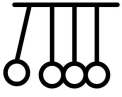


TURKEY'S UNHEARD VOICES

Siber Savaş ve Uluslararası İnsancıl Hukuk

LAW

ELAY DERİN ULAŞ

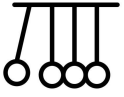


Giriş

Siber operasyonlar silahlı çatışma eşiğine ulaştığında, Uluslararası İnsancıl Hukukun ilkeleri tamamen uygulanabilir hâle gelir; ancak siber savaşın doğası bu normları derinden zorlamaktadır. Ayrım ilkesi, elektrik şebekeleri ve iletişim sistemleri gibi hem sivil hem de askerî amaçlarla kullanılan altyapıların çift kullanımlı yapısı nedeniyle karmaşık hâle gelmektedir; bu durum, meşru askerî hedefleri sivil zarara yol açmadan ayırt etmeyi zorlaştırır. Orantılılık ilkesi ise, siber operasyonların öngörülemez ve zincirleme etkileri nedeniyle baskı altındadır; bu etkiler birbirine bağlı sistemler üzerinden hızla yayılabilir ve tali zararların doğru biçimde değerlendirilmesini güçleştirir. Son olarak, askerî gereklilik ilkesi, siber operasyonların hukuka uygun bir askerî amaca ulaşmak için vazgeçilmez olmasını şart koşar ve yalnızca siyasi baskı ya da ekonomik çıkar amacıyla gerçekleştirilen eylemleri dışlar.

Uluslararası İnsancıl Hukuka Genel Bakış

Uluslararası İnsancıl Hukuk, çatışmaların yürütülmesini düzenleyen ve savaşın insani sonuçlarını en aza indirmeyi amaçlayan kamu uluslararası hukukunun bir dalıdır. Askerî gereklilik ile insan onurunun korunması arasında bir denge kurmayı hedefleyen hukuki bir çerçeve sunar. Uluslararası İnsancıl Hukuk, uluslararası ya da uluslararası nitelikte olmayan silahlı çatışma durumlarında uygulanır. Bu hukuk dalının temel dayanakları, 1949 tarihli Cenevre Sözleşmeleri ile bunlara ek olarak kabul edilen 1977 tarihli Ek Protokollerde yer almakta olup, birlikte modern insancıl hukukun temelini oluşturur. Lahey Sözleşmeleri de savaşın araç ve yöntemlerini düzenleyerek önemli katkılar sağlamaktadır. Bu metinler, sivillerin, savaş esirlerinin ve yaralıların insanca muamele görmesini güvence altına alan, devletler ve çatışmanın tarafları için bağlayıcı kuralları tesis eder. Uluslararası insancıl hukuk dört temel ilkeye dayanır. Birincisi, ayrım ilkesidir: çatışmanın tarafları, her zaman savaşımlar ile siviller arasında ayrım yapmak zorundadır. Saldırıları yalnızca askerî hedeflere yöneltilmelidir. İkincisi, beklenen askerî avantajla karşılaştırıldığında sivillere aşırı zarar verebilecek saldırıları yasaklayan orantılılık ilkesidir. Üçüncüsü, kuvvet kullanımının yalnızca meşru askerî hedeflere ulaşmak için gerekli olanla sınırlı olmasını ifade eden askerî gereklilik ilkesidir. Son olarak, tarafların gereksiz acıdan kaçınmasını ve çatışmalara doğrudan katılmayanları korumasını öngören insanlık ilkesi yer alır. Tüm bu ilkeler, çatışmaları yöneten etik ve hukuki temeli oluşturur. Uluslararası insancıl hukuk yalnızca silahlı çatışma durumlarında uygulanır; iç karışıklıklar veya barış dönemindeki gerilimlerde geçerli değildir. Çatışmayı hangi tarafın başlattığına bakılmaksızın tüm taraflar için bağlayıcıdır. Kuralları evrensel ve karşılıklı ilkesine bağlı olmayan niteliktedir; yani bir tarafın ihlali, diğer tarafın da ihlalini meşrulaştırmaz. 21. yüzyılda, siber savaş, otonom silahlar ve bilgi operasyonları gibi yeni ortaya çıkan tehditlerle birlikte uluslararası insancıl hukukun kapsamı da genişlemiştir. Çatışmaların dijitalleşmesi, geleneksel uluslararası

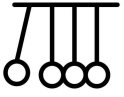


insancıl hukuk ilkelerinin siber uzayda nasıl uygulanacağına ilişkin, özellikle sivil ve askerî altyapının ayırt edilmesi bakımından, karmaşık hukuki ve etik sorular ortaya çıkarmaktadır.

Siber Savaşın Tanımı ve Niteliği

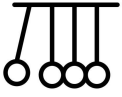
Modern çağda teknolojik gelişmeler, savaşın karakterini köklü biçimde dönüştürmüştür. Çatışmalar artık yalnızca fiziksel savaş alanlarıyla sınırlı değildir; giderek artan biçimde dijital alana da yayılmaktadır. Genellikle siber savaş olarak adlandırılan bu yeni çatışma boyutu, geleneksel uluslararası hukuk ve küresel güvenlik açısından en önemli meydan okumalardan birini temsil etmektedir. Siber operasyonlar, geleneksel silahlar kullanılmadan ulusal altyapıyı aksatma, askerî kapasiteyi zayıflatma ve sivil nüfusları tehdit etme potansiyeline sahiptir. Siber savaş teriminin uluslararası hukukta tek ve evrensel olarak kabul edilmiş bir tanımı yoktur. Genel olarak, bir devletin stratejik veya askerî amaçlarla başka bir devletin bilgisayar sistemlerine, ağlarına ya da dijital altyapısına zarar vermek, bunları aksatmak veya izinsiz kontrol altına almak için dijital saldırılar kullanmasını ifade eder. Siber Operasyonlara Uygulanabilir Uluslararası Hukuk konulu Tallinn Kılavuzu 2.0'a göre, bir siber operasyon; can kaybı, fiziksel yıkım ya da hayati hizmetlerin ciddi biçimde aksaması gibi geleneksel silahlı bir saldırıyla karşılaştırılabilir sonuçlar doğurduğunda bir "savaş eylemi" olarak nitelendirilir. Bu nedenle siber savaş, casusluk ve sabotajdan askerî ya da sivil altyapıya yönelik tam ölçekli saldırılara kadar uzanan geniş bir faaliyet yelpazesini kapsar. Siber savaş, geleneksel çatışma biçimlerinden birkaç temel açıdan farklıdır. İlk olarak, siber saldırılar görünmez dijital ağlar üzerinden gerçekleştirilir ve bu durum saldırının kaynağını ya da faili tespit etmeyi son derece zorlaştırır. Ayrıca siber operasyonlar anlık olarak gerçekleşebilir ve saniyeler içinde sınırları aşan geniş ağları etkileyebilir. Aynı zamanda, iletişim sistemleri veya enerji şebekeleri gibi birçok siber hedef hem sivil hem de askerî amaçlara hizmet eden çift kullanımlı niteliktedir; bu da savaşanlarla siviller arasındaki ayrımı bulanıklaştırır. Buna ek olarak, geleneksel askerî operasyonlarla karşılaştırıldığında siber saldırılar görece düşük maliyetlidir; ancak büyük ekonomik, politik veya stratejik zararlara yol açabilir. Son olarak, siber uzayın birbirine bağlı yapısı, tek bir saldırının dahi ulusötesi hatta küresel sonuçlar doğurabilmesi anlamına gelir. Günümüzde devletler, siber uzayı kara, deniz, hava ve uzayın yanında kritik bir savaş alanı olarak giderek daha fazla tanımaktadır. Siber yetenekler artık ulusal savunma stratejilerinin ayrılmaz bir parçasıdır ve doğrudan fiziksel çatışmaya girmeden saldırı ve savunma imkânı sağlamaktadır. Amerika Birleşik Devletleri, Rusya, Çin ve NATO üyesi devletler dâhil olmak üzere başlıca küresel aktörler, dijital alanda ulusal çıkarları korumakla görevli özel siber komutanlıklar kurmuştur. Siber savaşın stratejik önemi yalnızca yıkıcı potansiyelinden değil, aynı zamanda caydırıcılık, istihbarat toplama ve psikolojik etki yaratma kapasitesinden de kaynaklanmakta; bu da onu modern hibrit savaşın hayati bir aracı hâline getirmektedir.

Uluslararası İnsancıl Hukukun (UIH) Siber Operasyonlara Uygulanabilirliği

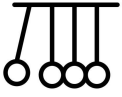


Dijital teknolojilerin hızla yayılması ve siber uzaya artan bağımlılık, modern çatışmaların doğasını köklü biçimde dönüştürmüştür. Devletler giderek daha fazla ciddi sonuçlar doğurabilecek siber operasyonlara başvururken, temel bir soru ortaya çıkmaktadır: Uluslararası İnsancıl Hukuk siber savaşa uygulanır mı? Bu soru, günümüzdeki uluslararası hukuk tartışmalarının merkezinde yer almaktadır. Geleneksel silahlı çatışmalar yerleşik hukuk kurallarıyla düzenlenmiş olsa da, siber savaşın dijital niteliği, uluslararası insancıl hukukun ne zaman ve nasıl uygulanacağını belirlemeyi zorlaştırmaktadır. Uluslararası İnsancıl Hukuk, uluslararası ya da uluslararası olmayan nitelikteki silahlı çatışma durumlarında uygulanır. Bu nedenle, siber operasyonlara UIH'nin uygulanabilirliği, söz konusu faaliyetlerin uluslararası hukukta tanımlanan silahlı çatışma eşiğini aşıp aşmadığına bağlıdır. Cenevre Sözleşmeleri'nin ortak 2. maddesine göre, savaş durumu resmen tanınmasa dahi devletler arasında meydana gelen her türlü ilan edilmiş savaş veya diğer silahlı çatışma hâllerinde uluslararası insancıl hukuk uygulanır. Dolayısıyla, bir siber operasyon; can kaybı, yaralanma ya da mülkiyetin tahribi gibi kinetik savaşla karşılaştırılabilir sonuçlar doğuruyorsa, bu durum silahlı çatışma teşkil edebilir ve uluslararası insancıl hukukun uygulanmasını tetikleyebilir. Siber Operasyonlara Uygulanabilir Uluslararası Hukuk konulu Tallinn Kılavuzu 2.0 da bu yorumu destekleyerek, etkileri geleneksel silahların yol açtığı sonuçlara eşdeğer olan siber operasyonlara uluslararası insancıl hukukun uygulanacağını belirtmektedir. Uluslararası insancıl hukukun siber operasyonlara uygulanmasındaki en büyük zorluklardan biri, bir siber faaliyetin ne zaman “silahlı saldırı” seviyesine ulaştığını belirlemektir. Çoğu akademisyen ve hukukçu, yalnızca siber casusluk, propaganda veya ekonomik aksamanın tek başına silahlı çatışma eşiğini aşmadığı konusunda hemfikirdir. Buna karşılık, fiziksel yıkıma, can kaybına yol açan veya enerji şebekeleri, hastaneler ya da hava trafik kontrol sistemleri gibi kritik altyapıları devre dışı bırakan siber operasyonlar, uluslararası insancıl hukuk kapsamında genellikle silahlı çatışma eylemleri olarak kabul edilmektedir. Atıf ilkesi de bu bağlamda hayati bir rol oynamaktadır. Uluslararası insancıl hukukun uygulanabilmesi için, siber operasyonun bir devlete ya da örgütlü bir silahlı gruba atfedilebilir olması gerekir; zira özel kişiler tarafından işlenen siber suçlar, insancıl hukuktan ziyade iç hukuk veya uluslararası ceza hukuku kapsamına girer. Uluslararası kuruluşlar ve devletler, uluslararası insancıl hukukun siber uzaydaki rolünün netleştirilmesinin önemini giderek daha fazla kabul etmektedir. Birleşmiş Milletler Hükümet Uzmanları Grubu ile Açık Uçlu Çalışma Grubu, mevcut uluslararası hukukun — buna uluslararası insancıl hukuk da dâhildir — siber uzayda uygulanabilir olduğunu teyit etmiştir. Ayrıca, birçok devlet silahlı çatışma sırasında yürütülen siber operasyonların uluslararası insancıl hukuk tarafından düzenlendiğini doğrulayan ulusal tutum belgeleri yayımlamıştır. Bununla birlikte, özellikle orantılılık ve sivillerin korunması konularında bu kuralların nasıl ve ne zaman uygulanacağına ilişkin yorum farklılıkları devam etmektedir.

Temel UIH İlkeleri: Ayrım, Orantılılık ve Askerî Gerekliklik

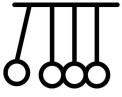


Ayrım ilkesi, uluslararası insancıl hukukun en temel ve evrensel olarak kabul edilen normlarından biridir ve Cenevre Sözleşmeleri'ne Ek I No'lu Protokol'ün 48. maddesinde kodifiye edilmiştir. Bu ilke, çatışmanın taraflarının her zaman muhariplerle sivilleri, askerî hedeflerle sivil nesneleri ayırt etmesini zorunlu kılar. Saldırıları yalnızca meşru askerî hedeflere yöneltilmelidir; sivilleri veya sivil altyapıyı kasıtlı olarak hedef alan operasyonlar kesin olarak yasaktır. Siber savaş bağlamında, ayrım ilkesinin uygulanması özellikle karmaşık hâle gelmektedir. İletişim sistemleri, enerji şebekeleri ve uydular gibi birçok siber ağ ve altyapı, hem sivil hem de askerî amaçlara hizmet eden çift kullanımlı niteliktedir. Bu kadar iç içe geçmiş sistemlerde hukuka uygun ve hukuka aykırı hedefleri ayırt etmek, günümüz çatışma düzenlemesindeki en acil sorunlardan biridir. Bu ilkeye uyulmaması, ayrım gözetmeyen saldırılara yol açabilir; bu tür saldırılar uluslararası insancıl hukukun ciddi ihlalleridir ve uluslararası ceza hukuku kapsamında savaş suçu teşkil edebilir. Orantılılık ilkesi, askerî gereklilik ile insani koruma arasında denge kurmayı amaçlayarak ayrım ilkesini tamamlar. Ek I No'lu Protokol'ün 51. maddesinde yer alan bu ilke, beklenen somut ve doğrudan askerî avantaja kıyasla sivillerin yaşamını kaybetmesine, yaralanmasına veya sivil nesnelerin zarar görmesine yol açması aşırı olacak saldırıları yasaklar. Siber alanda orantılılık değerlendirmeleri, siber operasyonların öngörülemeyen ve geniş çaplı etkileri nedeniyle özellikle zordur. Örneğin, bir askerî ağı devre dışı bırakmayı amaçlayan bir siber saldırı, aynı altyapıya bağlı sivil hastaneleri, ulaşım sistemlerini veya finans kuruluşlarını istemeden etkileyebilir. Bu tür operasyonlar birbirine bağlı sistemler içinde zincirleme yayılabildiğinden, siber uzayda orantılılığın doğru biçimde değerlendirilmesi ileri düzey teknik bilgi ve gerçek zamanlı risk analizini gerektirir. Bu nedenle komutanlar ve karar vericiler, siviller ve sivil altyapı üzerinde orantısız zarara yol açmamak için siber operasyonların dikkatle planlanmasını ve icra edilmesini sağlamak zorundadır. Askerî gereklilik ilkesi, kuvvet kullanımını meşru bir askerî hedefe ulaşmak için vazgeçilmez olanla sınırlar. Bu ilke, uluslararası insancıl hukukça yasaklanmadığı sürece, yalnızca düşmanın askerî kapasitesini zayıflatmak için gerekli olan önlemlere izin verir. Ayrım ve orantılılık ilkeleriyle yakından bağlantılıdır ve şiddetin aşırı ya da keyfî olmasını engeller. Siber savaş bağlamında gereklilik, siber operasyonların doğrudan meşru bir askerî amaca hizmet etmesini ve mümkün olan her durumda yan zararın önlenmesini ifade eder. Siyasi baskı, ekonomik çıkar veya psikolojik yıldırma amacı taşıyan ve açık bir askerî gereklilikten yoksun operasyonlar, bu nedenle uluslararası insancıl hukukun meşru sınırlarının dışında kalır. Bu ilke ayrıca, yıkıcı siber eylemlere başvurmada önce daha az zararlı alternatiflerin aranması yükümlülüğünü vurgular ve uluslararası insancıl hukukun tüm çerçevesini ayakta tutan insani kısıtlamayı güçlendirir. Ayrım, orantılılık ve askerî gereklilik farklı hukukî kavramlar olmakla birlikte, uluslararası insancıl hukuk sistemi içinde birbirine bağlı şekilde işler. Birlikte bir denge ve denetim mekanizması oluştururlar: ayrım meşru hedefleri belirler, orantılılık kuvvetin kapsamını sınırlar, gereklilik ise kuvvetin yalnızca askerî hedeflerle haklı kılındığında kullanılmasını sağlar. Siber operasyonlar alanında bu ilkelerin birlikte uygulanması, sivillerin korunmasını sürdürmek ve giderek daha karmaşık ve sınır tanımayan bir savaş ortamında hukukî hesap verebilirliği sağlamak açısından hayati öneme sahiptir.



Siber Uzayda Hukukî ve Etik Zorluklar

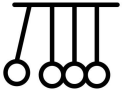
Dijital teknolojinin evrimi, yeni ve karmaşık bir çatışma alanı yaratmıştır. Siber operasyonlar devletlere stratejik ve savunma açısından avantajlar sağlarken, aynı zamanda derin hukukî ve etik sorunlar da doğurmaktadır. Siber uzayın kendine özgü yapısı, geleneksel uluslararası hukuk ve insancıl ilkelerin uygulanmasını zorlaştırmaktadır. Bu zorluklar; siber savaşı, hesap verebilirlik, meşruiyet ve insanî korumayı güvence altına alacak şekilde nasıl düzenlemek gerektiği konusunda politika yapıcılar, askerî stratejistler ve hukukçular arasında yoğun tartışmalara yol açmıştır. Siber uzaydaki en kritik hukukî sorunlardan biri, bir siber saldırının failini belirlemeye yönelik atıf (attribution) meselesidir. Geleneksel savaşta bir saldırının kaynağı çoğu zaman belirli bir toprak veya kuvvete bağlanabilirken, siber operasyonlar kolaylıkla gizlenebilir, yönlendirilebilir ya da üçüncü taraf sistemler üzerinden gerçekleştirilebilir. Bu anonimlik, uluslararası hukukun temel kavramlarından biri olan devlet sorumluluğunu tespit etmeyi güçleştirir. Uluslararası Hukuka Aykırı Fiillerden Dolayı Devletlerin Sorumluluğu Hakkında Maddeler'e göre bir devlet yalnızca kendisine atfedilebilen eylemlerden sorumlu tutulabilir. Ancak siber operasyonlarda saldırganlar vekil ağlar, botnetler veya devlet dışı hacker'lar kullanarak devlet ve devlet dışı aktörler arasındaki sınırı bulanıklaştırabilmektedir. Bu belirsizlik, caydırıcılığı zayıflatmakta, meşru karşılık vermeyi zorlaştırmakta ve yanlış atıfa dayalı tırmanma riskini artırmaktadır. Bir diğer temel soru, bir siber operasyonun Birleşmiş Milletler Şartı ve Uluslararası İnsancıl Hukuk kapsamında ne zaman "kuvvet kullanımı" ya da "silahlı saldırı" sayılacağıdır. Uluslararası insancıl hukuk yalnızca silahlı çatışma durumlarında uygulanır ve her siber olay bu eşiğe ulaşmaz. Siber casusluk, veri hırsızlığı veya geçici kesintiler silahlı saldırı olarak nitelendirilmeyebilir; ancak can kaybına, yaralanmalara veya kritik altyapının tahribine yol açan büyük ölçekli siber operasyonlar bu kapsamda değerlendirilebilir. Zorluk, birçok siber saldırıda fiziksel hasarın bulunmamasından kaynaklanır; bu durum dijital ortamda "kuvvet" kavramının yorumlanmasını güçleştirir. Sonuç olarak, açık hukukî eşiklerin olmaması, devletlerin öznel yorumlarına ve tutarsız uygulamalara alan bırakmaktadır. Bir başka acil sorun, sivillerin ve çift kullanımlı altyapının korunmasıdır. Modern toplumlar sağlık, ulaşım, enerji, iletişim ve finans gibi alanlarda birbirine bağlı dijital sistemlere bağımlıdır. Bu sistemlerin birçoğu hem sivil hem de askerî amaçlara hizmet eder; bu da meşru hedeflerle korunması gereken sivil varlıkları ayırt etmeyi zorlaştırır. Örneğin askerî bir iletişim sistemine yönelik bir siber saldırı, aynı altyapıya bağlı hastaneleri, acil servisleri veya su temin ağlarını istemeden devre dışı bırakabilir. Bu tür sonuçlar, uluslararası insancıl hukukun ayırım ilkesini doğrudan zorlar ve sivillere verilebilecek zararın orantılılığı ve öngörülebilirliği konusunda ciddi ahlaki kaygılar doğurur. Devlet dışı aktörlerin artan rolü de ek hukukî sorunlar yaratmaktadır. Bu aktörler çoğu zaman herhangi bir hükümetin kontrolü dışında hareket ederken, eylemleri sınır aşan sonuçlar doğurabilmektedir. Mevcut hukukî çerçeveler büyük ölçüde devlet merkezlidir ve bu nedenle devlet dışı siber aktörleri mevcut uluslararası hukuk kapsamında sorumlu tutmak güçtür. Ayrıca, özel teknoloji şirketleri artık devletlerin siber birimleri ile karşılaştırılabilir kapasitelere sahiptir; bu durum savaşın dinamiklerini etkilemekte ve sorumluluk sınırlarını bulanıklaştırmaktadır. Siber suçları düzenleyecek veya kovuşturacak kapsamlı uluslararası mekanizmaların yokluğu, bu alandaki



hesap verebilirlik açığını daha da derinleştirmektedir. Hukukî sorunların ötesinde, siber savaşın yürütülmesi ciddi etik ikilemler de doğurur. Fiziksel bir yüzleşme olmaksızın, uzaktan geniş çaplı zarar verme imkânı, karar vericileri eylemlerinin insanî sonuçlarına karşı duyarsızlaştırabilir. Siber operasyonlar, özellikle dijital hizmetlere bağımlı olan kırılgan toplulukları orantısız biçimde etkileyebilir. Ayrıca otomatik ve otonom siber sistemlerin kullanımı, yıkıcı veya ölümcül kararların makinelere devredilmesi gibi ahlaki soruları gündeme getirir. Bu tür sistemlerde insan denetiminin, ahlaki yargının ve etik sınırlamanın sağlanması, küresel ölçekte önemli bir endişe kaynağı olmaya devam etmektedir. Siber savaş özel olarak düzenleyen kapsamlı bir uluslararası antlaşmanın yokluğu, küresel iş birliği ihtiyacını acil hâle getirmektedir. Mevcut çerçeveler yorumlayıcı rehberlik sunsa da bağlayıcı değildir. Siber uzayda sorumlu davranış normlarını oluşturmak, hukukî eşikleri tanımlamak ve şeffaflık ile hesap verebilirliği güçlendirmek için birleşik ve bağlayıcı bir uluslararası yaklaşım gereklidir.

Uluslararası Çabalar ve Tallinn Kılavuzu

Siber savaş gelişmeye devam ederken, uluslararası toplum mevcut uluslararası hukukun siber operasyonlara nasıl uygulanacağını netleştirme ihtiyacını acil bir konu olarak görmektedir. Siber uzayı özel olarak düzenleyen bağlayıcı bir antlaşmanın bulunmaması, devletleri, uluslararası kuruluşları ve uzman gruplarını yorumlayıcı çerçeveler ve bağlayıcı olmayan rehberler geliştirmeye yöneltmiştir. Bu çalışmalar arasında Tallinn Kılavuzu, uluslararası hukukun siber faaliyetleri nasıl düzenlediğini analiz etmeye ve sistematik hâle getirmeye yönelik en kapsamlı girişim olarak öne çıkmaktadır. Tallinn Kılavuzu, 2007 yılında Estonya'ya yönelik gerçekleştirilen siber saldırıların ardından, Estonya'nın Tallinn kentinde bulunan NATO İşbirlikçi Siber Savunma Mükemmeliyet Merkezi tarafından başlatılan bir projeden doğmuştur. Hükümet sitelerini, bankaları ve medya kuruluşlarını hedef alan bu saldırılar, modern dijital altyapıların kırılganlığını ve bu tür olayları ele alacak açık bir hukukî çerçevenin yokluğunu gözler önüne sermiştir. Bunun üzerine, uluslararası hukuk alanında uzmanlardan ve uygulayıcılardan oluşan bir grup, Siber Savaşa Uygulanabilir Uluslararası Hukuk Üzerine Tallinn Kılavuzunu hazırlamış; daha sonra bu çalışmayı Siber Operasyonlara Uygulanabilir Uluslararası Hukuk Üzerine Tallinn Kılavuzu 2.0 adıyla genişletmiştir. Projenin temel amacı, mevcut uluslararası hukukun devletlerin siber uzaydaki davranışlarına nasıl uygulanacağını yorumlamaktır. Tallinn Kılavuzu 1.0, silahlı çatışmalar sırasında gerçekleşen siber faaliyetlere uluslararası hukukun uygulanmasına odaklanmış; “silahlı saldırı”nın tanımı, savaşçı statüsü ve sivilin korunması gibi konuları ele almıştır. Daha sonra yayımlanan Tallinn Kılavuzu 2.0 ise bu kapsamı genişleterek, silahlı çatışma eşığının altında kalan siber operasyonları da —casusluk, bilgi operasyonları ve devlet destekli siber müdahaleler gibi— incelemiştir. Kılavuz, egemenlik, kuvvet kullanımı, devlet sorumluluğu ve insan hakları hukuku dâhil olmak üzere çok çeşitli hukuk alanlarını kapsayan kurallar ve açıklayıcı yorumlardan oluşmaktadır. Hukuken bağlayıcı bir belge olmamakla birlikte, mevcut normları siber bağlamda yorumlaması sayesinde devletlere, politika yapıcılara ve askerî planlamacılara yetkin ve yönlendirici bir rehber sunmaktadır.

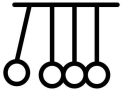


Gelecek Perspektifleri ve Öneriler

Teknolojinin sürekli gelişmesi ve dijital altyapıya artan bağımlılık, siber uzayı modern uluslararası ilişkilerin ve ulusal savunmanın ayrılmaz bir bileşeni hâline getirmiştir. Siber operasyonlar daha karmaşık ve yaygın hâle geldikçe, bunların uluslararası insancıl hukuk kapsamında nasıl düzenleneceği sorusu yalnızca mevcut hukukî çerçevelerin siber uzaya uygulanmasıyla değil, aynı zamanda bu çerçevelerin dijital alanın kendine özgü özelliklerine uyarlanması ve güçlendirilmesiyle yanıt bulacaktır. Bu bölüm, küresel siber güvenlik yönetişimini geliştirebilecek ve insancıl ilkelerin tüm siber operasyonların merkezinde kalmasını sağlayabilecek olası gelecek yönelimlerini, hukukî gelişmeleri ve politika önerilerini incelemektedir. En acil ihtiyaçlardan biri, doğrudan siber savaş düzenleyen bağlayıcı uluslararası anlaşmaların geliştirilmesidir. Tallinn Kılavuzu, BM Hükümet Uzmanları Grubu (UN GGE) ve Açık Uçlu Çalışma Grubu (OEWG) yorumlayıcı rehberlik sağlasa da, hukuken bağlayıcı değildir. Cenevre Sözleşmeleri örnek alınarak hazırlanabilecek gelecekteki bir Siber Savaş Sözleşmesi, devletlerin siber savaşta kullandıkları araç ve yöntemlere ilişkin somut yükümlülükleri kodifiye edebilir. Böyle bir sözleşme, geleneksel silahlı çatışmalar ile modern siber operasyonlar arasındaki mevcut normatif boşluğu kapatarak uluslararası hukukta kritik bir dönüşümü temsil edebilir. Aynı zamanda siber uzayda kabul edilebilir devlet davranışlarını belirleyen bağlayıcı standartlar getirerek daha fazla öngörülebilirlik, hesap verebilirlik ve insanî koruma sağlayabilir. Etkili olabilmesi için bir siber savaş sözleşmesi, dijital bağlamda kuvvet kullanımı ve silahlı saldırı eşiklerini açıkça tanımlamalı ve Birleşmiş Milletler Şartı'nın 2. ve 51. maddeleriyle uyumlu olmalıdır. Ayrıca devlet sorumluluğunu düzenleyerek bir siber operasyonun ne zaman bir devlete atfedilebileceğini ve devletlerin kendi topraklarından başlatılan zararlı faaliyetleri önleme yükümlülüklerini açıkça ortaya koymalıdır. Bunun yanı sıra, sivillere yönelik orantısız insani zarara yol açabilecek hastaneler, enerji şebekeleri, su sistemleri ve diğer temel hizmetlere karşı siber operasyonları yasaklayarak sivil altyapının korunmasını da güvence altına alabilecek bir çerçeve oluşturmalıdır.

Sonuç

Uluslararası insancıl hukukun güncelliğini korumasına rağmen, dijital alan özellikle atıf meselesi ve bir siber operasyonun ne zaman “kuvvet kullanımı” ya da “silahlı saldırı” sayılacağına ilişkin eşiklerin tanımlanması konusunda ciddi hukukî belirsizlikler yaratmaktadır. Bu belirsizlikler, hesap verebilirlik boşluğuna yol açmakta ve acil bir netlik ihtiyacını ortaya koymaktadır. Sivillerin korunmasını etkin biçimde sürdürmek ve bu sınır tanımayan alanda hesap verebilirliği sağlamak için, muhtemelen bir siber savaş sözleşmesi aracılığıyla yeni ve bağlayıcı bir hukukî çerçevenin oluşturulması gereklidir. Böyle bir sözleşme, kuvvet kullanımı eşiklerini açıkça tanımlamalı ve orantısız insani zarara yol açabilecek siber operasyonlara karşı kritik sivil altyapının korunmasını açık biçimde güvence altına almalıdır.



Kaynakça

- 1949 Cenevre Sözleşmeleri ve Ek Protokoller
<https://www.icrc.org/en/law-and-policy/geneva-conventions-and-their-commentaries>
- Ek Protokol I (1977)
https://www.icrc.org/sites/default/files/document/file_list/additional-protocols-geneva-conventions-1949-icrc-eng.pdf
- Siber Operasyonlara Uygulanabilir Uluslararası Hukuk Üzerine Tallinn Kılavuzu 2.0
<https://ccdcoe.org/research/tallinn-manual/>