genişlemesi ve sosyal ağların bireyleri ve toplumları birbirine bağlayan entegre ağlara dönüşmesi siber savaşın sadece teknik bir alanın parçası olmasının yanında insan ve toplumsal grupları barındıran unsurları da etkileyebileceği gerçekliğini gün yüzüne çıkarmaktadır.

İnternetin ve sosyal paylaşımın gündelik hayata etkileri değerlendirildiğinde sanal ortamda anlık veri akışı fiziksel alanın dışında bireyi ve toplumu etkileyen ve psiko-sosyal sonuçları barındıran bir gerçekliği gözler önüne sermektedir. Bu yönüyle siber savaşın boyutlarının ve etkilerinin tahmin edilmesi sadece teknik süreçlerin incelenmesini değil, aynı zamanda insan kaynaklı nedenlerinin kestirilmesini zorunlu kılmaktadır.

Siber Savaşlar Açısından Failliğin Kuramsal Çerçevesi

Savaşların bilimsel ve teknolojik ilerlemeler ile toplumsal değişimler nedeniyle biçim değiştirmesi modern dünyadaki politik ve askerî güç mücadelelerini de etkilemiştir. Aydınlanmanın araçsal aklı işlevsel kılan ilerleme ve düzen mottosu güç mücadeleleri açısından tersine bir sonuç oluşturarak toplumsal çatışmayı derinleştirmiştir. Modern toplumların ulus-devlet ve sınai örgütlenme gerçekliği üzerinden politik mücadele arayışları tarihsel açıdan bu süreçte yeni çatışmaları beraberinde getirmiş, büyük yıkımların yaşandığı dünya savaşlarının deneyimlenmesi sonrasında geleneksel savaşların şekil değiştirmesine ve savaşların yeni görünümleriyle güç mücadelesinin aracı olma özelliklerinin devam etmesine sebebiyet vermiştir. Özellikle sanayileşme ve ekonomik üretim başta olmak üzere devamında yaşanan dijitalleşmeyle birlikte toplumsal alanda görülen değişimler mücadele alanlarını genişletmiştir. Toplumsal gereksinimleri karşılayan alanlarda yapılan faaliyetlerin dijital alana taşınması ise şiddet çatışmalarında görülen riskleri farklı bir boyuta taşımıştır. Ekonomik, ticari ve askerî alanlar dışında toplumsal alanın söz konusu kurumsal yapılar üzerinden dijital alana taşınması ise temelini şiddet unsurundan alan savaş olgusunun da kimlik değiştirmesine ve de yeni görünümler almasını beraberinde getirmiştir.

Savaş biçimleri arasında gösterilen siber savaşın geleneksel savaşlar gibi değerlendirilemeyeceği tartışmaya açılırken içeriğinde ve doğasında yer alan farklılıklar da geleneksel savaşla karşılaştırma yapılmak suretiyle açıklanmıştır. Kuramsal düzlemde açıklama ihtiyacı gereği askerî teori bağlamında geleneksel savaş ile siber savaş karşılaştırılarak öngörülebilir stratejilerin değişim gösterdiği bulgulanmıştır. Bu çerçevede geleneksel askerî teorinin siber çatışmalara uygulanan dört zorluğunun anonimlik *"anonymity"*, nesne sürekliliği *"object permanence"*, ölçülebilir sonuçlar *"measurable results"*, hızlı dijital uygulama *"rapid digital execution"* boyutları olduğu tanımlanmıştır (Kallberg, 2016). Siber savaşları besleyen en temel özellik ise öngörülemez olması üzerine inşa edilmiştir. Siber savaşların geleneksel savaşların aksine düşman unsurlarını değerlendirebilecek anlık veri akışına sahip olmaması tahmin edilebilir değerlendirmeyi ise kısıtlamıştır.

Siber saldırıların (Lemos, 2002) bilgileri çalmaya veya bozmaya ya da verilerin meşru kullanıcılara yönelik elektronik hizmetleri reddetmeye yönelik olmasının dışında su kaynakları, elektrik iletişim hatları ve demiryolları gibi fiziksel altyapıyı yöneten bilgisayar sistemlerinin kontrollerini devre dışı bırakmaya ya da ele geçirmeye yönelik hedefleri içermesi, bilgi güvenliği kavramını önemli bir bileşen haline getirmiştir. Bu

durum bilgi sistemleri veya kritik öneme sahip altyapıların kontrol sürecini mücadele alanına çevirmiştir. Rosenfield (2009) yapmış olduğu değerlendirmede veri saldırılarının kontrol sistemi saldırılarından daha büyük bir tehdit içerdiğini savunmuştur. Gerekçe olarak ise; kontrol sistemi saldırılarının doğasında görülen zorluğu, modern toplumda üretilen bilginin genişlemesini, kritik altyapıyı kapsayan bilgisayar ağlarının esnekliği ile insan gözetimi ve yerleşik mekanik arızalara yönelik emniyet içeren tedbirlerin önemini sıralamıştır. Dolayısıyla bu değerlendirmelerle birlikte siber saldırılar açısından veriye yönelik saldırıların önemli olduğu ortaya koyulmuştur. Verinin siber saldırılar açısından önem teşkil etmesi ise siber saldırılar açısından bilginin dolaşım kaynaklarını ve geçerli bilginin nasıl yayılım gösterdiği ve elde edileceği sorusunu tartışmaya açmıştır. Bu bağlamda siber saldırıların gerçekleşmesinde bilginin bireyler ve kurumsal yapılar arasında aktarımı öne çıkarılmıştır (Freiburger ve Crane, 2008).

Zimbardo (1969) bireyselliğe karşı davranışların kontrolünün kaybedilişini ifade eden temaların; anonimlik *"anonymity"*, bireysellikten arındırma *"deindividuation"*, insanlıktan çıkarma *"dehumanization"* ve kontrol *"control"* olduğunu ifade etmiştir. Bu bağlamda üretilen verilerin güvenliğini sağlamanın dışında bilginin bireyler ve toplumsal gruplar arasında nasıl risk içeren bir yapıya dönüştüğünün tespit edilmesi gerekliliği ve bu sürecin kontrol altına alınmak istenmesi hedefi ise sistemsel bilgi edinim süreçlerini beraberinde getirmiştir.

Siber saldırının hedefine yerleştirilen ulusun sistematik açıdan uğrayabileceği zararın öngörülmesinde ya da bir ulusun siber saldırının olası etkilerini öngörebilmesi ve değerlendirebilmesi açısından kurumsal yapıların etkinliği doğrultusunda siber saldırıların öngörülmesi ise söz konusu risklerin azaltılmasını hedeflemiştir. Waldo (1948) tarafından ileri sürülen meşrutiyet, kurumsal bilgi, otorite, bürokratik kontrol, güven ilkeleri üzerinden ilerletilerek devletin siyasal yönetimini ayakta tutan ve karşılaşılması muhtemel olaylarda vereceği tepkinin etkinliğini gösteren kavramsal boyutlar söz konusu öngörüye açıklama sunmuştur (Kallberg vd., 2013). Dwight Waldo (1948) tarafından devletin idari yönetimine ilişkin tespit edilen beş ilke üzerinden açıklanan bilgiler dâhilinde Kallberg ve arkadaşları (2013) kurumsal zayıflıklar üzerinden siber saldırıları öngörerek teorik çerçeveyi ya da kavramsal risk algısını pratiğe dönüştürmüştür. Siber saldırılarının geleneksel savaşlardan ayrılan yönleri böylelikle elimine edilerek kurumsal bakış açısıyla çözümlenmeye çalışılmıştır. Dolayısıyla siber saldırıların etki alanları toplumsal açıdan önem arz eden kurumların faaliyet alanları ve sosyal ağlarda dolaşım gösteren bilginin yayılım özellikleri üzerinden öngörülebilir hale getirilmiştir.

Toplumsal ağların dijital alana aktarılması ise internet tabanlı uygulamaların gelişim göstermesiyle geniş kitleleri etkilemiştir. Özellikle geleneksel medya araçlarından farklı olarak bilginin üretimine imkân sağlayan web 2.0 teknolojilerinin getirdiği yenilikler bireyi ve toplumsal grupları da bilgi üretimi açısından merkezi bir konuma yerleştirmiştir. Toplumsal etkileşimi sağlayan sosyal medya gibi uygulamalar web 2.0'ın ideolojik ve teknolojik temelleri üzerine yapılandırılan ve kullanıcılar tarafından oluşturulan içeriklerin aktarılmasına ve değiş tokuşuna izin vererek toplumsal ağların dijital alana taşınmasına olanak sağlamıştır (Kaplan ve Haenlein, 2010). Sosyal medyanın bu yönüyle işlevleri değerlendirildiğinde siber saldırılar açısından kamuoyunu etkilemek veya düşmanları zarara sokmak için istihbarat toplama, propaganda yayma ve psikolojik operasyonlar için verimli bir dijital alan olma özelliği sunmuştur (Lange-Ionatamishvili vd., 2015).

Bu doğrultuda Sosyal-Bilişsel Teori'nin *"Social Cognitive Theory (Bandura, 1982)"* bakış açısıyla insan failliği dijital alanda varlık kazanan sosyal ağlardan da etkilenmiştir. Söz konusu bakış açısı insan davranışını anlayabilmek için önemli bir perspektif sunmuştur. Bu yaklaşım insan failliğini çevresel ve içsel eğilimlerin bileşkesi olarak değerlendirmektedir. Bu durumda insan failliği; işlevsel ya da fenomenal bilinç ile temellendirilen özellikler sunmaktadır. Bandura'ya (2001) göre ilgili özellikler; kasıtlılık ve öngörü yoluyla failliğin zamansal genişlemesini, öz-tepkisel etkiyle öz düzenlemeyi ve kişinin yetenekleri, işleyiş kalitesi ve kişinin yaşam arayışlarının anlamı ve amacı hakkında ise özdüşünümü içermektedir.

Bu yaklaşıma göre failliğin üç modu böylelikle kişinin kendi istek ve arzusu ile istediği sonuçları elde etmesini tanımlayan doğrudan kişisel faillik, sonuçları güvence altına almak için başkalarının itibar eden vekil faillik ile toplumsal açıdan koordine edici ve başkalarına bağlı çaba yoluyla uygulanan kollektif faillik olarak sıralanmıştır. Sosyolojik bağlamda insan düşüncesi ve eylemliliğini etkilemesi bakımından etkileşim süreçlerinin anlaşılması ve dijital alanda grup davranışının incelenmesi noktasında kuramsal bir değerlendirme sunan Sosyal-Bilişsel Teori'nin (Bandura, 2009) sayıltıları doğrultusunda kuramsal açıdan risk algısını pratiğe dönüştürmüştür.

Siber Savaşların Toplumsal Boyutlarını Aramak

Siber savaşların toplumsal ilişkiler açısından belirleyici olan yönleri bilgi teknolojilerinde yaşanan gelişmelerle yakından ilişkilidir. Bireylerin

sağlık, iletişim, finans, gıda, su, elektrik ve ulaşım gibi gereksinimlerinin tamamının giderek yazılıma daha bağımlı hale gelmesi ve bu durumun büyüyen bağımlılığı siber saldırıların zararlı ve olumsuz sonuçlarını siyasi çatışma, sosyal istikrarsızlık ve diğer travmatik olayların yaşandığı zamanlarda göstermelerini sağlamaktadır (Gandi vd., 2011). Bunun yanında veri iletimini mümkün kılan internet teknolojileri üzerinden yaşanan gelişmeler ise insanları, veri tabanlarını ve işlemcileri bir ağ üzerindeki kaynaklar olarak düşündürmeye başlamış ve siber saldırılar üzerinde etkilerini gösteren diğer bir boyutu oluşturmuştur (Arquilla ve Ronfeldt, 1993). Siber saldırıların yerleşik kurumsal yapıdaki sosyal güvene zarar verme eğilimi ise siber savaşların bir başka etkisini göstermektedir (Rid, 2012).

Siber savaşların kendi içerisinde siber sızma, siber manipülasyon, siber saldırı ve siber baskın gibi farklı saldırı modları içermesi bireylerin ve toplumsal kurumların faaliyetlerini etkilemektedir (Lanzendorfer vd., 2016). Siber alanların toplum için önem arz eden işlevlerinin bulunması ve bireysel eylemler tarafından yönlendirilmesi durumunun yanı sıra sosyal sorunların pek çok kaynağı da siber uzaydan etkilenmekte ve siber uzayı etkilemektedir. Bu kapsamda siber alanların bireylerin eylemleri tarafından yönlendirilmesi ikili bir sonuç üretmektedir (Ghanea-Hercock, 2012). Siber alanlar bireyleri güçlendirmesi bağlamında önemli bir araç olma özelliği ortaya koyarken, güvenliği etkilemesi durumunda sosyal kontrolü ortaya çıkarması ve politikaların merkezileşmesine kaynaklık etmesi nedeniyle dezavantajlı bir durum oluşturmaktadır (Ghanea-Hercock, 2012). Dolayısıyla bireysel ve toplumsal eylem süreçleri siber alanda önem teşkil etmektedir. Eylemlerin sorumluluk ve toplumsal normatif boyutlara uyumluluk süreçleri siber saldırılarının sosyolojik bağlamını incelenmeyi gerekli kılmaktadır.

Siber savaşların bilgi krizine mi yoksa bilgi güvenliğine mi neden olduğu sorusuna yanıt aranırken Türkiye'de geçmiş dönemlerde yaşanan siber saldırı olayları üzerinden ilgili karşılaştırma ele alınmış, MAXQDA programı üzerinden çözümlenmiştir. Bu bağlamda çalışma kapsamında doküman inceleme tekniği üzerinden Türkiye'ye yönelik alan yazında öne çıkan siber saldırı olayları incelenmiş, birincil kaynak taraması üzerinden araştırma sorunsalı tartışılarak dikotomik kavramsal karşılaştırma çözümlenmiştir.

Birincil kaynak taraması sonrasında Türkiye'ye yönelik gerçekleştiği ifade edilen siber saldırıların içerik analizi gerçekleştirilmiştir. Bu kapsamda farklı kategorileri ortaya çıkaran siber saldırı örnekleri aşağıda paylaşılmıştır. İlgili metin içeriklerinde ifade edilen alıntılar üzerinden siber

savaşların kavramsal inceleme süreçleri MAXQDA programında tamamlanmıştır. 2023 yılı öncesinde Türkiye'ye yönelik gerçekleştirildiği belirtilen siber saldırıların; siber saldırılara ilişkin nedenler ile hedeflenen kurumların işlevleri dâhilinde temalara ayrıldıkları tespit edilmiştir.

> *...Araştırmacılar, devlet destekli bir Orta Doğu bilgisayar korsanlığı grubunun Pakistan, Rusya, Suudi Arabistan, Türkiye ve Kuzey Amerika'da bulunan telekomünikasyon şirketlerini, devlet büyükelçiliklerini ve Rus petrol şirketini hedef aldığını bildirdi (Kod-3; Center For Strategic & International Studies, Aralık 2018).*
>
> *...2008'de Bakü-Tiflis-Ceyhan boru hattına siber saldırı sonrası patlama meydana gelmesi (Kod-7; Şenol, 2017).*
>
> *...İranlı bilgisayar korsanları, Türkiye'nin 81 ilinin 44'ünde 40 milyon insanı etkileyen 12 saatlik büyük bir elektrik kesintisi başlattı. İstanbul ve Ankara da elektrik kesintisi yaşayan yerler arasında yer aldı (Kod-6; Observer, Mart 2015).*

Siber saldırıların toplumsal kurumları hedef aldığı, saldırıların ise kamu kurumları ile telekomünikasyon firmaları, enerji, finans ve ulaşım sektörleri gibi alanda devam eden hizmetleri etkiledikleri ifade edilmiştir. Siber saldırıların toplumsal gereksinimleri karşılayan alanlara yönelik gerçekleştirildiği anlaşılmıştır. Bu bağlamda siber saldırılarının toplumun gereksinimleri üzerinden bilgi krizini hedefledikleri görülmektedir.

> *...Güvenlik araştırmacıları, İsrail, Suudi Arabistan, ABD, Almanya, Ürdün ve Türkiye'de hükümet kurumlarını, savunma şirketlerini, BT firmalarını ve daha fazlasını hedef almak için mızraklı kimlik avı ve sulama deliği saldırıları kullanan, 2013'ten beri faaliyet gösteren İran bağlantılı bir siber casusluk grubunu ortaya çıkardı (Kod-4; Center For Strategic & International Studies, Temmuz 2017).*
>
> *...Türkiye'nin internetteki imzası olan ".tr" ile biten bütün internet sitelerini etkileyen, tabiri yerindeyse .tr uzantılı sitelerin karargahı olan merkezin tek elden saldırıya uğraması şeklinde gerçekleşti (Kod-13; BBC News Türkçe, Aralık 2015).*
>
> *...2009'da zararlı bir yazılımın Atatürk Havalimanı bilgisayarlarını etkilemesi (Kod-8; Şenol, 2017).*
>
> *...Şüpheli İran hackerleri devlet kurumları, telekomünikasyon operatörlerini siber casusluk kampanyasının parçası olarak*

hedef aldı (Kod-1; Center For Strategic & International Studies, Ekim 2020).

Siber saldırıların hedef alınan toplumsal kurumlar dışında hangi siber saldırı tekniklerin kullanıldığı da bazı metinlerde ifade edilmiştir. Örneğin mızraklı kimlik avı ve sulama deliği gibi siber saldırı çeşitlerinin kullanıldığı, zararlı yazılımlar üzerinden kurumların siber saldırılara maruz kaldıkları belirtilmiştir.

...2016'da Sağlık Bakanlığı hastanelerine yönelik siber saldırılar ile veri tabanındaki bilgilerin çalınması ve silinmesi (Kod-12; Şenol, 2017).

...2015'te, 10 gün süreli saldırılar sonucu birçok banka, noter ve devlet kurumunun internet sitesine ve mobil uygulamalara erişim sağlanamaması (Kod-11; Şenol, 2017).

...Doğu Avrupa'daki bilgisayar korsanları, büyük bir siber casusluk kampanyasında ABD, İspanya, Fransa, İtalya, Almanya, Türkiye ve Polonya'daki enerji sektörlerini hedef aldı (Kod-5; Center For Strategic & International Studies, Temmuz 2014).

...2011'de saldırılar sonrasında Telekomünikasyon İletişim Başkanlığı'nın sitesinin devre dışı kalması (Kod-9; Şenol, 2017).

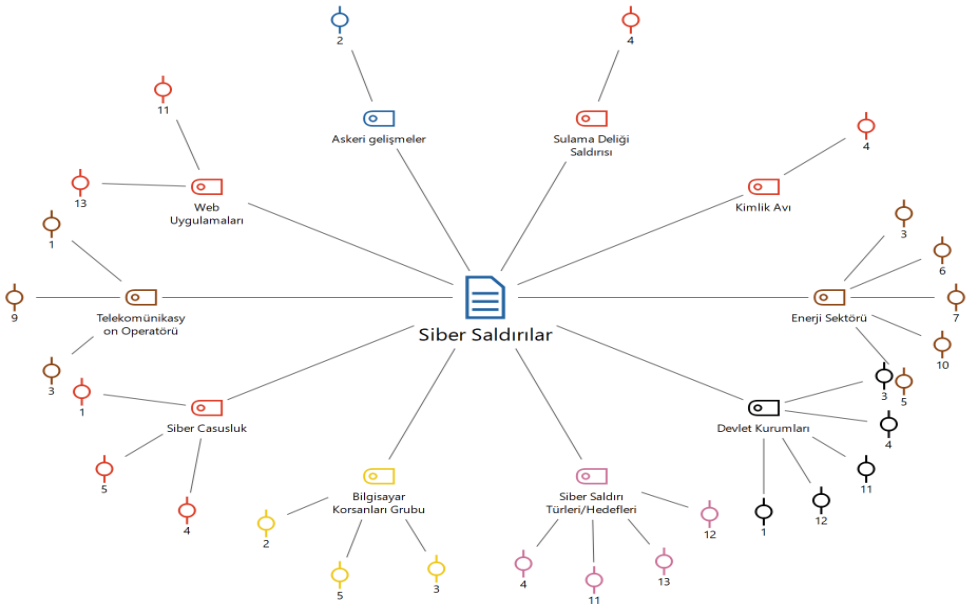
... Yunan bilgisayar korsanları, Ermenistan'ı desteklemek için Türk Parlamentosu'nun ve Azerbaycan hükümetinin 150 web sitesini hedef aldı (Kod-2; Center For Strategic & International Studies, Ekim 2020).

Gerçekleştirilen siber saldırılar sonucunda verilerin zarar gördüğü ve kurum hizmetlerine erişim sağlanması noktasında sorunlar yaşandığı belirtilmiştir. Siber saldırı hedeflerinin siber casusluk ve web uygulamalarını hedeflediği de belirtilen diğer içerikler arasında yer almaktadır. Siber saldırıların bilgi sistemlerinin güveliğini hedef alarak kurumsal faaliyetlere erişme ve ilgili faaliyetlerin erişim süreçlerinde aksamalara neden oldukları aktarılmıştır. Ayrıca siber saldırıların bilgisayar korsanları tarafından yaşanan gelişmelere bağlı olarak gerçekleştirildiği ve kurumsal hizmetlerle ilişkilendirildiği tespit edilmiştir. Bu nedenle kurumsal bilgi güvenliğinin sağlanmasının siber tehlikelerinin önlenmesi açısından önemli bir zorunluluk olduğu ortaya çıkarılmıştır.

Alan yazında birincil kaynak taraması gerçekleştirilmesi sonrasında Türkiye'ye yönelik siber saldırı içeriklerinin MAXQDA programında içerik analizine tabi tutulmasının ardından elde edilen kategoriler ise Şekil 1'de

gösterilmiştir. Siber saldırı içeriklerinin önemli bir kısmı devlet kurumları, enerji sektörü ve telekomünikasyon firmalarını hedeflemektedir. Ayrıca siber saldırılar bilgi sistemlerine zarar verme ve ilgili hizmetlerde aksamalara sebep olma gibi amaçlarla gerçekleştirilmektedir.

Siber saldırıların bilgisayar korsanları tarafından yapıldığı ifade edilerek devlet dışı aktörlerin sürecin parçası olduğu anlaşılmaktadır. Diğer taraftan askerî gelişmeler olarak ifade edilebilecek süreçlerin yaşanması, siber saldırı yaşanması sürecini etkilediği ve toplumsal alanı ilgilendiren diğer kurumların da siber tehditlere maruz kalma olasılığını artırdığı anlaşılmaktadır. Bu çerçevede toplumsal kurumların dışarıdan gelebilecek siber saldırılara yönelik bilgi güvenliğini sağlamalarının siber saldırıların önlenmesi açısından önem teşkil ettiği belirlenmiştir.



Şekil 1. Türkiye'ye Yönelik Gerçekleştirildiği Belirtilen Siber Saldırı İçerikleri Kapsamında Belirlenen Kategori ve Kod Şeması

Geçmiş dönemlerde öne çıkan siber saldırılar göz önünde bulundurularak birincil kaynak taraması sonucunda kamu kurumları ile toplum açısından öne çıkan iletişim, finans ve enerji gibi alanların siber

saldırılara maruz kaldığı anlaşılmıştır. Bu çerçevede ilgili sektörler üzerinden görüleceği üzere siber saldırıların bilgi sistemlerini hedef aldıkları ve bilgi krizine sebep oldukları görülmektedir. Bununla birlikte önem arz eden toplumsal gelişmelerin yaşanması durumunda toplumsal kurumlar da siber saldırıların hedefi olabilmektedir. Siber saldırılar açısından bilgi güvenliğine yönelik tedbirlerin öne çıktığı, siber saldırıların etkileri itibariyle kurumları ve bireyleri kapsadığı anlaşılmaktadır. Geçmiş dönemlerde yaşanan siber saldırı örnekleri siber saldırıların gerçekleşme zamanı ve hedeflediği kurumların işlevi üzerinden söz konusu sonucu serimlemektedir.

TARTIŞMA VE SONUÇ

Günümüzde olası risklere maruz kalan kavramlardan birisi de bilgisayar sistemlerinde üretilen, kullanılan ve paylaşılan bilgilerdir. Uluslararası toplum düzleminde değişen güç dengelerine kaynak olarak kullanılabilecek bilgilerin nasıl elde edilmesi gerektiği problemini düzenlemek temel bir meseledir. Bilginin parçalı ve kırılgan yapısı bir yandan elde edilme sürecine işaret ederken diğer taraftan üretiminde kullanılan usulün yöntemini akıllara getirmektedir. Bu bağlamda özne olarak devletlerin kendi yurttaşlarının kişisel verileri ile kamuya ilişkin önem içerikli verileri ulusal güvenlik nezdinde iç ya da dış tehditlere karşı koruması modern dünyanın öncelikli konuları arasında yer almakta, güvenliğe ilişkin genişleyen yeni anlayışlar bireyi ve toplumu kapsayan her alanda var olan tehditleri güvenliğin parçası haline getirmektedir. Bu bağlamda bahse konu çalışmada siber savaşların ortaya çıkış gerekçeleri incelenerek sosyolojik açıdan bilgi krizine mi yoksa bilgi güvenliğine mi neden olduğu sorusuna yanıt aranmıştır.

Bilginin kullanımına ilişkin eleştirilerin işlendiği post-modern tartışmaların ötesinde toplumsal yaşamı ve iletişimi düzenleyen, organize eden aynı zamanda toplumsal ilişkilere yönelik ağların kurulduğu devasa bilgi sistemleri dönemini yaşadığımız toplumsal bir alanda yaşamaktayız. Bununla birlikte dışarıdan ya da içeriden gelebilecek tehditler ile sistemsel açıdan yaşanabilecek sorunlara maruz kalabilen bilgi ise üretimi, kullanımı ve diğer aktörler ile paylaşımı açısından teknik kurallara bağlanması gereken bir süreci içermektedir. Ancak uluslararası düzlemde sınırları belli olmayan riskler bilgi ve bilginin güvenliği kavramı ile bilginin tehdit edilmesi durumlarını da etkilemekte, yeri geldiği zaman bilgiyi savaşların nesnesi haline getirebilmektedir. Tehdidin neredeyse her gün değişikliğe uğradığı günümüzde tehditlere karşı alınacak tedbirlerin de dinamik olması gerekmektedir, bu durum siber tehditleri farklılaştırarak sürekli takip ve izlemeyi gerektirmektedir (Bıçakçı, 2012).

Uluslararası alanda sadece teknoloji ve bilgi üretimi açısından değil aynı zamanda toplumsal yaşamı etkileyen pek çok gelişme de yaşanmaktadır. Bu durum toplumların güvenliğine ilişkin hususları ön plana çıkarmakta, eleştirel güvenlik çalışmaları toplumsal aktörlerin ve diğer kurumların konumundan kaynaklı riskleri ve konumlarını da tartışmaya açmaktadır. Bu bağlamda modernitenin oluşturduğu paradokslara vurgu yaparak güvenlik olgusunu yorumlayan eleştirel kuram, geleneksel güvenlik anlayışının temel argümanlarına karşı ileri sürülmüştür (Sandıklı ve Emeklier, 2012). Bu nedenle geleneksel savaş biçimlerinin aksine her alanda ortaya çıkan yeni risk ve tehditler bireyi, toplumu ve devletleri etkilemektedir. Dolayısıyla siber tehditler sadece askerî alanda değil, aynı zamanda toplumsal alanda da güvenliğin parçası haline gelmektedir.

Bu çalışma, eleştirel paradigmanın varsayımları altında güvenliğin genişleyen yapısını ve önemini bilgi ve bilginin güvenliği alanında ifade etmekten öte sosyolojik bakış açısıyla toplumsal ağların dijital ile buluştuğu süreçte fırsat ve risklerin güvenliğin parçası haline geldiğini ortaya çıkarmıştır. Toplumsal alanı siber savaş ile buluşturan gerçeklik ise bireyin özne olarak davranışlarından sorumlu olmasına karşın dijital alanda siber risklerin ürettiği failliğin toplumsal alanda yaşanan gelişmelerle birlikte genişlemesi ve bireyler ile toplumu etkilemesidir.

Araştırmanın temelde savladığı gerçeklik toplumsal alanda üretilen değer, fikir ve normların bireyi etkileyecek ağlar üzerinden aktarılma imkânının siber savaş açısından artan önemidir. Bu durum sosyolojik bağlamda özne konumunda olan bireyi ve toplumsal kurumları etkilemektedir. Dolayısıyla siber alanda güvenliğin birey ve toplum için de öne çıktığı bir toplumsal gerçeklikten bahsederken güvenliğin referans nesnesi genişlemektedir. Bu genişleme sadece aktör düzeyinde değil, bilgi üreten ve anlamlandıran özne boyutunda da anlam kazanmaktadır.

Bu bağlamda eleştirel güvenlik çalışmalarında Aberystwyth ekolünün varsayımları, siber güvenlik açısından devletin baskın rolünün yadsınamaz olduğu ancak bilgi güvenliği ilkelerinin toplumsala yayılarak bireyler ve diğer aktörler tarafından öneminin giderek belirginleşmesinin önemli bir gereksinim olduğunu ortaya çıkarmaktadır. Toplumsal süreçlerin sadece teorik düzlemde değil, siber saldırılar üzerinden güvenlik kavramının kapsamını genişlet(il)miş olması var olan riskler üzerinden bireyi, toplumu ve devletleri etkilemektedir. Dolayısıyla eleştirel güvenlik çalışmaları açısından siber savaşların devlet merkezli olduğu ancak siber tehditlerin birey ve toplumu da etkilediği gerçeğinden yola çıkmak ve bu durumu öncelemek önemli bir zorunluluk olarak ortaya çıkmaktadır. Güvenliğin referans nesnesi olarak bilgi ve bilginin güvenliğini sağlamak ise her alanda

olduğu gibi toplumsal alanda da önem teşkil etmektedir. Siber saldırıların toplumsal etki alanını keşfetmek ise üretilen bilginin topluma dönük sonuçlarını tahmin edebilmeyi zorunlu hale getirmektedir. Bu durum bilgi ve güvenliğini olası siber saldırıların hem bileşeni hem de aracı haline getirebilmektedir.

Türk kamu yönetiminin siber saldırılara karşı sunduğu çözümleri araştıran Güven (2022) siber tehditlere yönelik yeterli çözümlerin getirilmediği, siber güvenlik algısı ile farkındalığının istenilen düzeyde olmadığını belirtmiştir. Bu kapsamda siber güvenliğe yönelik farkındalığı ise; toplumu ve devleti korumak, siber saldırı kaynaklarını, siber tehditleri ve devlete ait sistemlerdeki zayıflıkları/açıklıkları tespit etmek, zayıflıklara/açıklıklara ve siber saldırılara uygun çözümlerle tepki vermek olarak sıralamıştır (Güven, 2022).

Bu kapsamda siber saldırılara ilişkin nitel araştırma sonucunda elde edilen kategorik boyutlardan da anlaşılacağı üzere kamusal alanda gerekli tedbirlerin alınmaması toplumsal açıdan bilgi krizine neden olabilmektedir, öte yandan bilgi krizinin yaşanmaması açısından toplumsal alanda öne çıkan ve sosyal sorunların kaynağı olan risklerin çözümlenmesi ise bilgi güvenliği süreçlerini öncelemesi ve riskleri toplumsal gelişmeler üzerinden anlamanın öneminin zorunluluk olduğunu ortaya çıkarmaktadır.

KAYNAKÇA

Acılar, A. (2009). İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü. Organizasyon ve Yönetim Bilimleri Dergisi, 1(1), 34-46.

Akdemir, İ. O., & Arslan, A. (2020). Yeni Güvenlik Epistemolojisi ve Çevresel Güvenlik Paradigması. Global Ecologıcal Securıty Küresel Ekolojik Güvenlik Uluslararası Sempozyum, Ed. Nesrin ALGAN, Duygu ÖZEL DEMİRALP, Feza Sencer ÇÖRTOĞLU, Ankara: Ankara Üniversitesi Yayınları.

Akgül-Açıkmeşe, S. (2011). Algı mı, Söylem mi? Kopenhag Okulu ve Yeni Klasik Gerçekçilikte Güvenlik Tehditleri. Uluslararası İlişkiler Dergisi, 8(30), 43-73.

Arquilla, J. & Ronfeldt, D. (1993). Cyberwar is Coming!, Comparative Strategy, 12(2), 141–165.

Arslanel, M. N. & Eryücel, E. (2012). Modern Devlet Anlayışının Felsefi Temelleri. Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 15 (2), 1-20.

Balzacq, T. (2009). Constructivism and securitization studies. In The Routledge handbook of security studies (pp. 72-88). Routledge.

Bandura, A. (2001). Social cognitive theory: An agentic perspective. Annual review of psychology, 52(1), 1-26.

Bandura, A. (2009). Social cognitive theory of mass communication. In Media effects (pp. 110-140). Routledge.

Baykara, M., Daş, R., & Karadoğan, İ. (2013, May). Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. In 1st International Symposium on Digital Forensics and Security (ISDFS'13) (Vol. 20, p. 21).

Baysal, B., & Lüleci, Ç. (2015). Kopenhag okulu ve güvenlikleştirme teorisi. Güvenlik Stratejileri Dergisi, 11(22), 61-96.

BBC News Türkçe (2015). Türkiye'ye siber saldırının 10 günü: Ne oldu?, https://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan adresinden alınmıştır.

Behrent, M. C. (2013). Foucault and technology. History and Technology, 29(1), 54–104.

Bıçakcı, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. Uluslararası İlişkiler Dergisi, Özel Sayı:

Türkiye'nin Üyeliğinin 60. Yılında NATO: Değişim, Dönüşüm, Süreklilik, 205-226.

Bilgin, P. (2010). Güvenlik çalışmalarında yeni açılımlar: Yeni güvenlik çalışmaları. SAREM Stratejik Araştırmalar Dergisi, 8(14), 69-96.

Birdişli, F. (2014). Eleştirel Güvenlik Çalışmaları Kapsamında Frankfurt Okulu ve Soğuk Savaş Sonrası Güvenlik Sorunlarına Eleştirel Bir Yaklaşım: Galler Ekolü. Güvenlik Stratejileri Dergisi, 10(20).

Booth, K. (1995), Human Wrongs and International Relations, International Affairs, 71, 103-126.

Booth, K. (2007). Theory of world security. Cambridge: Cambridge University Press.

Brauch, H. G. (2008). Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü. Uluslararası İlişkiler Dergisi, Special Issue: Security, 1-47.

Buzan, B. (1983) People, States and Fear: The National Security Problem in International Relations, University of North Carolina Press, Chapel Hill, NC.

Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). Security: A new framework for analysis. Boulder: Lynne Rienner Publishers.

Canbek, G. & Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. Politeknik Dergisi, 9 (3), 165-174.

Carr, J. (2012). Inside cyber warfare: Mapping the cyber underworld. " O'Reilly Media, Inc.".

Cavelty, M. D. (2018). Cybersecurity research meets science and technology studies. Politics and Governance, 6(2), 22-30.

Center For Strategic & International Studies (2023). Significant Cyber Incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents adresinden alınmıştır.

Clarke, R. A., & Knake, R. K. (2014). Cyber war. Old Saybrook: Tantor Media, Incorporated.

Çapar B. (2003). Bilgi Yönetimi: Nasıl Bir İnsan Gücü?, T. Büyükakın ve F. Büyükakın (Ed.) II. Ulusal Bilgi, Ekonomi Ve Yönetim Kongresi Bildiriler Kitabı İçinde (Ss. 421-432). İstanbul: Beta.

Denning, D. E., & Denning, P. J. (1979). Data security. ACM computing surveys (CSUR), 11(3), 227-249.

Emeklier, B. (2011). Thomas Hobbes ve John Locke'un Güvenlik Anlayışlarının Karşılaştırmalı Bir Analizi. Güvenlik Stratejileri Dergisi, 7 (13), 99-123.

Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir? Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11(4), 1-15.

Faleg, G. (2012). Between knowledge and power: epistemic communities and the emergence of security sector reform in the EU security architecture. European Security, 21(2), 161-184.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40.

Fierke, K. M. (2010). Critical theory, security, and emancipation. In Oxford Research Encyclopedia of International Studies.

Foucault, M. (1981). The history of sexuality (Vol. 1). Harmondsworth: Penguin.

Freiburger, T., & Crane, J. S. (2008). A Systematic Examination of Terrorist Use of the Internet. International Journal of Cyber Criminology, 2(1).

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. IEEE Technology and Society Magazine, 30(1), 28-38.

Ghanea-Hercock, R. (2012). Why cyber security is hard. Georgetown Journal of International Affairs, 81-89.

Green, J. A. (2015). Cyber Warfare A Multidisciplinary Analyses. New York:Taylor & Francis.

Güngör, M. (2015). Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma. TC Kalkınma Bakanlığı Bilgi Toplumu Daire Başkanlığı, Yayın, Yayın No:2919.

Güngör, U. & Güney, O. (2017). Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği Ve Siber Savaş. *Karadeniz Araştırmaları*, 14 (55) , 131-146.

Güntay, V. (2018). Siber güvenliğin uluslararası politikada etki aracına dönüşmesi ve uluslararası aktörler. Güvenlik Stratejileri Dergisi, 14(27), 79-111.

Güven, F. (2022). Siber Saldırılar ve Türk Kamu Yönetiminin Çözümleri, Süleyman Demirel Üniversitesi, Sosyal Bilimler Enstitüsü, Isparta.

Hansen (2009), The Evolution of International Security Studies, Cambridge: Cambridge University Press.

Kaiser, R. (2015). The birth of cyberwar. Political Geography, 46, 11-20.

Kallberg, J. (2016). Strategic cyberwar theory-A foundation for designing decisive strategic cyber operations. The Cyber Defense Review, 1(1), 113-128.

Kaplan, A. M., & Haenlein, M. (2010). Users of the 26orld, unite! The challenges and opportunities of Social Media. Business horizons, 53(1), 59-68.

Kolasi, K. (2014). Eleştirel Teori ve Güvenlik: Kimin İçin Güvenlik? Der. Osman ŞEN, Emre ÇITAK, Uluslararası İlişkilerde Güvenlik Kavramı: Teorik Değerlendirmeler içinde (121-154 ss.), Ankara: Uluslararası İlişkiler Kütüphanesi.

Küçük, M. N. (2021). Göç-Güvenlik Bağlantısını Yeniden Düşünmek: Eleştirel Güvenlik Yaklaşımları, Özgürleşme ve Türkiye'deki Suriyeli Mülteciler. Uluslararası İlişkiler Dergisi, 18 (69), 3-28.

Lange-Ionatamishvili, E., Svetoka, S., & Geers, K. (2015). Strategic communications and social media in the Russia Ukraine conflict. Cyber war in perspective: Russian aggression against Ukraine, 103-111.

Lanzendorfer, Q. E., Spangler, S. C., & DeLorenzo, G. J. (2016). Information Warfare: The Challenge Of Relating Intent With Technology In Cyber Intelligence. Issues in Information Systems, 17(3), 39-47.

Lemos, R. (2002). What are the real risks of cyberterrorism. ZDNet, August, 26.

Libicki, M., & Geers, K. (2015). The Cyber War that Wasn't. Cyber war in perspective: Russian aggression against Ukraine, 49-54.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365-404.

McGraw, G. (2013). Cyber war is inevitable (unless we build security in). Journal of Strategic Studies, 36(1), 109-119.

Observer (2023). Iran Flexes Its Power by Transporting Turkey to the Stone Age, https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/ adresinden alınmıştır.

Orend, B. (2014). Fog in the fifth dimension: The ethics of cyber-war. In The ethics of information warfare (pp. 3-23). Springer, Cham.

Özdemirci, F., & Torunlar, M. (2018). Bilgi-Değişim-Siber Güvenlik-Bağımsızlık. Bilgi Yönetimi, 1(1), 78-83.

Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. Procedia Computer Science, 48, 204-209.

Rid, T. (2012). Cyber war will not take place. Journal of strategic studies, 35(1), 5-32.

Rid, T. (2012). Cyber war will not take place. Journal of strategic studies, 35(1), 5-32.

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. Computers & security, 49, 70-94.

Rosenfield, D. K. (2009). Rethinking cyber war. Critical Review, 21(1), 77-90.

Rumelili, B., & Karadağ, S. (2017). Göç ve güvenlik: Eleştirel yaklaşımlar. Toplum ve Bilim, 140, 69-92.

Sandıklı, A., & Emeklier, B. (2012). Güvenlik Yaklaşımlarında Değişim ve Dönüşüm. Ed. Atilla SANDIKLI, Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri, İstanbul: Bilgesam Yayınları.

Sezgin, K. & Kaya, S. (2008). Uluslararası İlişkilerde Konstrüktivist Yaklaşımlar. Ankara Üniversitesi SBF Dergisi, 63 (03), 83-111.

Şenol, M. (2017). Türkiye'de Siber Saldırılara Karşı Caydırıcılık. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 3(2), 1-9.

Tabansky, L. (2011). Basic concepts in cyber warfare. Military and Strategic Affairs, 3(1), 75-92.

Taddeo, M. (2012). Information warfare: A philosophical perspective. Philosophy & Technology, 25(1), 105-120.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. KSÜ Doğa Bilimleri Dergisi, 11(1) , 132-137.

Topcu, N. (2021). Siber Güvenlik: Tehditler ve Çözüm Yolları. Cyberpolitik Journal, 6(12), 155-181.

Türkay, Ş. (2013). Siber Savaş Hukuku Ve Uygulanma Sorunsalı. Journal of Istanbul University Law Faculty, 71(1), 1177-1227.

Varlık, A. B. (2013). Savaşı tanımlamak: Terminolojik bir yaklaşım. Avrasya Terim Dergisi, 1(2), 114-129.

Vatis, M. A. (2001). Cyber-attacks during the war on terrorism: A predictive analysis. Dartmouth Coll Hanover Nh Inst for Security.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & security, 38, 97-102.

Vural, Y. & Sağıroğlu, Ş. (2013). Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23(2), 507-522.

Wallerstein, I. (2013). Bilginin Belirsizlikleri. İstanbul: Sümer Yayıncılık.

Wang, C., Wang, Q., Ren, K., & Lou, W. (2010, March). Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, 2010 Proceedings IEEE INFOCOM, 2010, pp. 1-9.

Whetham, D. (2016). Cyber Chevauchees: Cyber war can happen. In Binary Bullets: The Ethics of Cyberwar. Oxford University Press.

Woods, D. W., & Weinkle, J. (2020). Insurance definitions of cyber war. The Geneva Papers on Risk and Insurance-Issues and Practice, 45(4), 639-656.

Wright, Q. (1942). A study of war. 2 Vols. University of Chicago Press.

Yavuz, B. (2009). Ken BOOTH, Critical Security Studies and World Politics. Uluslararası İlişkiler Dergisi, 6 (21), 139-145.

Yayla, M. (2013). Hukuki bir terim olarak siber savaş. Türkiye Barolar Birliği Dergisi, 104, 177-202.

Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos. In Nebraska symposium on motivation. University of Nebraska press.

EXTENDED SUMMARY

Introduction

The focus of this study is the concept of cyberwarfare, which is shaped by information obtained from illegitimate ways. While the institutional and individual effects of this concept reveal security expectations, the requirements related to information security, which is at its center, affect the social actors. For this reason, cyberwarfare reveals an important theme in the social field and opens the door to sociological determinations.

We can list the narrowed framework of the research as searching for social dimensions that affect and activate cyber warfare as a national security problem and discussing the roles of state and non-state actors in the context of security. In this context, studies and sources related to the field were examined through the document analysis technique within the scope of the study. The dual conceptual comparison (information security or information crisis), which was put forward as a research problem, was resolved through the primary literature review. An answer to the research problem was sought in line with the critical paradigm. It is expected that the study will provide important outputs to portray the current reality in this field.

Information and Security

It is useful to express the processes that knowledge goes through before it is diagnosed on a social level in a hierarchical structure. It is necessary to consider the development process of knowledge in stages such as planning, decision making, comparison, analysis, evaluation, and estimation (Çapar, 2003; Güngör and Güney, 2017). Social change dynamics also play an important role in the development of knowledge. Information has become commodified with the influence of ideas and technology in the last century. Therefore, the evaluation of information as a power for individuals, companies, institutions, and states has also increased security problems in today's world (Eminağaoğlu and Gökşen, 2009).

Wallerstein (2013) emphasized that individuals and institutions are in conflict in the struggle for the control of information resources (Wallerstein, 2013; Özdemirci & Torunlar, 2018). In this context, information has come to a different position beyond its purpose of use and its storage over computer systems. The concepts of information and security have come to the fore outside of the production, storage, and processing of information.

Cyber Warfare

Wars, which changed form due to scientific and technological advances and social changes, have influenced political and military power struggles in the modern world. The Enlightenment's motto of progress and order, which makes instrumental reason functional, has created the opposite result in terms of power struggles and deepened social conflict. The pursuit of political struggle by modern societies over the reality of nation-states and industrial organizations has historically brought along new conflicts in this process. Traditional wars have changed shape after the experience of world wars in which great destruction was experienced. Wars have continued to be a tool of power struggles with their new appearances.

It has been discussed that cyberwars, which are shown among the forms of war, cannot be evaluated like traditional wars, and the differences in their content and nature are explained by comparing them with traditional wars. Cyberattacks are carried out with the aim of damaging data and data sets as well as physical infrastructure. Cyber-attacks (Lemos, 2002) appear to aim to steal and corrupt information or deny legitimate electronic services to legitimate users. It also seeks to disable or undermine the controls of computer systems that manage physical infrastructure such as water supplies, power lines and railways. Cyber-attacks offer a productive digital space for intelligence gathering, propagation, and psychological operations aimed at influencing public opinion or harming enemies (Lange-Ionatamishvili et al., 2015).

In this context, it is important to understand symbolic interaction to study group behavior (Bandura, 2009). Social Learning Theory explains how violence gains importance as a strategy in society. The theory argues that individuals learn deviant behaviors from other social groups. From the perspective of Social Cognitive Theory, human agency offers an important perspective for understanding human behavior. This approach considers human action as a combination of environmental and internal trends. In this case, human agency presents features based on functional or phenomenal consciousness. Zimbardo (1969) stated that the themes expressing the loss of control of behavior towards individuality are anonymity, deindividuation, dehumanization, and control.

Five principles regarding the administrative management of the public were identified by Dwight Waldo (1948). From this point of view, Kallberg et al. (2013) have made cyberattacks solvable through institutional weaknesses. Thus, the different aspects of cyber-attacks from traditional wars have been eliminated, and cyberattacks have been evaluated from a corporate perspective. The effectiveness of the institutional structure is

important in estimating the systematic damage to the target nation of the cyberattack or in estimating and evaluating the possible effects of the cyberattack on a nation.

Looking for the Social Dimensions of Cyber Warfare

After the primary literature review was carried out, the contents of the cyberattacks against Turkey were analyzed in the MAXQDA program. A significant portion of cyberattack content targets government agencies, the energy sector, and telecommunications companies. In addition, cyberattacks are carried out for purposes such as damaging information systems and causing disruptions in related services. It is stated that cyberattacks are made by hackers. It is understood that other actors other than the public are part of the process. On the other hand, the occurrence of military developments affects the realization of cyberattacks and puts the information security of other institutions that concern the social field in an important position.

It has been understood that cyberattacks target institutional contents and affect society and individuals through needs such as communication and energy, which are prominent in terms of society. It is seen that cyberattacks target information systems and highlight the information crisis. However, in the case of developments that may be important on the public level, social institutions may be the target of cyberattacks. Therefore, it is determined that the measures for information security are also of interest to institutions and individuals. Cyberattacks experienced in the past have revealed the information in question through the time of the cyberattacks and the function of the targeted institutions.

Conclusion

Expanding the scope of the concept of security through cyberattacks affects the individual, society, and states through existing risks. Therefore, in terms of critical security studies, it is necessary to start from the fact that cyber wars are state-centered, but cyber threats also affect individuals and society. In addition, paying attention to this situation is a necessity. As the reference object of security, ensuring the security of information is important in the social field as well as in every other field.

In this context, failure to take the necessary precautions regarding cyber-attacks causes an information crisis for society. On the other hand, in order not to experience an information crisis, situations that come to the fore

in the social field and are likely to be the source of social problems should be evaluated within the scope of information security. It has been determined that it is necessary to ensure information security in order not to experience an information crisis.