# SİBER SAVAŞLARDA *JUS AD BELLUM* VE *JUS IN BELLO*

# *JUS AD BELLUM* AND *JUS IN BELLO* IN CYBER WARS

**Onur GÖKÇER[*] & Pınar GÖZEN ERCAN[**]**

**ÖZ**

**Savaş kavramı, Soğuk Savaş dönemiyle birlikte dönüşmeye başlamış, yakın dönemde de Amerika Birleşik Devletleri'nin güttüğü "teröre karşı savaş politikası" ile bu durum perçinlenmiştir. Bu kavramsal dönüşüm çerçevesinde savaşların sadece devletler arasında gerçekleştiği artık düşünülmemektedir. Karakter olarak asimetrik ve genellikle sınırlı bir savaş alanından yoksun olan yeni savaşlar geleneksel savaşı tamamen değiştirememiş fakat geleneksel savaşlardaki tanımları ve ayırımları bulanıklaştırmış ve yeni kavramlar eklemiştir. Kavramsal dönüşümler ve yeni özellikler çerçevesinde ortaya çıkan yeni gri alanlar, uluslararası hukukun mevcut kuralları ve uygulanması açısından bazı zorlukları ve/veya sorunları da beraberinde getirmektedir. Ne var ki, uluslararası hukukun normatif gelişimi ve uygulamaları uluslararası politikadan bağımsız bir şekilde gerçekleşmemektedir. Bu çerçevede, bu makalede özellikle Uluslararası İlişkiler literatüründe az çalışılmış bir konu olan yeni savaşlarda *jus ad bellum* ve *jus in bello* prensiplerinin uygulanabilirliği siber savaşlar/saldırılar özelinde irdelenmekte ve Estonya, Gürcistan ve Stuxnet vakaları**

[*] Doktora Öğrencisi, İzmir Ekonomi Üniversitesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, onurgokcer@hotmail.com, ORCID ID: https://orcid.org/0000-0003-1335-0678.
[**] Doç. Dr., Hacettepe Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, Devletler Hukuku ABD, mpgozen@hacettepe.edu.tr, ORCID ID: https://orcid.org/0000-0002-6713-1641.

* Makale Geliş Tarihi: 01.09.2019
Makale Kabul Tarihi: 23.02.2020

**üzerinden literatürdeki örneklerinden farklı olarak "karşı çıkma kuramı" çerçevesinde tartışılmaktadır.**

**Anahtar Kelimeler: Yeni Savaşlar, Siber Savaş, *Jus Ad Bellum*, *Jus In Bello*, Karşı Çıkma Kuramı.**

**ABSTRACT**

**The concept of war has been transforming since the Cold War period, and such transformation has been strengthened by "the war against terror" policy of the United States of America. In light of this conceptual transformation, it is no longer argued that wars take place only between states. New wars—which are asymmetric and do not have a limited war zone—have not changed traditional wars all together, instead, they have blurred the definitions and distinctions pertaining to traditional wars and added new concepts. The grey zones that have emerged due to these transformations have also led to the rise of new challenges and problems related to the implementation of the rules of international law. The normative evolution of international law and its implementations do not take place independently of international politics. In this vein, this article focuses on a question that has been underexplored especially in the International Relations literature, namely the applicability of *jus ad bellum* and *jus in bello* in new wars through the lenses of contestation theory. To this end, in its attempt to contribute the existing literature, it discusses how norms are contested in instances of cyber wars/attacks with reference to the specific cases of Estonia, Georgia and Stuxnet.**

**Keywords: New Wars, Cyber War, *Jus Ad Bellum*, *Jus In Bello*, Contestation Theory.**

## GİRİŞ

Savaş kavramı, Soğuk Savaş dönemiyle birlikte dönüşmeye başlamış, yakın dönemde de Amerika Birleşik Devletleri'nin (ABD) güttüğü "teröre karşı savaş" politikası ile bu durum perçinlenmiştir. Bu kavramsal dönüşüm çerçevesinde savaşların sadece devletler arasında gerçekleştiği artık düşünülmemektedir (Franck, 2004: 686-688; Hajjar, 2006; Malender vd., 2009; Mello, 2010). Diğer taraftan, son dönemin "yeni savaşları" ile geleneksel savaş anlayışı hem

benzerlikler hem de farklılıklar göstermektedir. Geleneksel savaşlar,[1] simetrik güçler (devletler) arasında, belirli bir savaş alanı içerisinde, ahlaki olarak eşit olduğu varsayılan askerlerin karşı karşıya gelmesiyle gerçekleşmekteydi (Doswald-Beck, 1987). Yeni savaşlar ise, karakter olarak asimetriktirler ve genellikle sınırlı bir savaş alanından yoksundurlar (Barnard-Wills ve Ashenden, 2012; Gregory, 2011). Diğer taraftan yeni savaşlar geleneksel savaşı tamamen değiştirmemiş fakat tanımları ve ayrımları bulanıklaştırmış—savaşçı ve savaşçı olmayan ayrımı, savaş alanının anlamı gibi—ve bazı yeni kavramlar eklemiştir (Guillaume vd., 2016, Kaldor, 1996: 506). Örneğin, Kaldor (2005: 491) yeni savaşları eski savaşlardan ayırırken teknolojinin gelişimine değil savaşın sosyal ilişkilerine (*social relations of warfare*) vurgu yapmaktadır. Yeni savaş kavramı, başarısız devletler bağlamında şiddetin devlet ve devlet dışı aktörler tarafından daha çok sivillere yönlendirildiği durumları açıklamak için kullanılmaktadır (Kaldor, 2006: 1). Bunun yanı sıra, Münkler (2003: 9, 15) yeni savaşların en göze çarpan özelliklerinin asimetri ve silahların ucuzluğu olduğunu belirtmektedir.

Mevcut literatür, genel olarak yeni savaşların hukukî ve güvenlik yönlerine ve özellikle de devletlerin bu yeni güvenlik tehditleriyle nasıl başa çıkabileceğine odaklanmıştır (Baker-Beall, 2014; Bassiouni, 2008; Gregory, 2011; Hajjar, 2006). Bu nedenle, yeni savaşların özelliklerine dair analizler devlet merkezli olma eğilimindedir (Barnard-Wills ve Ashenden, 2012; Choucri, 2000; Kelsey, 2008; Reveron, 2012; Tikk, 2010). Literatürün güvenliğe odaklanan kısmı, değişen savaş kavramı ve yeni teknolojik silahlarla ilgilenmektedir. Bazı yazarlara göre yeni savaşlar savaş kavramını değiştirmemiştir (Echevarria II, 2007; Herberg-Rothe, 2009; Houweling ve Siccama, 1988; Lantis, 2006; Reid, 2003; Schuurman, 2010; Waldman, 2010). Diğer bazı yazarlar ise, yeni savaşları farklı ve yeni terimlerle açıklamayı tercih ederlerken bu savaşların ortaya çıkardığı tehditlerle başa çıkabilmek için yeni araçlar gerektiğini de iddia etmektedirler (Bassiouni, 2008; Daniel III ve Smith, 2015; Rosen, 2007). Bu bağlamda, güncel güvenlik literatürünün genellikle yeni teknolojiler ve bunların savaş ve devlet güvenliği üzerindeki etkileri ile ilgilendiğini söylemek mümkündür.

Literatürde savaşların hukukî yönüyle ilgili tartışmalar, pasifizm (*pacificism*), pürizm (*purism*) ve adil savaş (*just war*) olmak üzere üç farklı savaş teorisine dayandırılmaktadır. Bunlardan pasifizm savaş hukukuyla pek ilgilenmez çünkü temel olarak savaşı ve öldürmeyi reddetmektedir (bkz. McMahan, 2010a). Öte yandan, adil savaş teorileri, belirli koşullar altında savaşların haklı ve meşru

[1] Bu makalede "geleneksel savaş" ifadesi 18.yüzyıl sonrası Clausewitzçi savaşlar anlayışına karşılık gelecek şekilde kullanılmaktadır.

olabileceğini savunmaktadırlar (bkz. Coverdale, 2004). Son olarak, McMahan (2010b) gibi püristler ise, *jus ad bellum* ve *jus in bello*'nun tamamlayıcı kodlar olduğunu öne sürmektedirler. Mevcut literatürün ışığında, yeni savaşlar konusunda *jus ad bellum* ve *jus in bello*'nun yeni bir tartışma olduğunu söylemek mümkündür. Bu tartışmanın çıkış noktasını 11 Eylül terör saldırıları sonrasında ABD'nin güttüğü "teröre karşı savaş" politikası oluşturmaktadır.

Siber uzay ve siber saldırı kavramları, yeni savaş tartışmalarında uluslararası hukukun konumunu daha da zora sokmuştur. Bu yeni kavramların ve alanların ortaya çıkmasından sonra yeni çalışma alanları doğmuş, ancak literatürün ana odağı özellikle bir savaşı adil ya da adaletsiz olarak etiketlemekten ve savaşın gerekçelerini değerlendirmekten öteye geçememiştir. Durum böyleyken, "*jus ad bellum* ve *jus in bello,* yeni savaşlarda uygulanabilir mi?" sorusu literatürde tartışmalara yol açmıştır. Literatürde son on yıllık dönemde, Allenby (2014) gibi bazı yazarlar daha kısıtlayıcı (*restrictionist*) bir bakış açısı benimseyerek bu normları yeni savaşlarda kullanabilmenin mümkün olmadığını öne sürmüş, Finlay (2010) gibi bazı diğer yazarlar ise bu normlardan faydalanmanın mümkün olduğunu belirtmişlerdir.

Kavramsal dönüşümler ve yeni özellikler çerçevesinde ortaya çıkan bu gri alanlar, uluslararası hukukun mevcut kuralları ve uygulanması açısından bazı zorlukları ve/veya sorunları da beraberinde getirmektedir. Ne var ki, uluslararası hukukun normatif gelişimi ve uygulamaları uluslararası politikadan bağımsız bir şekilde gerçekleşmemektedir. Bu nedenle, Uluslararası İlişkiler (Uİ) perspektifinden norm oluşum süreçlerindeki karşı çıkmaları (*contestation*) irdelemenin gerekliliğini savunan bu makalede, özellikle Uİ literatüründe az çalışılmış bir konu olan yeni savaşlarda *jus ad bellum*[2] ve *jus in bello*[3] prensiplerinin uygulanabilirliği siber savaş, siber terörizm ve siber tehditler örneği özelinde "karşı çıkma"lar üzerinden irdelenmektedir.

Uluslararası siyaset ve hukuk bağlamlarının kesişiminde yer alan "savaş hukuku, yeni savaşların hızlı gelişen karakteriyle nasıl etkili bir şekilde başa çıkabilir?" ve "uluslararası normların yeni savaşlardaki, özellikle siber savaşlardaki yeri nedir?" sorularını merkezine yerleştiren bu makalede yeni savaşlarda *jus ad bellum* ve *jus in bello*'nun meşruiyetini tartışmak için sosyal inşacı perspektifin "karşı çıkma kuramı" (*contestation theory*) (bkz. Wiener, 2014; 2017;

[2] *Jus ad bellum* doktrini bir devletin hangi şartlar altında savaş açabileceğini ortaya koyan normdur. Haklı savaş nedenleri bu normun temel konusunu oluşturur (Kolb, 1997: 553).
[3] *Jus in bello* doktrini karşı karşıya gelen tarafların hangi araçlarla ve nasıl savaştıklarıyla ilgilenir. Düşmanlığın nasıl yürütüldüğüne odaklanır (Kolb, 1997: 553).

2018) kullanılmıştır. Dolayısıyla, önce makalenin teorik çerçevesi sunulacak ve *jus ad bellum* ile *jus in bello* tanımlamaları yapılacaktır. Ardından, siber uzay ve tehditlerinin kendine has özellikleri açıklanacak ve bu özelliklerin nasıl bir meşruiyet boşluğu oluşturduğu tartışılacaktır. Son olarak, Estonya, Gürcistan ve Stuxnet olayları incelenecek ve mevcut meşruiyet boşluğu karşı çıkma teorisi yardımıyla tartışılacaktır. Uluslararası hukukun yapımı ve uygulanması süreçleri göz önünde bulundurulduğunda, iç hukuk sistemlerinden farklı olarak, bu süreçlerin devletlerin iradesiyle olan bağlantısı göze çarpmaktadır. Bu bağlamda, bu çalışma ile uluslararası ilişkiler/siyaset perspektifinden uluslararası insancıl hukukun yeni savaşlardaki (spesifik olarak siber savaşlardaki) yeri gibi Uİ literatüründe özellikle kuramsal çerçeveden irdelenmemiş bir alan, karşı çıkma teorisi ile yakın dönem gelişmeleri ışığında incelenmiş olacaktır.

## 1. KARŞI ÇIKMA VE ULUSLARARASI NORMLAR

Yeni savaşlarda uluslararası hukuk kurallarının ve uluslararası normların meşruiyeti sorusu, değişen normlar ve normların kullanımdaki anlamını (*meaning-in-use*) değiştirmek gibi konuları incelemeyi gerektirmektedir. Anlam değişimlerini normlara karşı çıkışların ifade ediliş ve usullerinde gözlemlemek mümkündür. Çatışmaları ve değişimi anlamak için aktörlerin kültürleri, söylemleri ve sosyal teamülleri incelenmektedir. Bu bağlamda, Wiener'e (2014: 2) göre "bir sosyal aktivite olarak karşı çıkma, yönetişim normlarına ilişkin söylemsel ve eleştirel bir ilişki içerdiğinden ister sesli ister sessiz olsun, sosyal değişimin temelini oluşturur, çünkü her zaman eleştirel bir şekilde oyunun kurallarının düzeltilmesini/onarılmasını içerir" (Wiener, 2014: 2). Sonuç olarak, "karşı çıkma birbiriyle çelişen yaklaşımlara odaklanmış normatif ancak pratiğe dayalı bir yaklaşım olarak ortaya çıkmaktadır" (Wiener, 2017: 3). Dolayısıyla bu kuram, karşı çıkma ve aktörlerin normları eleştirmeleri gibi sosyal pratiklerin, normların anlamlarını nasıl etkileyebileceği ve değiştirebileceğiyle ilgilenmektedir.

Bu yaklaşım çerçevesinde bakıldığında, bu makalede yeni savaşlar bağlamında incelenmekte olan *jus ad bellum* ve *jus in bello* normları da kendiliğinden belirlenmiş (/anlamlandırılmış) değildir. Wiener'e (2014: 29) göre, normlar hem bir bağlam içerisinde hem de sosyal olarak oluşturulmaktadır. Ayrıca, normlar katı ve değişmeyen bir şekilde değil, esnek ve değişime açık bir biçimde ele alınmaktadır. Wiener'e (2014: 37) göre üç tür norm vardır: temel normlar (*fundamental norms*), düzenleyici prensipler (*organizing principles*) ve

standartlaştırılmış prosedürler (*standardized procedures*).[4] Wiener (2014: 37), böylesi bir sıralama ve sınıflandırma ile ahlaki olarak en geniş ölçekte tanımlanan temel normları siyaset ve siyasi süreçlerin veya hukuk ve hukuki süreçlerin oluşturduğu düzenleyici prensiplerden ayırt ederek ve bunları da basit talimatlar (/şartlar) içeren standartlaştırılmış prosedürlerden ayrı tutarak aktörler arasındaki belirli uyumluluk koşullarını, çekişmeleri ve olası çatışmaları incelemenin ve belirlemenin mümkün olduğunu vurgulamaktadır.

Bu sınıflandırma ışığında, *jus ad bellum* ve *jus in bello*, "politika yapılırken ve/veya politikalar yoluyla ortaya çıkarken normativitenin müzakere edildiği" (Wiener, 2014: 59) düzenleyici prensipler (diğer bir deyişle, temel normlar ile standartlar ve düzenlemeler arasındaki normlar) olarak ele alınabilir. Müzakere edilmiş normativite, bir normun tartışılmasına atıfta bulunur ve bu tartışma veya karşı çıkma, temel olarak normların kullanımına veya anlamlarına yöneltilen itirazlardan oluşur. Guzzini'nin (2005: 497) belirttiği gibi "anlamlar ve bilgi sosyal olarak inşa edilmektedir". Bu, karşı çıkmanın ve aktörler tarafından normlara karşı çıkılabilmesinin (*contestedness*) altında yatan düşüncedir. Tüm aktörlerin bir normun kullanım şeklini ve anlamını belirleyen farklı kültürel geçmişleri bulunmaktadır. Bunun sonucunda, her aktörün (/norm kullanıcılarının) kültürel geçmişine bağlı olarak belirli bir norm hakkında ve bu normun uygulanması ve onaylanmasında farklı fikri olabilir.

Farklı kültürel geçmişlerden dolayı, düşünceler ve söylemlerdeki çeşitlilik, normların politikalar üzerindeki etkilerini anlamanın yanında anlamlarını ve bir normun uygulanmasını kavramaya da yardımcı olabilir. Dünya, Soğuk Savaş'ın sona ermesinden sonra devletler arasında iletişimin ve sosyalleşmenin artmasıyla daha çoğulcu bir yer halini almıştır. Ancak bu durum, aktörlerin kültürel geçmişlerini arkalarında bıraktıkları anlamına gelmemektedir. Bu nedenle, Wolff ve Zimmermann'ın (2015: 11) da vurguladığı gibi "kültür ciddiye alınmalıdır". Sonuçta, farklı bakış açılarının yarattığı tartışma ve karşı çıkmalar, normlara meşruiyet kazandırabilecektir. Dünya siyaseti artık Soğuk Savaş döneminde olduğu gibi iki ideolojik kamp arasında bir denge sağlamakla sınırlı değildir. Artık norm kullanıcılarının ve normdan etkilenenlerin (*stakeholder*) söylemlerini, normların kullanımına ve anlamlarına yönelik fikirlerini şekillendiren çok sayıda kültür bulunmaktadır. Bu nedenle, çeşitli politikalar arasında sentez gerekmektedir. Sonuç olarak, "normların anlamları interaktif süreçlerde

[4] Temel normların örneklerini devletlerin iç işlerine müdahale etmeme prensibi, işkence yasağı, hukukun üstünlüğü vb. normlar oluştururken, yönetim prensiplerine Koruma Sorumluluğunu (*Responsibility to Protect, R2P*), standart prosedürlere ise anlaşmalar ile anlaşmaların veya sözleşmelerin şartlarını örnek göstermek mümkündür (Wiener, 2014: 37).

yaratıldığından ve belirli bağlamlardaki sosyal pratiklere dayandığından, normlar bitmeyen yorumlama (/anlamlandırma) döngülerinin bir parçasıdır" (Wolff ve Zimmermann, 2015: 11). Bu durum, normlara karşı çıkılabilmesinin altında yatan temel nedendir.

Wiener'e (2014: 19) göre, "bir normun aktörler tarafından ortak olarak tanınması (/aynı anlama gelmesi)" daha az olasıdır, çünkü norm kullanıcılarının farklı kültürel geçmişleri vardır. Bu kültürel geçmişler, Wiener'in uluslararası ilişkilere benzer olduğunu düşündüğü kültürlerarası ilişkileri oluşturur. Normdan etkilenen tüm aktörler, bir normun kullanımdaki anlamını tartışır veya buna itiraz ederler. Sonunda bu itiraz, temel normlar ve prosedürler (düzenlemeler) arasındaki meşruiyet boşluğuna işaret eder. Karşı çıkmanın amacı normdaki meşruiyet boşluğunu doldurmaktır ve "normatif anlamın yeniden inşası"na atıf yapmaktadır" (Wiener, 2014: 19).

Meşruiyet boşluğu problemini anlamak için, norm ile ilgili karşı çıkmaya kimlerin katıldığını ve katılanların geçmişlerini incelemek önem taşımaktadır. Karşı çıkma yaklaşımı "belirli bir norma ve bu normun uygulanmasına odaklanmak yerine, tartışma sürecine ve bunu çözmek için gelişen sürece ve uygulamalara odaklanır" (Tully'den alıntılayan Wiener, 2018: 89). Wiener'e (2018: 88) göre "karşı çıkmanın yeni fırsatlar doğurması muhtemeldir". Bu bağlamda, şu soruları odağa yerleştirmek mümkündür: Normlar hakkında birbiriyle çelişen fikirler, normların uygulanmasını ve temel normları nasıl etkiler? Normların meşruiyet boşluğunu karşı çıkma ile doldurmak mümkün müdür? Bu karşı çıkma süreci normların anlamlarını nasıl etkiler? Yeni savaşlarda aktörlerin eylemlerini *jus ad bellum* ve *jus in bello* çerçevesinde değerlendirmek ya da meşrulaştırmak mümkün müdür? Bu soruları cevaplamak ve bu normların anlamını evrenselleştirebilmek, aktörlerin yarattığı politikaların süreçlerini incelemeyi gerektirmektedir. Belirli durumlarda farklı aktörlerin stratejilerini incelemek ve bu normları meşrulaştırmak için çelişen fikirlerini ve politikalarını tespit etmek, normların anlamını değiştirebilecek durumların ortaya çıkarılması açısından önem taşımaktadır. Bu çerçevede öncelikle *jus ad bellum* ve *jus in bello* kavramlarının temel anlamlarını incelemekte fayda vardır.

## 2. *JUS AD BELLUM* VE *JUS IN BELLO*

*Jus ad bellum*, yeni savaşlar ile ortaya çıkmış bir norm değildir, geleneksel savaş anlayışı çerçevesinde ileri sürülmüştür ve temel olarak savaşın haklı bir gerekçeye dayandırılarak açılmasıyla ilgilenmektedir. Normun altı bileşenini adil/haklı sebep, doğru niyet, yetkili makam, makul başarı şansı, orantılılık ve son çare oluşturmaktadır (Howe, 2006: 45). Eğer uluslararası arenada bir aktör

haklı/adil bir savaş açacaksa, bu kriterleri gözetmesi gerekmektedir. İlk bileşen, savaş açmayı adil/haklı bir nedene dayandırma zorunluluğunu ifade ederken, doğru niyet kriteri ise destekleyici eylemlerde bulunmayı içermektedir (Dolan, 2005: 164). Murphy'e (2014: 45) göre yetkili makam ise, temelini hukuktan alan, insan hakları ve hukukun gücüne saygı duyan, devlet topraklarında etkin kontrole sahip meşru otoriteyi ifade eder (dolayısıyla başarısız ve haydut devletler bu tanımın dışında tutulmaktadır). Bu üç kriterin sağlanması ilan edilen bir savaşı haklı kılmaya yetmemektedir. Savaşın sonucunda eğer istikrarsız veya başarısız bir devlet doğacaksa ya da savaş gereksiz acılara ve zayiata neden olacaksa, makul bir başarı şansının olduğu söylenemez. Benzer şekilde, Murphy'nin (2014: 187) de belirttiği üzere orantılılık da gerçekleştirilecek fiilin sonuçlarının tartılmasını, kullanılan araçların hedefle orantılı olmasını ve kâr-zarar hesaplamalarının yapılmasını gerektirmektedir. Tüm bu değerlendirmeler, son çare kriterine göre, savaşı başlatmadan önce diğer alternatiflerin tüketilmesi ve bu alternatif yollarla başarıya ulaşılamaması durumunda anlam kazanacaktır. Eğer savaşa girmek akılcı değilse son çare olarak bile olsa savaşmak ihtimaller dahilinde değerlendirilmemelidir (Murphy, 2014: 160).

Diğer taraftan *jus in bello* normu savaş sırasındaki fiillere odaklanmaktadır. Bu normun zayiatları nasıl kısıtladığını anlamak için, "orantılılık, ayrımcılık ve sınırlı savaş kavramı" şartlarını anlamak önemlidir (Howe, 2006: 45). Orantılılık şartı, hedef ile hedefe ulaşmak için kullanılan araçların uyumlu olması gerekliliğini ortaya koyar. Bunun yanı sıra ayrımcılık şartı, savaşanlar ile savaşmayanların birbirinden ayrılması anlamına gelmektedir. Örneğin, siviller ile askerler birbirlerinden ayrılmadır, çünkü sivillerin kendilerini askerlerden koruyacak malzeme ve mühimmatı bulunmamaktadır (Meisels, 2012; Shue, 1978). Ayrımcılık şartının temelini simetrik güçler arasında gerçekleşen geleneksel savaşlar oluşturmaktadır. Son olarak, sınırlı savaş kavramı, topyekûn savaşın yaşanmaması için gereklidir. Bu üç gereksinim birbiriyle bağlantılıdır ve temel olarak savaşın aşırılıklara tırmanmasını ve savaşta nefreti önlemeye yöneliktir.

İkinci Dünya Savaşı, sivillerin korunması gerekliliğini aşikâr hale getirmiş ve savaş sonrası dönemde bu konuda adımlar atılmaya başlanmıştır. Sadece askeri güçler arasında savaşın yapılışına dair (savaş alanında yaralılara muamele ve savaş esirlerine muamele gibi) kuralları belirlemekle kalmayıp savaşların yeni aktörlerini ve mekanlarını göz önünde bulunduran ve savaş sırasında sivillerin korunmasına yönelik kurallar da ortaya koyan 1949 Cenevre Sözleşmeleri[5] bu

[5] Sırasıyla Sözleşmelerin tam başlıkları şöyledir: "Geneva Convention for the Amelioration of the Condition of the Wounded and Sick Armed Forces in the Field"; "Geneva Convention for the

anlamda uluslararası insancıl hukukun temel yapıtaşlarından birini oluşturmuştur. Charmatz ve Witt (1953: 39) bu sözleşmenin temelde savaş esirlerinin tehdit ve şiddetten korunması için tasarlandığını belirtmiştir. Diğer taraftan Pictet (1951: 468) bu sözleşme temelinde *jus in bello*'nun resmi olarak ilan edilen ya da edilmeyen bütün savaşlarda uygulanabilir olduğuna dikkat çekmektedir. Ne var ki, bu normların gerektirdiği şartların geleneksel savaşlara göre tanımlanmış olması yeni savaşlarda bu iki normun anlamına ilişkin tartışma alanları doğurmuştur.

Yeni savaşlar asimetrik bir yapıya sahip olduklarından, aktörlerin politikaları ve uygulamaları *jus in bello* normuna ve şartlarına bir karşı çıkma oluşturmuştur. Geleneksel savaşlarda askerlerin kahramanlığı savaşın en önemli parçalarından birini oluşturmaktaydı. Diğer taraftan, teknolojik gelişmeler ve artan medya kaynak ve kanalları beraberlerinde getirdikleri gerçek zamanlı bilgi akışıyla halkların bilincini de artırmıştır. Savaşlar sırasında sivil kayıpları en aza indirmek önemli bir konu olmakla beraber devletler kendi askerlerinin yaşamlarını korumayı daha ön plana çıkarmaya başlamışlardır. Sonuç olarak, "av(lanma) olarak savaş" kavramı (*war-as-hunt*) ortaya çıkmıştır (Guillaume vd., 2016). Bu nedenle, ayrımcılık kuralına yeni savaşlarda meydan okunmuştur ve ne uluslararası hukuk ne de *jus in bello* yeni savaşların belirsizliği ile başa çıkmayı başaramamıştır. Aynı sorun *jus ad bellum* için de geçerlidir. Bu nedenle, av olarak savaş kavramının oluşması sonucunda ve asimetrik savaş istisnadan ziyade kurala dönüştüğünden, bu iki norm yeni savaşları tam olarak kapsayamamıştır. Yine de bu normları ve düzenlemeleri yeni savaşlarda meşru araçlar olarak görmek mümkündür. Çünkü her iki norm da savaşlarda gereksiz acıları önlemek ve aşırılıklardan kaçınılmasını sağlamak amacıyla oluşturulmuştur. Aynı zamanda, savaş bağlamında temel insan haklarını korumaya çalışmaktadırlar. Kısacası, genel olarak devlet ve milli çıkar temelli değil insan temelli olan bu normlar, yeni savaşlarla başa çıkmada ve zararı en aza indirgemede güncel gereksinimleri karşılayamayan mevcut sözleşmelerden ve düzenlemelerden daha sağlam bir temele ve felsefi altyapıya sahiptirler. Bu iddiayı siber tehditler ve siber savaş örnekleri üzerinden desteklemek mümkündür.

## 3. SİBER UZAY, SİBER TEHDİTLER VE SİBER SAVAŞ

Siber tehditleri ve savaşları tartışmadan önce siber uzay kavramının açıklanması gerekmektedir. Siber uzay altı temel özelliğe sahiptir: karmaşıklık

Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea"; "Geneva Convention Relative to the Treatment of Prisoners of War"; "Geneva Convention Relative to the Protection of Civilian Persons in Time of War".

(Choucri, 2000: 125), hızlı gelişen yapı (Tikk, 2010: 110), anonim bir karakter, yönetilemez bir doğa (Barnard-Wills ve Ashenden, 2012: 116, 118), asimetrik savaş üretme eğilimi (Reveron, 2012: 148; Barnard-Wills ve Ashenden, 2012: 118) ve düşük maliyetli (siber) silah üretme kapasitesi (Kelsey, 2008: 1145). Bu özellikler siber tehditlerin başlıca kaynaklarını oluşturmaktadırlar ve siber alanın güvenli olmadığını düşündürtmektedirler.

Anonimliği, siber uzaydaki başlıca sorun olarak tanımlamak mümkündür. Bir saldırgan, geleneksel savaşın ve/veya saldırıların aksine, siber uzayda çok daha rahat saklanabilmektedir. Yakalanma ihtimalinin çok daha az olması yeni tehditler ve aktörleri doğururken diğer taraftan siber alanda sivillerin daha geniş çapta zarar görebileceği saldırı ihtimallerini ortaya çıkarmaktadır. Dönüşen/çeşitlenen kavramlar (gelenekselden yeniye, kahramanlıktan post-kahramanlığa) ve gelişen teknolojiler (süvarilerden hava kuvvetlerine ve siber uzaya), tüm dünyada uluslararası hukuk ve politika ile ilgili yeni rekabet ve çatışma alanları yaratmaktadırlar.

2000'li yılların başında bilgisayar bilimlerindeki gelişmeler sonucunda güvenlik uzmanları, siber güvenlik anlayışının ortaya çıkmasına sebep olan, farklı kavramlara ve analiz düzeyine sahip yeni bir güvenlik tehdidiyle karşı karşıya kalmışlardır. Küreselleşmenin ve karşılıklı bağımlılığın bir sonucu olarak siber tehditlerin önemi artmaktadır. Geleneksel savaş alanı veya savaşan anlayışı, ya da karşı karşıya gelerek savaşan askerler siber alanda mevcut değildir. Buradaki aktörler, gerilla savaşlarındaki kamuflajlı askerler gibi karanlık köşelerde saklanmaktadırlar. Silah ve kurşunlara karşılık olarak bilgisayar kodları ve virüsleri ortaya çıkmıştır. Nye'nin (2013) gözlemlediği gibi, dünya "bombalardan baytlara doğru" evirilmektedir. Dolayısıyla, bilgi çağıyla birlikte geleneksel savaş alanı ve asker anlayışı, siber uzay ve bilgisayar korsanlarını (*hacker*) içeren yeni bir dünyaya dönüşmektedir.

Cavelty ve Manuer'e (2010: 180) göre, üç siber tehdit oluşumu vardır: siber suç, siber terörizm ve siber savaş. Uluslararası toplumun tüm aktörleri bu tehditlere maruz kalabilir, çünkü "potansiyel zarar her yerdedir" (Gartzke, 2013: 52). Bununla birlikte, "siber uzay, siber iletişimin güvenliğini değil, iletişimin basitliğini en üst düzeye çıkarmak için tasarlanmıştır" (Eriksson ve Giacomello, 2006: 225). Dolayısıyla, Eriksson ve Giacomello (2006: 222) bilgi devriminin toplumun tüm kesimleri için daha güvenliksiz bir dünya yarattığını öne sürmektedir. Siber tehditlerin belirlenememesi, siber uzayın karmaşıklığı ve hızlı gelişen karakterinin bir sonucudur (Tikk, 2010: 110), bu nedenle de güvenlik teorileri siber sorunları uluslararası güvenliğe dahil etmeyi başaramamıştır. Sosyal

inşacılık dışında çoğu teori siber tehditleri güvenlik sorunu olarak açıklamakta yetersiz kalmaktadır. Özellikle ana akım teorileri siber uzaydaki tehlikeleri tehdit olarak nitelendirebiliyor olsalar da bunları ulusal güvenlik sorunları olarak görmemektedirler, çünkü mevcut vakalarda herhangi bir can kaybı olmamıştır. Sonuç olarak, "siber savaş" teriminin aldatıcı olduğu, çünkü yeterince şiddet içermediği iddia edilmektedir (Gartzke, 2013: 49). Yine de Kello'ya (2013: 8) göre askeri olmayan diğer tehditlerin ve geleneksel olmayan aktörlerin ekonomik ve sosyal zarar verebilme yeteneğinin güvenlik çalışmaları alanına önemli etkileri bulunmaktadır.

Siber tehditlerin nasıl gerçek, fiziksel, güvenliksizleştirici ve daimî hale geldiğini değerlendirebilmek için küreselleşmeyi de anlamak gerekmektedir. Keohane ve Nye'ye (2000: 105) göre "küreselleşme, mesafelerin önemli ölçüde küçülmesini ifade etmektedir". Küreselleşmenin etkilerini vurgulamak için Nye ve Welch (2011: 347) ise şu örneği sunmaktadırlar: "Çiçek hastalığının 1789'da Avustralya'ya ulaşması üç bin yıl kadar sürmüşken AIDS yaklaşık otuz yılda dünya çağında görülmeye başlanmış, ancak *love bug* [aşk böceği] isimli bilgisayar virüsü üç gün içinde tüm dünyaya yayılmıştır".

Ayrıca Keohane ve Nye'ye (2000) göre sadece ekonomik küreselleşme şeklinde tek tip bir küreselleşme yoktur. Askeri ve kültürel küreselleşmeler de mevcuttur. Aynı zamanda, günümüzde siber küreselleşmeden bahsetmek de mümkündür (Keohane ve Nye, 2000). Bilgi çağıyla birlikte dünya, uluslararası ve yerel arenalarda neredeyse tüm aktörleri etkileyen karşılıklı siber bağımlılığa tanıklık etmektedir. Çoğu devlet şu anda askeri ve ekonomik kapasitelerini artırmak için yüksek teknolojiye sahip siber sistemlere bağımlıdır. Bu nedenle, Nye'nin (2013) gözlemlediği gibi siber sistemlere bağımlılık, teröristlerin bu sistemleri sömürme ihtimali nedeniyle devletlere zarar verebilmektedir. Siber sistemler, askeri ve sivil kullanımları olan çift yönlü araçlardır ve bunları yakalanmadan kullanmak kolaydır. "Askeri ve ekonomik faaliyetlerin desteklenmesi için karmaşık siber sistemlere bağımlılık, büyük güce sahip devletlerde, devlet dışı aktörler tarafından sömürülebilecek yeni güvenlik açıkları yaratmaktadır" (Gartzke, 2013: 41). Sonuç olarak, siber uzayın karakteristik özellikleri sonucunda devlet egemenliği ve korunması tartışılabilir bir hal almaya başlamıştır. Ayrıca, siber uzay aktörlerin anlaşmazlıklarının daha sık gün yüzüne çıkmasına neden olabilmektedir. Bu nedenlerle, küreselleşme ve bilgi çağıyla birlikte yeni bir güvenlik anlayışı ve yeni savaş/tehdit kavramlarının ortaya çıktığı söylenebilir.

Bu tehditlerden biri olan siber terörizm genellikle devlet dışı aktörlerle ilintilidir (Nye, 2013, 9). Terörizm, "siyasi amaçlarla, savaşmayanları (*non-*

*combatants*) öldürmeye yönelik ya da şiddet içeren bir biçimde kasıtlı olarak hedef almak" olarak tanımlanabilir (Coady'den alıntılayan McMahan, 2004: 694). Bu tanım çerçevesinde, siber terörizm de savaşmayanları, siyasi emelleri doğrultusunda siber uzayı kullanarak öldürmeye yönelik hareketlerde bulunmak ya da şiddet içeren bir biçimde kasıtlı olarak hedef almak şeklinde değerlendirilebilir. Ancak bu tanımlamaya siber uzayın yapısı itibariyle ciddi ekonomik ve sosyal zarar verme eylemlerini de eklemek gerekmektedir.[6] Sonuç olarak siber uzay, teröristlerin devletlere, toplumlara, örgütlere ve bireylere karşı, siber uzayın anonimlik sağlayan unsurlarından ve (güvenlik anlamında) tam kontrolünün sağlanamıyor olmasından faydalanarak fiziksel bir tehdit oluşturabilmesine ve teröristlerin eylemlerini yakalanmadan gerçekleştirebilmelerine olanak sağlamaktadır. Bir terörist, interneti kullanarak bir devletin altyapısına ve ulusal güvenliğine büyük zarar verebilir. Ayrıca teröristler, web sitelerini kullanarak radikal düşüncelerini milyonlara iletebilmekte ve yaygın etki yaratabilmektedirler.[7]

Gartzke (2013), siber uzayda korunmanın tam olarak sağlanamayacağını ve diğer güvensizlik biçimleri de dahil olmak üzere siber uzayın farklı tehditler doğurabileceğini belirtse de siber teröristlerin oluşturduğu tehlikelerin sadece rahatsızlık ve öfkeye neden olan boş tehditler olduğunu ileri sürmektedir. Dolayısıyla, herhangi bir can kaybına yol açmadığı sürece, terörizm olarak adlandırılmaması gerektiğini öne sürmekte ve siber terörizmi gerçek ve etkili bir terörist eylem olarak tanımlamamaktadır (Gartzke, 2013: 51). Buna karşılık, mevcut teknolojiler fiziksel zararı da mümkün kılmıştır. Örneğin teröristler bir yolcu uçağının uçuş sistemine bağlanıp uçağın düşmesine ve yüksek sayıda can kaybına neden olabilirler. Bunun yanı sıra, siber uzay üzerinden gerçekleştirilebilecek saldırılarla teröristlerin toplumu ekonomik, kültürel ve/veya sosyal olarak etkileyebilme, vatandaşlar arasında korku, endişe ve yılgınlık yaratabilme, hükümetler içinse ciddi krizlere neden olabilme ihtimalleri söz konusudur.

[6] El Kaide lideri Usame Bin Ladin'in siber uzayı hem Amerikan ekonomisine hem de manevi değerlerine zarar verebileceği bir yer olarak tanımlaması bu tehdidi örnekler niteliktedir (Mueller III, 2013: 236).

[7] İnternetten alınan bilgi ile fiziksel bir saldırının kombinasyonu olan "melez saldırı" olarak değerlendirilebilecek bir örnekte, herhangi bir terör örgütü ile bağlantısı olduğu tespit edilmemiş radikal bir cihat destekçisi olarak tanımlanan Tsarnaev isimli şahıs 15 Nisan 2013'te Boston Maratonu'na bir saldırı düzenlemiştir. İnternetten edindiği bilgilerle düdüklü tencereyi bombaya dönüştürerek saldırısını gerçekleştiren Tsarnaev ve erkek kardeşlerinin saldırıyı gerçekleştirmeden önce militan İslami web siteleri okuduğuna ve bunlardan etkilendiklerine dair kanıtlar bulunmuştur (Mueller III, 2013: 236).

Diğer taraftan, devlet-dışı aktörlerce gerçekleştirildiği varsayılan siber terörizmden farklı olarak karşımıza çıkan siber savaş mevcut hukuk kuralları ile *jus ad bellum* ve *jus in bello*'ya karşı çıkmanın farklı bir boyutunu ortaya çıkarmaktadır. Gentry ve Eckert (2014) gibi bazı yazarlar, siber savaşı geleneksel savaşlardan farklı kavramlarla tanımlamışlardır. Böylesi bir yaklaşımla siber savaşların kavramsallaştırmasının savaş anlayışının derinliğini artıracağı söylenebilir. Kelsey (2008), siber savaşın bazı özgün özelliklerini ve bu özelliklerin sonuçlarını açıklamaktadır. 1899 ve 1907 Lahey Sözleşmeleri uyarınca devletlerin savaşan olmayanlara zarar vermesi uluslararası hukukta yasaklanmıştır. İkinci kısımda da belirtildiği üzere, 1949 Cenevre Sözleşmeleri ile de Uluslararası İnsancıl Hukuk bu kurallar netleştirilmiştir. Ne var ki, siber savaşta savaşan ve savaşmayanlar arasında bir ayrım yapılamamaktadır. Siber uzayın küresel ve çift kullanımlı/amaçlı teknolojilere dayanan yapısı dolayısıyla, savaşan ve savaşmayan ayrımı olmadan siber saldırılar herkese zarar verebilir. Ayrıca, kullanıcıların anonim/gizli kalma kabiliyetleri nedeniyle, siber dünyada düşmanları müttefiklerden ayırt etmek neredeyse olanaksız hale gelmiştir. Saldırılar, müttefik bir devletin sınırları içerisindeki bir düşman gruptan ya da bireyden gelebilir. Ayrıca siber savaş, geleneksel bir savaşı yürütmekten çok daha düşük maliyetlidir. Bu nedenle, aktörlerin saldırı tercihlerini siber savaştan yana kullanmaları muhtemeldir. Kelsey (2008: 1449), tüm bu özellikleri nedeniyle siber savaşı "insan hayatı ve kaynaklar kullanımında asgari zararla savaş" olarak tanımlamaktadır.

Siber uzayın hızla gelişen karakteri, siber saldırıya karşı tam bir savunmayı imkânsız hale getirmektedir. Siber saldırı, savunmadan çok daha düşük maliyetlidir. Bunun yanında anonimlik özelliği eylemi gerçekleştirenlerin yakalanma riskini oldukça düşürdüğünden siber saldırıyı/savaşı saldırganlar açısından daha cazip kılmaktadır. Sonuç olarak siber uzay, asimetrik bir savaş yaratmakta, bu da saldırganlar açısından elverişli görülmektedir. Bu nedenle Gartzke (2013: 44-45), ABD'nin veya diğer büyük güçlerin tehlike altında olduğunu, çünkü birçok küçük ulusun veya devlet dışı aktörün siber alanın asimetrik özelliğinden faydalanma eğiliminde olduğunu ve siber savaşın uluslararası toplum için gerçek ve sürekli bir tehdit haline geldiğini ileri sürmektedir. Lynn'in (2010: 99) örneğinde belirttiği gibi, "bilgisayar programcıları, sömürmeye açık bir zayıflık bulurlarsa, ABD'nin küresel lojistik ağını tehdit edebilir, operasyon planlarını çalabilir, istihbarat yeteneklerini kör edebilir veya hedeflerini vurma yeteneğini engelleyebilirler". Buna karşılık, Walt siber tehdidin siber uzayın karmaşıklığı ve belirsizliğinin bir sonucu olarak abartıldığını öne sürmektedir. Sıradan bir bireyin bilgisayar bilimlerini bilmeden siber tehditleri gerçekten anlayamayacağına ve siber saldırıdan ne kadar bilginin

çalındığının da açık olmadığına dikkat çeken Walt (2010), siber tehditlerin iddia edildiği kadar büyük bir tehlike olmadığını savunmaktadır.

Diğer taraftan siber tehditlerin boyutunu vurgulamak adına siber savaş ile Pearl Harbor saldırısı arasında benzetme yapılmaktadır (Naim, 2017: 88). Hem öngörülememeleri hem de çabuk gerçekleşmeleri nedeniyle ikisi de önlenmesi kolay olmayan saldırı özelliği taşımaktadır. Öngörülemezlik açısından Pearl Harbor saldırısı her ne kadar siber savaşa benzese de bir siber saldırı çok daha hızlı gerçekleşebilecektir. Diğer taraftan, siber saldırıda Pearl Harbor'a kıyasla can kaybının çok daha az olacağı varsayılabilir. Bu nedenle, elektronik Pearl Harbor'un geleneksel saldırılardan farklı yeni özellikleri ve sonuçları olacaktır. Böyle bir saldırıyla telefon sistemleri çökebilir, ulaşım durabilir, banka işlemleri yapılamaz hale gelebilir ve bunun sonucunda toplum ve yönetim normal fonksiyonlarını yerine getirme kabiliyetini yitirebilir (Eriksson ve Giacomello, 2006: 226). Dolayısıyla belirli siyasi, toplumsal ve/veya ekonomik emellere ulaşmak için yapılan bu tür bir saldırı devletlerin egemenliğine meydan okumak ve iç işlerine müdahale olarak yorumlanabilir. Siber uzayın karakteristik özelliklerinin beraberinde getirdiği tehditleri bir ulusal güvenlik meselesi olarak görmek mümkündür. Sonuç olarak bu yeni tehdit, devlet egemenliği ve iç işlerine müdahale etmeme[8] normlarına karşı yeni bir tartışma alanı (*contestation area*) ortaya çıkarmaktadır (Lantis ve Bloomberg, 2018: 161).

Ayrıca devletler, siber ve geleneksel taktikleri ve silahları birleştiren melez savaş (*hybrid war*) stratejilerini (Gürcistan savaşında yaşandığı gibi) kullanabilirler. Gartzke'ye (2013: 57) göre, bu sadece geleneksel anlamdaki güç unsurlarının kullanılmasından daha etkilidir, çünkü melez savaş ile şehirleri bombalamak gibi fiziksel yıkıma neden olan saldırılarla kısa vadeli bir etki bırakmanın ötesinde uzun süreli ya da kalıcı bir etki yaratılabilmektedir. Güvenlik çalışmalarında yeni kavramlar üretilse bile, "siber tehditler hızla gelişmekte ve dolayısıyla, eksiksiz bir siber tehdit listesi oluşturmak imkânsızlaşmaktadır" (Tikk, 2010: 110).

Yine de büyük güçler arasında bir siber savaş, aralarındaki karşılıklı bağımlılık nedeniyle yüksek olasılıklı olarak nitelendirilmemektedir (Brenner, 2013: 18). Öte yandan, iktidar boşluğundan dolayı çatışmaların yaşanmakta olduğu bölgelerde siber savaşlar veya saldırılar görülebilir ve/veya terör örgütleri bu bölgelerde siber alanda daha aktif olabilirler. Bu nedenle, siber alanı kapsayan

[8] BM Antlaşması (1945) Madde 2, Paragraf 7'ye göre, "İşbu Antlaşma'nın hiçbir hükmü, Birleşmiş Milletlere herhangi bir devletin kendi iç yetki alanına giren konulara müdahale yetkisi vermediği gibi üyeleri de bu türden konuları işbu Antlaşma uyarınca bir çözüme bağlamaya zorlayamaz; ancak, bu ilke VII. Bölümde öngörülmüş olan zorlayıcı önlemlerin uygulanmasını hiçbir biçimde engellemez".

uluslararası bir düzenlemeye gerek duyulmaktadır. Siber alanı kapsayacak, bağlayıcı nitelikte bir düzenleme yapılması bu makalenin açıklamaya çalıştığı temel soruyu ortaya koymaktadır: *jus ad bellum* ve *jus in bello* normlarını siber uzayda meşru kaynaklar olarak görmek nasıl mümkün olabilir?

20. yüzyılda, siber suç, siber terörizm ve siber savaş olgusu yoktu. Buna bağlı olarak, Birleşmiş Milletler (BM) Antlaşması'nın yeterince güncel olmadığını ve 21. yüzyıldaki yeni savaşların kendine has özelliklerini pek çok nedenden ötürü kapsamadığını söylemek mümkündür. En önemlisi, 1945 tarihli BM Antlaşması, siber savaş kavramını ve taktiklerini göz önünde bulundurmamaktadır, "çünkü içerdiği 'güç kullanımı' dili, siber savaş taktikleri için değil, kinetik silah kullanan saldırgan devletler için tasarlanmıştır" (Kim, 2011: 327). Haataja'nın (2019, 80) da ifade ettiği gibi mevcut hukuk anlayışını yansıtan BM Antlaşması (spesifik olarak Madde 2 Paragraf 4)[9] devletlerin egemenliğinin merkezde olduğu ve fiziksel şiddetin devletlere ve uluslararası düzene tehdit oluşturduğunu varsayan bir ontoloji üzerine kuruludur. BM Antlaşması'nın bütününe bakıldığında, özellikle VII. Bölüm'de Madde 41 ve Madde 42'de ifade edilen yetkiler çerçevesinde, güç kullanımı ile esas kastedilenin askeri güç kullanımı olduğu görülmektedir. Bu bağlamda, siber savaşlar konusundaki bir diğer sorunsalı da devlet dışı bir aktörün bir devlete siber saldırı yapması oluşturmaktadır. BM Antlaşması ve savaş hukukunu düzenleyen antlaşmalarda (1899 ve 1907 Lahey Sözleşmeleri ve 1949 Cenevre Sözleşmeleri gibi) devletlerin birbirlerine saldırmalarının ya da savaş açmalarının odakta olduğu görülmektedir. Haataja'nın (2019, 84) da dikkat çektiği üzere, "Madde 2 Paragraf 4 çerçevesinde hasara ya da zarara sebebiyet veren belirli bir tür devletlerarası şiddet içeren askeri güç kullanımı yasaklanmıştır". Bu tek yönlü bakış açısına ve günün gerekliliklerinin farklı olmasına rağmen hukuki eksiklikleri gidermek adına siber alanda devletlerin davranışlarını düzenleyen uluslararası anlaşmalar bulunmamaktadır.

Özetle, siber alan uluslararası hukuk açısından yeni bir sorunsal oluşturmaktadır. Siber alanın asimetrik olması ve anonimlik sağlaması ile devlet egemenliği ve iç işlerine müdahale etmeme normlarıyla çatışması bu alandaki meşruiyet sorununun özünü oluşturmakta ve mevcut meşruiyet açığını (*legitimacy gap*) genişletmektedir. Bu yüzden siber alanın devlet egemenliği ilkesi ve uluslararası insancıl hukuk prosedürleri ile olan ilişkisi bir karşı çıkma alanı olarak ortaya çıkmaktadır. Bu çerçevede, siber uzaya dair hukuki düzenlemeler

[9] BM Antlaşması (1945) Madde 2, Paragraf 4'e göre, "Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığına karşı, gerek Birleşmiş Milletler'in Amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar".

yapılıncaya dek *jus ad bellum* ve *jus in bello*'yu meşruiyet açığını kapatmak üzere kullanılabilecek yönetim prensipleri olarak görmek mümkündür. Bu normların kullanımdaki anlamlarını evrenselleştirebilmek için, bu tartışma/çatışma alanlarının ve karşı çıkmanın incelenmesi önemlidir. Bu amaçla, sonraki bölümde Gürcistan, Estonya ve Stuxnet vakalarına değinilecektir.

## 4. GÜRCİSTAN, ESTONYA VE STUXNET VAKALARI

Gürcistan ve Estonya vakalarının esas olarak Rusya'nın siber politikalarının bir sonucu olduğunu söylemek mümkündür. Rusya'nın siber alana dair çalışmaları önem arz etmektedir, çünkü bu alandaki girişimler, devletlerin çabaları ve karşılıklı iş birlikleriyle siber uzayda temel kuralların uygulanabileceğini göstermiştir. Ayrıca, siber alanın kendine has özelliklerinin uluslararası hukuk için bir rekabet alanı yaratabileceğini ve nihayetinde uluslararası normların güçlendirilmesine hizmet edebileceğini de ortaya koymuştur.

Siber uzay her ne kadar dünyanın her yerindeki devletleri, örgütleri ve bireyleri etkilese de Rusya'nın ayırt edici özelliği, istikrarsız ve çatışma içeren bölgelere yakınlığından kaynaklanmaktadır. Belirtildiği gibi, istikrarsız bölgelerde siber terörizm daha yaygın olma eğilimindedir. Siber uzayın ve Rusya'nın kendine has özelliklerinin bir sonucu olarak, Rusya "Bilgi Güvenliği Doktrini"ni oluşturmak zorunda kalmıştır. Doktrinin bilgi güvenliği olarak adlandırılması, Rusya'nın siber savaşı "bilgi savaşı" olarak değerlendirmesinden kaynaklanmaktadır (Choucri ve Goldsmith, 2012: 73). Bu söylem (ya da kavramsallaştırma), Rusya'nın tarihsel ve kültürel arka planını yansıtması nedeniyle önemlidir. Bu kavramsallaştırmanın Rus hükümetinin internette gizlenmiş olan bilgilerin siber alandaki tüm tehditlerden daha önemli olduğu algısından kaynaklandığını söylemek mümkündür. Choucri ve Goldsmith'e (2012: 73) göre, Rusya, bilgi savaşını "bir devletin, başka bir devletin politik, ekonomik ve sosyal düzenine zarar verme eylemi" olarak görmektedir. Rusya'nın siber uzayı ve siber savaş kavramını neden bu kadar önemsediğini gösteren ilk olay Çeçen savaşı olmuştur. Reveron'un (2012: 176) belirttiği gibi, 1994 ve 1996 yılları arasında gerçekleşen Birinci Çeçen Savaşı'ndaki Rus deneyimi—özellikle Çeçenler'in askerî harekât ve istihbarat işlemlerini yürütmek için bilgisayar ve iletişim teknolojilerini kullanması—Rus ulusal güvenlik camiasını bu yeni teknolojik tehlikelere karşı uyarmasının yanı sıra Rusya'nın bu yeni teknolojileri kullanma kabiliyetindeki zayıflığını (ve de isteğini) ortaya çıkarmıştır. Bu deneyim sonucunda Rusya kapsamlı bir siber politika oluşturmak için çalışmalara başlamıştır (Reveron, 2012: 176).

Rusya, Çeçen Savaşı'nda siber terörü, Ukrayna, Estonya ve Gürcistan'da ise siber savaşları tecrübe etmiş, *WikiLeaks* olayında ise (kapalı kapı diplomasisini ve bu toplantıların karar ve detaylarını siber araçlar aracılığıyla kamuoyuna sızdıran) siber casusluğa tanık olmuştur. Ayrıca, Rusya, "Arap Baharı" ile siber uzayın ne kadar güçlü bir araç olduğunu ve ne denli bir etkiye sahip olabileceğini deneyimlemiştir. Bu da siber uzayı bu deneyimler neticesinde ulusal sınırları olan bir alan olarak tanımlayan Rusya'yı, ulusal bir güvenlik sorunu olarak nitelendirdiği siber uzay stratejisini oluşturmaya itmiştir (Ebert ve Maurer, 2013: 1066; Giles, 2012b: 2). "Rus siber uzayına müdahale etmeme, internet egemenliği [*internet sovereignty*] ve bilgi alanını [*information space*] kontrol etme", Rusya'nın siber uzayı güvence altına alma konusunda başlıca hedeflerini oluşturmaktadır (Giles, 2012b: 2).

Savunma politikalarına uygun olarak, Rusya siber uzayda saldırı gücünü de artırmaya çalışmaktadır. Rusya'da, siber terörle ilgili sorunları ele almak için oluşturulan birkaç ekibin yanı sıra, bir de hacker okulu bulunmaktadır. Bu nedenle, Rusya'nın savaşlarda siber araçları kullanmayı düşündüğü iddia edilebilir. Clapper'in (2016: 3) belirttiği gibi, Rusya'nın kamuoyu incelemesi arttığında ve hatta bu alandaki eylemleri ortaya çıkarılsa bile siber alanda kritik altyapı sistemlerini hedef alma ve casusluk operasyonları yürütme konusundaki istekliliğinin bir sonucu olarak kendine daha güvenli bir duruş sergilediği görülmektedir.

Nitekim Dünya, Estonya ve Gürcistan'daki savaşlarda Rusya'nın siber araçları kullandığına tanık olmuştur. Rusya ne bu olayların sorumluluğunu üstüne almış, ne de açık ve net olarak konuyla ilişkisini yalanlamıştır. Bazıları, Rusya'nın bu siber saldırıların arkasında olduğunu iddia ederken, Deibert (2011: 4) ise o dönemde bu bağlantıyı kanıtlamanın imkânsız olduğuna dikkat çekmektedir. Bu örnekte olduğu gibi, herhangi bir devletin siber uzayı kendine has özelliklerinin bir sonucu olan zayıf yönlerinden faydalanmak ve güç elde etmek için kullanma ihtimali her zaman bulunmaktadır.

Rusya'nın siber ortamı kontrol altında tutarak güvence altına almak istemesi (Giles, 2012a: 65) ve Estonya ile Gürcistan'a yönelik eylemlerin Rusya tarafından gerçekleştirildiği iddiası, genel olarak uluslararası insancıl hukukun normlarına ve *jus ad bellum* ile *jus in bello*'ya bir karşı çıkma olarak değerlendirilebilir. Özetle, Estonya ve Gürcistan savaşları, bu normların anlamlarının, kapsamının ve meşruiyetinin siber uzayda güçlendirilmesi gerektiğini göstermektedir. Bu nedenle, Estonya ve Gürcistan vakalarını incelemek, Rusya'nın uluslararası savaş norm ve yasalarına karşı çıkmasını daha iyi anlamak için önem taşımaktadır.

Estonya Soğuk Savaş bittikten sonra bağımsızlığını kazanmış ve yüzünü Avrupa'ya çeviren ilk eski Sovyet Bloğu devleti olmuştur. 1995 yılında Avrupa Birliği (AB) üyeliğine başvuran Estonya, 2004 yılından beridir AB ve Kuzey Atlantik Antlaşması Örgütü'nün (NATO) üyesidir. Rusya için stratejik önemi olan Estonya'nın bu hamleleri Rusya'yı rahatsız etmiştir. Özellikle İkinci Dünya Savaşı'ndan sonra Rusya, Avrupa'yı güvenilmez bir aktör olarak görmüş ve şüpheyle yaklaşmıştır. İki dünya savaşında da kendisine karşı tüm saldırıların başta Almanya olmak üzere Avrupa'dan gelmiş olması nedeniyle Rusya, Estonya ve Gürcistan'ın bağımsızlığından sonra milli güvenliği için bu iki ülkeyle Ukrayna'nın bulunduğu alanı içeren bir tampon bölge oluşturma eğiliminde olmuştur (Haas, 2009: 4). Mearsheimer'a (2016: 28) göre Estonya yüzünü Avrupa'ya çevirdiğinde, Rusya bunu bir tehdit olarak değerlendirmiş ve Estonya örneğinin diğer eski Sovyet bloğu devletlerini de teşvik edebileceğinden endişelenmiştir.

Estonya-Rusya çatışmasındaki tetikleyici neden, Nisan 2007'de Estonya'nın (Rusya'nın Estonyalıları nasıl kurtardığını irdeleyen bir bağımsızlık sembolü olarak nitelendirilen) Bronz Asker Heykeli'ni sökmesi olmuştur. Bunu takiben, Rusya'nın Estonya internet ağları (*network*) üzerindeki siber saldırılara başladığı iddia edilmiştir. Böylesi bir siber stratejinin Rusya için avantajlı olduğu söylenebilir, çünkü Estonya'da Wi-Fi internet ağları ülkenin hemen hemen tamamını kapsamakta, kamu hizmetleri online olarak sunulmakta ve nüfusun %86'sı bankacılık işlemlerini online olarak yapmakta olduğu için Estonya'nın internete oldukça ihtiyaç duyduğunu söylemek mümkündür (Kozlowski, 2014: 238). Bu nedenle Delerue'nin (2017: 5) belirttiği gibi, Estonya, Rusya'nın siber saldırısını silahlı saldırı olarak değerlendirmiş ve NATO Antlaşması'nın 5. Maddesi'nin uygulanmasını talep etmiştir. Ancak, Rusya suçlamaları reddetmiş, NATO da Estonya'nın çağrılarını kabul etmemiştir.

Adı geçen dönemde ülkeler arasında gerçekleşen bu siber saldırılar savaş olarak nitelendirilmemiştir. Yine de bu siber saldırıları ve politikaları, uluslararası hukuka karşı çıkma olarak anlamlandırmak mümkündür. Bu karşı çıkma, Rusya'nın (sınırlara sahip) siber uzay anlayışından ve siber alanda öngördüğü egemenlik kuralından kaynaklanmaktadır. Siber uzayın anonimlik sağlaması ve asimetrik olması Rusya'nın kendi siber politikasını oluşturmasında belirleyici unsurlar olmuştur. Bunun yanı sıra, savaştan sonra Estonya internet güvenliğini hızla artırmıştır. Robinson'un da (2017: 134) belirttiği gibi, "2007'de Estonya'ya yapılan ve kısa bir süre boyunca ülkenin büyük kısmında internet kesintisine neden olan siber saldırılar, tüm dünya açısından bir uyandırma servisi işlevi görmüştür". Dünyanın daha önce şahit olmadığı bir melez savaş örneği olan

Gürcistan olayında ise siber uzayın getirdiği tehditler daha gözle görülür hale gelmiştir.

Gürcistan, Sovyetler Birliği'nin 1991 yılında dağılmasından sonra bağımsızlığını kazanmış ve Güney Osetya Gürcistan'ın egemenliği altındaki bir bölge olarak kabul edilmiştir. 7 Ağustos 2008'de, Güney Osetya'da bazı Rusya destekli ayrılıkçıların başlattığı hareketi bastırmaya karar veren Gürcistan askeri saldırı başlatmış, Rusya'nın ertesi gün karşılık vermesiyle de savaş başlamıştır. Bu savaş yaklaşık bir hafta içinde sona ermiş olmakla beraber siber saldırılar 27 Ağustos 2008 tarihine kadar devam etmiştir. Tikk'in (2010: 71) belirttiği gibi, "Gürcistan'a yönelik siber saldırılar, Estonya olayındakine benzer şekilde, öncelikle kamuya açık web sitelerinin tahrif edilmesini ve çok sayıda kamu ve özel (finansal ve medya) hedeflere yönelik DDoS [*Distributed Denial of Service*] saldırılarını içermektedir". Swaine'ye (2008) göre, "bilgisayar korsanları, Gürcistan internet sitelerine yönelik olarak, bir siteye aynı anda binlerce ziyaretçi yönlendirmeleri ve bu yoğunluğun da siteleri çevrimdışı hale getirmesi için DDoS saldırılarını kullanmışlardır". Resmî açıklamalarında "Gürcistan Hükümeti, siber saldırıların, Gürcistan'ın eyaleti olarak kabul edilen Güney Osetya'da iki devletin arasında sürmekte olan ihtilafın bir parçası olarak Rusya'nın yaptığı eylemlerden kaynaklandığını belirtmiştir" (Swaine, 2008). Rusya ise siber saldırılara dair suçlamaları reddetmekle beraber askeri kuvvetleriyle Güney Osetya ve Gürcistan topraklarına girmiştir (Clarke ve Knake, 2012: 21).

Estonya vakasının tanık olunan ilk siber savaş olduğu iddia edilebilir fakat geleneksel savaşlar gibi şiddet içermediği düşünüldüğü için siber savaş olarak kabul görmemiştir. Fakat Rusya-Gürcistan Savaşı'nda, Rusya'nın geleneksel savaş taktiklerinin yanında siber savaş taktiklerini de kullanması Gürcistan vakasının siber savaş olarak nitelendirilmesi için yeterli olmuştur. Rusya'nın geliştirmekte olduğu siber politikaların ve itham edildiği siber saldırıların bir sonucu olarak NATO, siber saldırıları NATO Antlaşması'nın 5. Maddesi'ni tetikleyecek silahlı bir saldırı olarak kabul edilmesi konusunu değerlendirmeye başlamıştır. 2014 yılında "NATO'nun Geliştirilmiş Siber Savunma Politikası"nda (*the Enhanced NATO policy on Cyber Defence*) belirtildiği üzere "ilk defa siber savunma, NATO Antlaşması'nın 5. Maddesi'ndeki kolektif savunma şemsiyesi altına alınmıştır" (Robinson, 2017: 137). Galler'deki Kuzey Atlantik Konseyi Toplantısı'nın sonucu olan Galler Zirvesi Bildirgesi siber tehdit ve saldırıların "daha yaygın, karmaşık ve potansiyel olarak zararlı olmaya devam" edeceği görüşünden yola çıkarak "Gelişmiş Siber Savunma Politikası"nı onaylamıştır. Geleneksel bir saldırının boyutlarında zarara neden olabileceği ifade edilen siber saldırılara istinaden "NATO'nun temel siber savunma sorumluluğunun kendi

ağlarını savunmak olduğunu[n] ve Müttefiklerin de ulusal ağların korunmasına yönelik uygun yeteneklerin geliştirilmesi konusunda sorumluluğu olduğunu"nun vurgulandığı belgede "uluslararası insancıl hukuk ve BM Antlaşması da dahil olmak üzere uluslararası hukukun siber alana uygulanabilirliği" kabul edilmiştir. Ayrıca "Siber savunmanın NATO'nun toplu savunma görevinin bir parçası olduğunu"nun kabul edildiği bu belgede 5. Madde'nin siber saldırı durumlarında uygulanmasının her durum için Kuzey Atlantik Konseyi tarafından ilgili duruma göre (*case-by-case*) ele alınacağı da ifade edilmektedir (NATO, 2014). Bu bildirgenin en önemli sonuçlarından biri siber saldırıların silahlı saldırı tanımı altına alınabilme ihtimali olmuştur. Bu nedenle siber uzay, NATO için uluslararası insancıl hukukun konusu haline gelmiştir. Robinson'un (2017: 137) belirttiği gibi, "Galler'deki bu bildirge ile uluslararası insancıl hukuk ve BM Antlaşması da dahil olmak üzere uluslararası hukukun siber uzayı kapsayacağı kabul edilmiştir".

Rusya'nın politikaları ve siber uzay anlayışı uluslararası hukuk çerçevesinde siber savaş teriminin kullanılmasına sebebiyet vermiştir. Daha önce ifade edildiği üzere, Rusya'nın Estonya'ya yönelik eylemleri siber savaş olarak kabul edilmemiştir (Waterman, 2007). Bu durum, *jus ad bellum* ve *jus in bello*'nun siber alandaki meşruiyetinin o dönemde zayıf olduğu şeklinde değerlendirilebilir. Özetle, uluslararası toplum (meşruiyet boşluğunun bir sonucu olarak) bu iki normun siber uzayda etkili olacağını değerlendirmemiştir. Ancak, Rusya'nın Gürcistan'a yönelik eylemleri bu düşünce tarzını değiştirmiştir. Rusya'nın uluslararası hukuktaki meşruiyet boşluğundan ve siber uzayın kendine has özelliklerinden faydalanmasının bir sonucu olarak *jus ad bellum* ve *jus in bello*'nun kapsamı yeni savaşları da dahil edecek biçimde değerlendirilmeye başlanmış ve NATO, uluslararası insancıl hukuk ve BM Antlaşması dahil, uluslararası hukukun siber alana uygulanabilirliğini kabul etmiştir. Sonuç olarak, Rusya'nın devletlerin egemenliği normuna karşı çıkması—siber uzayın özelliklerinden faydalanarak Estonya ve Gürcistan'ın iç işlerine müdahale etmesi yani egemenlik alanını ihlal etmesi—en azından NATO için *jus ad bellum* ve *jus in bello*'yu siber alanda meşru normlar haline getirmiştir. Bu konudaki karşı çıkma ve bu normların siber alandaki anlam ve önemi Stuxnet olayında daha da belirgin hale gelmiştir.

Uluslararası toplumun neden siber alanda uluslararası prosedürlere ihtiyaç duyduğunun önemli bir örneğini oluşturan Stuxnet vakası, Estonya ve Gürcistan'a yönelik saldırılardan daha karmaşık, can kaybı olmamasına rağmen fiziksel hasara sebebiyet vermiş ve oldukça gelişmiş teknolojilerin kullanıldığı bir örnek olarak karşımıza çıkmaktadır. Bu noktada, İran'ın Natanz nükleer tesisine düzenlenen saldırıyı irdelemek önemlidir. 2005 yılında Uluslararası Atom Enerjisi

Ajansı'nın aldığı karara göre, "İran'ın ihlal ve kusurları NPT'den [Nükleer Silahların Yayılmasının Önlenmesine İlişkin Anlaşma] doğan yükümlülüklerine aykırılık teşkil etmektedir". İran, Natanz'daki nükleer santrali silah geliştirmek için değil, yalnızca sivil araçların altyapısını iyileştirmek için kurulduğunu iddia etmiş olsa da stratejik ve tarihsel nedenlerden dolayı İran'ın bu girişiminin İsrail'i rahatsız etmiş olabileceği varsayımı mantıklı görünmektedir. Washington Post'ta yayınlanan bir habere göre "Stuxnet ilk olarak George W. Bush yönetimi sırasında geliştirilmişti ve asıl amacı, nükleer santraldeki başarısızlıkların neden gerçekleşmiş olabileceği konusunda, İranlı bilim adamları arasında kafa karışıklığı yaratıp, kademeli olarak İran'ın nükleer kabiliyetine zarar vermekti" (Nakashima ve Warrick, 2012). Neticede 2010 yılında Natanz'daki uranyum zenginleştirme tesisinin santrifüj sistemlerine yerleştirilen Stuxnet virüsü, İran'ın nükleer programını 18-24 aylığına durdurmuştur. Bu virüs, santrifüjlerin gereğinden fazla çalışarak tesise zarar vermesine yol açmıştır. Virüs "güvenlik sistemlerini kapatmış, böylece operatörlerin her şeyin yolunda olduğunu düşünmelerini sağlamıştır", görevini tamamladığında ise kendisini yok etmiştir. Ayrıca, "belirli bir konfigürasyon bulamazsa, virüs nispeten zararsız kalmaktadır" (Fildes, 2010), bu nedenle, o güne dek görülen en gelişmiş bilgisayar virüsü olduğu söylenebilir.

İran saldırı sonucunda can kaybı olmadığını ancak ekonomik kayıp ve farklı sıkıntıların yaşandığını belirtmiştir. Stuxnet'te yaşanan ikincil/tali zararlar (*collateral damage*) ise geleneksel savaşlara kıyasla daha az olmuştur. Ne var ki, sebep olduğu toplam zararın %60'lık bölümü İran'ı etkileyen Stuxnet virüsü, İran dışında Hindistan, Endonezya, Çin, Azerbaycan, Güney Kore, Malezya, ABD, İngiltere, Avustralya, Güney Kore, Finlandiya ve Almanya'daki yaklaşık 60.000 bilgisayarı da etkilemiştir (Farwell ve Rohozinski, 2011: 34). Ayrıca, Stuxnet virüsünün diğer ülkelerdeki bilgisayarlara nasıl yayıldığı konusu da açıklığa kavuşturulamamıştır (Farwell ve Rohozinski, 2011: 34). Brenner'e (2013: 17) göre, "Stuxnet, Microsoft işletim sistemlerinde önceden bilinmeyen en az dört ayrı güvenlik açığını kullanan oldukça sofistike, çok adımlı bir saldırıydı". Bir birey ya da örgütün kendi başına geliştirmesine imkân tanımayacak derecede gelişmiş teknolojisine ve gerektiği yatırıma istinaden ABD ve İsrail'in Stuxnet'in arkasında olduğunu iddia edilmiştir (Nakashima ve Warrick, 2012). Fakat saldırıyı gerçekleştirenler anonim kalmayı başarmışlar ve bu saldırıyla İran'a, nükleer emellerinden ve her ne kadar barışçıl niyetli olduğu iddia edilse de uranyum zenginleştirme tutkusundan vazgeçmesi için bir mesaj vermişlerdir (Farwell ve Rohozinski, 2011: 31). Sonuç olarak, İran'ın uluslararası ilişkilerindeki yalnızlığı, siber uzayın özellikleri ve uluslararası hukukta siber uzaya dair tanımlamaların ve kısıtlayıcı/tanımlayıcı kuralların eksikliği, temel olarak Stuxnet'in

gerçekleşebilmesinin ve yaptırımsız kalmasının arkasındaki nedenleri oluşturmaktadır.

Temel uluslararası hukuk prensipleri çerçevesinde değerlendirildiğinde, bir ülkenin nükleer tesislerini bombalamak bir uluslararası hukuk ihlali olarak ve saldırı suçu olarak nitelendirilebilir. Fakat, yapılageliş itibariyle Stuxnet'i bir savaş açma eylemi ya da saldırı suçu olarak düşünmek mümkün müdür? Yukarıda belirtildiği gibi BM Antlaşması ve geçmiş Güvenlik Konseyi ve Genel Kurul kararları spesifik olarak siber saldırıları savaş nedeni olarak ele almamanın yanı sıra bir saldırı eylemi[10] olarak da tanımlamamaktadır. Normal şartlarda saldırı fiilinin gerçekleşmesi saldırıya uğrayan devletin BM Antlaşması'nın 51. Maddesi ışığında meşru savunma hakkını kullanmasına imkân verecektir. Geleneksel yaklaşımlara göre böyle bir saldırıyı BM Antlaşması'nın 51. Maddesi ya da Madde 2(4) altında ele almak mümkün olmasa da değişen koşullar sonucunda geleneksel yaklaşımlara karşı çıkıldığını söylemek mümkündür. *Jus ad bellum* ve *jus in bello*'nun siber alanda kullanımı, bu karşı çıkmaların bir sonucu olarak gerçekleşebilecektir.

Uluslararası Hukukun temel süjesi olarak kabul edilen devletler, BM Antlaşması çerçevesinde birbirlerinin iç işlerine karışması ve birbirlerine karşı güç kullanması yasaklanmış egemen eşitler olarak görülmektedir. Böylesi bir yaklaşım da devletleri "statik ve doğası itibariyle hudutlarıyla kendilerini tanımlayan (bölgesel) varlıklar olarak gördüğü için, sadece belirli şiddet türlerinin devlete ve uluslararası barış ve güvenliğe tehdit oluşturduğu" kabul edilmektedir (Haataja, 2019: 80). Örneğin, Estonya'ya yapılan saldırının o zamanlar siber savaş olarak algılanmaması araştırmacıların siber saldırıların/savaşların klasik anlamda şiddet içermediğini düşünmelerinden kaynaklanmıştır (Gartzke, 2013: 41-73). Daha sonra tecrübe edilen Gürcistan ve Stuxnet vakaları ise siber savaşın devletlere ve uluslararası topluma verebileceği potansiyel zararın ve meşruiyet boşluğunun kanıtlarını oluşturmuştur. Haataja'nın (2019: 79) da ifade ettiği gibi, uluslararası hukuk somut etkileri olan siber saldırıları yönetebilir durumda olmasına rağmen maddi zarar doğurmayan saldırılar söz konusu olduğunda sınırlı bir kapasiteye sahiptir.

## 5. MEŞRUİYET BOŞLUĞUNUN SORGULANMASI VE YENİ POLİTİKALAR

Gelişmekte olan siber teknoloji ve savaş teknolojileri düşünüldüğünde uluslararası hukuka ve normlara karşı çıkmaların artması olağan görünmektedir.

[10] Bkz., BM Genel Kurulu'nun 3314 Sayılı Kararı.

Diğer taraftan, bu karşı çıkmaların meşruiyet boşluğunun kapatılmasına yardımcı olması da söz konusudur. Nitekim Estonya, Gürcistan ve Stuxnet vakaları sonrasında ortaya çıkan tartışmalar ve NATO gibi örgütlerin bu anlamda geliştirmeye başladıkları yeni politikalar yaygın etki sağlayabilecek niteliktedir. Bunların önemli bir örneğini Gürcistan ve Estonya vakaları sonrasında NATO Cooperative Cyber Defence Centre of Excellence inisiyatifle Michael Schmitt editörlüğünde Uluslararası Hukuk uzmanlarınca hazırlanmış, ilk versiyonu 2013'te ikinci versiyonu ise 2017'de yayımlanan Tallinn El Kitabı (tam adıyla *Tallinn Manual on the International Law Applicable to Cyber Warfare*) oluşturmaktadır (CCDCOE, 2019). Siber operasyonlara dair kuralları belirlemeye ve siber saldırıların yasak olup olmadığına ve yasaksa ne zamanlarda yasak olduğuna dair bir çalışma olan El Kitabı, kuralları tanımlarken *jus ad bellum* ve *jus in bello* normlarını temel almaktadır (Schmitt, 2017: 3).[11]

Resmi bir belge olmayan ve herhangi bir kurum ya da kuruluşun görüşlerini temsil etmediği ifade edilen (Schmitt, 2017: 2) Tallinn El Kitabı'nın mevcut hukuki açığı kapatmaya yönelik önemli bir yumuşak hukuk girişimi olduğunu söylemek mümkündür. Diğer taraftan, BM çatısı altında konunun değerlendirmeleri ciddi önem arz etmektedir. BM Genel Sekreteri'nin 2010'daki Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanındaki Gelişmelere İlişkin Raporu'nda belirtilen görüş şöyledir: "mevcut uluslararası hukukun siber alana uygulanabilirliği hakkında ciddi tartışmalar mevcuttur […] ve görüşümüz, hem kuvvet kullanımı hem de silahlı çatışma hukuku konusundaki mevcut uluslararası hukuk ilkelerinin, siber uzaydaki çatışmaları tanımlamak ve analiz etmek bağlamında kullanımının uygun olduğu yönündedir" (BMGK, 2010). Özellikle Stuxnet'ten sonra BM raporları, siber alanda barışı korumada BM Antlaşması'nın, uluslararası insancıl hukukun ve normların öneminden bahsetmektedir. Sonuç olarak, 2013 yılında gerçekleşen, "Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanındaki Gelişmelere İlişkin Hükümet Uzmanları Grubu BM Raporu"nun 16. ve 19. paragraflarında belirtildiği üzere:

> Devletlerin Bilgi ve İletişim Teknolojilerini (BİT) kullanımıyla ilgili mevcut uluslararası yasalardan türetilen normların uygulanması, uluslararası barış, güvenlik ve istikrarın sağlanmasında önemli bir kaynaktır. Bu tür normların Devlet davranışına nasıl uygulanacağına dair ortak anlayışlar geliştirmek ve devletlerin bu teknolojileri nasıl kullanması

[11] Örneğin, *jus ad bellum* temelinde (silahlı) saldırıyı meşru müdafaa hakkını doğuran bir siber operasyon olarak tanımlayan El Kitabı (bkz. Kural 71), *jus in bello* çerçevesinde ise savunma ya da saldırı amaçlı, şiddet içeren belirli bir askeri operasyon (bkz. Kural 92) olarak yorumlamaktadır (Schmitt, 2017: 5).

> gerektiği konusu daha fazla çalışmayı gerektirmektedir. BİT'lerin benzersiz özellikleri göz önünde bulundurulduğunda, zaman içinde ek normlar geliştirilebilir (BMGK, 2013).

Bu bağlamda, Uluslararası Hukuk ve özellikle BM Antlaşması, barışı ve istikrarı korumak ve açık, güvenli, barışçıl ve erişilebilir bir BİT ortamını teşvik etmek için uygulanabilir bir kaynaktır ve aynı zamanda bu hedefe ulaşmak için gereklidir.

Son olarak, 2015 yılındaki "BM Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanındaki Gelişmelerle İlgili Hükümet Uzmanları Grubu Raporu", siber uzaydaki normların önemine vurgu yapmıştır. Bu raporun 10. fıkrasında belirtildiği üzere:

> Normlar, uluslararası toplumun beklentilerini yansıtmaktadır, devlet davranışına standartlar getirir ve uluslararası toplumun, devletlerin faaliyetlerini ve niyetlerini değerlendirmesine olanak sağlar. Normlar, BİT ortamındaki çatışmayı önlemeye yardımcı olabilir ve BİT'lerin küresel sosyal ve ekonomik kalkınmayı artırmaktaki görevini tam anlamıyla yerine getirmesi için bu araçların barışçıl kullanımına katkıda bulunabilir. (BMGK, 2015).

Bu raporlar, *jus ad bellum* ve *jus in bello*'nun meşru araçlar olduğunu ve yeni savaşlarda kullanılmalarının yeni gelişmelerle güçlenebileceğini göstermektedir. Buna göre, Uluslararası Kızılhaç Örgütü'nün (ICRC) 2018'deki insani gündeminde bu normların yeni savaşlardaki yerini ve anlamlarını genişletmek için siber uzay konusu ele alınmıştır. "Siber saldırılar[ı], son zamanlarda ortaya çıkan sorunlardan bir tanesi" olarak tanımlayan ICRC, hükümetleri ve şirketleri, sanal dünyadaki çatışmanın insanî sonuçlarıyla ilgilenmeye ve kritik soruları ele almaya çağırmaktadır (Maurer, 2018). Güvenlik sorunu ile savaş eylemi arasındaki fark nedir? Orantılılık ilkesi nasıl uygulanır? Siber saldırılarda sivil hedefler ile askeri hedefler arasında nasıl bir ayrım yapılabilir? Bu soruların cevaplanması ve sivilleri siber saldırı ve savaşlarda çatışmadan ve zarardan korumak için daha güçlü ve daha özenle hazırlanmış kuralların geliştirilmesi günümüz uluslararası hukuku için elzemdir. Başlangıç olarak da Tallinn El Kitabı'nda temelleri atıldığı üzere, uluslararası insancıl hukukun temel kuralları baz alınarak siber savaşlara ve diğer yeni teknolojilere uygulanabilir hale getirilmelidir.

## 6. SONUÇ

Devletlerin siber politikaları ve siber savaş deneyimleri *jus ad bellum* ve *jus in bello* normlarının siber alanda meşru araçlar olarak görülebildiğini—en azından

NATO, BM ve ICRC nezdinde—kanıtlamıştır. Kısacası, bu iki normun tarihsel anlamı değişmemiştir. Savaşların insanileştirilmesi ve savaşlarda dahi insancıl davranılması bu iki normun temelini oluşturmaktadır. Estonya, Gürcistan ve Stuxnet tecrübeleri bu iki normun siber uzaydaki anlamını ve meşruiyetini güçlendirmiştir. Bu nedenle, bu makalenin temel iddiası, *jus ad bellum* ve *jus in bello*'nun kullanımdaki anlamlarının incelenen tartışmalar ve karşı çıkmalar sonucunda siber uzayda da evrensel olarak kabul edilebileceğidir. Geniş ve kapsamlı bir siber güvenlik tanımı[12] yapılarak siber alanın karakteristik özellikleri temelinde sadece can kaybına dayalı bir zarar anlayışının geride bırakılması ve siber güvenliği uluslararası hukukun ele aldığı bir uluslararası güvenlik konusu olarak tanımlanması önemli ilk adımlar olacaktır. Nye ve Welch, bilgi çağının bir sonucu olarak yakın gelecekte ulus-devlet yapısının çözülmesini öngörmektedir. Tıpkı süvariler ve barutun Orta Çağ'da kaleleri yıktığı gibi, şimdi de internetin ulus-devlet dönemini kapatacağını ileri sürmektedirler. Askerlerin "kahramanca mücadele ettiği" simetrik (geleneksel) savaşlar kaybolurken küreselleşme ve bilgi çağı siber tehditleri gittikçe daha gerçek ve sürekli hale getirmektedir (Nye ve Welch, 2011: 425).

Uluslararası sistemin ve devletlerin dönüşümü her ne ile sınırlı kalırsa kalsın kavramsal ve uygulamadaki değişim ve dönüşümler ile devlet pratiklerinin ortaya koyduğu mevcut normlara karşı çıkmalar uluslararası hukukta güncel düzenlemelerin gerekliliğini gözler önüne sermektedir. Sonuç olarak, uluslararası hukukun günün gerekliliklerine karşılık verebilmesi ve devlet ve/veya devlet dışı aktörlerin meşruiyet boşluğunu suiistimal etmesini engellemek için mevcut güvenlik anlayışının derinleştirilmesi, saldırı tanımının gözden geçirilmesi ve siber uzayı kapsayacak kontrol mekanizmalarının oluşturulması gerekmektedir.

## KAYNAKÇA

Allenby, Braden R. (2014), "Are New Technologies Undermining the Laws of War?", Bulletin of the Atomic Scientists, 70 (1): 21-31.

Baker-Beall, Christopher (2014), "The evolution of the European Union's 'fight against terrorism' discourse: Constructing the terrorist 'other'", Cooperation and Conflict, 49 (2): 212-238.

[12] Güvenlik tehditlerinin yokluğu, siber güvenlik ve siber alana yönelik tehditlerin olmaması olarak tanımlanmaktadır (Eriksson ve Giacomello, 2006: 222).

Barnard-Willis, David ve Debi Ashenden (2012), "Virtual Space: Cyber War, Cyber Terror, and Risk", Space and Culture, 15 (2): 110-123.

Bassiouni, Cherif M. (2008), "The New Wars and the Crisis of Compliance with the Law of Armed Conflict by Non-State Actors", The Journal of Criminal Law and Criminology, 98 (3): 711-810.

Birleşmiş Milletler (1945), Birleşmiş Milletler Antlaşması ve Uluslararası Adalet Divanı Statüsü, https://www.ombudsman.gov.tr/contents/files/6535501-Birlesmis-Milletler-Antlasmasi.pdf (29.11.2019).

Birleşmiş Milletler Genel Kurulu (BMGK), (14 Aralık 1974), "Definition of Aggression, United Nations General Assembly", Karar 3314 (XXIX).

Birleşmiş Milletler Genel Kurulu (BMGK) (30 Temmuz 2010), "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/65/201.

Birleşmiş Milletler Genel Kurulu (BMGK) (24 Haziran 2013), "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/68/98.

Birleşmiş Milletler Genel Kurulu (BMGK) (22 Temmuz 2015), "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174.

Brenner, Joel F. (2013), "Eyes wide shut: The growing threat of cyber attacks on industrial control systems", Bulletin of Atomic Scientists, 69 (5): 15-20.

Cavelty, Myriam Dunn ve Victor Manuer (2010), The Routledge Handbook of Security Studies (New York: Routledge).

Charmatz, Jan P. ve Harold M. Witt (1953), "Repatriation of Prisoners of War and the 1949 Geneva Convention", Yale Law Journal, 62 (3): 391-415.

Choucri, Nazli (2000), Cyberpolitics in International Relations: Context, Connectivity and Content (Cambridge: MIT Press).

Choucri, Nazli ve Daniel Goldsmith (2012), "Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security", Bulletin of the Atomic Scientists, 68 (2): 70-77.

Clapper, James R. (2016), "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community",

https://www.dni.gov/files/documents/SASC_Unclassified_ 2016_ATA_SFR_FINAL.pdf (28.05.2018).

Clarke, Richard A. ve Robert Knake (2012), Cyber War: The Next Threat to National Security and What to Do About It (New York: Harper Collins).

Coverdale, John F. (2004), "An Introduction to the Just War Tradition", Pace International Law Review, 16 (2): 221-277.

Daniel III, J. Furman ve Brian A. Smith (2015), "Burke and Clausewitz on the Limitation of War", Journal of International Political Theory, 11 (3): 313-330.

Deibert, Ronald (2011), "Tracking the Emerging Arms Race in Cyberspace", Bulletin of the Atomic Scientist, 67 (1): 1-8.

Delerue, François (2017), "State Responses to Cyber Operations", Global Relations Forum Young Academics Program Policy Paper Series 5.

Dolan, Chris J. (2005), "Waging War Against Iraq: *Jus ad Bellum* Considerations", Politics and Ethics Review, 1 (2): 158-176.

Doswald-Beck, Louise (1987), "The Civilian in the Crossfire", Journal of Peace Research, 24 (3): 251-262.

Ebert, Hannes ve Tim Maurer (2013), "Contested Cyberspace and Rising Powers", Third World Quarterly, 34 (6): 1054-1074.

Echevarria II, Antulio J. (2007), "On the Clausewitz of the Cold War Reconsidering the Primacy of policy in On War", Armed Forces & Society, 34 (1): 90-108.

Eriksson, Johan ve Giampiero Giacomello (2006), "The Information Revolution, Security, and International Relations: (IR)relevant Theory?", International Political Science Review, 27 (3): 221-244.

Farwell, James P. ve Rafal Rohozinski (2011), "Stuxnet and the Future of Cyber War", Survival, 53 (1): 23-40.

Fildes, Jonathan (23 Eylül 2010), "Stuxnet worm 'targeted high-value Iranian assets'", BBC News, http://www.bbc.com/news/ technology-11388018 (15.11.2018).

Finlay, Christopher J. (2010), "Terrorism Resistance, and the Idea of 'Unlawful Combatancy'", Ethics & International Affairs, 24 (1): 91-104.

Franck, Thomas M. (2004), "Criminals, Combatants, or What? An Examination of the Role of Law in Responding to the Threat of Terror", The American Journal of International Law, 98 (4): 686-688.

Gartzke, Erik (2013), "The Myth of Cyber war: Bringing War in Cyberspace Back Down to Earth", International Security, 38 (2): 41-73.

Gentry, Caron E. ve Amy E. Eckert (2014), The Future of Just War (Athen: University of Georgia Press).

Giles, Keir (2012), "Russia's Public Stance on Cyberspace Issues", 4th International Conference on Cyber Conflict, 63-75.

Giles, Keir (2012), "Russian Cyber Security: Concepts and Current Activity", Conflict Studies Research Centre–Chatham House, 1-3.

Gregory, Derek (2011), "The Everywhere War", The Geographical Journal, 177 (3): 238-250.

Guillaume, Xavier, Rune S. Andersen ve Juha A. Vuori (2016), "Paint It Black: Colours and Social Meaning of the Battlefield", European Journal of International Relations, 22 (1): 49-71.

Guzzini, Stephan (2005), "The Concept of Power: A Constructivist Analysis", Millennium Journal of International Studies, 33 (3): 495-521.

Haas, Marcel de (2009), "NATO-Russia Relations after the Georgian Conflict", Atlantisch Perspectiefrre, 33 (7): 4-9.

Haataja, Samuli (2019), Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics (New York: Routledge).

Hajjar, Lisa (2006), "International Humanitarian Law and 'Wars on Terror': A Comparative Analyses of Israeli and American Doctrines and Policies", Journal of Palestine Studies, 36 (1): 21-42.

Herberg-Rothe, Andreas (2009), "Clausewitz's 'Wondrous Trinity' as a Coordinate System of War and Violent Conflict", International Journal of Conflict and Violence, 3 (2): 204-219.

Houweling, Henk W. ve Jan G. Siccama (1988), "The Risk of Compulsory Escalation", Journal of Peace Research, 25 (1): 43-56.

Howe, Brendan (2006), "Normative War-Fighting and the New World Order", Politics and Ethics Review, 2 (1): 38-61.

Kaldor, Mary (1996), "A Cosmopolitan Response to New Wars", Peace Review: A Journal of Social Justice, 8 (4): 505-514.

Kaldor, Mary (2005), "Old Wars, Cold Wars, New Wars, and the War on Terror", International Politics, 42 (4): 491-498.

Kaldor, Mary (2006), "The 'New War' in Iraq", A Journal of Social and Political Theory, 109: 1-27.

Kelsey, Jeffrey T.G. (2008), "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", Michigan Law Review, 106 (7): 1421-1451.

Kello, Lucas (2013), "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", International Security, 38 (2): 7-40.

Keohane, Robert O. ve Joseph S. Nye JR. (2000 Bahar), "Globalization: What's New? What's Not? (And So What?)", Foreign Policy, 118: 104-119.

Kim, Jasper (2011), "Law of War 2.0: Cyberwar and the Limits of the UN Charter", Global Policy, 2 (3): 322-328.

Kolb, Robert (1997 Ekim), "Origin of the Twin Terms *jus ad bellum/jus in bello*", International Review of the Red Cross, 37 (320): 553-562.

Kozlowski, Andrzej (2014), "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan", European Scientific Journal, 3: 237-245.

Lantis, Jeffrey S. (2006), "Strategic Culture: From Clausewitz to Constructivism", SAIC, 3-31.

Lantis, Jeffrey S. ve Daniel J. Bloomberg (2018), "Changing the Code? Norm Contestation and US Antipreneurism in Cyberspace", International Relations, 32 (2): 149- 172.

Lynn III, William J. (2010), "Defending a New Domain", Foreign Affairs, 89 (5): 97-108.

Malender, Erik, Magnus Öberg ve Jonathan Hall (2009), "Are 'New Wars' More Atrocious? Battle Severity, Civilians Killed and Forced Migration Before and After the End of the Cold War", European Journal of International Relations, 15 (3): 505-536.

Maurer, Peter (2018), 7 issues that will shape the humanitarian agenda in 2018, ICRC, https://www.icrc.org/en/document/7-issues-will-shape-humanitarian-agenda-2018 (20.02.2018).

McMahan, Jeff (2004), "Ethics of Killing in War", Ethics, 114 (4): 693-733.

McMahan, Jeff (2010), "Pacifism and Moral Theory", Diametros, 23: 44-68.

McMahan, Jeff (2010), "The Just Distribution of Harm Between Combatants and Noncombatants", Philosophy & Public Affairs, 38 (4): 342-379.

Mearsheimer, John (2016), "Defining a New Security Architecture for Europe that Brings Russia in from the Cold", Military Review, 96 (3): 27-31.

Mello, Patrick A. (2010), "In search of new wars: The debate about a transformation of war", European Journal of International Relations, 16 (2): 297-309.

Meisels, Tamar (2012), "In Defense of the Defenseless: The Morality of the Laws of War", Political Studies, 60: 919-935.

Mueller III, Rober S. (2013), "Cyber Security: Safeguarding Our Cyberspace", D. Frank Hsu ve Dorothy Marinucci (Der.), Advances in Cyber Security (New York: Fordham University Press).

Murphy, James G. (2014), War's Ends (Washington DC: Georgetown University Press).

Münkler, Herfried (2003 Mart), "The Wars of the 21st Century", Revue Internationale de la Croix-Rouge/International Review of the Red Cross, 85 (849): 7-22.

Nakashima, Ellen ve Joby Warrick (2 Haziran 2012), "Stuxnet Was Work of US and Israeli Experts Officials Say", *Washington Post*, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officialssay/2012/06/01/gJQAlnEy6U_story.html (15.11.2018).

Naim, Moises (2017), "Why Democracies are at a Disadvantage in Cyber Wars", Journal of International Affairs, 70 (Special Anniversary Issue): 85-91.

NATO (5 Eylül 2014), "Wales Summit Declaration" https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en (22.05.2019).

Nye JR., Joseph S. (2013), "From Bombs to Bytes: Can our Nuclear History Inform Our Cyber Future?", Bulletin of the Atomic Scientists, 69 (5): 8-14.

Nye JR., Joseph S. ve David A. Welch (2011), Küresel Çatışmayı ve İşbirliğini Anlamak (İstanbul: Türkiye İş Bankası Kültür Yayınları).

Pictet, Jean S. (1951), "The New Geneva Conventions for the Protection of War Victims", The American Journal of International Law, 45 (3): 462–475.

Reid, Julian (2003), "Foucault on Clausewitz Conceptualizing the Relationship Between War and Power", Alternatives, 28: 1-28.

Reveron, Derek S. (2012), Cyberspace and National Security (Washington DC: Georgetown University Press).

Robinson, Neil (2017), "Cyber Defense at NATO: From Wales to Warsaw and Beyond", Turkish Policy Quarterly, 16 (3): 133-143.

Rosen, David M. (2007), "Child Soldiers, International Humanitarian Law, and the Globalization of Childhood", American Anthropologist, 109 (2): 296-306.

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

Schuurman, Bart (2010 Bahar), "Clausewitz and the 'New Wars' Scholars", Parameters, 40 (1): 89-100.

Shue, Henry (1978), "Torture", Philosophy and Public Affairs, 7 (2): 124-143.

Swaine, Jon (11 Ağustos 2008), "Georgia: Russia 'conducting cyber war'", The Telegraph, https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html (02.05.2019).

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2019), Tallinn Manual 2.0, https://ccdcoe.org/research/tallinn-manual/ (29.12.2019).

Tikk, Eneken (2010), "Global Cybersecurity-Thinking About the Niche for NATO", SAIS Review of International Affairs, 30 (2): 105-119.

Uluslararası Atom Enerjisi Kurumu (24 Eylül 2005), "Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran", GOV/2005/77, https://www.iaea.org/sites/default/files/gov2005-77.pdf (22.05.2019).

Waldman, Thomas (2010), "Politics and War: Clausewitz's Paradoxical Equation", Parameters, 40 (3): 1-12.

Walt, Stephen M. (30 Mart 2010), "Is the Cyber Threat Overblown?", Foreign Policy, https://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/ (15.05.2016).

Waterman, Shaun (11 Haziran 2007), "Who Cyber Smacked Estonia?" United Press International, https://www.upi.com/Defense-News/2007/06/11/Analysis-Who-cyber-smacked-Estonia/26831181580439/ (18.01.2020).

Wiener, Antje (2014), A Theory of Contestation (Londra: Springer).

Wiener, Antje (2017), "Agency of the Governed in Global International Relations: Access to Norm Validation", Third World Thematics: A TWQ Journal, (online first): 1-17.

Wiener, Antje (2018), "Responsibility Contestations: A Challenge to the Moral Authority of the UN Security Council", Cornelia Ulbert, Peter Finkenbusch, Elena Sondermann ve Tobias Debiel (Der.), Moral Agency and the Politics of Responsibility (Londra: Routledge): 85-103.

Wolff, Jonas ve Lisbeth Zimmermann (2015), "Between Banyans and Battle Scenes: Liberal Norms, Contestation, and the Limits of Critique", Review of International Studies, 42 (3): 1-22.