NOVUS ORBIS

Siyaset Bilimi ve Uluslararası İlişkiler Dergisi
Journal of Politics and International Relations

Department of International Relations
Uluslararası İlişkiler Bölümü

Cilt 1 | Sayı 2 | 2019
Volume 1 | Number 2 | 2019

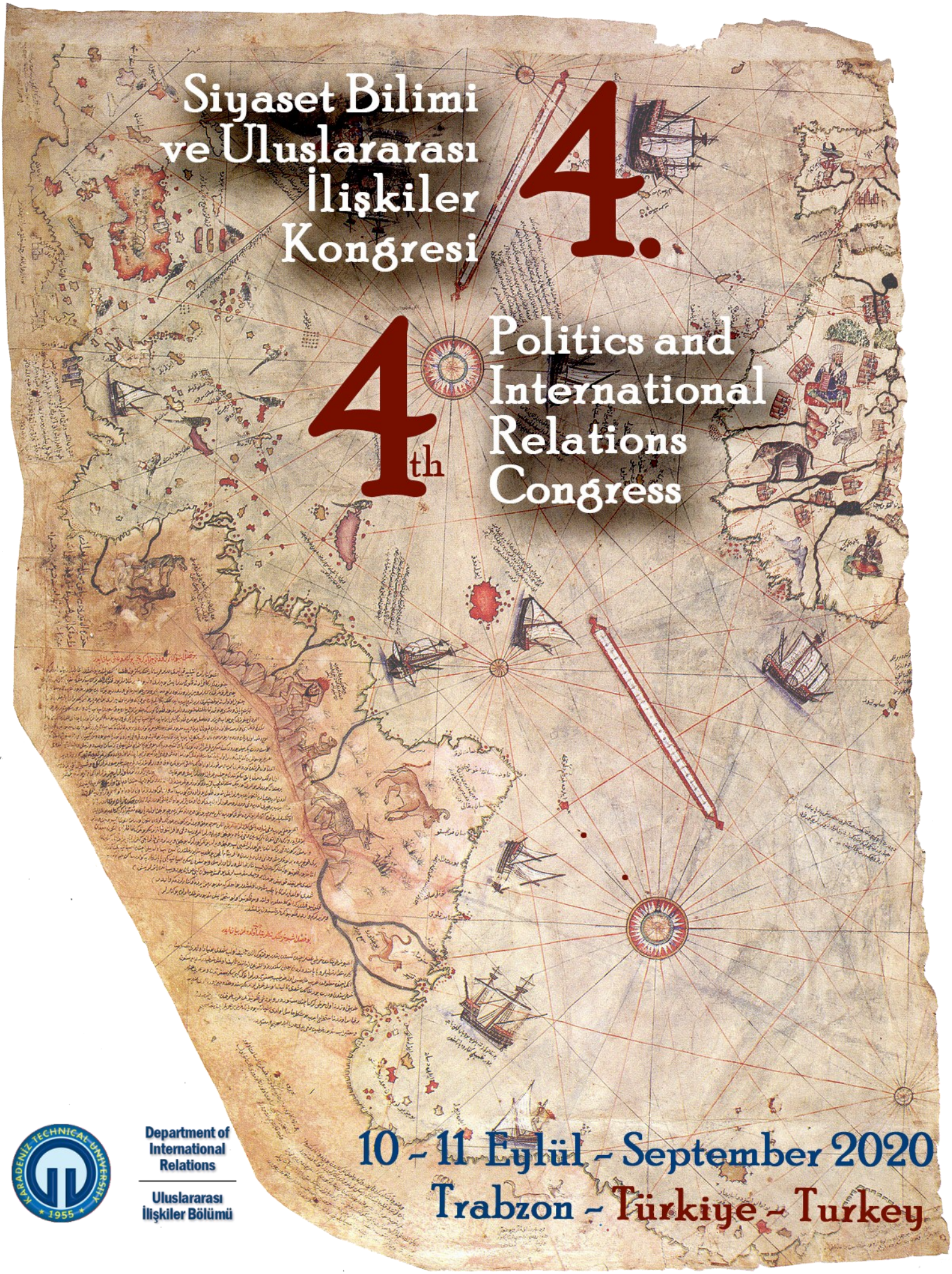
Editörler Kurulu / Editorial Board

Novus Orbis
Siyaset Bilimi ve Uluslararası İlişkiler Dergisi
Journal of Politics and International Relations

Cilt 1 | Sayı 2 | 2019
Volume 1 | Number 2 | 2019

İçindekiler / Table of Contents

Araştırma Makaleleri / Research Articles



KARADENİZ TECHNICAL UNIVERSITY 1955

Department of International Relations

Uluslararası İlişkiler Bölümü

NOVUS ORBIS
Journal of Politics and International Relations
Siyaset Bilimi ve Uluslararası İlişkiler Dergisi
Volume 1 ▪ Number 2 ▪ 2019

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

21. Yüzyıl Paradoksu Olarak Siber Uzay ve Uluslararası Hukuk

Vahit GÜNTAY*

Received 11 October 2019
Accepted 22 November 2019

Öz

Uluslararası ilişkiler ve güvenlik temelindeki çalışmalar teknolojik gelişmelerle birlikte farklı bir araştırma konusunu karşımıza çıkarmıştır. Teknik bir alanın ilgi odağında olan siber güvenlik politik bir temelde de tartışılmaya başlanmıştır. Siber politikalar, siber caydırıcılık ya da siber savaş gibi isimlerle tartışılmaya başlanan güvenliğin siber boyutu devletlerin de siyasi ajandalarına girmeyi başarmıştır. Uluslararası aktörlerin merkezinde olan devletlerin ilgisi siber güvenliği uluslararası hukukun inceleme alanına taşımıştır.Bu çalışma dahilinde siber güvenliğe ilişkin tarihsel süreç ve teorik yaklaşım uluslararası ilişkiler disiplini temelinde ele alınmış ve uluslararası hukuka dair sorunlar detaylandırılmaya çalışılmıştır. Çalışmanın özüne dair yaklaşım farklı verilerle de desteklenmiştir.

Anahtar Kelimeler: Uluslararası İlişkiler, Siber Güvenlik, Uluslararası Hukuk, Siber Saldırı, Siber Suç

* Dr. Öğr. Üyesi, Karadeniz Teknik Üniversitesi, Uluslararası İlişkiler Bölümü, vahitguntay@gmail.com

Cyber Space and International Law as a 21st Century Paradox

Abstract

The studies in the base of international relations and security have revealed a different research subject with the developments of technology. Cybersecurity that is in the focus of the technical area has also been argued in the political base. The cyber dimension of security with discussing concepts like cyber politics, cyber deterrence or cyberwar has succeeded to remain on the agenda of states. As a central actor of the international system, states' interest in cybersecurity has carried this subject to the international law research area. In this study, the historical process and theoretical approach have been evaluated in the base of international relations discipline and it is practised to detail problems about international law. Different data have also supported the approach to the core of this study.

Keywords: International Relations, Cybersecurity, International Law, Cyberattack, Cybercrime

Giriş[1]

Siber uzay gelişen dünyanın teknolojik alandaki bütünlüğünü ifade eder. Bu bütünlük yeni bir çatışma düzeyini beraberinde getirmiştir. Uluslararası ilişkiler çalışmalarında da kendisine yer bulan siber güvenlik her geçen gün önemini artırmaktadır. Uzunca bir süredir psikolojik ve felsefi yönlerinin de tartışıldığı siber alan sosyal bilimler içinde güncel bir çalışma alanı gibi görünse de derin bir geçmişe sahiptir.

Siber güvenlik, uluslararası ilişkilerin çalışma düzlemlerinden olan güvenlik temelinde kendine yer bulmaktadır ve uluslararası hukuk tartışmalarında da adından söz ettirmektedir. Uluslararası aktörlerin etkileşiminin arttığı siber alanda yaşanan gelişmeler tartışmalı boyutunu her geçen gün artırmaktadır. Devletlerin ana aktör olarak yer aldığı uluslararası sistemde siber suçlara ilişkin farkındalık ve taraf olma durumu tüm bireyleri de tehdit eder hale gelmiştir.

Siber tehditlerin uluslararası ilişkilerde kapsadığı alan organizasyonel boyutuyla ve kapsadığı aktörlerle birlikte çok taraflı bir hale gelmiştir. Tarihsel gelişimi itibariyle bu sorunlar siber terörizm olgusuyla birlikte daha karmaşık bir hal almıştır. Siber tehditlerin ulaştığı boyut hukuksal bir zeminde tartışılmaya başlanmışken, fiziksel hasarlar bırakacak bir çehre alması yeni düzenlemeler gerektirmektedir. Özellikle kritik altyapıların korunmasında, devletlerarasındaki düzenlemeler ve

atılacak adımlar uluslararası hukukun temel normları içerisinde tartışılmaktadır.

Siber terörizmin desteklendiği bir ortam ise uluslararası hukuku yetersiz kılmaktadır. Soğuk Savaş'ın kendi içerisindeki düzensizliği ve çatışmacı boyutu günümüz sistemine bazı sorunlu konuları da miras bırakmıştır. Caydırma temelli yaklaşım siber saldırı ve savunma konularına ilişkin hukuksal düzenlemeleri ihtiyaç haline dönüştürmüştür. Bu dönüşümün temelinde küresel mücadeledeki karmaşıklık ve değişim etkili olmaktadır.

Çalışma dahilinde siber güvenliğin uluslararası sistemde tarihsel dönüşümüne ilişkin temel tespitler irdelenmiş ve uluslararası hukuk boyutuna dair bazı veriler sunulmuştur. Siber suçların getirmiş olduğu karışıklık ve uluslararası hukukun yetersizliği bu çalışma dahilinde tartışmaya açılan diğer bir husus olmuştur. Hukuksal güçlükler ve siber uzaydaki karmaşık algının kırılmasına dair tespitler ele alınan diğer konular arasındadır. Siber güvenliğe ilişkin antlaşmalar ve uluslararası düzenlemeler kendi boyutuyla da tartışmaya açılmıştır.

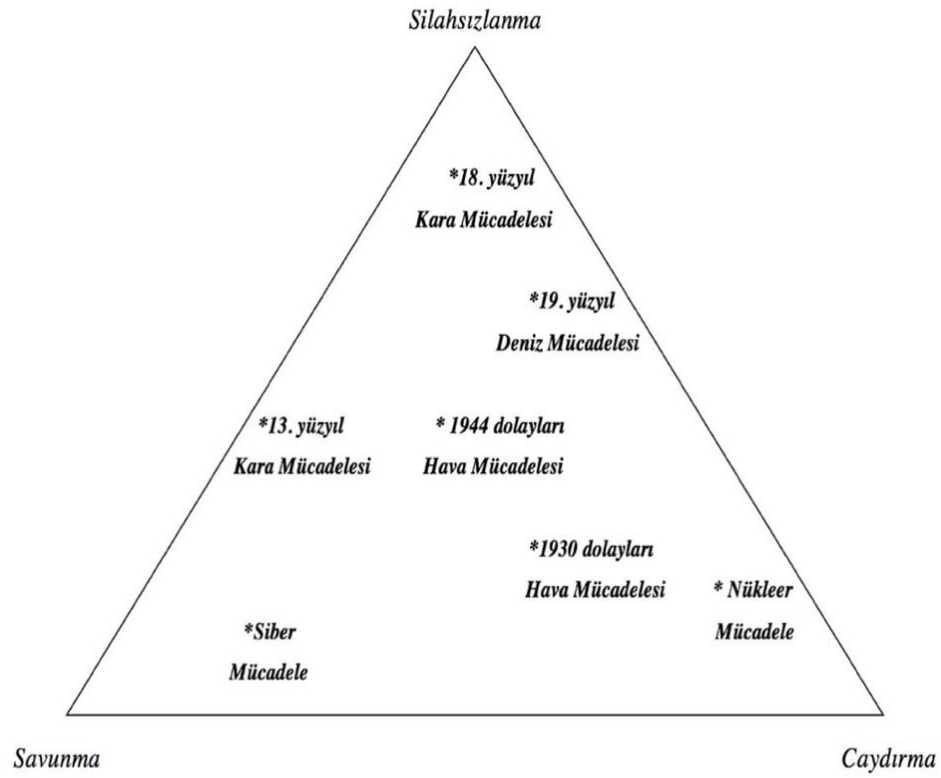
1) Siber Güvenliğin Politik Düzlemde Dönüşümü

Günümüzde savaşlar sadece askeri teknolojiler yardımıyla yapılmamaktadır. Kamu hizmetleri, ulaşım, iletişim ve enerji gibi kritik endüstrileri aksatan veya yok eden bilgisayar programları uzaktan serbest bırakılan bir müdahele ile yapılmaktadır. Böyle saldırılar ilave olarak askeri unsurların hareketlerini, savaş uçaklarının rotalarını ve savaş gemilerinin komuta kontrolünü sağlayan ağları da etkisiz hale getirebilmektedir.

Rakibini etkisiz hale getirebilme mücadele alanı arayan aktörlerin zamanla iştahlarını kabartmıştır. Bilginin ve yönetimsel olarak verilerin sahip olunmasına ilişkin arzu siber güvenlik kavramını uluslararası politika alanında daha belirgin kılmıştır. Devletler kendi içerisindeki yasal düzenlemeler gibi uluslararası alanda tüm konular üzerinde şeffaf ve adil olamamaktadır. Siber saldırıların ve terörizmin vermiş olduğu avantaj, uluslararası güvenliğe ilişkin sorunları da artırmıştır. Siber güvenlik kavramı politik bir düzlemde ilerlerken uluslararası bir boyut kazanımına ile ilgili bir soru güvenlik çalışmalarında artan bir hassasiyete sahip olmuştur. Bu sorunun temel olarak gelişiminde özgün bir tarihi arka plan da mevcuttur. Teknoloji ve sibernetiğe dair gelişmeler özellikle Soğuk Savaş dönemiyle birlikte bir devinim kazanmıştır.

Soğuk Savaş dönemindeki çekişme her alanda kendini hissettirirken gelecekle ilgili felsefi tartışmalar bu mücadelenin içinde yerini almıştır. Soğuk Savaş'ın sonra ermesi ve özellikle hegemon bir güç olarak ABD'nin siber uzay ile ilgili çalışmaları başdöndürücü bir şekilde gelişmiş ve siber politika çalışmalarının temelini oluşturmuştur.

Libicki'nin şekil 1'de ortaya koyduğu caydırma-silahsızlanma-savunma üçgeninde, yakınlıkları açısından gruplandırdığı mücadele türleri alanın gelişimini güzel bir şekilde yansıtmaktadır. Yakın dönemde özellikle siber ve nükleer mücadelenin diğer mücadele türlerinden çok daha net bir şekilde savunma ve caydırma unsurlarına yaklaştığını görmekteyiz. Siber mücadele gelişim itibariyle saldırıların bilinmezliği açısından savunma alanında paralel bir gelişmeyi sağlamıştır. Nükleer gelişmeler ise caydırıcılık olarak en uç noktada gelişimini sürdürmektedir.



Şekil 1. Mücadele Çeşitlerinin Caydırma-Silahsızlanma-Savunma Üçgeninde Duruşu (Libicki, 2009: 175).

a) Tarihsel Olarak Siber Güvenlik Kavramının Uluslararasılaşması

Savaş ve şiddetin yok edilip edilemeyeceği sorunsalı I. Dünya Savaşı'nın ardından farklı çalışmaların merkezinde yer

almıştır. Soğuk Savaş sonrası dönemin getirdiği yenilik uluslararası ilişkiler literatürü üzerinde önemli bir etkide bulunan güvenliğin doğasına dair yeni yaklaşımlar ortaya çıkarmıştır (Baylis, 2008: 71).

Özellikle savaş teknolojilerindeki gelişim ve istihbarat yapısı ile ilgili genel değişim siber güvenlik kavramına dair yaklaşımları ve uluslararası ilişkiler boyutundaki değişimi hızlandırmıştır. Son yıllarda uluslararası güvenlik konusunda farklı ve kendine özgü bir bakış açısı geliştiren normatif uluslararası ilişkiler yaklaşımlarıyla siber güvenliğe ilişkin teorik düzlem harmanlanmış ve siber güvenlik kavramının uluslararası alandaki belirginliği daha da artmıştır.[2]

Devletlerin çıkar amaçları yeni savaş ve saldırı yöntemlerini beraberinde getirmiştir. Siber Terörizm, siber saldırılar, siber caydırıcılık, siber güvenlik olarak ele alınan kavramlar uluslararası arenada farklı bir çatışma alanını ortaya çıkarmıştır. Farklı düzeylerde yapılan bu siber saldırılar maliyet açısından devletleri zorlamazken saldırıları da kimin yaptığına çoğu zaman ulaşılamamaktadır. Bu durum karar alıcıların elini güçlendirmektedir.

Nükleer caydırıcılığın aksine siber caydırıcılıkta taarruz kabiliyeti, yeri ve zamanı bilinmezken; telafi edilemez ekonomik kayıplar verdirilebilmekte ve can kaybı yaşanmamaktadır. Diğer taraftan hem saldırı hem de savunma ayağında daha etkili manevralar yapılabilmekte ve zarar en aza inebilmektedir. Fakat bu türden saldırıların veya terörizmin caydırıcılığı sadece somut olarak uygulandığında gerçekleşebilmektedir. Caydırıcılık yönünün artmasıyla siber güvenlik uluslararasılaşan bir kavram haline dönüşmüştür. Her ne kadar tartışılabildiği boyut Soğuk Savaş döneminin klasik caydırma teorileriyle açıklanamasa da süper güçlerin yükselişiyle etkisini artıran siber güvenlik kavramı II. Dünya Savaşı öncesine kadar uluslararası sistemde kendisine yer bulamamıştır (Zagare ve Kligor, 2000: 5).

Siber güvenlik kavramının uluslararası ilişkiler alanında inceleme boyutuna sahip olmasının başında caydırıcılık ve uygulama alanına ilişkin somut olayların artması gelmektedir. Siber olayların tarihsel gelişimine dair süreç özellikle siber casusluk ve siber savaşa ilişkin parametrelerin artışıyla paralellik göstermektedir. Soğuk Savaş'ın bitişi ve bu parametrelerdeki gelişimin hız hazanması daha önce vurguladığımız siber terörizm, siber savaş ve siber güvenlik gibi kavramların devletlerarası ilişkilerde incelenmesini zorunlu hale getirmiştir. Siber savaşın yönü Soğuk Savaş sonrasında aynı hızıyla devam ederken, zararlı yazılım ve siber suçlara ilişkin uluslararası çapta etki yaratması ve olayların artışı devletlerarasında iş birliğini de gerekli kılmıştır.

Siber olayların tarihsel gelişimi içerisinde güvenlik boyutuna evrilmesi, 1960 ve 1970'li yıllar boyunca tartışılan bilgi devriminin medya araçlarını ve inovasyon yönündeki unsurları etkilemesiyle alakalıdır. Kimi halk hareketlerinde ve verilerin sızdırılması amacıyla gerçekleşebilecek anlık iletişimde siber araçlar etkin bir şekilde kullanılmaktadır ve bu araçlar devletlerin yakın takiplerindedirler (Cavelty, 2008: 13). Bu takip içinde devletlerin adını tam koyamadağı ve kimi araştırmacılara göre radikalleş(tir)me aracı olarak da kullanılan internet ve medya etkileşimi yeni bir savaş aracı olarak kabul edilmektedir.[3] Özellikle toplumsal hareketlenmelerde bu durum daha da hissedilir bir hal almılştır (Hoskins ve O'Loughin, 2008: 31).

b) Soğuk Savaş Dönemi Gelişmeleri Çerçevesinde Siber Güvenlik

II. Dünya Savaşı sonrasında uluslararası sistemi tanımlamak için kullanılmış olan Soğuk Savaş kavramı iki kutuplu sistemde Batı ve Doğu Blokları arasında gerginlik ve kısmi çatışma biçiminde sürdürülen mücadele olarak karşımıza çıkmıştır. Ulusal güvenlik Soğuk Savaş dönemindeki uluslararası sistemi şekillendiren ve ulus devletler arasındaki ilişkileri düzenleyen en temel unsur olarak belirginleşmiştir.

II. Dünya Savaşı sonrasında istihbarata ilişkin teknolojik verilerin artması siber güvenliğin bu süreçte yıldızını parlatmıştır. İstihbarat sadece savaş kazanmak için gerekli görülürken sinyal ve görüntü istihbaratına ilişkin önemin farkedilmesi teknolojik arayışları siber güvenliğin uluslararası ilişkiler boyutuna itmiştir.[4] Çok kısa bir zamanda U-2 Keşif Uçakları, uzay programları, bilgisayarların en eski örnekleri ve örtülü operasyonlar ile ilgili özel vasıtaların gelişimi konusunda önemli adımlar atılmıştır (Yılmaz ve Salcan, 2008: 25).

Özellikle ABD'nin Sovyet uydusu Sputnik'e karşılık olarak ileri bilimsel ve teknolojik projeleri hayata geçirmekle görevli ARPA'yı harekete geçirmesi 1958 yılını bir milat haline getirmiştir. 1969 yılına gelindiğinde Amerika'nın önde gelen üniversite ve enstitüleri kendi aralarında bilgi alışverişi sağlamak amacıyla ABD Savunma Bakanlığı tarafından desteklenen ve o güne kadar daha çok askeri amaçlı kullanılan ARPAnet ağına katılmışlardır.[5]

1974 yılına gelindiğinde Bob Kahn ve Vint Cerf adlı bilimadamları birbirinden bağımsız ağlardaki kullanıcıların iletişim kurabilmesi ve veri gönderimi sağlayabilen devrim niteliğindeki TCP protokolünü yazmıştır. Özellikle siber

güvenliğin uluslararası alanda öneminin artması TCP'nin hızlı bir şekilde gelişmesiyle başlamıştır.

Sovyetler Birliği 1980'lerin ortalarına kadar bilgisayar teknolojilerinin tümünü KGB aracılığıyla batıdan çalmaya devam etmiştir. Sovyetler Birliği'nin bilgi alma operasyonları 1981 yılında ABD ve Fransa'nın düzenlediği ortak bir operasyonla ortaya çıkmıştır.[6] Rusya'nın özellikle günümüze kadar uzanan bölgesel siber saldırganlığı ve hegemon bir bölgesel siber güç olarak bölge ülkeleri takibi 1980'lerdeki bu tür faaliyetlerine uzanmaktadır (Hansen ve Nissenbaum, 2009: 1169).

Soğuk Savaş'ın bitimine yakın devletlerin kendi altyapılarının da ciddi bir şekilde etkilendiği Morris virüsü bilişimin karanlık boyutuna geçen bir çok yazılımcı açısından iştah kabartıcı olmuştur ve uluslararası boyut açısından siber alandaki verilerin önemine dair ciddi bir gelişme olmuştur. Dijital saldırganlık ve yakın gelecekteki süreç açısından ipuçları sunan, Soğuk Savaş sonu gelişmeleri siber güvenliğin bilgi çağında hem teknik boyutuyla adından söz ettireceğini hem de sosyal bilimler ve uluslararası ilişkiler adına yer edineceğini ortaya koymuştur.

c) Soğuk Savaş Sonrasında Uluslararası Güvenlik ve Siber Alan

II. Dünya Savaşı'nın ardından Soğuk Savaş'ın başlamasıyla birlikte yeni bir güvenlik rejimi ortaya çıkmıştır. Sıcak çatışmadan uzak kalınan bu dönemde tedirginlik ve tansiyon hep yüksek olmuştur. 1989 yılında Berlin Duvarı'nın yıkılması sonrasında 25 Aralık 1991'de Sovyetler Birliği'nin dağılmasıyla birlikte uluslararası sistem için gerilimli bu iki kutuplu dönem sona ermiştir (Bıçakçı, 2012: 206).

Sovyetler Birliği ve liderliğini yaptığı Doğu Blok'unun ortadan kalkmasıyla birlikte somut bir düşman olarak karşıtını yitiren NATO'nun meşruiyeti sorgulanmaya başlanmıştır. NATO'nun misyonunun artırılması ve ittifakın güvenlik alanının genişletilmesi için 1990 yılında Londra Konferansı'nda yeni bir strateji geliştirilmesi kararı alınmış, 1991 Roma Zirvesi ile yeni stratejik konsept geliştirilmiştir (Bayraktar, 2015: 37). Siber güvenliğe ilişkin gerek politik düzlemde, gerekse yeni adımlarla NATO kendine ciddi misyonlar edinmiştir.Birbiri ardına gelen tatbikat ve zirvelerle siber güvenlik ile ilgili her adım NATO'yu öne taşımıştır (Healey ve Jordan, 2014: 3).

Soğuk Savaş dönemi boyunca simetrik bir düşmanı bulunan ve Ortodoks güvenlik anlayışıyla hareket eden NATO, Kosova Savaşı'nda maruz kaldığı siber saldırılar neticesinde bu

anlayışını günümüze dek modernize ederek en ciddi atılımı yapan örgütlenme olmuştur. Sırasıyla 11 Eylül saldırıları ve bir NATO müttefiki olan Estonya'ya yönelik siber saldırılar NATO ve üye ülkeleri siber tehditler ve siber güvenlik konularında daha fazla ihtiyatlı olmaya yöneltmiştir (Boyraz, t.y.).

Soğuk Savaş süresince tartışılan ve uluslararası çalışmalarda önemli bir yere sahip olan konvansiyonel ve nükleer caydırıcılık yanına siber caydırıcılık kavramının eklenmesi ile devletler arasındaki yeni bir etkileşim doğmuştur. Siber caydırıcılığın da konvansiyonel ve nükleer caydırıcılık gibi işlev göreceğine ilişkin somut veriler ortaya konulmaya başlanmıştır.

Siber caydırıcılık ile ilgili somut verilerin Soğuk Savaş sonrasında etkili oluşunda askeri-stratejik ortama dair değişim etkili olmuştur. Özellikle 2010 yılı başlarına kadar konvansiyonel unsurların etkinliğini koruması ve değişkenlerin sadece bu silahların etkinliğinin artırılması üzerine kurulması finansal olarak da kaynakları bu yöne kaydırmıştır. Son yıllarda yaşanan finansal krizler daha az maliyetle caydırıcı olabilme adına siber yeteneklerin ön plana çıkarılmasını bir gereklilik halinden çıkararak zorunluluğa dönüştürmüştür.

1990-2001	*2002-2011*	*2012-2015*
Bölgesel Rekabet ve Tehditler	*Terörle Savaş/ Ayaklanmalar*	*Sürekli Gerilim/ Aşırı Şiddet*
Körfez Savaşı/Barışı Koruma Operasyonları	*Afganistan ve Irak Savaşları*	*Sürekli Savaş/Asya Pasifik'e Odak Kayması*
Çeşitli Askeri Operasyonlar	*Artan Operasyon Hızı ve Stres*	*Vekilli Savaşlar/Siber Yetenekler*
Azaltılan Finansal Kaynaklar	*Artırılan Finansal Kaynaklar*	*Azalan Finansal Kaynaklar*
Orduların İnsan Sayısının Artırılması	*Kara Kuvvetleri ve Özel Kuvvet Artışı*	*Küçülen Kuvvet Yapıları/Siber Ordular*
Teknolojiyi Entegre Etme	*Dönüşüm Kabiliyetleri*	*Dengeli Kabiliyet/Teknoloji*
Soğuk Savaş Kabiliyetinin Muhafazası	*Mevcut Kabiliyetleri İdame, Yenileme*	*Envanterden Çıkarma, Sıfırlama ve Yeni Yatırım*

Tablo 1. Soğuk Savaş Sonrası Askeri Stratejik Ortamda Değişimler (Yılmaz, 2016).

Siber yeteneklerin ön plana çıkarılması gelişmiş ülkelerle birlikte tüm ülkelerin öncelikli hedeflerinden biri haline dönüşmüştür.1990'lı yılların ortalarında Çin, Körfez Savaş'ından çıkarttığı dersler doğrultusunda kendi stratejisini

değiştiren ülkelerin başında gelmiştir ve siber etki açısından Soğuk Savaş sonrasında ciddi anlamda yükselen bir güç olmuştur. Çin ordusunu küçültüp yeni teknolojilere yatırım yapan ülkeler arasına girmiştir (Clarke ve Knake, 2011: 33). Bu gelişmelerle güvenlik ikileminin askeri döngüsü siber savaş alanına kaymaya başlamıştır.[7] İdeolojik yakınlıklar ile birlikte güçsüz ülkelerin birbirlerine olan yaklaşımının yakın gelecekte siber güvenliği canlı tutacağı ve farklı politik birliktelikleri beraberinde getireceği tartışılan hususlar arasındadır (Hare, 2010: 216).

2) Siber Alan ve Uluslararası Hukuka İlişkin Sorunlar

Uluslararası hukuk devletler arasındaki ilişkileri düzenlemeye yönelik bir ilkeler bütünü olarak ifade edilmektedir ve farklı kişi veya okulların hemen hepsinin, farklı uluslararası hukuk tanımlarına rastlamak mümkündür. Uluslararası hukukun özüne ve eksikliklerine vurgular yapılırken bu alanın siber güvenliğe dair olaylar ve gelişmeler karşısında eksik kaldığı yadsınamaz bir gerçektir.

Devletlerin temel olarak uluslararası hukuk kurallarına uymalarının çeşitli nedenleri vardır. Devletler kısmen bir alışkanlık çerçevesinde uluslararası hukuka verilen değerden dolayı, kısmen de söz konusu kuralların olmaması halinde ortaya çıkacak kaostan duydukları endişe dolayısıyla uluslararası hukuk kurallarına uymaktadırlar (Sönmezoğlu, 2000: 644). Ne olursa olsun bireyin doğal olarak kendi özünde yönetimsel anlamda kurallar bütününe ihtiyaç duyması siber uzaya ilişkin hukuksal bir yaklaşımı ve kimi zaman sorunları beraberinde getirmiştir. Bilişim suçları iç güvenlik açısından kendi içerisinde belirli sorunları ihtiva ederken siber uzaya ilişkin uluslararası hukukun eksik kaldığı noktalar farkındalık oluşturma ve belli antlaşmalarla aşılmaya çalışılmaktadır.

a) Bilişim Suçları

Kişisel verilerin hukuksuz olarak ele geçirilmesinden siber suçlara, siber terörden siber savaşa ve uluslararası bazda siber istihbarata kadar siber güvenliğe ait temalar bireyleri, toplumu ve devleti tehdit etmektedir. Geçmişte meydana gelen geleneksel güvenlik tehditlerinin ve suç korkusunun yerini siber uzayda meydana gelebilecek korkular almıştır (Yeşilyurt, 2015: 16). Farklı tehditler ve araçlar, yasa dışı faaliyetlerle birlikte farklı ve yeni bir suç grubunu oluşturmuştur.Bu gelişmelerle birlikte yasal düzenlemeler de gecikmemiştir. Yasal düzenlemeleri zorlayan unsur siber uzayın tanımlanmasına

ilişkin uluslararası toplumun yaklaşımı olmuştur (Schmitt ve Vihul, 2014: 17).

Bilişim suçu olarak isimlendirilen eylemler bilgileri otomatik olarak işleme tabi tutabilen ya da veri iletişimi sağlayabilen diğer elektronik, manyetik veya mekanik araçlarla bunları veri iletişimi için birbirine bağlayan soyut ya da somut ağlar üzerinde işlenebilmektedir (Erdağ, 2010: 279). Yasal düzenlemelerin boyutu iç ve dış güvenlik açısından sonuçlar doğurabilmektedir. Uluslararası alanda yapılan bir dizi hukuki düzenleme olsa da sınırlar arasındaki sorunlarda devletler ciddi bir koordinasyon eksikliğine sahiptir.

Bilişim suçları ülkelerin sadece iç ve dış politika çıktıları açısından sorun oluşturmamaktadır. Küresel çapta bu suçların ülkelere maliyetleri de faturayı kabartmaktadır. Verilerin kaybı ve çoğu zaman kurumların işlerliğindeki yavaşlama veya durma, bankalar üzerinden yapılan faaliyetler her bir devlet için maliyet yükü oluşturmaktadır. Bu konuda devletler tedbir olarak siber suçlara karşı anlık hareket edememekte ve maliyet her geçen gün artmaktadır.

Bilişim suçlarında maddi boyutların ciddi rakamlara ulaşmasında ve suçların uluslararası boyut kazanarak devletleri etkilemesinde siber suçlunun ya da suçluların koordineli olduğu durumlarda saldırganların amaçları, kararları ve araçları belirleyici olmaktadır. Siber suçlar açısından hedefin faaliyetlerini yavaşlatma veya durdurma, dolaylı olarak maddi zararlara sebep olan DDoS saldırılarıyla sıkça karşılaşılmaktadır.[8] Bu tarz saldırı türleri teknik bir kurgu gerektirmediğinden, saldırıların kaynağı tarafından sistemlere giriş yapma zorunluluğu bulunmamaktadır (Durcan, 2015: 325).

b) Siber Uzayda Sanal Saldırı Ağı ve Uluslararası Hukukun Yetersizliği

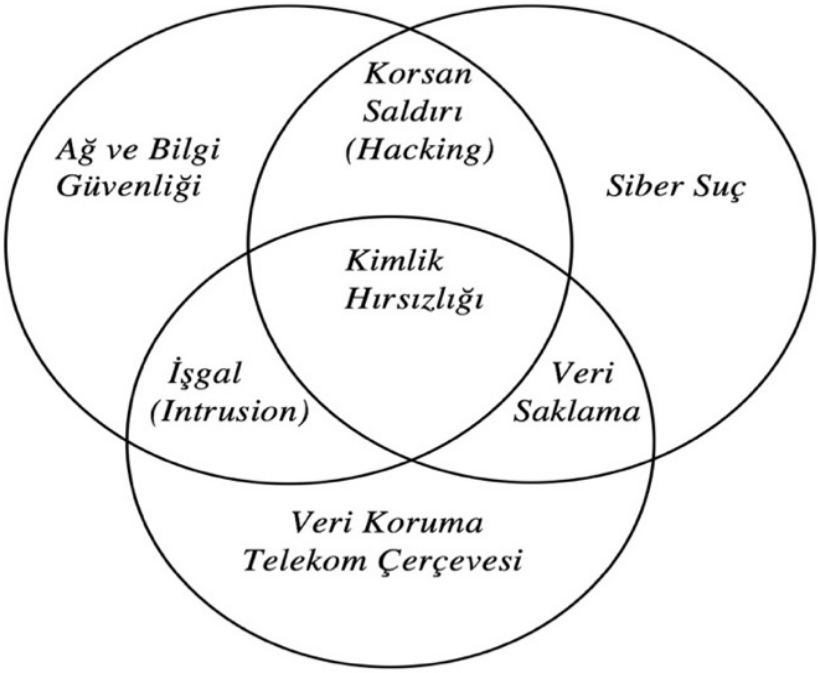
Siber savaş alanı aslında günlük hayatta kullanılan cihazlar ve bunları birbirine bağlayan diğer öğelerden ibaret gözükmemektedir. Siber uzaydaki saldırı ağında bilgisayarların içerisindeki işlemciler, cihazları birbirine bağlayan ve yer altından geçen kablolar ve fiber optik kablolarını taşıyan hatlar da yer almaktadır.[9] Bu tespitten hareketle uluslararası hukukun ilgi alanına giren nokta siber uzaydaki tüm bigisayar ağları ve bu ağlara bağlı olan cihazlarla onların kotrol ettiği unsurlardır (Keleştemur, 2015: 195). Bu unsurların kendi içerisinde oluşturduğu bilgi savaşı tüm aktörlerin yer aldığı uluslararası sistemde çıkarsal bütünlük ile teknolojik gelişmenin buluştuğu

noktada daha büyük bir etkileşimi ve bilişim kavramını ortaya çıkarmaktadır (Delibasis, 2008: 95).

Bilişim kavramı kontrol edilen unsurlar ile ilgili olarak saldırı ağına yönelik ortaya çıkarılmış bir kelimedir.Günümüzde bilgisayar dışında yazılımla çalışan, verileri depolayan, işleme tabi tutan ve ileten elektronik cihazların çeşitlenmesi ile birlikte bilgisayara oranla daha kapsayıcı olan bilişim kavramı ortaya çıkmıştır. Uluslararası hukukun bilişim suçları boyutunda ne ifade ettiği ve devletler arasındaki uyum eleştiri noktasını oluşturmaktadır.

Siber suçlarla mücadelede, ihtiyaçlara paralel olarak hukuk sisteminde yapılan iyileştirmeler ile beraber yasal mevzuat etkin ve hızlı bir reaksiyona imkan sağlasa da internetin tasarımından kaynaklanan açıklar iz sürmeyi ve planlamayı güçleştirmektedir. Gerek ulusal anlamda, gerekse uluslararası hukukun ihtiyaçlarını giderme adına internetin güvenilir bir kullanıcı grubuna hizmet edeceğinin düşünülmesi nedeniyle IP paketleri içerisindeki bilgilerin orijinal halinin korunmasına yönelik bir şifreleme önlemi alınmamıştır (Bayraktar, 2015: 99). Bu gibi durumlarda ilk kaynağa ulaşma gibi hususlar zorlaşmaktadır ve uluslararası hukukun alana ilişkin yorumu yetersiz kalmaktadır. Gelişen ülkeler için bu durum daha da çok hissedilmektedir (Schalhoub ve Al Qasimi, 2010: 36).

Uluslararası alanda yapılan düzenlemeler ve saldırı ağlarına ilişkin ortak politikalar oluşturma, konvansiyonel ve nükleer hususlarda dahi ortak anlaşmalara varılamamışken kısa vadede zor gözükmektedir. Politika alanlarda hangi temel çerçevenin baz alınacağı ve kapsayıcı olduğu tartışma konusu olacaktır ve devletlerin gelişmişlik düzeyi ile tarihi süreç bu konudaki samimiyeti azaltmaktadır.



Şekil 2. Bilgi Güvenliği Politika Alanları ve Etkileşim (Commision of The European Communities, 2001: 3).

Uluslararası hukukun etkileşim boyutu açısından siber ağları tamamen güvenli hale getirmek bir ütopya gibi görünse de siber saldırıları engellemek için küresel anlamda iş birliğine ihtiyaç olduğu bir gerçekliktir. Devletlerin siber tehditlere karşı yaklaşım ve yorumları farklı olduğu için hukuki anlamda ortak bir çözüm zorlaşmaktadır (Yayla, 2013: 217). Siber alanın fiziksel alanı etkilediği noktalarda saldırganın tespiti, saldırgan aktörün niteliği gibi hususlar uluslararası alanda ortak bir yaklaşımı daha da zorlaştırmaktadır ve bu konuda atılan adımlar oldukça yetersizdir.

c) Siber Güvenlik Antlaşmaları ve Uluslararası Düzenlemeler

Devlet örgütlenmesi ile birlikte oluşan iç hukukta, yasa yapıcı bir yasama organı, hukuk sistemi içerisindeki tutum ve davranışları bu yasalara uygunluk açısından denetleyen mahkemeler ve yasaların uygulanması açısından gerektiğinde önlemler alan kolluk kuvvetleri bulunmaktadır. Uluslararası hukukta aynen iç hukuktaki benzer yapılanmaya ulaşmak mümkün değildir fakat uluslararası hukukta da benzer fonksiyonlar gören unsurlardan söz edilebilir (Sönmezoğlu, 2000: 644). Bunlar arasında en önemlisi uluslararası antlaşmalardır. Malcolm N. Shaw (2008: 944) uluslararası

antlaşmaların düzenlendiği alana bakılmaksızın *jus cogens* konseptine aykırı olmamasını ve sonuçlarının da gözetilmesini özellikle vurgulamaktadır.

Uluslararası hukuk açısından siber güvenliğe kaynak oluşturabilecek başlıca kaynaklardan olan antlaşmalar haricinde; teamül, genel hukuk ilkeleri ve uluslararası hukuk yazarlarının doktrinleri oldukça geri planda kalmaktadır. Bunun temel sebepleri özellikle siber terörizm ve siber savaşa ilişkin başlıklarda özetlenmişti. Antlaşmaların siber güvenliğe ilişkin düzenlemelerde baskın bir şekilde ön plana çıkmasının temel sebebi karşılaşılan bir sorunda nasıl bir karşılık verileceği ile ilgilidir.

Uluslararası düzenlemeler içerisinde savaşa ve silahlı çatışmalara ilişkin düzenlemeler yapılırken, siber saldırılara dair yaklaşımda silahlı bir cevap verilip verilemeyeceği ile ilgili bir kesinlik yoktur. Bu noktada atılan adımlar siber suçlarla mücadele konusundaki düzenlemelerle sınırlı kalmaktadır. Fakat devletler siber saldırılar sonrasında ciddi mağduriyetler de yaşamaktadır.

Uluslararası anlamda eskiye oranla daha ciddi ve somut adımların atıldığı siber güvenlik ile ilgili düzenlemelerde karşılıklı güven ilişkisine dair ciddiyet eksikliği halen devam etmektedir. Siber güvenliğe ilişkin yapılmış bazı önemli uluslararası antlaşmaları ve düzenlemeleri şöyle özetleyebiliriz:

- Talin El Kitabı (Tallinn Manual): Orijinal adı "Tallinn Manual on the International Law Applicable to Cyber Warfare" olan Tallinn Manual, bağlayıcılığı olmayan akademik bir çalışma olarak uluslararası hukukun siber savaş ve çatışmalara uygulanabilirliğini tartışan bir çalışmadır. 2009-2012 arasında NATO tarafından davetli yaklaşık 20 uzmanın hazırladığı el kitabı, 2013 yılında Cambridge University Press tarafından yayınlanmıştır. Söz konusu çalışmaya Kızıl Haç Uluslararası Komitesi, NATO ve ABD Siber Komutanlığı da gözlemcilik yapmıştır. Çalışmada günümüz uluslararası yasalarının siber ortamda nasıl uygulanacağına yönelik yorumlar mevcut olup ilave yasa maddesi önerilmemektedir. Türkiye'de MGK tarafından resmi sitede yer verilen kitap, siber savaşta BM'nin siber saldırılara karşı uluslararası askeri operasyon dahil önlemleri alabilmesine imkân tanımaktadır.
- Avrupa Konseyi Siber Suçlar Sözleşmesi: Bilgisayar ve internet suçları ile ilgili düzenlemeler getiren ve Budapeşte Sözleşmesi olarak da bilinen çalışma 1 Temmuz 2004 tarihinde yürürlüğe girmiştir. 48 maddeden oluşan sözleşme özellikle telif haklarının

ihlalleri, bilgisayarlarla ilgili sahtekarlık eylemleri, çocuk pornografisi ve ağ güvenliğine ilişkin suçları tanımlamaktadır.

- Siber Suçlara Karşı BM Kararları: BM siber suçlarla iligli etkin bir çalışma içindedir. Bu konuda iki karar ön plana çıkmaktadır.
- 57/239(2002) numaralı BM kararı: Siber güvenlik konusunda bir kültür oluşturmaya yönelik dokuz kıstas tanımlanmıştır.[10]
- 58/199(2004) numaralı BM kararı: Siber güvenlik küresel kültürünün geliştirilmesi ve kritik altyapıların korunması üzerine odaklanmaktadır (Çifçi, 2012: 104).
- Bilgisayarla İgili Suç: Yasal Politikanın Analizi Raporu (Computer Related Crime: Analysis of Legal Policy): OECD tarafından 1986 yılında yayınlanarak üye ülkelere hangi ihlallere cezai yaptırım uygulaması gerektiğinden bahsedilmektedir.
- Ülkelerarası Organize Suçlarla Etkin Mücadelede Tavsiyeler Raporu: G8'in Fransa Zirvesi'nde 40 temel noktanın üzerinde durulmuştur. Ülkelerin iç hukuklarını modern teknoloji ihlallerini cezai müeyyide ile karşılayacak şekilde yeniden düzenlemeleri belirtilmiştir (Çakmak ve Katman, 2009: 178).

Siber güvenlik düzenlemeleri ile ilgili uygulama alanında yaşanan sorunlardan en temeli yargılama yetkisi sorunu ve ülkeler arasındaki uyumdur. Siber suçlar genellikle birden fazla ülkeyi ilgilendirecek bir nitelik sergilemektedir (Sandvik, 2012: 3). Uluslararası alanda düzenlemelerin uygulanması ile ilgili diğer bir temel sorun ise fiziksel arama ya da haberleşmelerin takibi/dinlenmesi hususunda yasal sürecin başlatılması ve harekete geçilmesi yönündeki güçlüklerdir.

d) Karşılaşılan Hukuksal Güçlükler, Algının Kırılması ve Farkındalık

Uluslararası aktörlerin üzerinde uzlaştıkları bir siber alan tanımı yapılmamıştır. Bu durum ülkelerin tanımlamaya çalıştıkları siber alanın sınırlarının belirgin olmamasına neden olmakta ve siber alan üzerinden yapılan saldırılarda hukukun nasıl uygulanacağı konusunda sorunsal oluşturmaktadır (Bayraktar, 2015: 104). Siber güvenliğin genel tanımında olduğu gibi siber alanın ve siber savaş kavramının tartışıldığı noktada uluslararası hukuk uzmanları arasında bir anlaşmazlık söz konusudur.[11] Siber savaş kavramı yerine *Siber Silahlı Çatışma* kavramıyla da sıkça karşılaşılmaktadır (Schmitt ve Vihul: 8).

İnternet hizmetlerinde ve kullanımındaki artış, aktarılan bilgi hacmindeki yoğunluk suçların ve suçluların tespitinde

yaşanan önemli bir güçlüktür. Uluslararası hukuk adına çoğu zaman devletlerin birbirlerine ilişkin söylemleri de iddia bazında kalmaktadır. Hukuksal anlamda izlenecek yol doğal olarak askıda kalmaktadır. Bilgi güvenliğinin uluslararası normlarla tartışılması en azından siber ortama ilişkin devletler arasındaki güven algısını arttırıcı bir etken olacaktır.

İnternet hizmetlerinde ve kullanımındaki artış, aktarılan bilgi hacmindeki yoğunluk, suçların ve suçluların tespitinde yaşanan diğer bir güçlüktür. Tüm suçlarda olduğu gibi siber ortamda gerçekleştirilen suçlarda, suçun oluşabilmesi için manevi unsurun bulunması yani failin eylemi kasten veya taksirle işlemiş olduğunun ispatlanması gerekmektedir (Bayraktar, 2015: 105).

Siber ortamda suçlar herhangi bir yere ve kimi zaman bir merkeze bağımlı olmadan dünyadaki ağ sistemleriyle başka herhangi bir yere kanalize olabilme özelliğine sahiptir. Saniyenin de daha az zaman dilimlerinde, ışık hızında müdaheleler dünyanın bir ucundan diğer ucuna gerçekleşmektedir. Sınır tanımayan siber saldırılar karşısında devletlerin iş birliği yapmaları gerekliliğine karşın bu konuda farkındalığın azlığı dikkat çekicidir (Çakmak ve Katman, 2009: 167). Uluslararası düzenlemelerin teknolojik gelişmelere adapte edilmesi gerekliliği vurgulanması gereken diğer bir husustur. Nükleer anlamda tesislerin kurulması ve nükleer geliştirmelere ilişkin uluslararası hukukta nasıl adımlar atılıyorsa benzer süreçler siber güvneliğe de uyarlanabilir (Chatterjee, 2014: 8).

e) Siber Saldırılar ve Jus Ad Bellum-Jus In Bello

Uluslararası hukukta, kuvvet kullanma hakkı (*jus ad bellum*) ile kuvvete başvurulduğunda uyulması gereken çatışma kuralları (*jus in bello*) arasında bir ayrım yapılmaktadır.[12] Buna göre silahlı çatışma hukuku kurallarının uygulanmasının bu hakka sahip olunup olunmadığı sorunundan tamamen bağımsız olduğu kabul edilmektedir (Yayla, 2013: 202).

Siber saldırılar ve silahlı çatışma hukukuna ilişkin kurallar özellikle uluslararası düzenlemelerde netlik kazanmayan hususlar arasındadır. Kuvvete başvurma ve bu konuda kararlar alma uluslararası kamuoyunun ilgisi dahilindedir ve anlayış olarak somut bir siber saldırı çıktısı gözetilmektedir. Siber alanda yaşanan gelişmelere ilişkin kuvvete başvurma gibi tedbirlerin var olması gerektiği çoğu zaman belirli ülkelerle sınırlı kalmaktadır.

Siber saldırıların kaynağını bulmayı amaçlayan teknolojiler geliştiği ölçüde siber saldırıların kaynağını gizleyen teknolojiler de gelişme göstermektedir. Bir fiil ya da

hareketsizliğin devlete atfedilebilir olması için söz konusu fiilin o devletin *de facto* ve *de jure* organları ya da ajanları tarafından yapıldığının ispat edilebilir olması gerekmektedir (Kurtdarcan ve Mumcu, 2014: 182). Siber saldırıların oluşturulması aşamasında siber harekatın yöneliş şeklinin temelinde yer alan siber casusluk ve siber suçların çıkış noktası karar alıcılar ya da bireyler olmaktadır. Siber harekât düzlemine göre siber müdahele ve siber saldırı şeklinde devam eden süreçte harekatın çıkış noktası doğru bir şekilde tespit edilebilirse *kuvvet kullanma hakkı* (*jus ad bellum*) işletilebilir (Melzer, 2011: 6).

Siber ortam bir devletin kuvvet kullanımına varmayan harekatlara ilaveten ölümlü veya yaralanmalı sonuçlar doğurabilecek harekatlar yapmasına olanak sağlayabilir. Ölüm, yaralanma veya maddi kayıplara sebep olan siber eylemler uluslararası hukuk açısından silahlı saldırı veya kuvvet kullanımı olarak değerlendirilebilir. ABD Siber Komutanlığı tarafından tanımlandığı şekliyle siber eylemler, siber casusluktan erişim operasyonlarına ve en son noktada ölüm veya maddi kayıplara sebep olan aktivitelere kadar yayılan geniş bir eylem spektrumu boyunca görülebilir.

Geniş eylem sürecine sahip olan siber ortam kendi kapasitesinin başlangıcı itibariyle siber suç veya casusluğa yönelik olsa da özellikle kritik altyapılara ilişkin saldırılarda ve müdahelelerde fiziksel bir zarara ilişkin saldırı türüne dönüşmektedir. Caydırıcılık amaçlı olan ve daha az gizliliğe sahip olan fiziksel sonuçlu bu tür saldırılarda savaş hukukuna ilişkin süreç klasik savaşa ilişkin uluslararası düzenlemelerde olduğu gibi sonuçlar doğurabilmektedir.[13]

Sonuç

Savaşların kaynakları ve biçimleri sahip olduğu öz dahilinde evrilmektedir. Çatışmaların sahip olduğu tehdit geniş bir alana hitap etmektedir. Kritik altyapı olarak adlandırdığımız her temel saldırı tehlikesiyle karşı karşıyadır.Bu temellerin korunmasına ilişkin yasal düzenlemeler artık yetersiz kalmaktadır. Siber güvenlik kavramının sivrildiği uluslararası politikada terörizmin getirmiş olduğu zorluklar bu düzenlemelerin olgunlaşmasını zorlaştırmaktadır.

Şiddetin ve sahip olduğu sarmalın uluslararası hukuk açısından yok edilemeyeceği konusunda araştırmacılar ortak bir algıya sahip gözükmektedir.Savaş teknolojilerindeki gelişim ve siber suçlara ilişkin veriler kapalı kapılar arkasında kendisine gizlenecek bir karanlık her zaman bulabilmektedir. Özellikle son yıllardaki teorik düzey pratik alana katkı sağlayamamaktadır.

Uluslararası hukuk temel anlamda uluslararası aktörlerin ortak hareket etmesiyle bütünlük kazanabilir. Bu düzeyin merkezinde yer alan devletler varoluş sebeplerine ilişkin temel sorunlar hakkında dahi ortak tavır alamazken siber güvenlik gibi karmaşık boyutlarda daha da zorlanacaklardır. Bilişim suçları ve iç güvenliğe ilişkin tehditler daha da artış gösterecek ve uluslararası hukuk bu konuda geri planda kalacak gibi gözükmektedir.

Siber uzaya artan bağımlılıkla birlikte devletlerin tartışma alanını aşıp uluslararası örgütlerin de ilgisini çeken düzey devletlerin bu örgütler sevsiyesindeki cılız seslerini bizlere yansıtmaktadır. Devletlerin siber suçlara ilişkin yaklaşımları bir çıkar mücadelesinden öteye gidememektedir. Güç ve getirmiş olduğu algı özellikle II. Dünya Savaşı sonrasında tercih edilen öncelik haline gelmiştir.

Uluslararası hukukun etkileşim boyutu açısından siber ağları tamamen güvenli hale getirmek ütopik bir yaklaşım olarak kalmaktadır ve bu düzey devletleri siber tehditlere her geçen gün daha da açık hale getirmektedir. Siber alanda ortak hareket edebilmek güçlü aktörlerin biraraya gelmesiyle oluşturulacak bir düzey değildir. Olayların seyri bu konuda çok taraflıdır ve aktörleri de aşan yoğunluktadır. Bu yoğunluk oluşturulacak samimiyete bağlı olarak değişkenlik gösterebilir.

Extended Abstract

The question of whether war and violence can be eradicated has been at the centre of different studies after the First World War. The post-Cold War innovation brought new approaches to the nature of security, which had a significant impact on international relations literature.

In particular, the general change in the development of war technologies and intelligence structure has accelerated the approaches to the concept of cybersecurity and the change in the dimension of international relations. In recent years, the normative international relations approaches that have developed a different and unique perspective on international security have been blended with the theoretical plane of cybersecurity, and the concept of cybersecurity has increased in the international arena.

At the beginning of the study, the concept of cybersecurity in the field of international relations has evaluated in concrete events related to deterrence and application field. The process of the historical development of cyber events is mainly parallel to the increase in parameters related to cyber espionage and cyber warfare. The end of the

Cold War and the acceleration of the development of these parameters made it necessary to examine the concepts such as cyber terrorism, cyberwar and cybersecurity, which we have already emphasised, in interstate relations. While the direction of cyberwar continued at the same pace after the Cold War, the international impact of malware and cybercrime and the increase in incidents required cooperation between states.

Cybersecurity takes its place based on security, which is one of the working planes of international relations and makes a name for itself in the discussions of international law. Developments in cyberspace, where the interaction of international actors are increasing, increase its controversial dimension with each passing day. In the international system, where states are the main actors, awareness and involvement of cybercrime has become a threat to all individuals.

An environment in which cyber terrorism is supported by renders international law inadequate. The irregularity and confrontational dimension of the Cold War inherited some problematic issues. The deterrence-based approach has transformed the legal arrangements on cyber-attack and defense issues into need. The complexity and change in the global struggle are based on this transformation.

The establishment of common policies on international regulations and attack networks seems complicated in the short term, even when there is no common agreement on conventional and nuclear issues. It will be controversial which policy framework will be based and inclusive in policy areas, and the level of development of states and the historical process will reduce sincerity.

Except for the treaties, which are the primary sources that can be a source for cybersecurity in terms of international law. The main reasons for this were summarised in particular on the topics of cyber terrorism and cyber warfare. The main reason why the treaties come to the forefront in the regulations on cybersecurity is related to how responding to a problem encountered.

In cyberspace, crimes can be channelled anywhere and sometimes to any other place in the world without being dependent on a centre. At less than a second, light-speed interventions take place from one end of the world to the other. Despite the necessity of cooperation of states in the face of cyberattacks without borders, the lack of awareness on this issue is remarkable. The necessity of adapting international regulations to technological developments is another point that should be emphasized. Similar steps can be adopted to

cybersecurity, just as international law on the establishment of nuclear facilities and nuclear developments is being taken.

While arrangements regarding war and armed conflicts are made within international regulations, there is no certainty as to whether an armed response can be given in the approach to cyber-attacks. The steps taken at this point are limited to the regulations on the fight against cybercrime. However, states suffer serious grievances after cyber attacks.

Within the scope of this study, the initial determinations related to the historical transformation of cybersecurity in the international system are examined and some data on the international law dimension are presented. The confusion of cybercrime and the inadequacy of international law have been the subject of discussion in this study. Legal challenges and determinations of breaking the complex perception in cyberspace are among the other issues addressed. The treaties and international regulations on cybersecurity are also open to discussion in their own dimensions.

Kaynakça

Baylis, J.(2008). Uluslararası İlişkilerde Güvenlik Kavramı, Uluslararası İlişkiler Dergisi, 5/18, 69-85.

Bayraktar, G. (2015). Siber Savaş ve Ulusal Güvenlik Stratejisi. İstanbul: Yeniyüzyıl Yayınları.

Bıçakçı, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu, Uluslararası İlişkiler Dergisi, 9/34, 205-226.

Boyraz, M. (t.y.). NATO'nun Siber Güvenlik Politikası: Tarihsel Süreç ve Kırılma Noktaları, Research Turkey, Türkiye Politika ve Araştırma Merkezi. Son güncelleme Eylül 14, 2016. http://researchturkey.org/tr/natos-cyber-security-policy-the-historical-process-and-critical-junctures/.

Cavelty, M.D. (2008). Cyber-Security and Threat Politics: US Efforts to Secure The Information Age. New York: Routledge Publishing.

Clarke, R. A. ve Knake, R. K. (2011). Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit. Çev., Murat Erduran. İstanbul: İKÜ Yayınevi.

Commission of the European Communities, (2001). "Network and Information Security: Proposal for a European Policy Approach" Son güncelleme Şubat 14, 2016. http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf.

Chatterjee, B. B. (2014). International Law and Cyber Warfare: An Agenda for Future Research, Lancaster University Law School, Security Lancaster.

Chatterjee, B. B. International Law and Cyber Warfare: An Agenda for Future Research, Lancaster University Law School, Security Lancaster. Son güncelleme Nisan 7, 2017. http://www.research.lancs.ac.uk/portal/en/publications/international-law-and-cyber-warfare(267aeb20-9ace-4f8d-b9ba-815d5af20339).html

Çakmak, Haydar Çakmak ve Katman, Filiz. "Siber Tehditlerin Uluslararası ve İç Hukuktaki Yeri". *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, ed. Haydar Çakmak ve Taner Altınok. Ankara: Barış Platin Kitabevi, 2009.

Çifçi, H. (2012). Her Yönüyle Siber Savaş. Ankara: TÜBİTAK Bilim Kitapları.

Delibasis, D. (2008). Information Warfare Operations within The Concept of Individual Self-Defence, Cyber Conflict and Global Politics, ed. Athina Karatzogianni. London: Routledge Chapman Hall.

Durcan, E. (2015). Siber Suçlarda Suçlunun karar Verme Süreci, Siber Suçlar: Tehditler, Farkındalık ve Mücadele, ed. Fatih Tombul ve diğerleri. Ankara: Global Politika ve Strateji Yayınları.

Erdağ, A.İ. (2010). Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda), Gazi Üniversitesi Hukuk Fakültesi Dergisi, 14/2, 275-303.

Hansen, L. ve Nissenbaum, H. (2009).Digital Disaster, Cyber Security and The Copenhagen School, International Studies Quarterly, Vol. 53, 1155-1175.

Hare, F. (2010). The Cyber Threat to National Security: Why can't We Agree?, *Conf*erence on Cyber Conflict Proceedings, ed. C. Czosseck ve K. Podins. Tallinn: CCD COE Publications.

Healey, J.ve Tothova Jordan, K. NATO's Cyber Capabilities: Yesterday, Today and Tomorrow, Atlantic Council Brent Scowcroft Center on International Security Issue Brief. Son güncelleme Eylül 10, 2014. https://www.files.ethz.ch/isn/183476/NATOs_Cyber_Capabilities.pdf.

Hoskins, A. ve O'Loughin, B. (2008). The Internet as a Weapon of War? Radicalisation, Publics and Legitimacy, Cyber

Conflict and Global Politics, ed. Athina Karatzogianni. London: Routledge Chapman Hall.

Keleştemur, A. (2015). Siber İstihbarat, İstanbul: Level Kitap.

Kurtdarcan, B. ve Mumcu,Ö. (2014). Geleceğin Savaşları ve Silahları: Yeni Silah Teknolojilerinin Silahlı Çatışmalar Hukuku Işığında İncelenmesi. Ankara: Umag Vakfı Yayınları.

Libicki, M. (2009). Cyber deterrence and Cyberwar. Santa Monica: Rand Corporation.

Melzer, Nils. (2011). Cyberwarfare and International Law, Ideas for Peace and Security UNIDIR Resources. Son güncelleme Ağustos 1, 2017, http://unidir.org/files/publications/pdfs/ cyber warfare-and-international-law-382.pdf.

Sandvik, K. B. (2012). Cyberwar as an Issue of International Law, Prio Policy Brief, Volume 4, 1-4.

Schalhoub, Z.K.ve Al Qasimi, S.L. (2010). Cyber Law and Cyber Security in Developing and Emerging Economies. Cheltenham: Edward Elgar Publishing.

Schmitt, M. N. (2012).International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, Harvard International Law Journal, Vol. 54, 13-37.

Schmitt, M. N. ve Vihul, L. (2014). The Nature of International Law Cyber Norms, The Tallinn Papers, Paper No. 5, Special Expanded Issue.

Shaw, M. N. (2008). International Law, 6th Edition. Cambridge: Cambridge University Press.

Sönmezoğlu, F. (2000).Uluslararası Politika ve Dış Politika Analizi. İstanbul: Filiz Kitabevi.

Yayla, M. (2013). Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma, TBB Dergisi, Sayı 107, 199-220.

Yeşilyurt, H. (2015). Ulusal Güvenlik Perspektifinde Siber Güvenlik, Siber Suçlar: Tehditler, Farkındalık ve Mücadele, ed. Fatih Tombul ve diğerleri, Ankara: Global Politika ve Strateji Yayınları.

Yılmaz, S. (2016). Savaş ve General. Son güncelleme Mayıs 16, 2016, http://www.ulusal.com.tr/savas-ve-general-makale,5307.html.

Yılmaz, S. ve Salcan, O. (2008). Siber Uzay'da Güvenlik ve Türkiye. İstanbul: Mileynyum Yayınları.

Zagare, F. C. ve Kligor, D. M. (2000). Perfect Deterrence. Cambridge: Cambridge University Press.

[1]Bu çalışmanın teorik altyapısı ve kurgusu yazarın 12-13 Aralık 2016 tarihinde, V. Uluslararası Mavi Karadeniz Kongresi'nde sunduğu *"Russian Hegemony in The Black Sea As a Cyber Power; Data of 2015-2016 Cyber War"* adlı tebliğ ve *"Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Teorisi (Micro-CAT)"* adlı doktora çalışmasından derlenmiştir.

[2] Örnek olarak David Campbell uluslararası ilişkilerin geleneksel söylemlerine paralel bir şekilde ittifak ile güvenliğin devlet tarafından kullanılacak bir dizi araçla sağlanacağını savunmaktadır ve genel olarak bu anlayış kabul görmektedir. Fakat savunma ve dış politika arasındaki bağlantı farklı bir şekilde anlaşılabilmektedir. Dış politikanın bir parçasını oluşturduğu güvenlik her şeyden önce siyasi düzeni oluşturan bir söylem olarak karşımıza çıkmaktadır.

[3] Yapılan analizlerde sosyal medyanın ve siber kanallar vasıtasıyla oluşturulan haberleşme unsurlarının etkisiyle başta Arap Baharı olmak üzere birçok hareketin örgütlendiği tespit edilmiştir. Sosyal medya Tunus'ta devrim günlerinde yaygınlaşmış ve devrimden sonra da etkileri hissedilmeye başlanmıştır. Fakat Mısır'da Arap Baharı'ndan çok daha önce sosyal medya faaliyetleri organize olmada bir araç olarak kullanılmıştır.

[4] 4 Haziran 1956'da Sovyetler Birliği üzerinde U-2'lerin ilk uçuşundan iki ay sonra bir keşif uydusu üretimi için operasyonel gerekçeler aranmaya başlanmıştır. Uydular görüntü elde etme, sinyal toplama, iletişim, erken ikaz ve diğer çeşitli istihbarat görevlerinin yerine getirilmesinde kullanılmıştır.

[5] 1968 yılında Sovyet bilim adamları KGB'nin yardımları ile IBM'in o dönemdeki en güçlü modeli olan IBM System/360'ın bir benzerini yapmaya başlamıştır. Bu bilgisayar Ay'a ilk adım atılan projede kullanılmıştır.

[6] Soğuk Savaş esnasında, Sovyetler Birliği'ne ait verilerin elde edilerek ABD'nin avantajlı hale gelmesine dair planlar dikkat çekicidir. CIA'in o dönemki başkanı olan Bill Casey, KGB'nin verileri çalmasına izin verilmesini fakat çalınacak şeylere hatalar yerleştirilmesini planlamıştır. KGB ajanları hatalı verileri ülkelerine götürmeye başlamış ve sistemsel sorunlar içine girmişlerdir.

[7] Çin, ABD gibi 1990'lı yılların sonunda kalitatif askeri eksikliklerini giderme amacıyla siber savaş birlikleri kurmuştur. Çin son yıllarda uluslararası alandaki mücadelesini deniz kuvvetlerine ve siber savaş alanındaki kuvvetlerine kaydırmıştır.

[8] DDoS saldırıları temel olarak iki şekilde gerçekleştirilmektedir. Bunlardan birinde çok sayıda farklı kullanıcının sosyal medya, forum, chat gibi kanallar üzerinden organize olarak aynı anda bir sisteme erişmeye çalışması şeklinde olmaktadır. Diğerinde ise Botnet üyesi olan zombi makinelerin bilinçsizce sisteme erişimi şeklinde gerçekleşmektedir.

[9] Siber uzayın sadece internetten ibaret olmadığını kavramak ilk başlarda zor gelebilmektedir. Ancak internet herkesin kolayca girebileceği, birbirine bağlı olan ağlardan oluşan açık ağdır. İnternette bulunan, bu ağa bağlı herhangi bir cihazla iletişim kurmak mümkündür. Ancak siber uzay içerisinde internet ile birlikte internetten erişilemeyen, farklı ağlar da bulunmaktadır.

[10] Bunlar; *farkındalık, sorumluluk, mukabele, ahlak, demokrasi, risk değerlendirmesi, güvenlik tasarımı ve gerçekleştirimi, güvenlik yönetimi* ve *yeniden değerlendirmedir*. BM kararlarının, farklı kıstaslarla gündeme getirmeye çalıştığı siber güvenlik çalışmalarında yaşanan temel sorunsal devletlerin alana bakış açısının ciddi derecede farklılık içermesidir. Tüm üye ülkeler açısından konunun ele alınışındaki ciddiyet aynı derecede ortak bir tavır alınışında gerekli potansiyele ulaşamamıştır.

[11] Bir siber suçun failini tespit edebilmek için öncelikle suçlunun yerini bulmak, yani saldırı kaynağının IP adresini tespit etmek gerekmektedir. Bunun için izlenen yöntem hedeften geriye doğru yönlendirici takip etmektir.

[12] Savaş hukuku incelenirken kuvvet kullanılmasının hukuka uygun olup olmadığı hususu ile silahlı kuvvet kullanılması sırasında seçilen hedef, araç ve yöntemlerin hukuka uygunluğu hususunun birbirinden ayrı incelenmesi ve düşünülmesi gerekmektedir. Siber saldırı durumunda devletlerin buna karşılık verme hakkı, kuvvete başvurma hakkına ilişkin (jus ad bellum) kuralların incelenmesini gerekli kılmaktadır.

[13] Uluslararası hukukta meşru müdafaa haricinde kuvvet kullanmanın yasaklanması ile beraber *jus in bello,* haklı savaş teorisinden koparak kendine bağımsız bir alan kazandırmıştır. Bu bağımsız olma hali nedeniyle siber saldırıya ilişkin *jus in bello* kurallarını, *jus ad bellum* siber saldırı ilişkisine dair kurallardan farklı olarak ele almak gerekecektir.