T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANA BİLİM DALI

SİBER OPERASYONLAR VE *JUS AD BELLUM*

YÜKSEK LİSANS TEZİ

Kaan ERDOĞAN

DANIŞMAN: Dr. Öğr. Üyesi Bleda Rıza KURTDARCAN

EYLÜL 2020

ÖNSÖZ

James William Fulbright tarafından isabetli bir şekilde ifade edildiği üzere "*Uluslararası hukuk riayet edildiği ölçüde, bizlere istikrar ve düzen ile karşılıklı hukuki yükümlülüklere sahip olduğumuz kimselerin davranışlarını öngörebilme imkanı sağlar.*" Siber operasyonların uluslararası hukuk çerçevesinde incelenmesine dair aralarına her geçen gün yenileri eklenen tartışmaların, uluslararası hukukun sayılan vasıflarından faydalanılmak suretiyle, güvenli ve barışçıl bir siber alana kavuşma amacı açısından büyük bir ehemmiyet taşıdığı kanaatiyle gerçekleştirdiğim bu çalışmadan oldukça keyif aldım.

Bu vesileyle, bu çalışmayı kendisinin rehberliğinde gerçekleştirmekten büyük bir gurur ve mutluluk duyduğum değerli hocam Dr. Öğr. Üyesi Bleda Rıza Kurtdarcan'a tez sürecimin her aşamasında göstermiş olduğu desteği sebebiyle şükranlarımı sunmayı borç bilirim. Ayrıca tez jürisinde bulunmalarından onur duyduğum Doç. Dr. Ceren Zeynep Pirim Kızılca ve Dr. Öğr. Üyesi Dolunay Özbek'e de kıymetli görüşleriyle katkıda bulundukları için müteşekkirim.

Son olarak, her fırsatta ideallerime erişme hususunda beni yüreklendiren ailem, Hasan, Reyhan ve Tuğçe Erdoğan'a teşekkürlerimi sunuyor; bu çalışmayı kendilerine ithaf ediyorum.

Kaan Erdoğan

İstanbul, 2020

İÇİNDEKİLER

KISALTMALAR

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
a.g.e.	: adı geçen eser
a.g.m.	: adı geçen makale
art.	: article (madde)
ARSIWA	**:** Uluslararası Hukuka Aykırı Eylemlerden Dolayı Devletlerin Sorumluluğuna İlişkin Metin
bkz.	: bakınız
BM	: Birleşmiş Milletler
Çev.	: Çeviren
CERT	: Bilgisayar Acil Müdahale Ekipleri
CCD COE	: Siber Savunma Mükemmeliyet Merkezi
ÇHC	: Çin Halk Cumhuriyeti
CIA	: ABD Merkezi İstihbarat Teşkilatı
DOD	: ABD Savunma Bakanlığı
Ed.	: Editör
EU	: European Union
EYUCM	: Eski Yugoslavya Uluslararası Ceza Mahkemesi Temyiz Kurulu
FBI	: ABD Federal Soruşturma Bürosu
GRU	: Rusya Federasyonu Askeri İstihbarat Teşkilatı
GTsST	: GRU Özel Teknolojiler Merkezi
KDHC	: Kore Demokratik Halk Cumhuriyeti
NASA	: ABD Ulusal Havacılık ve Uzay Dairesi
NATO	: Kuzey Atlantik Antlaşması Örgütü
OPCW	: Kimyasal Silahların Yasaklanması Örgütü
OSCE	: Avrupa Güvenlik ve İşbirliği Teşkilatı
para.	: paragraf
s.	: sayfa
SCADA	: Merkezi Kontrol ve Veri Toplama Sistemi
UAD	: Uluslararası Adalet Divanı
UN	: United Nations
UK	: United Kingdom
US	: United States
USOM	: Ulusal Siber Olaylara Müdahale Merkezi

RÉSUMÉ

Le sujet de recherche est l'évaluation des cyber opérations dans le cadre du *jus ad bellum,* la branche qui examine les conditions dans lesquelles la force peut être appliquée dans le domaine du droit international. Conformément à l'article 2 (4) de la Charte des Nations Unies interdisant la menace ou l'emploi de la force contre la souveraineté, l'intégrité territoriale et l'indépendance politique du tout État à l'exception du droit de la légitime défense prévu dans l'article 51 et le recours à la force dans le cadre de la sécurité collective réglementée au chapitre, la Charte des Nations Unies, tout en limitant le *jus ad bellum* moderne, a intégré divers concepts tels que "le recours à la force", "l'agression" et "l'agression armée" et appliqués différents critères pour évaluer une action dans la nomenclature de ces concepts modernes. Avec la prise de conscience que les cyber opérations menées par les gouvernements via l'utilisation de divers cyber outils peuvent avoir des effets dévastateurs, les cyber opérations font aussi l'objet de discussion.

Bien que les cyber opérations soient définies et circonscrites par le droit international comme un recours à la force : le fait qu'elle puisse entraîner l'usage de la force est l'objet principal de l'étude. Ce sujet de recherche tripartite se fonde sur l'étude des conventions internationales, du droit coutumier international et des principes juridiques généraux qui constituent les ressources générales du droit international et sur lesquels s'établissent les décisions judiciaires actuelles.

Dans la première partie de l'étude, les principes généraux du *jus ad bellum* feront l'objet d'un résumé puis les cyber opérations seront évaluées dans le cadre des normes juridiques internationales. En effet, les cyber opérations étant un nouveau concept, un accord interétatique, réglementant cette nouvelle problématique, n'a pas encore été signé. Il en est de même pour la formation du droit international coutumier, source du droit international. En effet, le fait que les États doivent se mettre d'accord sur la règle en question et la nécessité que cette situation se prolonge dans le temps conduit à déterminer que réponse qui doit se conformer au droit international coutumier comporte certaines difficultés. Cependant, étant donné que même si les concepts inclus dans une règle juridique internationale ne couvrent pas directement les cyber opérations, la problématique peut être résolue dans le cadre de ces normes et dans la mesure où le problème est approprié. Il est possible d'éliminer les incertitudes en appliquant les normes juridiques internationales traditionnelles aux cyber opérations. Bien que les cyber-opérations puissent être examinées dans le cadre des normes existantes, il faut tenir compte du fait qu'une telle recherche dans le domaine peut conduire à des interprétations différentes. En effet, les inférences avancées en

compilant les opinions défendues dans la doctrine doivent être analysées en tenant compte de la pratique des États sur la question.

Dans la première partie de l'étude, les concepts de cyberespace et de cyber opérations sont également expliqués et définis en tenant compte des caractéristiques importantes du droit international. Le cyberespace est la zone accessible via une infrastructure physique, exploitée par logiciel et où les utilisateurs du monde entier peuvent stocker, faire circuler et utiliser toutes sortes d'informations. La cyber opération peut être définie comme tout type d'opération effectuée dans le cyberespace ou à travers le cyberespace à l'aide de cyber-outils. Dans les recherches menées dans le domaine de notre recherche, il a été observé que les termes "cyberguerre", "opération d'information", "attaque de réseau informatique" ou "cyberattaque" peuvent remplacés la notion de cyber opération. D'autre part, étant donné que la cyber opération a une portée plus large par rapport aux nomenclatures susmentionnées et qu'elle ne contient pas de limites susceptibles de prêter à confusion dans l'analyse des problèmes soulevés par notre problématique. Nous avons jugé plus approprié de conserver aux le concept même de cyber opération pour traiter de ses évaluations et des conséquences.

La deuxième partie de l'étude propose un examen progressif des circonstances dans lesquelles les cyber opérations violent le droit international. Avant que la question ne soit examinée dans le cadre du *jus ad bellum*, la possibilité que les cyber opérations constituent un délit international sera d'abord évaluée. En effet, une opération agressive n'atteindra pas le seuil du recours à la force en toutes circonstances et les États pourront recourir à des cyber opérations de faible impact afin d'éviter de recourir à la force. D'un autre côté, ces cyber opérations peuvent avoir de nombreuses conséquences négatives indésirables sur l'État vers lequel elles sont dirigées. De plus, l'interdiction de l'usage de la force n'est pas la seule restriction aux actions des Etats dans leurs relations internationales. Dans ce contexte, la question sera examinée d'abord dans le cadre du principe de souveraineté puis de l'interdiction de l'ingérence dans les affaires intérieures. De cette manière, il vise à examiner les cyber opérations qui n'atteignent pas le seuil du recours à la force et à éviter que ces cyber opérations ne soient exclues de l'évaluation. En effet, dans la mesure où l'existence du cyberespace dépend de la couche physique, elle peut s'exprimer au niveau national sur la région où les cyber opérations sont menées ou les résultats sont révélés. De même, puisque l'interdiction de l'ingérence dans les affaires intérieures est interdite, on peut dire qu'il existe une possibilité de violer l'interdiction de l'ingérence dans les affaires intérieures si les cyber opérations sont utilisées comme moyen de répression, car il est interdit à un État de faire pression sur des questions relevant du pouvoir souverain d'un autre État.

Dans la deuxième partie de l'étude, les cyber opérations sont examinées dans le cadre du *jus ad bellum* et les cyber opérations sont évaluées dans le cadre de l'interdiction de l'usage ou de l'usage de la force. À cet égard, tout d'abord, les notions d'usage de la force et de menace d'usage de la force seront analysées et les conditions dans lesquelles « l'usage de la cyber-force » constituerait une violation de l'article 2 (4) de la Charte des Nations Unies examinées. Tout en évaluant si une cyber opération atteint le seuil du recours à la force, trois approches différentes sont adoptées : la première est axée sur les instruments, la deuxième est axée sur les objectifs et la troisième sur l'effets. L'approche axée sur les instruments évalue si une action constitue un recours à la force et fait valoir que l'action peut être considérée comme un recours à la force si les outils utilisés sont comparables à des armes cinétiques. Cette approche a fait l'objet de critiques : il serait improbable qu'une cyber opération puisse être évaluée dans le cadre de l'usage de la force conformément à ces critères. L'approche n'a pas été appuyée au motif qu'elle ne convenait pas à l'évaluation de nouvelles opérations militaires résultant du développement de technologies. Contrairement à l'approche orientée outils, l'approche orientée cible a évalué la violation de l'interdiction d'une cyber opération en prenant la cible contre laquelle elle est dirigée. Par conséquent, si une cyber opération est dirigée contre l'infrastructure critique nationale d'un État, elle peut être considérée comme un recours à la force. L'approche axée sur les objectifs s'est avérée trop flexible car elle considère toute cyber opération dirigée contre l'infrastructure critique nationale comme un recours à la force, sans prescrire des critères pour la gravité de la cyber opération. Le point de vue prédominant dans la doctrine est une approche axée sur l'impact qui vérifie si une cyber opération atteint le seuil du recours à la force, à travers l'impact de la cyber opération en question. L'approche axée sur l'impact suggère principalement que si une cyber-opération cause des dommages physiques, elle peut être considérée comme un recours à la force. Certains auteurs, qui ont évalué l'approche axée sur l'impact, ont critiqué le fait que les cyber-opérations destructrices ne causant pas de dommages physiques n'étaient pas prises en compte. En interprétant cette approche avec une approche axée sur les objectifs, il a été avancé que les cyber opérations dirigées vers l'infrastructure nationale critique d'un État et provoquant des échecs d'accès à long terme peuvent également être considérées comme un recours à la force.

Dans la suite de la deuxième partie, les cyber opérations sont également évaluées sous l'angle du concept d'agression. Conformément aux normes de sécurité collective inscrites au chapitre 7 de la Charte des Nations Unies, le Conseil de sécurité a été autorisé à recourir à des mesures non coercitives ou coercitives, selon la nécessité de la situation, en cas de menace de paix, de rupture de la paix ou d'agression. Tout en expliquant le concept d'agression dans la Décision sur la définition de l'agression numérotée 3314 par l'Assemblée générale des Nations Unies, le concept de l'usage de la force a été utilisé. Considérant qu'une cyber opération peut atteindre le seuil du

recours à la force, on peut conclure que ce type de cyber opération peut également constituer une agression. En outre, le Conseil de sécurité a utilisé ses pouvoirs au chapitre 7 au cours de la période écoulée, mais plutôt sur la base d'une "menace à la paix et à la sécurité internationales". Considérant que le Conseil de sécurité des Nations Unies a un pouvoir discrétionnaire à la condition qu'une action nécessite l'utilisation de ses pouvoirs existants dans le cadre du chapitre 7 et quels pouvoirs seront utilisés, à condition qu'il "agisse conformément aux buts et principes des Nations Unies". Si les membres du Conseil de sécurité parviennent à un consensus sur cette question, il est possible de recourir à des mesures non coercitives ou coercitives pour les cyber opérations, ou d'utiliser les cyber opérations dans le cadre des mesures énumérées.

Après avoir évalué les cyber opérations en termes d'utilisation de la force et des concepts d'agression, la question a également été examinée à travers le concept d'agression armée. En fait, avec le 51e article de la Charte des Nations Unies, l'utilisation du droit de légitime défense d'un État est une condition préalable à l'agression. Il est indiqué dans la jurisprudence établie de la Cour Internationale de Justice que seuls les actes de force les plus graves constitueront une agression armée. Lorsqu'on évalue si un acte de recours à la force est une agression armée ou non, il est stipulé de mesurer l'ampleur et les effets de l'action comme critère. Par conséquent, une cyber opération peut être acceptée comme une agression armée si elle entraîne de graves conséquences physiques en termes de taille et d'effet, par exemple en provoquant une explosion entraînant des pertes de vies humaines en interférant avec les systèmes cyber physiques d'une installation nucléaire. Dans ce cas, l'Etat exposé à une agression armée pourra recourir à la légitime défense individuelle ou collective en cyber ou en cinétique contre la cyber-opération, à condition qu'il agisse conformément aux principes de proportionnalité, de nécessité et d'urgence.

Étant donné que les évaluations visant à déterminer si une cyber opération constitue une agression armée peuvent varier en fonction de la situation, la deuxième partie comprend également l'analyse des cyber opérations sur la base d'exemples actuels. Dans ce contexte, les cyber opérations sont divisées en sous-titres de cyber-espionnage, de cyber exploitation, de cyber-ingénierie sociale et de cyber opérations qui affectent la fonctionnalité des cyber-systèmes et les cyber opérations qui causent des dommages physiques. Il a été conclu que ces cyber opérations ne violent pas le droit international, car il suffit de fournir un accès non autorisé à des données confidentielles lors de la réalisation d'actes de cyber espionnage. D'un autre côté, la cyber-exploitation et les opérations d'ingénierie cybernétique peuvent être considérées comme une violation de l'interdiction de l'ingérence dans les affaires intérieures, puisqu'elles peuvent être utilisées comme moyen de pression sur un État, mais on peut dire que ces cyber opérations ne causent pas de dommages physiques et n'empêchent

pas l'accès aux infrastructures critiques nationales. Les cyber opérations affectant la fonctionnalité des cyber-systèmes peuvent être considérées comme une violation de l'interdiction du recours à la force si elles empêchent l'accès aux infrastructures critiques nationales pendant une longue période. Cependant, étant donné que seul le recours le plus sérieux à la force atteint le seuil de l'agression armée, on peut dire que de telles cyber opérations sont peu susceptibles d'être considérées comme une agression armée. En conséquence, le seul type de cyber opération qui peut atteindre le seuil d'agression armée est celui des cyber opérations qui causent des dommages physiques. Cependant, il convient de noter que ces cyber opérations ne peuvent constituer une base de légitime défense que si elles sont de grande ampleur et ont des effets graves.

Dans la troisième partie de l'étude, la question de l'attribution des cyber opérations à l'État responsable est examinée. Parce qu'une cyber opération constitue une agression armée, la capacité à utiliser le droit de légitime défense contre l'État effectuant ou à appliquer des contre-mesures contre une cyber opération qui viole l'interdiction de recourir à la force, même si elle ne constitue pas une agression armée, dépend de l'attribution de l'action à l'État responsable. Dans ce contexte, tout d'abord, la pratique des États a été observée et les critères utilisés par les États pour l'attribution des cyber opérations ont été évalués. Par la suite, conformément aux normes relatives à la responsabilité des États pour des actes contraires au droit international, la question a été examinée en termes d'économies d'organes ou de personnes ou entités étatiques exerçant des pouvoirs publics et de celles des acteurs non étatiques. En fait, les économies réalisées par les organes de l'État ou les personnes ou unités utilisant les pouvoirs publics peuvent être attribuées à l'État, même en cas de dérogation. De même, les actions des acteurs non étatiques, si les actions sont menées sous les instructions, la gestion ou le contrôle de l'Etat, conduisent à la responsabilité juridique internationale de l'Etat.

ABSTRACT

This thesis concerns itself with the evaluation of cyber operations within the framework of *jus ad bellum*, the branch that examines under which conditions it is possible to resort to force in accordance with international law. As per article 2(4) of the United Nations Charter, the unilateral use of force or threat of force is prohibited with the exceptions to the inherent right of self-defence stipulated in Article 51 and the use of force within the context of collective security regulated in Chapter 7. The United Nations Charter referred to various terms such as "the use of force", "aggression", and "armed attack" while limiting the modern *jus ad bellum* and different criteria are applied in order to regard an action within the scope of each term. With the realization of the fact that cyber operations conducted by governments through the use of various cyber tools may have devastating effects, cyber operations have also become the subject of discussion from the perspective of *jus ad bellum*.

Although the main focus of this thesis is to evaluate whether cyber operations may constitute the use of force, aggression, or armed attack, and if they do, how a state may respond to them in accordance with the international law; other topics related to these questions are also reviewed with the aim of providing integrated analysis of the subject. This tripartite research has been formed by interpreting international conventions, international customary law, and general legal principles, which constitute the general sources of international law, in the light of judicial decisions and within the framework of opinions put forward in the doctrine.

The first part of the thesis summarizes the general principles of jus ad bellum and then assess cyber operations in the context of international legal norms. As cyber operations are a new concept, an interstate agreement regulating this new issue has not yet been signed. A similar situation appears in terms of the formation of customary international law, considering the fact that the States must agree on a rule and act accordingly for a prolonged time in order to determine the existence of a custom, which involves certain difficulties with regard to the cyber operations. However since an international norm may be applied to an issue to the extent appropriate even if the concept is not covered by such norms directly, uncertainties regarding cyber operations may be resolved by applying traditional international law to the matter. On the other hand, while cyber operations may be examined within the framework of existing international norms, it must be taken into account that such interpretation may cause different conclusions; consequently, the issue in question must be analyzed by inferences advanced through compiling the opinions defended in the doctrine and state practice.

Another heading under the first chapter of the thesis is defining and explaining terms of cyberspace and cyber operations in view of their important features from the point of international law. Cyberspace is an area accessible through a physical

infrastructure and operated by software where users around the world can store, circulate and use all kinds of information. Cyber operation can be defined as any type of operation performed in cyberspace or through cyberspace using cyber tools. It has been observed that different terms such as "cyber war", "information operation", "computer network attack" or "cyber attack" has been used instead of cyber operation by certain researches conducted within the area of this thesis. On the other hand, given that the cyber operation has a broader scope compared to the aforementioned terms which allow avoiding confusion in the analysis that may be encountered in case of implying other terms; it has been decided that the term of cyber operations is more appropriate to be used in our assessment.

The second part of the thesis provides a graded examination of the circumstances in which cyber operations may violate international law. Before the matter is assessed under *jus ad bellum*, the possibility that cyber operations constitute an international wrongful act will be reviewed. Indeed, an aggressive cyber operation is more likely to not reach the threshold for the use of force in all circumstances and States may also prefer to resort to low impact cyber operations in order to refrain from violating the prohibition on the use of force. On the other hand, even such cyber operations may have many undesired negative consequences on the state to which they are directed. Moreover, the prohibition of the use of force is not the only restriction on the actions of States in their international relations. In this context, the question will be examined first in the framework of the principle of sovereignty and then of the principle of non-intervention in internal affairs. In this way, it is aimed to examine cyber operations that do not meet the use of force threshold and to ensure that these cyber operations are not excluded from the assessment. Indeed, insofar as the existence of cyberspace depends on the physical layer, a cyber operation may be expressed at the national level on the region where such operations are carried out or the results are revealed. Likewise, since the interference of a sovereign state's internal affairs is prohibited according to the non-intervention principle, it is possible to generalize that the principle of non-intervention may be violated once cyber operations are used as a means of coercion on the matters falling within the sovereign power of another state.

In the second part of the thesis, while cyber operations are examined from the perspective of *jus ad bellum*, firstly cyber operations are assessed within the context of prohibition of the use of force or threat of force. In this regard, first of all, the concepts of use of force and threat of use of force will be analyzed and the conditions under which "the use of cyber-force" would constitute a violation of Article 2 (4) of the Charter of the United Nations reviewed. While assessing whether a cyber operation may reach the use-of-force threshold, three different approaches are applied; the first is instrument-based, the second is target-based and the third is effect-based. The instrument-based approach argues a cyber operation may constitute a use of force only when tools used for the cyber operations are comparable to kinetic weapons. This approach has been criticized due to the fact that it is unlikely to be able to regard a cyber operation as a use of force under such criteria. The instrument-based approach has not been supported on the grounds that it is unsuitable for evaluating new military operations resulting from the development of technology. Unlike the instrument-based approach, the target-based approach assessed the violation of the use of force by

considering the target aimed by the cyber operation. Accordingly, a cyber operation directed to the national critical infrastructure of a state may be considered as a use of force. The target-based approach has proven to be too flexible since it considers any cyber operation directed to the national critical infrastructure as a use of force, without prescribing criteria for the gravity of the cyber operation. The predominant view in doctrine is the effect-based approach that examines whether a cyber operation reaches the use of force threshold, through the effects that are resulted from the cyber operation in question. The effect-based approach primarily suggests that if a cyber operation causes physical damage, it may be regarded as a use of force. Some authors, who evaluated the effect-based approach, criticized the fact that destructive cyber operations that did not cause physical damage were not taken into account by this approach. Thus by interpreting this approach with the target-based approach, they argued that cyber operations directed to a state's national critical infrastruce and causing long-term access failures should also be regarded as a violation of the prohibition of use of force.

Cyber operations are also assessed from the perspective of the concept of aggression by the second part of the thesis. In accordance with the collective security norms enshrined in Chapter 7 of the United Nations Charter, the Security Council is authorized to resort to non-coercive or coercive measures, as occasion requires, in case the existence of any threat to the peace, breach of the peace, or act of aggression. The United Nations General Assembly based on the term of use of force while explaining the concept of aggression in the Resolution on the Definition of Aggression numbered 3314. Considering the fact that a cyber operation may reach the threshold of the use of force, it may be concluded that such an operation may also constitute an aggression. In addition, the Security Council has exercised its Chapter 7 powers during the past period on the basis of a "threat to international peace and security" rather than relying on the existence of an aggression. The United Nations Security Council has a discreationary power provided that the Council acts "in accordance with the purposes and principles of the United Nations" while executing its powers under Chapter 7. Therefore, if the members of the Security Council reach consensus on the issue, it is possible to resort no non-coercive or coercive measures against cyber operations, or to use cyber operations as part of such measures.

Following an evaluation of cyber operations in terms of the use of force and the aggression, the question is also examined through the concept of the armed attack by the second chapter of this thesis. An armed attack has been foreseen as a precondition to use of force under the inherent right of self-defence as per the 51st Article of the United Nations Charter. Moreover, it is stated in the established jurisprudence of the International Court of Justice that only the most grave acts of force will constitute an armed attack. Hence an act of use of force must be evaluated in terms of its scale and effects in order to be considered as an armed attack. Consequently, a cyber operation may be regarded as an armed attack if it results in severe physical consequences in terms of scale and effect, for example by causing an explosion resulting in loss of life by interfering with the cyber physical systems of a nuclear facility. In this case, the State exposed to an armed attack may resort to individual or

collective self-defense in cyber or kinetics against the cyber-operation, provided that it acts in accordance with the principles of proportionality, necessity and immediacy.

Since assessments to determine whether a cyber operation constitutes an armed attack may vary depending on the situation, the last chapter of the second part also includes the analysis of cyber operations based on current examples. In this context, cyber operations are divided into subheadings of cyber espionage, cyber exploitation, social cyber engineering and cyber operations which affect the functionality of cyber systems and cyber operations which cause physical damage. It was concluded that cyber espionage does not violate international law, as it is sufficient to provide an unauthorized access to confidential data to complete such operations successfully. On the other hand, cyber exploitation and cyber socail engineering operations may be regarded as a violation of the principle of non-intervention, since they may be used as means of pressure on a state; however it may be stated that these cyber operations should not be considered as use of force because they do not prevent access to national critical infrastructures or cause physical damage. Cyber operations affecting the functionality of cyber systems may be considered a violation of the prohibition on the use of force if they prevent access to national critical infrastructure for a long period of time. However, given that only the most grave acts of use of force reaches the threshold of armed attack, it can be said that such cyber operations are unlikely to be considered as an armed attack. As a result, the only type of cyber operation that can reach the armed attack threshold is cyber operations that cause physical damage. However, it should be noted that these cyber operations can only constitute a basis for self-defense if they are in large-scale and have serious effects.

The third part of the study focuses on the issue of attribution of cyber operations to the responsible states. Because even if cyber operations constitute an armed attack, the ability to use the right of self-defense against the source of attack depends on the attribution of the action to the responsible state. The same applies to the cyber operations that do not reach the armed attack threshold but allows a state to apply counter-measures. In this context, state practice is observed in order to analyze the criteria used with an attempt to attribute cyber operations to the responsible state, if there is any. Subsequently, in accordance with the norms relating to the responsibility of states for international wrongful acts, the question was examined in terms of the conducts of organs of a state, persons or entities exercising elements of governmental authority and non-state actors. In fact, conducts made by state organs and persons or entities exercising governmental authority are attributed to the state which they belong, even such conducts are ultra vires acts. On the other hand, the conduct of non-state actors may also lead to the international legal responsibility of the state in case they are acting under state instructions or directed or controlled by the state.

ÖZET

Çalışmanın konusunu siber operasyonların uluslararası hukukun hangi koşullarda kuvvete başvurulabileceğini inceleyen dalı *jus ad bellum* çerçevesinde değerlendirilmesi oluşturmaktadır. Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesi uyarınca devletlerin tek taraflı olarak kuvvet kullanması veya kuvvet kullanma tehdidinde bulunması yasaklanmış; 51. maddede yer verilen meşru müdafaa hakkı ve 7. Bölüm'de düzenlenen kolektif güvenlik kapsamında kuvvete başvurulması ise söz konusu yasağın yegâne istisnaları olarak öngörülmüştür. Birleşmiş Milletler Şartı ile modern *jus ad bellum* sınırlanırken "kuvvet kullanma", "saldırı" ve "silahlı saldırı" başta olmak üzere çeşitli kavramlara yer verilmiş ve zaman içerisinde bir eylemin sayılan kavramlar çerçevesinde değerlendirilmesi amacıyla farklı kıstaslara başvurulmuştur. Devletler tarafından belirli amaçlarla ve çeşitli siber araçlar vasıtasıyla gerçekleştirilen siber operasyonların da günümüzde yıkıcı etkilere yol açabileceğinin fark edilmesiyle birlikte, mesele siber operasyonlar açısından da tartışılır hale gelmiştir.

Bu doğrultuda, her ne kadar siber operasyonlar uluslararası hukukun konuyla ilişkilendirilebilecek diğer alanları açısından da ele alınmışsa dahi, siber operasyonların kuvvet kullanma teşkil edip etmeyeceği ve kuvvet kullanma teşkil ettiği takdirde hangi hallerde saldırı yahut silahlı saldırı eşiğine erişip söz konusu siber operasyona karşılık uluslararası hukuka uygun bir şekilde kuvvet kullanımına yol açabileceği hususu çalışmanın esas odak noktasını oluşturmaktadır. Uluslararası hukukun genel kaynaklarını oluşturan uluslararası sözleşmeler, uluslararası teamül hukuku ve genel hukuk ilkelerinin mevcut yargı kararları ışığında ve öğretide ileri sürülen görüşler çerçevesinde konu açısından yorumlanmasıyla oluşturulmuş bu çalışma üç bölümden oluşmaktadır.

Çalışmanın birinci bölümünde öncelikle *jus ad bellum*un genel esasları özetlenmekte, akabinde siber operasyonların uluslararası hukuk normları kapsamında ne şekilde değerlendirilebileceği irdelenmektedir. Nitekim siber operasyonların yeni bir kavram olması sebebiyle henüz doğrudan bu alanı düzenleyen devletlerarası bir sözleşme imza edilmemiştir. Keza bir diğer uluslararası hukuk kaynağı olan uluslararası teamül hukukunun oluşması için devletler arasında söz konusu kurala ilişkin büyük oranda uzlaşılması ve bu durumun belirli bir süre devam etmesi gerekliliği meselenin uluslararası teamül hukuku uyarınca çözümlenmesinin de birtakım zorlukları barındırdığı yönünde tespitlere yol açmıştır. Lakin bir uluslararası hukuk kuralında yer verilen kavramların doğrudan siber operasyonları karşılamadığı takdirde dahi konuya uygun düştüğü ölçüde meselenin söz konusu normlar çerçevesinde çözümlenebileceği dikkate alındığında, geleneksel uluslararası hukuk normlarının siber operasyonlara uygulanması yoluyla belirsizliklerin giderilebileceği düşünülmektedir. Elbette her ne kadar siber operasyonlar mevcut normlar çerçevesinde incelenebilmekteyse de böyle bir incelemenin de kendi içerisinde farklı

yorumlara yol açabileceği hesaba katılmalı; öğretide savunulan görüşler derlenerek öne sürülen çıkarımlar konuya ilişkin devlet uygulaması göz önünde bulundurularak tahlil edilmelidir.

Çalışmanın birinci bölümünde ayrıca siber alan ve siber operasyon kavramları okuyucuya açıklanmakta ve söz konusu kavramlar uluslararası hukuk açısından önem taşıyan özellikleri göz önünde bulundurularak tanımlanmaktadır. Siber alan fiziki altyapı aracılığıyla erişilen, yazılımlar aracılığıyla işletilen ve dünya çapında kullanıcıların her türlü bilginin depolanması, dolaşımı ve kullanılması faaliyetlerinde bulunabildiği alandır. Siber operasyon ise siber araçlar kullanılarak siber alanda yahut siber alan vasıtasıyla gerçekleştirilen her türlü operasyon olarak ifade edilebilmektedir. Çalışma konusu alanda gerçekleştirilen araştırmalarda zaman zaman siber operasyon kavramı yerine "siber savaş", "bilgi operasyonu", "bilgisayar ağı saldırısı" veya "siber saldırı" gibi isimlendirmelerin de tercih edilebildiği gözlemlenmiştir. Öte yandan siber operasyonun sayılan isimlendirmelere kıyasla daha geniş bir kapsama sahip olması ve bu sayede meseleye ilişkin tartışmalı hususların incelenmesi esasında anlam karmaşasına yol açabilecek sınırlamalar barındırmaması sebebiyle yapılacak değerlendirmelerin siber operasyon kavramı üzerinden gerçekleştirilmesi daha uygun görülmüştür.

Çalışmanın ikinci bölümü, siber operasyonların hangi koşullarda uluslararası hukuku ihlal ettiğine dair kademeli bir inceleme sağlamaktadır. Bu doğrultuda meselenin *jus ad bellum* çerçevesinde incelemesine geçilmeden evvel öncelikle siber operasyonların uluslararası haksız fiil teşkil etme ihtimali değerlendirilecektir. Nitekim saldırgan bir operasyon her koşulda kuvvet kullanma eşiğine erişmeyeceği gibi devletler de kuvvet kullanma yasağını ihlal etmekten kaçınmak amacıyla daha düşük tesirli siber operasyonlara başvurabilecektir. Öte yandan bu tip siber operasyonlar da yöneltildiği devlet üzerinde istenmeyen birçok olumsuz sonuç doğurabilecektir. Kaldı ki devletlerin uluslararası ilişkilerinde başvurduğu eylemlerine ilişkin yegâne sınırlama kuvvet kullanma yasağı değildir. Bu kapsamda mesele öncelikle egemenlik ilkesi ardından da içişlerine karışma yasağı kapsamında irdelenecektir. Böylelikle kuvvet kullanma eşiğine erişmeyen siber operasyonların da incelenmesi sağlanarak bu tip siber operasyonların değerlendirme dışında kalmasının önlenmesi amaçlanmaktadır. Nitekim siber alanın varlığı fiziksel katmana bağlı olduğundan siber operasyonlar gerçekleştirildiği veya sonuçlarının ortaya çıktığı bölge üzerinden ülkesel olarak ifade edilebilmektedir. Keza içişlerine karışma yasağı ile herhangi bir şekilde bir devletin başka bir devletin egemenlik yetkisi kapsamındaki hususlarda baskıda bulunması yasaklandığından siber operasyonların baskı aracı olarak kullanılması halinde içişlerine karışma yasağını ihlal etme ihtimali olduğu söylenebilmektedir.

Çalışmanın ikinci bölümünde siber operasyonların *jus ad bellum* kapsamında incelenmesine geçilirken öncelikle siber operasyonların kuvvet kullanma veya kuvvet kullanma tehdidinde bulunma yasağı çerçevesinde değerlendirilmesine yer verilmiştir. Bu doğrultuda öncelikle kuvvet kullanma ve kuvvet kullanma tehdidi kavramları açıklanarak "siber kuvvet kullanma" eylemlerinin hangi koşullarda Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesinin ihlali teşkil edeceği tartışılmıştır. Öğretide bir siber operasyonun kuvvet kullanma eşiğine erişip erişmediği değerlendirilirken araç odaklı,

hedef odaklı ve etki odaklı olmak üzere üç farklı yaklaşım benimsenmiştir. Bunlardan araç odaklı yaklaşım bir eylemin kuvvet kullanma teşkil edip etmediğini kullanılan araçlar üzerinden değerlendirmekte ve kullanılan araçların kinetik silahlarla kıyaslanabilir olduğu takdirde eylemin kuvvet kullanma olarak kabul edilebileceğini savunmaktadır. Araç odaklı yaklaşıma söz konusu kıstaslar doğrultusunda bir siber operasyonun kuvvet kullanma kapsamında değerlendirilebilmesinin çok düşük bir ihtimal olacağı eleştirileri yöneltilmiş; yaklaşım gelişen teknolojiler sonucu ortaya çıkan yeni askeri operasyonları değerlendirmek için elverişsiz olması gerekçesiyle destek görmemiştir. Hedef odaklı yaklaşım ise araç odaklı yaklaşımdan farklı olarak bir siber operasyonun kuvvet kullanma yasağını ihlal etmesini yöneltildiği hedefi kıstas alarak değerlendirmiştir. Buna göre, bir siber operasyon bir devletin ulusal kritik altyapısına yöneltilmesi halinde kuvvet kullanma olarak kabul edilebilecektir. Hedef odaklı yaklaşım siber operasyonun şiddetine ilişkin herhangi bir kıstas öngörmeksizin ulusal kritik altyapıya yöneltilen her siber operasyonu kuvvet kullanma olarak değerlendirmesi sebebiyle fazla esnek bulunmuştur. Öğretide baskın olan görüş, bir siber operasyonun kuvvet kullanma eşiğine erişip erişmediğini söz konusu siber operasyonun yarattığı etki üzerinden denetleyen etki odaklı yaklaşımdır. Etki odaklı yaklaşım esas olarak bir siber operasyonun fiziksel zarara yol açması halinde kuvvet kullanma olarak kabul edilebileceğini ileri sürmektedir. Etki odaklı yaklaşımı değerlendiren kimi yazarlarca fiziksel zarara yol açmayan yıkıcı siber operasyonların göz önüne alınmadığı eleştirisinde bulunulmuş; bu yaklaşım hedef odaklı yaklaşım ile birlikte yorumlanarak bir devletin ulusal kritik altyapısına yöneltilen ve uzun süreli erişim aksaklıklarına yol açan siber operasyonların da kuvvet kullanma olarak değerlendirilebileceği savunulmuştur.

İkinci bölümün devamında siber operasyonlar ayrıca saldırı kavramı açısından değerlendirilmiştir. Birleşmiş Milletler Şartı'nın 7. Bölüm'ünde yer bulan kolektif güvenlik normları uyarınca Güvenlik Konseyi'ne barışın tehdidi, barışın bozulması veya bir saldırının mevcut olması halinde durumun gerekliliğine göre zorlayıcı olmayan veya zorlayıcı önlemlere başvurma yetkisi tanınmıştır. Birleşmiş Milletler Genel Kurulu tarafından 3314 sayılı Saldırının Tanımı Kararı'nda saldırı kavramı açıklanırken kuvvet kullanma kavramı üzerinden hareket edilmiştir. Bir siber operasyonun kuvvet kullanma eşiğine erişebileceği dikkate alındığında, bu tip bir siber operasyonun aynı zamanda saldırı da teşkil edebileceği sonucuna ulaşılabilmektedir. Kaldı ki Güvenlik Konseyi geçmiş dönemde 7. Bölüm'deki yetkilerini kullanırken daha ziyade "uluslararası barış ve güvenliğe tehdit" oluşması gerekçesine dayanmıştır. Birleşmiş Milletler Güvenlik Konseyi'nin bir eylemin 7. Bölüm kapsamında mevcut yetkilerini kullandırmayı gerektirmesi ve hangi yetkilerin kullanılacağı konusunda "Birleşmiş Milletler'in Amaç ve İlkeleri'ne uygun hareket etmek" kaydıyla takdir yetkisi olduğu değerlendirildiğinde; Güvenlik Konseyi üyelerinin bu konuda görüş birliğine ulaşması halinde, siber operasyonlara yönelik de zorlayıcı olmayan veya zorlayıcı önlemlere başvurulması yahut sayılan önlemler kapsamında siber operasyonların kullanılması mümkündür.

Siber operasyonların kuvvet kullanma ve saldırı kavramları açısından değerlendirilmesinin ardından mesele ayrıca silahlı saldırı kavramı üzerinden de irdelenmiştir. Nitekim Birleşmiş Milletler Şartı'nın 51. maddesi ile bir devletin meşru

müdafaa hakkını kullanması silahlı saldırıya uğramış olması ön şartına bağlanmıştır. Uluslararası Adalet Divanı'nın yerleşik içtihatlarında ancak en vahim kuvvet kullanma eylemlerinin silahlı saldırı teşkil edeceği belirtilmiş; bir kuvvet kullanma eyleminin aynı zamanda silahlı saldırı olup olmadığı değerlendirilirken eylemin boyutu ve etkilerinin kıstas alınması öngörülmüştür. Dolayısıyla bir siber operasyon da bir nükleer tesisteki siber-fiziksel sistemlere müdahale edilerek can kaybına da yol açan bir patlamaya neden olunması gibi boyut ve etki olarak ciddi fiziksel sonuçlara yol açtığı takdirde silahlı saldırı olarak kabul edilebilecektir. Bu takdirde silahlı saldırıya maruz kalan devlet, ölçülülük, gereklilik ve aciliyet ilkelerine uygun hareket etmek kaydıyla, siber operasyona karşılık siber veya kinetik olarak bireysel yahut kolektif meşru müdafaaya başvurabilecektir.

Bir siber operasyonun silahlı saldırı teşkil edip etmemesine ilişkin değerlendirmelerin duruma göre değişebilmesi sebebiyle, ikinci bölümde ayrıca siber operasyonların güncel örnekler üzerinden analizine yer verilmiştir. Bu kapsamda siber operasyonlar gerçekleştiriliş amaçlarına göre siber casusluk, siber faydalanma, siber sosyal mühendislik ile siber sistemlerin çalışırlığını etkileyen siber operasyonlar ve fiziksel zarara yol açan siber operasyonlar alt başlıklarına ayrılmıştır. Siber casusluk eylemleri gerçekleştirilirken gizli verilere izinsiz erişimin sağlanması yeterli olması sebebiyle söz konusu siber operasyonların uluslararası hukuku ihlal etmediği sonucuna ulaşılmıştır. Öte yandan siber faydalanma ve siber sosyal mühendislik operasyonları ise bir devlet üzerinde baskı aracı olarak kullanılabileceğinden içişlerine karışma yasağının ihlali olarak değerlendirilebilecekse de bu tip siber operasyonların fiziksel zarara yol açmaması ve ulusal kritik altyapıya erişimi engellememesi sebebiyle kuvvet kullanma eşiğine erişmediği söylenebilmektedir. Siber sistemlerin çalışırlığını etkileyen siber operasyonlar ise ulusal kritik altyapıya erişimi uzun bir süre engellediği takdirde kuvvet kullanma yasağının ihlali olarak değerlendirilebilecektir. Ancak sadece en vahim kuvvet kullanma eylemlerinin silahlı saldırı eşiğine eriştiği dikkate alındığında, bu tip siber operasyonların da silahlı saldırı kabul edilmesinin olası olmadığı söylenebilmektedir. Sonuç olarak, silahlı saldırı eşiğine erişebilecek tek siber operasyon tipi fiziksel zarara yol açan siber operasyonlardır. Lakin bu siber operasyonların da ancak geniş boyutta olması ve ciddi etkilere yol açması halinde meşru müdafaaya dayanak oluşturabileceğini belirtmek gerekir.

Çalışmanın üçüncü bölümünde siber operasyonların sorumlu devlete atfedilebilmesi hususu irdelenmiştir. Zira bir siber operasyonun silahlı saldırı teşkil etmesi sebebiyle gerçekleştiren devlete karşı meşru müdafaa hakkının kullanılabilmesi yahut silahlı saldırı teşkil etmese dahi kuvvet kullanma yasağını ihlal eden bir siber operasyona yönelik karşı önlemlerin uygulanabilmesi söz konusu eylemin sorumlu devlete isnat edilebilmesine bağlıdır. Bu kapsamda öncelikle devlet uygulaması gözlemlenerek devletlerin siber operasyonların atfedilmesinde başvurduğu kıstaslar değerlendirilmiştir. Bunun ardından devletlerin uluslararası hukuka aykırı eylemlerden sorumluluğuna ilişkin normlar uyarınca mesele devlet organlarının veya kamu gücü yetkilerini kullanan kişi ya da birimlerin tasarrufları ve devlet dışı aktörlerin tasarrufları açısından incelenmiştir. Nitekim devlet organlarının veya kamu gücü yetkilerini kullanan kişi ya da birimlerin tasarrufları, yetki aşımı söz konusu olduğu takdirde dahi, devlete atfedilebilmektedir. Keza devlet dışı aktörlerin de

eylemleri, söz konusu eylemler devletin talimatları, yönetimi yahut kontrolü altında gerçekleştirildikleri takdirde devletin uluslararası hukuk sorumluluğunun doğmasına yol açmaktadır.

GİRİŞ

Siber alan esasında "0" ve "1"lerden oluşmakla birlikte, günümüzde internet vasıtasıyla erişilen sanal bir dünyadan çok daha fazlasını ifade etmektedir. Nitekim hayatımıza girişi oldukça yeni olan siber alan çok kısa sürede günlük hayatın vazgeçilmez bir parçası haline gelmiştir. Zira bu kapsamda topluma sunulanlar her geçen gün daha da çeşitlenmekte, bireyler çevirim içi sistemler üzerinden birbirleriyle haberleşmenin yanı sıra bankacılık hizmetlerinden alışverişe sayısız ihtiyaçlarını karşılamaktadır. Öyle ki siber alan bir ticari kanal veya sosyal hayat enstrümanı olmanın da ötesine geçerek devletlerin vergi toplama, seçim sürecini yürütme gibi vatandaşlık işlemlerini yürüttüğü bir araç halini almış; hatta milli savunmaya ilişkin pek çok faaliyetin ayrılmaz bir parçası haline gelmiştir.

Ne yazık ki siber alanın önemiyle birlikte kötü niyetli kimselerce kullanılması riski de artmış; dolayısıyla sunulan imkanlar yeni tehditleri de beraberinde getirmiştir. Devletler her geçen gün artan zararlı siber aktivitelerin olası sonuçlarını dikkate alarak tıpkı fiziksel dünyada olduğu gibi siber alanda da güvenliğin sağlanabilmesi için önlemler almaya başlamıştır. Lakin bu kapsamda atılan ilk adımlar "siber suç" kavramı çerçevesinde yoğunlaşmış; devletler mevzuatlarına siber suçluların tespiti ve cezalandırılması yönünde yeni hükümler eklemiştir. Öte yandan siber alanda mevcut tehditler siber suçlularla sınırlı olmadığı gibi devletlerin siber alandaki varlıklarını arttırmasıyla birlikte son dönemde daha da popülerleşen "siber operasyon" kavramı açısından da benzer bir yaklaşıma ihtiyaç duyulduğu ortaya çıkmıştır.

Gerçekten de günümüzde devletler siber alanda güvenliğin sağlanabilmesi için kolluk kuvvetlerinin yanı sıra silahlı kuvvetlerinden de faydalanmaya başlamış; hatta içlerinde Türkiye'nin de bulunduğu birçok devlet siber savunma komutanlığı oluşturulması yoluna giderek askeri personelinin bu alanda aktif olarak görev yapmasına olanak sağlamıştır. Nitekim günümüzde silah teknolojilerinin çeşitlenmesi

ve özellikle yeni teknolojilerin kontrolünün siber alan vasıtasıyla sağlanıyor olması bu alanda askeri yapılanmaya gidilmesini bir zorunluluk kılmaktadır. Elbette devletlerin siber alanda askeri amaçla gerçekleştirdiği faaliyetlerin her zaman savunma ile sınırlı kalmaması ihtimali mevcuttur. Bir devletin politik yahut stratejik amaçları için saldırgan nitelikte siber operasyonlara başvurması ise devletler arasında çatışma yaşanmasını olası kılmaktadır. Zira yakın tarihimizde devletlerin saldırgan siber operasyonlar[1] sonucu ciddi zarar gördüğü örneklerle karşılaşılmış; hatta bu tip saldırılara maruz kalan devletler tarafından söz konusu siber operasyonlar belirli bir devlete atfedilerek uluslararası hukuk aracılığıyla soruna bir çözüm bulunması gerektiği işaret edilmiştir.

Çalışmanın amacı da özellikle son dönemde artan saldırgan siber operasyonları uluslararası hukuk açısından değerlendirerek siber alanda barışçıl devlet ilişkisinin sağlanmasına yönelik tartışmalara katkı sunmaktır. Bu kapsamda saldırgan siber operasyonların uluslararası hukuk açısından durumu irdelenecek, mevcut uluslararası hukuk normlarından faydalanılarak devletlerin siber alanda faaliyet gösterirken hangi ilkeler çerçevesinde hareket etmesi gerektiği yorumlanacaktır.

Çalışma üç bölümden oluşmakta olup ilk bölümde çalışmanın sınırları belirlenecek ve çalışma kapsamında değinilen kavramlar aydınlatılacaktır. Öğretide saldırgan siber operasyonlar değerlendirilirken konunun *jus ad bellum* ve *jus in bello* açısından tartışıldığı gözlemlenmektedir. Bu çalışmada ise saldırgan siber operasyonların sadece *jus ad bellum* çerçevesinde incelenmesi tercih edilmiş; gerçekleştirilecek inceleme kuvvet kullanma yasağı ve bu yasağın istisnaları üzerine temellendirilmiştir. Siber operasyonları doğrudan düzenleyen bir uluslararası hukuk normu bulunmaması sebebiyle, bu noktada ilk çözümlenmesi gereken husus siber operasyonlar değerlendirilirken hangi uluslararası hukuk kaynaklarının göz önüne alınması gerektiğidir. Zira yeni bir kavram olması sebebiyle henüz saldırgan siber

[1]Bütün askeri operasyonlar gibi siber operasyonlar da sadece belirli önlemlerin alınması veya saldırıların savuşturulması ve benzeri savunmaya yönelik amaçlarla icra edilebilecektir. Öte yandan çalışma kapsamında bu tip operasyonlardan ziyade doğrudan bir etki doğurma niyetiyle gerçekleştirilen siber operasyonlar incelenecek olup bu sebeple ilgili ayrımın sağlanabilmesi adına "saldırgan siber operasyon" (*offensive cyber operation*) isimlendirmesine başvurulmuştur.

operasyonlara yönelik bir uluslararası hukuk normu mevcut olmasa dahi bu husus geleneksel uluslararası hukuk normlarının meseleye uygulanmasına engel değildir. Lakin uluslararası hukuk normlarının meseleye uygulanmasından evvel "siber alan" ve "siber operasyon" terimleri ile neyin kastedildiğinin de izah edilmesi gerekmektedir. Bu doğrultuda, öncelikle siber alan tanımlanacak ve ardından siber alanın tanımından faydalanarak siber operasyon kavramının kapsamı açıklanacaktır.

Çalışmanın ikinci bölümünde ise saldırgan siber operasyonların devletlerin hasmane eylemlerine karşı uluslararası hukuk uyarınca öngörülen sınırlamalar çerçevesinde incelenmesine geçilecektir. Her ne kadar çalışmanın esas konusu olarak *jus ad bellum* belirlenmişse de saldırgan siber operasyonların büyük bir kısmının silahlı saldırı teşkil etmeyeceği, hatta kuvvet kullanma eşiğine dahi erişmeyeceği varsayımıyla mesele öncelikle uluslararası haksız fiiller açısından değerlendirilmiştir. Nitekim saldırgan siber operasyonlar kuvvet kullanma yasağını ihlal etmediği hallerde dahi devletler açısından yıkıcı etkilere yol açabilmektedir. Kaldı ki bu takdirde söz konusu siber operasyonlar içişlerine karışma yasağının ihlali teşkil edebileceğinden uluslararası hukuka aykırı kabul edilebilecektir.

Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesi uyarınca devletlerin "kuvvet kullanma" veya "kuvvet kullanma tehdidinde" bulunması yasaklanmış; bu yasağa istisna olarak ise Birleşmiş Milletler Şartı'nın 7. Bölümü uyarınca Birleşmiş Milletler Güvenlik Konseyi'nin yetkilendirmesi ve Birleşmiş Milletler Şartı'nın 51. maddesi uyarınca meşru müdafaa hakkının kullanılması öngörülmüştür. Öte yandan Birleşmiş Milletler Şartı çerçevesinde devletlerin tek taraflı olarak kuvvete başvurmasına ilişkin kuvvet kullanmanın yanı sıra "saldırı" ve "silahlı saldırı" da dahil olmak üzere farklı kavramlara da yer verilmiş; bunlardan saldırı kolektif güvenlik normları uyarınca Güvenlik Konseyi kararı doğrultusunda kuvvet kullanılmasına olanak sağlayan durumlardan sayılmıştır. Öte yandan "silahlı saldırı" açısından ise saldırı kavramından daha yüksek bir eşik öngörülmüş; devletin meşru müdafaaya başvurabilmesi silahlı bir saldırıya maruz kalması ön şartına bağlanmıştır.

Bu kapsamda çalışmanın ikinci bölümünde siber kuvvet kullanma, siber saldırı ve siber silahlı saldırı alt başlıkları oluşturulmuş; sayılan kavramların geleneksel uluslararası hukuk açısından durumu açıklandıktan sonra mesele siber operasyonlar açısından irdelenmiştir. Saldırgan siber operasyonların hangi koşullarda kuvvet kullanma, saldırı yahut silahlı saldırı teşkil edeceğinin değerlendirilmesinin akabinde edinilen çıkarımların farklı siber operasyon çeşitlerine uygulanarak meselenin güncel örnekler üzerinden tahlil edilmesine çalışılmıştır.

Çalışmanın üçüncü bölümünde ise saldırgan bir siber operasyonun bir devlete atfedilebilmesi hususu incelenmiştir. Zira devlet bir tüzel kişilik olması sebebiyle eylemlerini kendi organları ya da kamu gücü yetkilerini kullanan kişi veya birimler aracılığıyla gerçekleştirmektedir. Keza devletler amaçlarına erişebilmek amacıyla devlet dışı aktörlerden de faydalanabilmektedir. Saldırgan bir siber operasyonun herhangi bir şekilde uluslararası hukuku ihlal etmesi ve bu kapsamda söz konusu operasyona karşılık verilebilmesi için öncelikle eylem sorumlu devlete atfedilmelidir. Siber operasyonların gizli yürütülebiliyor olması ve uluslararası hukukta atfedilebilirlik hususunda başvurulması gereken delillere dair kesin kurallar bulunmaması meseleyi daha da önemli kılmaktadır. Ancak yine de yakın tarihimizde devletler tarafından çeşitli teknik isnat yöntemleriyle saldırgan siber operasyonların kaynağı tespit edilerek sorumlu olan devlete atfedildiği örnekler mevcuttur. Bu kapsamda güncel gelişmeler de dikkate alınarak saldırgan bir siber operasyonun sorumlu devlete atfedilebilmesi hususu devletlerin uluslararası hukuk sorumluluğuna ilişkin normlar çerçevesinde değerlendirilecektir.

BİRİNCİ BÖLÜM:

SİBER OPERASYONLAR VE *JUS AD BELLUM*: KAVRAMLARIN NETLEŞTİRİLMESİ

Bu bölümde öncelikle genel hatlarıyla *jus ad bellum* özetlenerek çalışma kapsamında inceleme gerçekleştirilecek konu başlıkları açıklanacaktır. Çalışmanın inceleme alanının netleştirilmesinin ardından öncelikle siber operasyonların uluslararası hukuktan ne şekilde etkilendiği meselesi tartışılacaktr. Nitekim *jus ad bellum* çerçevesinde yapılacak olanlar da dahil olmak üzere, konunun uluslararası hukuk açısından değerlendirilebilmesi için öncelikle ele alınan hususun tabi olduğu bir uluslararası hukuk normunun olup olmadığı ve var ise devletler açısından yarattığı sonuçların aydınlatılması gerekmektedir. Ayrıca çalışma ile geleneksel uluslararası hukuk kurumlarının yeni bir tartışmaya uygulanması amaçlandığından, gerçekçi sonuçlara ulaşabilmek adına inceleme konusu kavramların tanımlanarak kapsamının belirlenmesi de büyük önem arz etmektedir. Zira çalışmada "siber operasyon" kavramına sıklıkla başvurulacağından gerçekleştirilen inceleme sonucu elde edilen çıkarımların verimli bir şekilde tahlil edilebilmesi için siber operasyon kavramı ile neyin kastedildiği hususu açıklığa kavuşturulmalıdır. Öte yandan siber operasyon kavramının açıklanabilmesi için öncelikle konuya ilişkin diğer bir kavram olan "siber alan" tanımlanmalı ve kavramın uluslararası hukuk ile nasıl ilişkilendirilebileceği sorunu irdelenmelidir. Bu sayede konunun genel hatlarının okuyucu tarafından benimsenmesi sağlanarak çalışmanın sonraki bölümlerinde yer verilecek tartışmaların söz konusu kavramlar üzerinden inşa edilebilmesi hedeflenmektedir.

1.1. Genel Olarak "*Jus Ad Bellum*"

Latince bir terim olan *jus ad bellum* "kuvvete başvurma hakkı" olarak tercüme edilebilir[2]. *Jus ad bellum* ile uluslararası ilişkilerde kimlerin kuvvete başvurabileceği ve hangi hallerde bir kuvvete başvurma hakkını haiz olunduğu uluslararası hukuk

[2]Robert Kolb, **An Introduction to the International Law of Armed Conflicts**, Oxford, Hart Publishing, 2008, s. 9.

çerçevesinde incelenmektedir[3]. 18. yüzyılda bir devletin kuvvete başvurması egemenlik hakkının bir parçası olarak görülmüşken 19. yüzyılın sonlarında bu yaklaşım yerini daha sınırlı bir *jus ad bellum* anlayışına bırakmıştır[4]. Bu yaklaşım günümüze değin devam etmiş; Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesi ile 39 ve 51. maddeleri modern *jus ad bellum*un temellerini oluşturmuştur[5]. Nitekim Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesi uyarınca, devletlerin kuvvet kullanması yahut kuvvet kullanma tehdidinde bulunması yasaklanmış; hatta kuvvet kullanma yasağı uluslararası teamül hukukunun da bir parçası olarak değerlendirilmiştir[6]. Her ne kadar 2(4) numaralı madde ile tek taraflı kuvvete başvurma sıkı bir şekilde sınırlanmışsa da BM Şartı ile söz konusu yasağa ilişkin istisnalara da yer verilmiş; 39. maddede yer verilen kolektif güvenlik normları uyarınca bir devletin Birleşmiş Milletler Şartı'nın 42. maddesi doğrultusunda yetkilendirilmesi durumunda veya silahlı saldırıya uğraması halinde 51. madde uyarınca meşru müdafaa hakkı kapsamında uluslararası hukuka uygun olarak kuvvete başvurmasına olanak sağlanmıştır[7].

Birleşmiş Milletler Şartı çerçevesinde tek taraflı kuvvet kullanımı incelenirken ayrı bölümlerde "kuvvet", "saldırı" ve "silahlı saldırı" kavramlarına yer verilmiş; bu kavramlardan kuvvet kullanma kuvvete başvurmanın en genel şekli olarak 2(4)

---

[3]Johanna Frimen, **Revisiting the Concept of Defence in the Jus ad Bellum: The Dual Face of Defence**, Hart Publishing, 2017, s. 7; Lindsay Moir, **Reappraising the Resort to Force: International Law, Jus ad Bellum and the War on Terror**, Hart Publishing, 2010, s. 5; Stuart Casey-Maslen, **Jus ad Bellum: The Law on Inter-State Use of Force**, Hart Publishing, 2020, s. 1; Kolb, **a.g.e**, s. 9.

[4]Kolb, **a.g.e**, s. 10; Yoram Dinstein, **War, Aggression and Self-Defence**, Cambridge, 5. Baskı, Cambridge University Press, 2011, s. 163; Judith Gardam, **Necessity, Proportionality and the Use of Force by States**, New York, Cambridge University Press, 2004, s. 44. Bu yaklaşıma Kellogg-Birand Paktı ile savaşın bir ulusal politika olarak kullanılmasının yasaklanarak bunun yerine barışçıl çözümlerin tercih edilmesi gerektiği yönündeki düzenleme örnek gösterilebilir. (Dinstein, **a.g.e**, s. 85)

[5]Kolb, **a.g.e**, s. 11-12; Dinstein, **a.g.e**, s. 87; Frimen, **a.g.e**, s. 11.; Peter Valek, "Legality versus Legitimacy and the Use of Force", **Progress in International Law**, Ed: Russel A. Miller / Rebecca M. Bratspies, Leiden, Martinus Nijhoff Publishers, 2008, (615-633), s. 626; International Committee of the Red Cross, **International Humanitarian Law: Answers to Your Questions**, ICRC Publications, *https://shop.icrc.org/droit-international-humanitaire-reponses-a-vos-questions-2616.html*, s. 8, (erişim tarihi: 02.05.2020)

[6]Christine Gray, **International Law and the Use of Force**, New York, 3. Bası, Oxford University Press, 2008, s. 30.

[7]Ido Kilovaty, "Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare", **National Security Law Brief 5**, No. 1, 2014, (91-124), s. 100; Oscar Schachter, "The Lawful Resort to Unilateral Use of Force", **Yale Journal of International Law**, Vol. 10, No. 2, 1985, (291-294), s. 291.

numaralı madde uyarınca yasaklanmışken, silahlı saldırı ise en yüksek şiddet eşiğine erişmiş kuvvet kullanma yöntemi olarak meşru müdafaa hakkına başvurulmasının ön koşulu olarak düzenlenmiştir[8]. Bu sayede sadece belirli bir boyutta olan ve ciddi sonuçlar yaratan kuvvet kullanma eylemleri silahlı saldırı olarak kabul edilebilecek, küçük çaptaki kuvvet kullanma eylemleri sebebiyle meşru müdafaaya başvurulması sonucu çatışma ortamının şiddetlenmesinin önüne geçilebilecektir[9]. Öte yandan BM Şartı çerçevesinde çeşitli kavramlara yer verilmesi ve bu kapsamda bir eylemin uluslararası hukuk açısından değerlendirmesinde farklı eşikler öngörülmesi devlet uygulamasında karşılaşılan durumların söz konusu normlar çerçevesinde değerlendirilmesine ilişkin tartışmaları da beraberinde getirmiştir. Keza bu husus nispeten yeni bir kavram olmakla birlikte hem sayıları hem de etkileri her geçen gün artan siber operasyonlar açısından da söz konusu olmuş; yıkıcı etkiye sahip saldırgan siber operasyonların *jus ad bellum* açısından yarattığı sonuçlar yukarıda özetlenen normlar çerçevesinde değerlendirilerek mesele çözümlenmeye çalışılmıştır[10].

1.2. Uluslararası Hukuk Normlarının Siber Operasyonlara Uygulanabilirliği

Siber operasyonlar uluslararası hukuk açısından değerlendirilirken öncelikle siber operasyonların uluslararası hukuka tabi olup olmadığı ve tabi olduğu takdirde hangi normların ne şekilde uygulanması gerektiğinin netleştirilmesi önem arz etmektedir. Zira bir uluslararası hukuk normunun devletler üzerinde bağlayıcı olması resmi bir uluslararası hukuk kaynağına dayanmasına bağlıdır[11]. Uluslararası Adalet Divanı Statüsü'nün 38. maddesinde uluslararası hukukun temel kaynakları ise '*taraf devletlerce açıkça tanınan kurallar koyan genel ya da özel uluslararası antlaşmalar,*

[8]François Delerue, **Cyber Operations and International Law**, Cambridge, Cambridge University Press, 2020, ss. 328-29.
[9]Henning Lahmann, **Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution**, Cambridge, Cambridge University Press, 2020, s. 48; Marco Roscini, **Cyber Operations and the Use of Force in International Law**, New York, Oxford University Press, 2014, s. 72.
[10]Dinstein, **a.g.e**, s. 33.
[11]Hugh Thirlway, "The Sources of International Law", **International Law**, Ed: Malcolm D. Evans, Oxford University Press, 2010, (117-145), s. 119.

hukuk olarak kabul edilmiş genel bir uygulamanın kanıtı olarak uluslararası teamül, uygar uluslarca kabul edilen genel hukuk ilkeleri' olarak sayılmıştır[12].

Öncelikle belirtmek gerekir ki siber aktivitelerin günlük hayatın ayrılmaz bir parçası haline gelmesi ve hem bireylerin hem de devletlerin bu alanda yoğun faaliyet göstermesinin bir sonucu olarak uluslararası hukuk çerçevesinde de siber alana yönelik çeşitli sözleşmelere yer verilmiştir[13]. Öte yandan hâlihazırda mevcut siber aktivitelere ilişkin düzenlemeler devletlere atfedilebilecek saldırgan siber operasyonlara ilişkin herhangi bir norm sağlamamaktadır. Hatta yakın geçmişte karşılaşılan ve aralarına her geçen gün yenileri eklenen siber operasyonlar örnek gösterilerek bu hususun bir eksiklik olduğuna işaret edilmiş; Microsoft siber operasyonlara ilişkin devletlerin davranışlarının kurallara bağlandığı bir Dijital Cenevre Sözleşmesi'nin siber alandaki barışı korumak ve çatışmaları önlemek için elzem olduğu tespitinde bulunmuştur[14]. Ancak siber operasyonları doğrudan düzenleyen bir uluslararası antlaşmanın bulunmaması mevcut uluslararası antlaşmaların siber operasyonlara uygulanamayacağı biçiminde yorumlanmamalıdır.

---

[12]United Nations, Statute of the International Court of Justice, 18 April 1946; Uluslararası antlaşmalar ve uluslararası teamül hukuku arasında hiyerarşik bir ilişki bulunmadığından aynı konuda bu iki uluslararası hukuk kaynağı arasında farklı düzenlemeler bulunması halinde meselenin özel hükümler getiren düzenlemenin genel hükümler getiren düzenlemelere tercih edilmesi (*lex specialis derogat generali*), daha güncel olan düzenlemelerin esas alınması (*lex posterior derogat priori*) ve özel hükümler taşıyan hukuk düzenlemelerin daha sonra getirilen genel hükümlere ilişkin bir düzenlemeye tercih edilmemesi (*lex posterior generalis non derogat priori speciali*) ilkeleri çerçevesinde çözümlenmesi öngörülmektedir (Antonio Cassese, **International Law**, 2. Bası, Oxford University Press, 2005, s. 154.) Öte yandan kapsamı sıklıkla tartışma konusu edilen genel hukuk ilkelerineyse uluslararası antlaşmalar yahut uluslararası teamül hukukunda düzenleme bulunmaması halinde başvurulması gerektiği savunulmaktadır (Gerhard Von Glahn, **Law Among Nations an Introduction to Public International Law**, 7. Baskı, Longman, 1996, s. 18.)

[13]Siber aktivitelerin nispeten yeni bir kavram olması sebebiyle bu alanı doğrudan düzenleyen pek fazla sözleşme bulunmamakla birlikte önemli örnekleri olarak Birleşmiş Milletler Siber Suçlar Konvansiyonu ve 2006 Ek Protokolü, Şanghay İşbirliği Örgütü'nün Uluslararası Bilgi Güvenliği Antlaşması, Uluslararası Telekomünikasyon Birliği Kuruluş Tüzüğü ve Konvansiyonu, Uluslararası Telekomünikasyon Düzenlemeleri sayılabilir. (Michael N. Schmitt / Liis Vihul, "The Nature of International Law Cyber Norms", **Tallinn Paper No. 5 Special Expanded Issue**, Tallinn, CCDCOE Publications, 2014, s. 12); Keza 1 Temmuz 2014 tarihinde yürürlüğe giren Siber Suç Hakkında Budapeşte Antlaşması da devletlerin iç hukuklarında belirli siber suçları yaptırıma tabi tutması, kendi bölgelerinde yahut kendi vatandaşları tarafından işlenen siber suçlara ilişkin soruşturma ve kovuşturmalarda karşılıklı destek sağlanması hususlarında düzenlemeler getirmesi açısından önemli sayılabilir. (Roscini, **Cyber Operations and the Use of Force in International Law**, s. 19)

[14]Microsoft, A Digital Geneva Convention to Protect Cyber Space, Microsoft Policy Papers, *https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH*,(erişim tarihi: 09.02.2020)

Uluslararası Adalet Divanı, Kosta Rika ve Nikaragua arasında görülen seyrüsefer ve ilişkili haklara ilişkin uyuşmazlıkta "*tarafların bir sözleşmede genel terimler kullandığı hallerde, tarafların terimin zaman içerisinde evrimleşebileceğinin farkında olduğu, sözleşmenin çok uzun bir süreliğine yürürlüğe girdiği yahut devam eden süreli olduğu durumlarda tarafların, genel bir kural olarak, terimlerin evrimleşen anlamlara sahip olması niyetinde oldukları kabul edilmelidir*" tespitinde bulunmuştur[15].Yine bu doğrultuda, Uluslararası Adalet Divanı Nükleer Silahlara İlişkin Tavsiye Kararı'nda Birleşmiş Milletler Şartı'nın kuvvet kullanma yasağına ilişkin düzenlemesinin belirli silahlara ilişkin olmadığını ve belirli bir silahın kullanımına dair yasaklama yahut izin verme içermediğini belirtmiştir[16]. Bu kapsamda doğrudan bu alanı düzenlemese dahi siber operasyonlara uygulanabilecek uluslararası hukuk normlarına söz konusu operasyonların uluslararası hukuk açısından yarattığı sonuçların değerlendirilmesi amacıyla başvurulabilecektir[17].

Lakin siber operasyonların kendine has özellikleri sebebiyle bu yönde bir değerlendirmenin nasıl gerçekleştirilebileceği de ayrı bir tartışma konusudur. Bu hususun netleştirilebilmesi adına uluslararası antlaşmalara başvurulması savunulabilecekse de kanımızca yakın gelecekte böyle bir girişimin başarıya ulaşması öngörülmemekte ve konunun devlet uygulamaları aracılığıyla açıklığa kavuşacağı tahmin edilmektedir. Bu sebeple siber operasyonların tabi olduğu uluslararası hukuk normları incelenirken uluslararası teamül kurallarının[18] da göz önünde bulundurulması gerekmektedir.

---

[15]*Dispute Regarding Navigational and Related Rights* (Costa Rica v Nicaragua), Judgment, 13 July 2009, ICJ Reports 2009, ("Nikaragua Davası"), para 66.

[16]Uluslararası Adalet Divanı, *Nükleer Silahların Kullanımı veya Kullanım Tehdidinin Yasallığı, Tavsiye Kararı*, 1. C.J. Reports 1996, ("Nükleer Silah Tavsiye Kararı") s. 226, para. 39.

[17]Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis*"*, S**tanford Law & Policy Review**, Vol. 25, (269-299), s. 272; Harold H. Koh, "International Law in Cyberspace", **Harvard International Law Journal**, vol. 54, 2012, (1-12), s. 3; Benjamin Mueller, "The Laws of War and Cyberspace On the Need for a Treaty Concerning Cyber Conflict*"*, **LSE Ideas Strategic Update 14.2**, 2014, s. 1.

[18]Uluslararası teamül kuralları devletlerin belli bir davranışı bir çeşit yasal zorunluluk (*opinio juris*) olarak değerlendirip uzun bir süre boyunca uygulaması ile bu davranışın uluslararası hukukun bağlayıcı bir kaynağı haline gelmesi olarak özetlenebilir. (Roozbeh B. Baker, *"*Customary International Law in the 21st Century: Old Challenges and New Debates", T**he European Journal of International Law**, vol. 21, No.1, 2010, (173-204), s. 176.)

Her ne kadar siber operasyonların nispeten yeni bir kavram oluşu uluslararası teamül kurallarının oluşması için uzun bir süre uygulanıyor olma şartının sağlanması açısından soru işaretleri oluştursa da Uluslararası Adalet Divanı tarafından Kuzey Denizi Kıta Sahanlığı Davası Kararı'nda belirtildiği üzere, çıkarları özellikle etkilenen devletlerin de dahil olması koşuluyla, çok yaygın bir katılımın olduğu bir kural önemli bir süre geçmeden bile uluslararası teamül hukukunun bir parçası haline gelebilecektir[19]. Nitekim Birleşmiş Milletler Genel Kurulu nezdinde yürütülen çalışmalardan hem siber alanda uluslararası güvenlik kapsamında sorumlu devlet davranışının geliştirilmesi hem de bilgi ve telekomünikasyon alanındaki gelişmelerin uluslararası güvenlik açısından incelenmesi üzerine alınan kararlarda bu alanda uluslararası hukukun ne şekilde uygulanması gerektiği hususu üzerinde durulmuştur[20]. Bu kapsamda Birleşmiş Milletler Hükümet Uzmanları Çalışma Grubu bilgi teknolojileri ve uluslararası güvenliğe ilişkin gerçekleştirmiş olduğu çalışmalarda istikrarlı bir şekilde siber operasyonların da uluslararası hukuka tabi olduğu yönünde görüş bildirmiştir[21].

Öte yandan, gerek siber operasyonların gizlilik içerisinde yürütülüyor olması sebebiyle saldırgan bir siber operasyona maruz kalan bir devletin her zaman söz konusu operasyonu analiz ederek sorumlu devlete atfedemiyor olması, gerekse devletlerin siber operasyonları sorumlu devlete atfedebilecek teknolojiye sahip olduğu hallerde dahi operasyonel yahut diplomatik tercihler sebebiyle bu yönde bir girişimde bulunmama ihtimali uluslararası teamül kurallarının oluşmasının önünde bir engel olarak değerlendirilebilecektir[22]. Ancak bu tip yaklaşımlar söz konusu olsa dahi siber

---

[19]*North Sea Continental Shelf Cases* (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands) , I.C.J. Reports 1969, p.3, International Court of Justice (ICJ), 20 February 1969, para. 73; Keza Yargıç Sorensen de söz konusu karara ilişkin muhalefet şerhinde günümüzdeki fazlasıyla dinamik olan norm evrimleşme sürecine dikkat çekerek yeni uluslararası teamül kurallarının hızlı bir şekilde ortaya çıkabileceği tespitinde bulunmuştur. (*North Sea Continental Shelf Case*, Diss. Op. Judge Sorensen [1969] ICJ Reports, 244)

[20]Resolution adopted by the General Assembly on 22 December 2018, A/RES/73/266; Resolution adopted by the General Assembly on 5 December 2018, A/RES/73/27

[21]Birleşmiş Milletler Genel Kurulu Hükümet Uzmanları Çalışma Grubu, **Developments in the Field of Information and Telecommunications in the Context of International Security**, A68/98, 24 Haziran 2013, s. 9.

[22]Garry Brown / Keira Poellet, "The Customary International Law of Cyberspace*"*, **Strategic Studies Quarterly**, 2012, (126-145), s. 129.

operasyonlara yönelik her geçen gün artan devlet uygulamaları ve uluslararası platformların norm tespitine yönelik çalışmaları sayesinde aday uluslararası hukuk normlarının belirlenmeye başladığı söylenebilmektedir[23]. Dolayısıyla mevcut uluslararası hukuk kaynaklarının geleneksel silahlara ilişkin bir sınırlama içermediği gerçeği göz önüne alındığında, evrimleşme teorisi çerçevesinde siber operasyonların da ilgili uluslararası hukuk normlarına uygun bir şekilde yürütülmesi gerektiği sonucuna ulaşılabilecektir[24].

Uluslararası hukukun kaynakları sayılırken yargı organlarının kural yokluğu (*non liquet*) sebebiyle yargı işlevini yerine getirememesi ihtimali de öngörülmüş; bu duruma karşı hukukun genel ilkelerine de bir uluslararası hukuk kaynağı olarak yer verilerek uluslar tarafından kabul edilmiş temel hukuk ilkelerinin yargıçlar tarafından saptanarak uyuşmazlık konusu meseleye uygulanmasına olanak sağlanmıştır[25]. Dolayısıyla farklı hukuk sistemlerinde benimsenen ortak ilkeler uluslararası hukuk düzeninde uygulanabilir olduğu takdirde saldırgan siber operasyonlara ilişkin herhangi bir uyuşmazlıkta gündeme gelebilecektir. Genel hukuk ilkelerinin sınırlayıcı olarak tespiti mümkün olmamakla birlikte verilen bir zararın onarılması, savaşanların yasal savunma nedeniyle tarafsızlara verecekleri zararlardan sorumlu tutulmaları, hakkın kötüye kullanılmaması ve devletin bağımsızlığı ilkesi örnek gösterilebilir[26]. Zira korudukları değerler dikkate alındığında, sayılan genel hukuk ilkelerinin saldırgan siber operasyonlar sebebiyle söz konusu olabilecek uyuşmazlıklarda mevcut uluslararası antlaşmalarda yahut uluslararası teamül hukukunda herhangi bir norm

---

[23]Brian M. Mazanec, **The Evolution of Cyber War: International Norms for Emerging-Technology Weapons**, University of Nebraska Press, 2015, s. 162.

[24]Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace", **Texas National Security Review**, 2020, *https://tnsr.org/2020/07/taming-the-lawless-void-tracking-the-evolution-of-international-law-rules-for-cyberspace/*,(erişim tarihi: 01.08.2020); Mazanec, **a.g.e**, s. 177.

[25]Lassa F. L. Oppenheim, **International Law a Treatise, Vol. I. – Peace**, Ed: Hersh Lauterpacht, 8. Bası, Londra, Longmans, 1955, s. 29; Ian Brownlie, **Principles of Public International Law**, 4. Bası, New York, Oxford University Press,1990, s. 15-16; Thirlway, **a.g.m**, s. 130; Glahn, **a.g.e**, s. 18; Melda Sur, **Uluslararası Hukukun Esasları**, İstanbul, Beta, 2014, s. 85.

[26]Brownlie, **Principles of Public International Law**, s. 18; Malcolm N. Shaw, **International Law**, 5. Bası, Cambridge, Cambridge University Press, 2003, s. 97; Thirlway, **a.g.m**, ss. 131-32; Hüseyin Pazarcı, **Uluslararası Hukuk**, 7. Bası, Ankara, Turhan Kitabevi Yayınları, 2008, s. 120.

bulunmadığı takdirde hakkaniyete uygun bir çözüme ulaşılması için değerlendirilebileceği söylenebilmektedir.

Uluslararası Adalet Divanı Statüsü'nün 38. maddesinde uluslararası hukukun kaynakları belirlenirken açıkça ayrım yapılarak uluslararası antlaşmalar, uluslararası teamül hukuku ve genel hukuk ilkeleri uluslararası hukukun asıl kaynakları olarak sayılmışken, uluslararası yargı kararları ve bilimsel çalışmalara tamamlayıcı kaynak olarak yer verilmiştir[27]. İlgili düzenlemenin yorumlanmasından da anlaşılacağı üzere, uluslararası hukuka ilişkin bir uyuşmazlık yorumlanırken söz konusu uyuşmazlığa dair normların tespitinde yahut bu normların uygulanmasında yardımcı kaynaklardan faydalanılabilecektir.

Uluslararası Adalet Divanı Statüsü'nün 59. maddesi ise "*Divan'ın kararı taraflar ve ilgili dava haricinde bağlayıcı güce sahip değildir*" düzenlemesini haizdir. Öte yandan, uluslararası hukukun halen gelişmekte olan bir alan olmasının da etkisiyle gerek uyuşmazlıkları çözmeye yetkili makamların gerekse uyuşmazlığa taraf devletlerin özellikle mevcut kuralların yorumuna ilişkin daha önceki yargı kararlarına atıfta bulundukları görülmektedir[28]. Eklemek gerekir ki yardımcı kaynak olarak dikkate alınabilecek yargı kararları uluslararası yargı kararları ile sınırlı tutulmadığından ulusal yargı organlarının kararları da bu kapsamda değerlendirilebilecektir[29]. Her ne kadar saldırgan siber operasyonlara ilişkin birçok uyuşmazlık gündeme gelmişse de bu çalışmanın hazırlandığı döneme değin henüz bu uyuşmazlıklara ilişkin uluslararası yargı organlarınca verilmiş bir karar bulunmamaktadır. Dolayısıyla bir yardımcı kaynak olarak yargı kararları değerlendirilirken doğrudan siber alana ilişkin olmayan yargı kararlarının uygun düştüğü ölçüde meseleye uygulanması gerekecektir.

Diğer bir yardımcı kaynak olan bilimsel çalışmalar ise yargı kararlarının aksine kısa zamanda oldukça gelişme göstermiştir. Zira siber alanla tanışılmasının ilk

---

[27]United Nations, Statute of the International Court of Justice, 18 April 1946
[28]Oppenheim, **International Law a Treatise, Vol. I. – Peace**, s. 31; Brownlie, **Principles of Public International Law**, ss. 19-20; Shaw, **a.g.e**, s. 103; Glahn, **a.g.e**, ss. 19-20; Yücel Acer / İbrahim Kaya, **Uluslararası Hukuk**, Ankara, Seçkin, 2014, s. 59.
[29]Thirlway, **a.g.m**, s. 133.

günlerinden itibaren uluslararası hukuk kapsamında yaratabileceği etkiler pek çok hukukçu tarafından tartışılmaya başlanmış; zaman içerisinde siber alanın gelişmesiyle bu kapsamda üretilen akademik çalışmalarda da artış yaşanmıştır[30]. Dolayısıyla ilerleyen süreçte özellikle doğrudan siber alanı ilgilendiren normların yokluğu sebebiyle, mevcut uluslararası hukuk normlarının yorumlanmasında ve doğabilecek uyuşmazlıklara uygulanmasında bilimsel çalışmaların yardımcı kaynak olarak önemli bir rol oynayacağı tahmininde bulunulabilir.

1.3. Siber Alanın Tanımı ve Kapsamı

Siber operasyonların incelemesine geçilmeden evvel siber operasyonların tanımlanabilmesi için açıklanması ihtiyacı hissedilen siber alan kavramı üzerinde durulmalıdır. Siber alan dilimize, sözlük karşılığı "*dünya üzerindeki bilgisayar kullanıcılarının birbirleriyle iletişim kurmalarını yahut herhangi bir amaçla bilgiye ulaşmalarını sağlayan elektronik sistem*"[31] olan İngilizce "*cyberspace*" kelimesinin tercümesi yoluyla geçmiş olup literatürde siber alan terimi yerine aynı anlamda siber uzay, siber dünya ve siber ortam adlandırmaları da kullanılmaktadır[32]. Lakin ilk ortaya çıktığı dönemden beri, siber alanın hukuksal çerçevede değerlendirilebilmesi için daha kapsamlı bir tanımının yapılmasına ihtiyaç duyulmuştur[33]. Kuzey Atlantik Antlaşması Örgütü'nün ("NATO") bu alanda çalışan akademisyenleri bir araya getirmesiyle

[30]Bunlardan en önemlilerine değinmek gerekirse, yukarıda da anılan Birleşmiş Milletler Genel Kurulu'nun talebi üzerine Birleşmiş Milletler Genel Sekreteri tarafından uluslararası güvenlik kapsamında siber aktivitelerin değerlendirilmesi amacıyla kurulan Birleşmiş Milletler Resmi Uzmanlar Grubu'nun uluslararası hukukun bu alana nasıl uygulanacağına dair ortak anlayış yaratmaya çalıştığı raporlardan söz edilebilir. (Brian J. Egan, "International Law and Stability in Cyberspace", Vol. 35 **Berkeley Journal of International Law**. 2017, (169-180), s. 170) Kuzey Atlantik Paktı Örgütü'nün (*North Atlantic Treaty Organization* - "NATO") önceliğinde Kuzey Atlantik Paktı Örgütü Siber Savunma Mükemmeliyet Merkezi ("NATO CCDCOE") alanında öncü birçok akademisyeni bir araya getirerek bu çalışmada da sık sık değinilen Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı ("Tallinn El Kitabı") ve Siber Operasyonlara Uygulanacak Hukuk Hakkında Tallinn El Kitabı 2.0'ın ("Tallinn El Kitabı 2.0") hazırlanmasına vesile olmuştur. Keza bu alanda bağımsız olarak da çalışma yürüten pek çok akademik kuruluş da bulunmakta olup bunlara uluslararası hukuk normlarının siber alandaki devlet faaliyetlerine nasıl uygulanması gerektiğine ilişkin araştırmalar yürüten Siber Normlar için Hague Programı (*The Hague Program for Cyber Norms*) örnek gösterilebilir.

[31]Cambridge Dictionary, *https://dictionary.cambridge.org/tr/sözlük/ingilizce/cyberspace*,(erişim tarihi: 31.01.2020)

[32]Hasan Çiftçi, **Her Yönüyle Siber Savaş**, Ankara, TÜBİTAK Popüler Bilim Kitapları, 2013, s. 2.

[33]Peter W. Singer / Allan Friedman, **Cybersecurity and Cyberwar: What Everyone Needs to Know**, Oxford University Press, 2014, ss. 12-13.

hazırlanan çalışmalarda siber alan özetle, "*bilgisayar ağları kullanılarak veri depolanması, değiştirilmesi yahut takasının gerçekleştirildiği, maddesel ve soyut bileşenlerden oluşan ortam*" olarak tanımlanmıştır[34]. NATO kapsamında incelemeler gerçekleştiren uluslararası uzmanlar grubu tarafından siber alan tanımlanırken bilgisayar ağları aracılığıyla gerçekleştirilebilen faaliyetlerin esas alındığı görülmektedir[35]. Kanımızca siber alanın daha net anlaşılabilmesi için tanımda bu alanda gerçekleştirilebilen faaliyetler kadar siber alanı oluşturan unsurlara da yer verilmesi gerekmektedir[36]. Bu kapsamda siber alanın bilgisayarlar, entegre devreler, kablolar ve iletişim altyapısından oluşan fiziki katman; yazılımlardan oluşan mantıksal katman; onların üzerindeyse veri paketi ve elektronikleri haiz anlamsal katman olmak üzere üç ana katmandan[37] oluştuğu söylenebilecektir[38]. Sonuç olarak, siber alanın fiziki altyapı aracılığıyla erişilen, yazılımlar aracılığıyla işletilen ve dünya çapında kullanıcıların her türlü bilginin depolanması, dolaşımı ve kullanılması faaliyetlerinde bulunabildiği alan olarak tanımlanabileceği kanaatindeyiz.

1.4. Siber Operasyonun Tanımı ve Kapsamı

Siber operasyonların uluslararası hukuk açısından incelenmesine ilişkin çalışmalarda siber muharebe, bilgi operasyonu (*information operation*), bilgisayar ağı

---

[34]NATO Müşterek Siber Savunma Mükemmeliyet Merkezi ("NATO CCD COE"), **Tallinn Manual on the International Law Applicable to Cyber Warfare**, Ed: Michael N. Schmitt, Cambridge University Press, 2013, ("Tallinn Manual"), s. 258; NATO Müşterek Siber Savunma Mükemmeliyet Merkezi, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, Ed: Michael N. Schmitt, Cambridge University Press, 2017, ("Tallinn Manual 2.0"), s. 564.

[35]Birleşik Krallık da siber güvenlik stratejisi kapsamında yaptığı çalışmalarda benzer bir yöntemle siber alanı "*bilginin depolanması, değiştirilmesi ve nakledilmesi için kullanılan dijital ağlardan oluşan etkileşimli alan*" olarak tanımlamıştır. (Birleşik Krallık Kabine Ofisi, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, Birleşik Krallık Hükümeti, 2011, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf*, erişim tarihi: 31.01.2020, s. 11.)

[36]Nitekim Amerika Birleşik Devletleri Savunma Bakanlığı tarafından siber alanın "*internet dahil olmak üzere, birbirine bağlı şebekelerden oluşan bilgi teknolojisi altyapıları ve yerleşik veriler, telekomünikasyon şebekeleri, bilgisayar sistemleri ve gömülü işlemciler ve denetleyicilerden oluşan bilgi ortamı içerisindeki küresel alan*" olarak tanımlandığı görülmektedir (Amerika Birleşik Devletleri Savunma Bakanlığı, **DOD Dictionary of Military and Associated Terms**, Washington DC, 2020, s. 55.)

[37]Keza bu katmanlara fiziksel altyapı, mantıksal yapılar ve bilgiye ek olarak insanı da dahil eden görüşler de bulunmaktadır (Güzin Ulutaş, "Siber Güvenlik", **Siber Güvenlik ve Savunma, Farkındalık ve Caydırıcılık**, Ed: Şeref Sağıroğlu / Mustafa Alkan, Ankara, BGD Siber Güvenlik ve Savunma Kitap Serisi, 2018, ss. 87-88.)

[38]Martin C. Libicki, **Cyberdeterrence and Cyber War**, RAND Corporation, 2009, s. 12.

saldırısı (*computer network attack – "CNA"*) yahut siber saldırı (*cyber attack*) gibi terimlerin de sıklıkla kullanıldığı gözlemlenmektedir[39]. Siber muharebe terimi teknik olarak, sadece silahlı çatışma sırasında siber teknolojiler kullanılarak gerçekleştirilen düşmanca hareketleri çağrıştırması sebebiyle siber operasyonlara kıyasen daha dar kapsamlı olduğu için bu çalışmada tercih edilmemiştir[40]. Öte yandan bilgi operasyonu kavramı ise kendi içerisinde bilgisayar ağı operasyonlarının yanı sıra psikolojik operasyonlar, askeri aldatma operasyon güvenliği, elektronik muharebe ana başlıklarını içerdiğinden çalışmanın esas konusu olan siber alandaki saldırgan operasyonları ifade etmek için fazla geniş kapsamlı bir isimlendirme olacaktır[41]. Bilgisayar ağı saldırısı kavramı ise bilgisayar ağı operasyonları doktrini ile ayrılmaz bir ilişki içerisinde olmasının yaratabileceği olası karmaşıklıklar sebebiyle zaman içerisinde yerini siber saldırı kavramına bırakmıştır[42]. Ancak siber saldırı terimi ise kuvvet kullanma eşiğine erişen yahut özel olarak düşman bilgisayar sistemlerini veya verilerini aksatmak, engellemek, geriletmek, manipüle etmek yahut yok etmek amacıyla gerçekleştirilen siber operasyonları karşılamaktadır[43]. Dolayısıyla bu çalışma kapsamında, inceleme gerçekleştirilen alandaki tartışmalı hususların değerlendirilebilmesi adına bu yönde bir sınırlamadan kaçınılarak genel olarak siber operasyon isimlendirmesinin kullanılması uygun görülmüştür. Zira siber operasyon kavramı siber alanda gerçekleştirilen eylemlerin açıklanması için başvurulan kapsayıcı bir terim olarak kullanılmaktadır[44]. Bu doğrultuda siber operasyon kısaca, "*belirli*

---

[39]Reese Nguyen, "Navigating "Jus Ad Bellum" in the Age of Cyber Warfare", **California Law Review**, Vol. 101, No. 4, 2013, (1079-1129), s. 1085.

[40]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 11.

[41]Fred Schreier, "On Cyberwarfare", **DCAF Horizon 2015 Working Paper No. 7**, *https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf,* (erişim tarihi: 09.05.2020)

[42]Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates, **Joint Terminology for Cyberspace Operations**, 2010, s. 6, *http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf,* (erişim tarihi: 09.05.2020) Zira bilgisayar ağı saldırısı şeklinde bir kullanımın benimsenmesi halinde, siber casusluk ve benzeri amaçlarla gerçekleştirilen bilgisayar ağı faydalanma operasyonları (*network exploitation operations*) kavramın kapsama alanı dışarısında kalacaktır. (Delerue, **Cyber Operations and International Law**, s. 35) Oysaki bu çalışmada devletler tarafından başvurulabilecek saldırgan siber operasyonların uluslararası hukuk açısından yarattığı sonuçlara ilişkin genel bir inceleme sağlanması amaçlanmaktadır.

[43]Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates, Joint Terminology for Cyberspace Operations, s. 6.

[44]Delerue, **Cyber Operations and International Law**, s. 35.

amaçlara erişebilmek niyetiyle çeşitli siber araçların kullanıldığı ve siber alanda yahut siber alan aracılığıyla gerçekleştirilen operasyonlar" olarak tanımlanabilir[45].

[45]NATO CCD COE, **Tallinn Manual**, s. 258; NATO CCD COE, **Tallinn Manual 2.0**, s. 564.

İKİNCİ BÖLÜM:

SALDIRGAN SİBER OPERASYONLARIN ULUSLARARASI HUKUKU İHLAL ETTİĞİ HALLER

İlk bölümde özetlendiği üzere, günümüzde devletlerin başka bir devlete karşı kuvvet kullanması uluslararası hukuka aykırılık teşkil edecektir. Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesiyle öngörülen bu yasağın istisnaları ise yine Birleşmiş Milletler Şartı'nın 51. maddesiyle doğal bir hak kabul edilen meşru müdafaa hakkının yerine getirilmesi ve BM Şartı'nın 7. Bölümü uyarınca Güvenlik Konseyi'ne tanınan yetkiler doğrultusunda kuvvet kullanılmasıdır. Bu kapsamda çalışmanın bu bölümünde siber operasyonların söz konusu düzenlemelere hangi hallerde ve ne şekilde uygulanabileceği tartışılacaktır.

2.1. Saldırgan Bir Siber Operasyonun Uluslararası Haksız Fiil Teşkil Etmesi

Her ne kadar çalışmada siber operasyonlar *jus ad bellum* açısından incelenecekse de siber operasyonların kuvvet kullanma yasağı yahut silahlı saldırı kapsamında tartışılmasından evvel kuvvet kullanma eşiğine erişmeyen siber operasyonların durumuna da değinilmesi gerektiği kanaatindeyiz. Nitekim kuvvet kullanma veya kuvvet kullanma tehdidi (*forcible coercion*) yasağı, bu bölümde incelenecek olan içişlerine karışma (*dictatorial coercion*) yasağının en belirgin görünüşüdür[46]. Keza her iki yasak arasında net bir şekilde ayrım yapmak her zaman mümkün olmamaktadır. Son olarak eklemek gerekir ki en zararlı saldırgan siber operasyonlar kuvvet kullanma yasağını aşmamakla birlikte bir ülkenin kritik altyapısını ve ilişkili bilgi sistemlerini hedef alan siber operasyonlardır[47]. Zira ilerleyen bölümlerde detaylı bir şekilde inceleneceği üzere yakın tarihimizde tanık olunan

[46]Maziar Jamnejad / Michael Wood, "The Principle of Non-Intervention", **Leiden Journal of International Law**, Vol. 22, 2009, (345–381), s. 359.
[47]Marina Kaljurand, "United Nations Group of Governmental Experts: the Estonian Perspective", **International Cyber Norms: Legal, Policy & Industry Perspectives**, Ed: Anna-Maria Osula & Henry Rõigas, Tallinn, NATO CCD COE Publications, 2016, (111-127), s. 119.

önemli siber operasyonların büyük bir kısmının bu kategoride olduğu değerlendirilmektedir.

Bu bölümde öncelikle egemenlik kavramı ele alınarak siber operasyonların egemenlik ilkesinden ne şekilde etkilendiği tartışılacaktır. Bu amaçla, egemenliğe dair uluslararası hukuk normlarının siber operasyonlara nasıl uygulanabileceği sorularının cevaplanabilmesi adına siber alanın egemenlikle ilişkisi kurulmaya çalışılacaktır. Siber operasyonların egemenlik ilkesi kapsamında incelenmesini takiben egemenlik ilkesiyle yakın ilişkili bir uluslararası hukuk normu olan içişlerine karışma yasağı açısından konu irdelenecektir.

2.1.1. Saldırgan Siber Operasyonların Egemenlik İlkesi Kapsamında İncelenmesi

Öğretide siber operasyonlar uluslararası hukuk açısından incelenirken siber alan kavramı üzerinden tanımlanan bir egemenlik ve bu egemenliğe ilişkin olarak ülkesel egemenlik[48] ilkesinden kaynaklanan hak ve yetkiler doğrultusunda bir değerlendirme yapma eğilimi olduğu gözlenmektedir[49]. Zira egemenlik mahiyetindeki haklar ve yükümlülükler büyük oranda ülke kavramı üzerine inşa edilmiştir[50]. Lakin belirli bir kara, deniz veya hava bölgesinde egemen devletin haklarını ihlal edecek faaliyetlerde bulunmanın uluslararası hukuka aykırılık teşkil edeceği sonucuna kolaylıkla ulaşılabiliyorken aynı çıkarımı siber alan üzerinden sağlayabilmek için egemenlik ile korunan değerlerin siber alan kavramı üzerinden incelenmesi gerekmektedir.

Egemenlik, Birleşmiş Milletler Şartı'nın 2. maddesinde atıfta bulunulan devletlerin eşitliği, bölgesel bütünlük ve siyasi bağımsızlık ilkelerinin bir dayanağı olarak uluslararası hukukun temel kavramlarından biri olarak kabul edilmiş; devletlerarası ilişkiler başka bir devletin bölgesi üzerindeki egemenlik haklarına saygı

[48]Uluslararası hukuk bağlamında ülke kavramı irdelenirken geleneksel olarak devletlerin kara ülkesi esas alınarak kıyılarından oniki mile kadar olan alanı kaplayan deniz ülkesi belirlenmiş; kara ile deniz ülkelerinin üzerinde yer alan hava ülkesi de egemenlik alanı içerisine dahil edilmiştir. (Vaughan Lowe, "Jurisdiction - The Scope of Sovereignty", **International Law**, Ed: D. Malcolm D. Evans, 1. Basım, New York, Oxford University Press, 2003, (329-357), s. 336.)
[49]NATO CCD COE, **Tallinn Manual**, s. 16.
[50]Shaw, **a.g.e**, s. 409.

ilkesi üzerine kurulmuştur[51]. Devletlerarası ilişkiler kapsamında temel inceleme konusu olan egemenlik *Westphalian* egemenlik anlayışıdır[52]. Zira uluslararası hukukta devletin kurucu öğeleri olarak insan topluluğu, ülke ve başka bir otoriteye sahip olmayan siyasal yönetim kabul edilmekte olup bu faktörlerden ülke, egemenlik yetkilerinin ilke olarak sınırını oluşturması münasebetiyle öteki devletler tarafından bütünlüğüne saygı duyulması zorunluluğu bulunan mekânsal bir oluşum olarak karşımıza çıkmaktadır[53].

Siber operasyonların fiziki ortamda herhangi bir sınır ihlali yaşanmadan gerçekleştirilebiliyor olması devletin bütünlüğü ilkesi kapsamında ne şekilde değerlendirilmesi gerektiği sorusunu da beraberinde getirmiştir[54]. Bir görüşe göre, siber alanın var olabilmesi ve işleyebilmesi için bir oluşum tarafından kontrol edilmesi gerektiği; siber alanda kurulan finansal ilişkilerin ve gerçekleştirilen işlemlerin belli hukuk kuralları çerçevesinde gerçekleştiriliyor oluşu; siber alanda oluşan durumların dış dünyayı etkileyebilmesi ve devletlerin siber alanda ulusal güvenliklerini ilgilendirecek ölçüde varlık gösterdiği hususları birlikte değerlendirildiğinde, siber alanın da egemenliğe tabi olduğu sonucuna ulaşılabilmektedir[55]. Öte yandan siber alanda sınırların belli olmaması geleneksel kuralların sadece sınırlı bir kapsamda uygulanabileceği uyarılarının yapılmasına da yol açmaktadır[56]. Keza yine bu tartışmalar kapsamında teknolojik ilerlemeler sayesinde erişilen ortamların tıpkı hava

---

[51]Ian Brownlie, **Principles of Public International Law**, s. 287-88; Martin Dixon / Robert McCorquodale, **Cases & Materials on International Law**, 4. Bası, New York, Oxford University Press, 2003, s. 234.

[52]Krasner'e göre egemenlik kavramı genel olarak, bir devlette kamu otoritesinin örgütlenmesi ve bu otoritelerce yerine getirilen etkili kontrol seviyesi anlamında iç egemenlik; kamu otoritelerinin sınır aşan hareketleri kontrol etme yetisi anlamında birbirine bağlı (*interdependence*) egemenlik; devletlerin ve diğer kurumların karşılıklı olarak tanınması anlamında uluslararası hukuki egemenlik ve iç otorite yapılanmalarının dış unsurlardan hariç tutulması anlamına gelen *Westphalian* egemenlik olmak üzere en az dört farklı anlamda kullanılmaktadır. (Stephen D. Krasner, **Sovereignty: Organized Hypocrisy**, New Jersey, Princeton University Press, 1999, s. 9.)

[53]Brownlie, **Principles of Public International Law**, ss. 72-73, 107-108; Shaw, **a.g.e**, ss. 178-79; Pazarcı **a.g.e**, s. 144

[54]Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", **Columbia Journal of Transnational Law**, Vol. 37, 1999, (885-937), s. 888.

[55]Patrick W. Franzese, "Sovereignty in Cyberspace: Can It Exist?", **Air Force Law Review**, Vol. 64, 2009, (1-42), ss. 12-13.

[56]Katrin N. Metcalf, "A Legal View on Outer Space and Cyber Space: Similarities and Differences", **Tallinn Paper No. 10**, Tallinn, NATO CCD COE Publications, 2018, s. 9.

sahası gibi bölgesel egemenlik kapsamında değerlendirilebileceği yahut açık denizler gibi insanlığın ortak kullanım alanı (*res comminus omnium*) olarak kabul edilebileceği de savunulmuştur[57].

Siber alanın egemenlik ilkesinden ne şekilde etkilendiğinin tespit edilebilmesi için öncelikle siber alan kavramı ile egemenlik ilkesi arasındaki ilişkinin netleştirilmesi gerekmektedir. İlk bölümde kavramlar açıklanırken yer verilen tanımlarda da görüldüğü üzere, siber alan katmanlı bir yapıya sahiptir. Siber alanın fiziksel katmanına dışarıdan gerçekleştirilen müdahalelerin kendisi de fiziki karakterde olacağından bu tip müdahaleler siber operasyon kapsamında değerlendirilmeyecektir[58]. Dolayısıyla siber alanda devletin bütünlüğü ilkesi kapsamında egemenlik sınırlarının belirlenmesine ilişkin tartışmaların "sanal" ortamdaki ikinci ve üçüncü katmanla sınırlı olduğu tespiti yapılabilecektir. Siber alanın var olabilmesi için fiziki altyapıya ihtiyaç duyduğu ve bu sebeple sanal ortamın da fiziki katmandan bağımsız düşünülemeyeceği göz önüne alındığında, siber operasyonların da gerçekleştirildiği yahut sonuçlarının ortaya çıktığı bölge üzerinden ülkesel olarak ifade edilebileceği sonucuna ulaşılabilmektedir[59]. Öte yandan, bizim de katıldığımız görüşe göre, devlet uygulamasının gösterdiği üzere siber alanda egemenliğin ülkesel boyutu ortadan kalktığından, egemenliğin uluslararası hukuk açısından sonuç doğuran bir kural yerine devletlerin etkileşimlerine rehberlik eden bir uluslararası hukuk ilkesi olarak değerlendirilmesi daha gerçekçi sonuçlara ulaşmaya olanak sağlamaktadır[60]. Bunun sonucu olarak, egemenlik ilkesi her siber operasyon açısından hesaba katılmalıysa da, devletler üzerinde başka bir devletin siber

[57]Christopher C. Joyner / Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework", **European Journal of International Law**, Vol. 12, 2001, (825-865), s. 843.
[58]Peter Z. Stockburger, "Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum", **American University International Law Review**, Vol. 31, Issue: 4, Article 2, 2016, (545-591), s. 553.
[59]Marco Roscini, **Cyber Operations and the Use of Force in International Law**, New York, Oxford University Press, 2014, s. 24.
[60]Gary P. Corn / Robert Taylor, "Sovereignty in the Age of Cyber", **AJIL Unbound**, Vol. 111, 2017, (207-212), s. 208.

altyapısına karşı gerçekleştirilen ve kuvvet kullanımı yahut içişlerine karışma teşkil etmeyen siber operasyonlara ilişkin mutlak bir kısıtlama oluşturmamaktadır[61].

2.1.2. Saldırgan Siber Operasyonların İçişlerine Karışma Yasağını Kapsamında İncelenmesi

İçişlerine karışma[62] bir devlet tarafından mevcut durumu sürdürmek yahut mevcut durumu değiştirmek amacıyla başka bir devletin meselelerine amirane bir şekilde müdahale edilmesi olarak tanımlanabilir[63]. İçişlerine karışma kavramı devletlerin hem dâhili hem harici ilişkilerine müdahaleyi kapsamakta olup, birtakım istisnalara sahip olmakla birlikte, devletlerin uluslararası kişiliklerinin korunması kapsamında yasaklanmıştır[64]. İçişlerine karışma politik, ekonomik, sosyal ve kültürel sistem ile dış politikanın yönetilmesi gibi egemenlik ilkesi kapsamında özgürce karar verilebilen hususlarda, bir devletin başka bir devletin haksız baskısı sonucu bir şey yapma ya da yapmamaya zorlanıyor olması sebebiyle salt egemenliğin ihlalinden; silahlı kuvvete başvurmadan da gerçekleştirilebiliyor olması ile de kuvvet kullanma yasağından ayrılmaktadır[65].

İçişlerine karışma yasağı devletin harici bağımsızlığı ile bölgesel ve şahsi egemenlik ilkelerinin korunması anlayışı üzerine temellendirilmiştir[66]. 1928 tarihli Palmas Adası Davası Hakemlik Kararı'nda devletlerarası ilişkilerde egemenliğin bağımsızlık anlamına geldiğinden bahisle, küresel açıdan bağımsızlığın "*devlet işlevinin başka bir devletten gayrı olarak yerine getirilmesi hakkı*"[67] olarak

---

[61]Jeremy Wright, Cyber and International Law in the 21st Century, 23 Mayıs 2018, *https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century*, erişim tarihi: 17.07.2020; Corn / Taylor, **a.g.e**, s. 209.

[62]Bu noktada içişlerine karışma (*intervention*) ve müdahale (*interference*) kavramlarının farkına da değinmek gerekmektedir. Her ne kadar devletler tarafından içişlerine karışma yerine müdahale kavramı kullanılabiliyor olsa dahi Birleşmiş Milletler ve Uluslararası Adalet Divanı tarafından daha ziyade içişlerine karışma kavramı tercih edilmekte olup içişlerine karışma bir devletin başka bir devletin egemenlik yetkilerine müdahale niteliğindeki zorlayıcı hareketlerle sınırlı olması sebebiyle terim olarak müdahale kavramına kıyasla daha dar bir kapsama sahiptir. (NATO CCD COE, **Tallinn Manual 2.0**, s. 313)

[63]Oppenheim, **International Law a Treatise, Vol. I. – Peace**, s. 305.

[64]**Ibid**.

[65]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 63.

[66]Oppenheim, **International Law a Treatise, Vol. I. – Peace**, s. 305.

[67]*Island of Palmas Case (or Miangas*), United States v Netherlands, Award, (1928) II RIAA 829, ICGJ 392 (PCA 1928), 4th April 1928, Permanent Court of Arbitration [PCA], s. 838

tanımlandığı değerlendirildiğinde her iki ilkenin de birbiriyle yakından ilişkili olduğu tespit edilebilecektir. Nitekim uluslararası hukukun yerleşik bir prensibi haline gelen içişlerine karışma yasağına 1933 tarihli Devletlerin Hakları ve Yükümlülüklerine İlişkin Montevideo Sözleşmesi başta olmak üzere birçok uluslararası sözleşmede atıfta bulunulmuştur[68].

Her ne kadar Birleşmiş Milletler Şartı içişlerine karışma yasağına ilişkin açık bir hüküm içermese dahi BM Şartı'nın 2(1) numaralı maddesinde Birleşmiş Milletler'in tüm üyelerin egemen eşitliği ilkesi üzerine kurulduğu ifade edilmiştir. Keza Birleşmiş Milletler Genel Kurulu nezdinde hazırlanan 1965 tarihli Devletlerin İç İlişkilerine Müdahalenin Kabul Edilemezliği ile Devletlerin Bağımsızlıkları ve Egemenliklerinin Korunması Bildirisi[69], 1970 tarihli Birleşmiş Milletler Şartı'na Uygun Olarak Devletler Arasında İşbirliğine ve Dostça İlişkilere İlişkin Uluslararası Hukuk İlkeleri Bildirisi[70], 1976 tarihli Devletlerin İçişlerine Müdahale Etmeme Bildirisi[71], 1981 tarihli Devletlerin İçişlerine Karışma ve İç İlişkilerine Müdahale Etmenin Kabul Edilemezliği Bildirisi[72] bu alanda Birleşmiş Milletler Şartı'nın

[68]Montevideo Convention on Rights and Duties of States, opened for signature 26 December 1933, 165 LNTS 19 (entered into force 26 December 1934); Montevideo Sözleşmesi'nin 8. maddesi "*Hiçbir devlet başka bir devletin dahili veya harici ilişkilerine müdahale etme hakkına sahip değildir*" düzenlemesini haizdir.

[69]UN General Assembly, **Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty**, 21 December 1965, A/RES/2131(XX); ilgili bildirinin 1. maddesi "*Hiçbir devlet, doğrudan yahut dolaylı olarak, hiçbir gerekçeye dayanarak başka bir Devletin dahili veya harici ilişkilerine müdahil olma hakkına sahip değildir. Dolayısıyla, silahlı müdahale ve bütün diğer biçimdeki müdahaleler yahut Devletin kişiliğine veya Devletin politik, ekonomik, kültürel unsurlarına karşı gerçekleştirilen tehdit teşebbüsleri kınanmaktadır.*" şeklindedir.

[70]UN General Assembly, **Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations**, 24 October 1970, A/RES/2625(XXV); ilgili bildiri "*Hiçbir Devlet, Diğer bir Devletin egemen haklarını kendisine bağımlı şekilde kullanmasına ve ondan diğer herhangi bir menfaat sağlamayı temin etmek amacıyla, onu zorlayacak ekonomik, siyasi veya diğer herhangi bir tipteki tedbirleri kullanamaz veya kullanılmasını teşvik edemez.*" kabulünü içermektedir.

[71]UN General Assembly, **Non-interference in the internal affairs of States**, 14 December 1976, A/RES/31/91;ilgili bildirinin 4. maddesi de benzer şekilde "Diğer devletlerin politik, sosyal veya ekonomik düzenini bozmayı veya ekonomilerini dış kontrol veya manipülasyondan kurtarmak isteyen hükümetleri istikrarsızlaştırmayı amaçlayan her türlü açık, zımni ve oldukça çok yönlü baskı, yıkım ve iftira teknikleri kınanmaktadır" açıklamasına yer vermiştir.

[72]UN General Assembly, **Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States**, 9 December 1981, A/RES/36/103; bildirinin ilk maddesiyle bir devlet veya devlet gruplarının başka bir devletin iç veya dış meselelerine her türlü müdahalesi yasaklanırken ikinci madde ile bu kapsamda korunan haklara ve devletlere düşen görevlere yer verilmiş; bu kapsamda 2 (j) maddesi uyarınca içişlerine karışma yasağı "*Devletlerin ve insanlarının (...) müdahale olmaksızın kendi*

kabulünden sonra gerçekleştirilen çalışmalara örnek gösterilebilir. Nitekim Uluslararası Adalet Divanı; 1986 tarihli Nikaragua'ya Karşı Gerçekleştirilen Askeri ve Paramiliter Faaliyetlere İlişkin Dava'da, Birleşmiş Milletler Şartı'nın uluslararası hukukun yürürlükteki bütün ilkelerini kapsama amacıyla oluşturulmadığından bahisle ve uluslararası teamül hukukunda içişlerine karışma yasağına ilişkin *opinion juris*in varlığına ilişkin kolayca erişilebilecek çok sayıda beyanın mevcut olduğuna atıfta bulunarak, içişlerine karışmama ilkesinin uluslararası teamül hukukunun bir parçası olduğu tespitinde bulunmuştur[73].

İçişlerine karışma yasağı kural olarak sadece devletler tarafından ihlal edilebilmektedir. Lakin özel kişiler yahut gruplarca gerçekleştirilen müdahaleler de devlete atfedilebilir olduğu takdirde yasağın ihlali anlamına gelebilecektir[74]. İçişlerine karışma yasağı devletlerin kendi çıkarları amacıyla gerçekleştirdikleri faaliyetlerin sınırlanmasına yönelik olarak öngörüldüğünden, devletlerarası örgütler tarafından yahut devletlerarası örgütler adına gerçekleştirilen müdahalelerin yasak kapsamında değerlendirilip değerlendirilemeyeceği tartışma konusu olmuştur[75]. Birleşmiş Milletler Şartı'nın 2(7) numaralı maddesi uyarınca, VII. Bölüm'de öngörülen zorlayıcı önlemlerin uygulanması haricinde, Birleşmiş Milletler herhangi bir devletin kendi iç yetki alanına giren konulara müdahale yetkisini haiz değildir. Kanımızca Birleşmiş Milletler Şartı'nda dahi açık hükümle devletlerin içişlerine karışma yasağı öngörülmüşken devletlerarası örgütlerce yahut devletlerarası örgütler adına gerçekleştirilecek müdahalelerin içişlerine karışma yasağı kapsamı dışında tutulması uluslararası hukuka uyarlık göstermeyecektir[76]. Keza aksi yönde bir yaklaşım, devletlerce içişlerine karışma yasağı kapsamında olan faaliyetlerin devletlerarası

"bir devletin, başkalarının içişlerine müdahale etmek veya müdahale etmek amacıyla herhangi bir karalayıcı kampanya, iftira veya düşmanca propagandadan kaçınma görevi"ni de kapsayacak şekilde geniş yorumlanmıştır.

[73]*Case Concerning Military and Paramilitary Activities In and Against Nicaragua* (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986, para. 202.

[74]Delerue François, **Cyber Operations and International Law**, s. 235.

[75]Oppenheim, **International Law a Treatise, Vol. I. – Peace**, s. 320.

[76]NATO CCD COE, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations** s. 325; Jamnejad / Wood, **a.g.m**, s. 377.

örgütler aracılığıyla gerçekleştirilerek yasağın korumuş olduğu ilkelere zarar verilmesi riskini de beraberinde getirecektir.

İçişlerine karışma yasağının iki esaslı unsuru bulunmakta olup bunlardan ilki bir devletin dâhili yahut harici meselelerine yönelik bir müdahalenin bulunmasıdır[77]. Bu yüzden, herhangi bir faaliyetin içişlerine karışma yasağı teşkil edip etmediğinin değerlendirilebilmesi için meselenin devletin içişlerine dair olup olmadığı hususunun ne şekilde tespit edilebileceği belirlenmelidir. Genel olarak bir uluslararası sözleşme, uluslararası teamül hukuku yahut diğer uluslararası hukuk kurallarınca düzenlenmemiş (*domaine réservé*) tabir edilen ulusal yetki kapsamındaki meselelerin devletin içişlerine ilişkin olduğu söylenebilmektedir[78]. Ulusal yetki kavramının kapsamı zaman içinde evrimleşmeye müsait olup bir devletin egemenliğinin esaslı unsurlarından olan politik sistemini ve organizasyonunu zayıflatmaya ilişkin bir müdahale içişlerine karışma yasağı kapsamında değerlendirilebilecek faaliyetlere örnek gösterilebilir[79].

Bir müdahalenin içişlerine karışma yasağı kapsamında değerlendirilebilmesinin ikinci şartı ise zorlayıcı (*coercive*) olması olup bu husus Uluslararası Adalet Divanı tarafından içişlerine karışma yasağının özü olarak nitelendirilmiştir[80]. Nitekim sözlü ve yazılı eleştiri, sivil toplum kuruluşlarının fonlanması, hatta ekonomik yaptırım gibi diplomatik araçlar zorlayıcı nitelik taşımadığından yasak kapsamında olmayıp bu tip temaslara devletlerce dış ilişkilerin yürütülmesi esnasında sıklıkla başvurulmaktadır[81]. Öte yandan bir devletin uluslararası hukuk kapsamında yapma yetkisini taşıdığı herhangi bir şeyi yapmaması yahut yapmama hakkını haiz olduğu herhangi bir şeyi yapmaktan çekinmesini sağlamak amacıyla başka bir devletin iradesini etkilemeye yönelik herhangi bir

[77]NATO CCD COE, **Tallinn Manual 2.0**, s. 314.
[78]Brownlie, **Principles of Public International Law**, s. 291-92*; Advisory Opinion No. 4, Nationality Decrees Issued in Tunis and Morocco*, 4, Permanent Court of International Justice, 7 February 1923, s. 24.
[79]NATO CCD COE, **Tallinn Manual 2.0**, ss. 314-15.
[80]*Case Concerning Military and Paramilitary Activities In and Against Nicaragua* (Nicaragua v. United States of America), para. 205.
[81]Steve R. Ratner, **The Thin Justice of International Law: A Moral Reckoning of the Law of Nations**, New York, Oxford University Press, 2015, s. 127.

meşruiyet zeminine sahip olmayan her türlü zorlayıcı müdahale içişlerine karışma yasağı kapsamında değerlendirilebilir[82]. Bu kapsamda müdahil olunan devletin kendi rızasıyla uyum göstermesi yahut müdahalenin makul bir şekilde direnilebilecek seviyede olması halinde, devletin egemen iradesi değiştirilmediğinden, müdahalenin zorlayıcı olmadığı ve içişlerine karışma yasağını ihlal etmediği söylenebilecektir[83]. Uluslararası Adalet Divanı tarafından Kongo'daki Silahlı Faaliyetler Kararı'nda açıklandığı üzere, bir müdahalenin içişlerine karışma yasağı olarak kabul edilmesi müdahalede bulunan devletin niyetine bağlı olmayıp gerçekleştirilen müdahalenin niteliğine göre değerlendirilmelidir[84].

Uluslararası Adalet Divanı Korfu Boğazı Davası'nda ise içişlerine karışmaya ilişkin hak iddialarını güç politikasının bir tezahürü olarak nitelendirerek, böyle bir hakkın geçmişte ciddi ihlallere yol açtığına atıfla, güçlü devletler tarafından uluslararası adaletin yanıltılması amacıyla kullanılması tehlikesine işaret etmiştir[85]. Buna karşılık, içişlerine karışma yasağı mutlak olmayıp farklı nedenlerle meşrulaştırılabileceği gibi böyle bir meşruiyetin varlığı halinde içişlerine karışma teşkil eden eylemler uluslararası hukuka aykırılık teşkil etmeyecektir. Bu kapsamda, Birleşmiş Milletler Güvenlik Konseyi tarafından Birleşmiş Milletler Şartı'nın 7. Bölümü uyarınca, devlet veya devletlerin müdahale için yetkilendirildiği takdirde gerçekleştirilen eylemler; içişlerine karışma yasağı kapsamındaki müdahalenin karşı önlem olarak uygulandığı haller veya müdahaleye maruz kalan devletin müdahaleye rıza gösterdiği durumlarda, bu rıza doğrultusunda uygulanan eylemler uluslararası hukuk bakımından ihlal teşkil etmeyebilecektir[86].

---

[82]Terry D. Gill, "Non-Intervention in the Cyber Context", **Peacetime Regime for State Activities in Cyberspace**, Ed: Katharina Ziolkowski, Tallinn, NATO CCD COE Publications, 2013, (217-238), s. 222.

[83]Jamnejad Maziar / Wood Michael, **a.g.e**, s. 348.

[84]*Case Concering Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*; Request for the Indication of Provisional Measures, International Court of Justice (ICJ), 1 July 2000, para 163.

[85]*Corfu Channel Case (United Kingdom v. Albania)*; Merits, International Court of Justice (ICJ), 9 April 1949, s. 35.

[86]Jamnejad / Wood, **a.g.m**, s. 377

Sonuç olarak, bir devletin politik, ekonomik, sosyal ve kültürel sistem ile dış politikanın yönetilmesi gibi özgürce karar verebildiği hususlarda, herhangi bir şekilde başka bir devlet tarafından bir şeyi yapmaya ya da yapmamaya zorlanması hali içişlerine karışma yasağı kapsamında değerlendirileceğinden, bu yönde bir müdahale niteliği taşıyan siber operasyonların da içişlerine karışma yasağının ihlalini teşkil ettiği çıkarımı yapılabilmektedir[87]. Nitekim içişlerine karışma yasağının zorlayıcılık unsuru belirli yöntemlerle sınırlanmadığından böyle bir müdahalenin bir siber operasyonlar aracılığıyla gerçekleştirilmesi de olasıdır[88]. Dolayısıyla ilerleyen bölümlerde inceleneceği üzere, kuvvet kullanma, kuvvet kullanma tehdidinde bulunma yahut silahlı saldırı teşkil etmeyen siber operasyonlar, içişlerine karışma yasağı kapsamında uluslararası hukuka aykırılık teşkil edebilecektir.

2.2. Siber Kuvvet Kullanma: Siber Operasyonların Birleşmiş Milletler Şartı 2(4) Numaralı Madde Uyarınca Kuvvet Kullanma veya Kuvvet Kullanma Tehdidinde Bulunma Yasağı Kapsamında Değerlendirilmesi

Birleşmiş Milletler Şartı 2(4) numaralı maddesi ile üye devletlerin 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 kullanımına başvurması*" yasaklanmıştır[89]. Uluslararası Adalet Divanı tarafından kuvvet kullanma veya kuvvet kullanma tehdidinde bulunma yasağının uluslararası teamül hukukunun bir yansıması olduğuna kanaat getirilmiş; hatta Uluslararası Hukuk Komisyonu'nun antlaşmalar hukukunun tedvinine yönelik çalışmalarında söz konusu yasağın *jus cogens* olarak değerlendirildiği yönündeki tespite de atıfta bulunulmuştur[90]. Dolayısıyla kuvvet kullanma yasağı Birleşmiş Milletler üyesi olmayan devletler açısından da bağlayıcılık taşımaktadır[91].

[87]Gill, **Non-Intervention in the Cyber Context**, s. 232.
[88]Ratner, **a.g.e**, s. 128.
[89]United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI
[90]*Nikaragua Davası Kararı*, para 190.
[91]NATO CCD COE, **Tallinn Manual 2.0**, s. 330.

Önceki bölümlerde incelendiği üzere, uluslararası hukuk normları uygun düştüğü ölçüde siber operasyonlara da uygulanabilecektir. Dolayısıyla siber operasyonların da kuvvet kullanma veya kuvvet kullanma tehdidinde bulunma yasağının ihlali teşkil etmesi olasıdır. Çalışmanın bu bölümünde öncelikle kuvvet kullanma ve kuvvet kullanma tehdidi kavramları irdelenerek kapsamları belirlenmeye çalışılacak; akabinde bir siber operasyonun hangi koşullarda ilgili kavramlar çerçevesinde yorumlanabileceği tartışılacaktır.

2.2.1. Kuvvet Kullanma Kavramı

Öncelikle belirtmek gerekir ki kuvvet kullanma yasağının sadece devletlerarası ilişkiler açısından öngörülmüş olması sebebiyle devletlerin kendi bölgelerindeki isyancı hareketlerin bastırılması gibi maksatlarla askeri güce başvurması benzeri hususlar 2(4) numaralı madde kapsamında incelenmemektedir[92]. Ancak yine de kuvvet kullanma yasağının kapsamının tespit edilebilmesi için hangi eylemlerin uluslararası hukuk açısından "kuvvet" teşkil ettiği ve söz konusu eylemlerin hangi koşullar altında bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığına karşı gerçekleştirildiğinin kabul edileceği hususları netleştirilmelidir.

Gelişmekte olan devletler kuvvet kullanma kavramının ekonomik baskıları da kapsadığını iddia etmişse de gelişmiş devletler tarafından kuvvet kullanma ile kastedilenin silahlı kuvvet olduğu görüşü benimsenmiştir[93]. Birleşmiş Milletler Şartı'nın Başlangıç bölümü ile 41 ve 46. maddelerinde silahlı kuvvet ibaresi tercih edilmişken 2(4) numaralı maddede sadece "kuvvet" veya "kuvvet kullanma tehdidi" kavramlarıyla yetinilmiştir[94]. Ancak bu yaklaşım, Birleşmiş Milletler Şartı ile savaş kelimesinin yerine askeri hareketleri kapsayan daha geniş bir kelime olarak kuvvet kavramının tercih edildiği şeklinde açıklanmıştır[95]. Gerçekten de ekonomik hak ve

---

[92]Cassese, **International Law**, s. 56; Dinstein, **War, Aggression and Self Defence**, s. 87.
[93]Christine Gray, "The Use of Force and the International Legal Order", **International Law**, Ed: Evans D. Malcolm, New York, Oxford University Press, 2003, (589-620), s. 592.
[94]Dinstein, **War, Aggression and Self-Defence**, s. 88.
[95]Thomas M. Franck, **Recourse to Force: State Action Against Threats and Armed Attacks**, Cambridge, Cambridge University Press, 2002, s. 20; Oscar Schachter, **International Law in Theory and Practice**, Hollanda, Developments in International Law, vol. 13, Martinus Nijhoff Publishers, 1991, s. 110.

yükümlülüklere ilişkin uluslararası antlaşmalarda dahi ekonomik baskı unsuru değerlendirilirken Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesi uyarınca bir değerlendirme yapılmamış; mesele daha ziyade egemenlik hakları çerçevesinde ele alınmıştır[96]. Günümüzde de baskın olan görüş kuvvet kullanma yasağı ile kastedilenin doğrudan yahut dolaylı olarak askeri amaçlı kuvvet kullanımı olduğu, dolayısıyla ekonomik baskıların kuvvet kullanma yasağı kapsamında değerlendirilemeyeceği yönündedir[97]. Nitekim kuvvet kullanma kavramı, kinetik yahut elektronik, şiddet eylemleri açısından öngörülmüş olup psikolojik veya ekonomik baskıların bu kapsamda yasaklanması kuvvet kullanma yasağının amacıyla bağdaşmamaktadır[98].

2(4) numaralı maddenin kuvvet kullanma veya kuvvet kullanma tehdidinde bulunmayı yasaklarken "*toprak bütünlüğüne ya da siyasal bağımsızlığına karşı"* ve "*Birleşmiş Milletler'in Amaçları ile bağdaşmayacak herhangi bir biçimde"* ifadelerine yer vermesi ise söz konusu yasağın neden ve amaç özelinde bir sınırlama içerip içermediği yönünde tartışmaların doğmasına yol açmıştır. Kuvvet kullanma yasağını dar yorumlayan görüşe göre kuvvet kullanmanın kapsamı, başta meşru müdafaaya ilişkin olanlar olmak üzere, Birleşmiş Milletler Şartı'ndan önce de var olan uluslararası teamül hukuku kuralları çerçevesinde yorumlanmalıyken; geniş yorum taraftarları 2(4) numaralı madde ile uluslararası hukukta devletlerin tek taraflı kuvvet kullanımının tamamen yasaklandığını savunmuştur[99].

Nitekim Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesinde "*uluslararası ilişkilerde*" kuvvet kullanmanın yasaklandığından hareketle, devletlerin kendilerine ait olduğunu iddia ettikleri bölgeleri yeniden ele geçirmek için kuvvet kullanmalarının meşru olduğu birtakım devletler tarafından ileri sürülmüştür[100]. Öte yandan Birleşmiş Milletler Şartı Doğrultusunda Devletler Arasında Dostça İlişkiler ve İşbirliğine İlişkin

---

[96]Schachter, **International Law in Theory and Practice**, s. 110.
[97]James Crawford, **Brownlie's Principles of Public International Law**, Oxford University Press, 2012, s. 747; Tom Ruys, "The Meaning of "Force" and the Boundaries of Jus ad Bellum: Are Minimal Uses of Force Excluded From UN Charter Article 2(4)?", **The American Journal of International Law**, Vol. 108, No. 2, 2014, (159-210), s. 163; Cassese, **a.g.e**, s. 56.
[98]Dinstein, **War, Aggression and Self-Defence**, s. 88.
[99]Gray, **International Law and the Use of Force**, s. 31-33; Shaw, **a.g.e**, s. 1019; Yusuf Aksar, **Teoride ve Uygulamada Uluslararası Hukuk – II**, Ankara, 4. Bası, Seçkin Yayınları, 2017, s. 111.
[100]Gray, **The Use of Force and the International Legal Order**, s. 592.

Uluslararası Hukuk İlkeleri Konusunda Bildirge'nin 1. maddesi kapsamında kuvvet kullanma veya kuvvet kullanma tehdidinden kaçınma yükümlülüğünün, toprak anlaşmazlıkları ve devletlerin sınırları ile ilgili sorunların çözümünde araç olarak kullanılmasını da kapsadığı ifade edildiği dikkate alındığında, bu yaklaşımın uluslararası hukuk nezdinde destek görmediği tespiti yapılabilir[101].

Bir diğer görüş kapsamında ise Birleşmiş Milletler Şartı ile kuvvet kullanma yasağı düzenlenirken "*başka bir devletin toprak bütünlüğüne ya da siyasal bağımsızlığına karşı*" gerçekleştirilen kuvvet kullanma eyleminden kaçınma çağrısında bulunulduğundan, söz konusu yasağın dar yorumlanarak bir devletin toprak bütünlüğü ya da siyasal bağımsızlığının hedef alınmadığı kuvvet kullanma eylemlerinin meşru olduğu yorumunda bulunulmuştur[102]. Örneğin, Amerika Birleşik Devletleri ve İsrail gibi devletler vatandaşlarının kurtarılması amacıyla kuvvet kullandıkları eylemlerde, yasağın dar yorumlandığı görüşe eylemlerinin meşruiyet dayanağı olarak yer vermişlerdir[103].

Keza kimi yazarlarca demokratik düzenin tesisi için kuvvet kullanılması halinde, söz konusu eylemin yasak kapsamında değerlendirilmemesi gerektiği ileri sürülmüştür. Bu kapsamda D'amato, Amerika Birleşik Devletleri'nin Panama'ya karşı kuvvet kullanmasının Panama'nın bölgesel bütünlüğüne tehdit teşkil etmemesi ve Amerika Birleşik Devletleri'nin müdahalesinin sadece demokrasinin tesis edilmesi amacına dayanması sebebiyle, Birleşmiş Milletler Şartı ile korunmaya çalışılan ilkeleri tehdit etmediğini, dolayısıyla da yasak kapsamında değerlendirilemeyeceğini

[101]Nitekim Arjantin Cumhuriyeti'nin 1982 senesinde Falkland Adaları'na söz konusu gerekçe ile gerçekleştirdiği müdahalenin uluslararası hukuka aykırı bulunduğu yönündeki yaygın kanaat bu tespite örnek olarak gösterilebilir. (Henry Etienne, "The Falklands/Malvinas War – 1982", **The Use of Force in International Law: A Case-based Approach**, Ed: Tom Ruys / Olivier Corten, Oxford, Oxford University Press, 2018, (361-379), s. 372-73) Nispeten benzer bir konu olan self-determinasyon hakkı kapsamında kuvvet kullanılması günümüzde çalışma konusu alana uygulanması olası bir tartışmanın mevcut olmaması sebebiyle bu bölümde incelenmeyecektir. Zira devletlerin yaklaşımı da self-determinasyon hakkı kapsamında kuvvet kullanılmasının sömürge dönemleri ile sınırlandığı ve günümüzde self-determinasyona dayanılarak kuvvet kullanılmasının meşru görülmeyeceği yönündedir. (Cassese, **International Law**, s. 63; Gray, **International Law and the Use of Force**, s. 64; Aksar, **a.g.e**, s. 116)

[102]Shaw, **a.g.e**, s. 1021.

[103]Gray, **The Use of Force and International Legal Order**, s.594.

savunmuştur[104]. Her ne kadar Amerika Birleşik Devletleri söz konusu girişimini böyle bir yaklaşımla meşrulaştırmamış; Panama'da yaşayan vatandaşları adına meşru müdafaa hakkını kullandığını savunmuşsa da benzer görüşler takip eden süreçte tekrar gündeme gelmiş; başta Birleşik Krallık olmak üzere birçok devlet 2(4) numaralı maddenin uygulamasının zaman içinde değiştiği ve uluslararası hukukun yeni durumlara çözüm bulması gerektiği nedenleriyle insani müdahale doktrinini ileri sürmüştür[105].

İnsani müdahale doktrinine göre, diplomatik girişimlerin sonuç vermemesi halinde herhangi bir devletin başka bir devletin halkına zulmeden despot bir liderden kurtulması, iç savaşların sona erdirilmesi, soykırımların önlenmesi gibi amaçlarla kuvvet kullanması halinde 2(4) numaralı maddenin ihlalinden söz edilemeyecektir[106]. Zira tamamen insani amaçlarla gerçekleştirilen bir müdahale, başka bir devletin toprak bütünlüğüne yahut siyasal bağımsızlığına halel getirmeyecek; aksine iyileştirici bir etki sağlayacaktır[107]. Kaldı ki bu görüş taraftarlarına göre, böyle bir müdahale insan hakları ve temel özgürlükleri koruma amacına dayandığından, 2(4) madde uyarınca yer verilen "*Birleşmiş Milletler Amaçları'na aykırı*" bir kuvvet kullanma eylemi de teşkil etmeyecek, hatta bu amaçların gerçekleştirilmesine yardımcı olacaktır[108]. İnsani müdahale doktrinine karşı çıkanlar ise temel olarak, Birleşmiş Milletler Şartı ile bir devletin kuvvet kullanmasına silahlı bir saldırıya maruz kaldığı halde müsaade edilmesi sebebiyle, bir hükümetin kendi vatandaşlarının temel insan haklarını ihlal etmesinin dahi bu kapsamda bir silahlı saldırı sayılamayacağı ve dolayısıyla böyle bir müdahalenin de kuvvet kullanma yasağının ihlalini teşkil edeceğini savunmaktadırlar[109]. Gerçekten de Birleşmiş Milletler Şartı'nın hazırlık çalışmaları incelendiğinde "*herhangi bir devletin bağımsızlığına veya toprak bütünlüğüne karşı*" ibaresine kuvvet kullanma yasağını sınırlamak amacıyla değil, aksine küçük devletlere

[104]Anthony D'amato, "The Invasion of Panama was a Lawful Response to Tyranny", **Faculty Working Papers**, Paper 137, 1990, ss. 4-5.
[105]Gray, **The Use of Force and International Legal Order**, s. 595.
[106]Franck, **a.g.e**, ss. 135-36
[107]Sean D. Murphy, **Humanitarian Intervention: The United Nations in an Evolving World Order**, Philadelphia, University of Pennsylvania Press, 1996, s. 71.
[108]Murphy, **a.g.e**, s. 78.
[109]Franck, **a.g.e**, s. 136.

güvence tesis etmek amacıyla yer verildiği sonucuna ulaşılmaktadır[110]. Sonuç olarak, Birleşmiş Milletler Şartı çerçevesinde yer verilen istisnalar haricinde, kuvvet kullanma yasağının mutlak bir niteliği bulunduğu söylenebilecektir[111].

Uluslararası Hukuk Derneği Kuvvet Kullanımı ve Saldırıya İlişkin Final Raporu kapsamındaki değerlendirmelerinde siber operasyonlara da değinmiş; saldırgan siber operasyonların belirli koşullarda kuvvet kullanma eşiğine erişebileceği dikkate alındığında Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesinin ihlaline yol açabileceği tespitinde bulunmuştur[112]. Saldırgan siber operasyonların hangi koşullarda kuvvet kullanma teşkil ettiği hususu ise çalışmanın ilerleyen bölümlerinde öğretide mevcut yaklaşımlar doğrultusunda detaylı olarak değerlendirilecektir.

2.2.2. Kuvvet Kullanma Tehdidi Kavramı

Birleşmiş Milletler Şartı 2(4) numaralı maddesi ile kuvvet kullanma eyleminin yanı sıra kuvvet kullanma tehdidinin de uluslararası hukuka aykırı olduğu belirtilmiştir. Birleşmiş Milletler Şartı'nın kuvvet kullanma tehdidini tanımlamamış olması hangi eylemlerin bu kapsamda yasaklandığı hususunda birtakım tartışmaları da beraberinde getirmiştir[113]. Brownlie kuvvet kullanma tehdidinin "*bir hükümet tarafından başka bir hükümete yöneltilen, belirli taleplerin kabul edilmemesi halinde kuvvet kullanılacağına dair açık veya zımni taahhüt*" olarak tanımlamıştır[114]. Öte yandan Roscini, kuvvet kullanma tehdidinin belirli taleplerin kabul edilmemesi şartına bağlanmasının Birleşmiş Milletler Şartı uyarınca öngörülmemesini de dikkate alarak, "*bir veya birkaç devlete yönelik açıkça veya örtülü olarak yöneltilen, gelecekte*

---

[110]Ian Brownlie / C.J. Apperley, "Kosovo Crisis Inquiry: Memorandum on the International Law Aspects", **International and Comparative Law Quarterly**, Vol. 49, 2000, (878-906), s. 885, para. 36; Crawford, **Brownlie's Principles of Public International Law**, s. 747; Cassese, **International Law**, s. 56.

[111]Lassa F. L. Oppenheim, **International Law a Treatise Vol. II Disputes, War and Neutrality**, Longmans, Seventh Edition, Ed: H. Lauterpacht, 1952, s. 154.

[112]International Law Association Use of Force Committee, Final Report on Aggression and the Use of Force, 2018, s. 25, https://ila.vettoreweb.
com/Storage/Download.aspx?DbStorageId=11391&StorageFileGuid=6a49934
0-074d-4d4b-851b-7a56871175d6, erişim tarihi: 31.07.2020

[113]Nikolas Stürchler, **The Threat of Force in International Law**, New York, Cambridge University Press, 2007, s. 92.

[114]Ian Brownlie, **International Law and the Use of Force by States**, New York, Oxford University Press, 1963, s. 364.

gerçekleşecek hukuka aykırı bir kuvvet kullanma taahhüdü"nün kuvvet kullanma tehdidi olduğunu ifade etmiştir[115]. Gerçekten de her ne kadar uygulamada kuvvet kullanma tehdidinin bazı eylemlerin gerçekleştirilmesi veya gerçekleştirilmemesi yönünde bir baskı aracı olarak kullanılması daha olası olsa da hukuken kuvvet kullanma tehdidine yönelik bir sınırlama olmaması sebebiyle, ikinci yaklaşım meselenin daha isabetli bir şekilde yorumlanmasına olanak tanımaktadır.

Kuvvet kullanma tehdidinin uygulamada karşılaşılan en belirgin örneği, bir devletin başka bir devlete yönelttiği ve herhangi bir hususta kuvvet kullanmaya hazır olduğunu bildiren *ültimatom*lardır[116]. Lakin kuvvet kullanma tehdidine dair biçimsel bir sınırlama öngörülmediğinden, kuvvet kullanma tehdidiyle sözlü veya yazılı bir açıklama şeklinde karşılaşılabileceği gibi bu tip herhangi bir açıklama olmaksızın gerçekleştirilen eylemler de kuvvet kullanma tehdidi olarak yorumlanabilecektir[117]. Örneğin, rutin dışı askeri yığınaklar, manevralar veya bir devlet tarafından başka bir devlete kuvvet kullanılmasına yönelik hazırlığı gösteren diğer eylemler bu kapsamda değerlendirilebilir[118]. Keza her ne kadar kuvvet kullanma ve kuvvet kullanma tehdidinde bulunma farklı kavramlar olsa da özellikle düşük şiddetteki kuvvet kullanma eylemlerinin bazı hallerde aynı zamanda kuvvet kullanma tehdidi de teşkil etmesi mümkündür[119]. Öte yandan bir devletin kuvvet kullanmada başvurulabilecek araçları edinmesi tek başına kuvvet kullanma tehdidi olarak değerlendirilemeyecek olduğundan[120], böylesi bir çıkarım ancak tehdit eden devletin mağdur devlete yönelik baskı oluşturma niyetiyle böyle bir yaklaşım benimsemesi halinde söz konusu olabilecektir[121]. Nitekim devlet uygulaması da silahlanmaya dair yetkilerinin

---

[115]Marco Roscini, "Threats of Armed Force and Contemporary International Law", **Netherlands International Law Review**, 2007, (229-277), s. 235

[116]Stürchler, **a.g.e**, ss. 258-59.

[117]Romana Sadurska, "Threats of Force", **The American Journal of International Law**, Vol. 82, No. 2, 1988, (239-268), ss. 242-43; Stürchler, **a.g.e**, s. 113.

[118]Stürchler, **a.g.e**, s. 113; Devletlerin askeri tatbikatları kural olarak uluslararası hukuka tamamen uygun olup söz konusu ayrımın yapılmasında askeri tatbikatın rutin-dışı gerçekleştirilmesinin yanı sıra gerek gerçekleştirildiği zaman ve bölge gerekse boyutu ile olası bir askeri çatışmaya hazırlık amacıyla uygulandığı mesajını içermesi gibi hasmane bir niyetle gerçekleştirdiğini gösteren hususlar dikkate alınmalıdır. (Stürchler, **a.g.e**, s. 261)

[119]Strüchler, **a.g.e**, s. 262.

[120]*Nükleer Silahlara İlişkin Tavsiye Kararı*, para. 48.

[121]Roscini, **Threats of Armed Force and Contemporary International Law**, s. 240.

uluslararası antlaşmalar uyarınca sınırlanmış bir devletin söz konusu antlaşmaları ihlal edecek boyutta silahlanması halinde dahi bu durum tek başına kuvvet kullanma tehdidi olarak yorumlanmamış; meselenin Birleşmiş Milletler Şartı'nın 7. Bölümü uyarınca barışın tehdit edilmesi açısından değerlendirilmesi tercih edilmiştir[122].

Hangi eylemlerin kuvvet kullanma tehdidi kapsamında yasaklandığı değerlendirilirken nelerin tehdit olarak değerlendirilebileceğinin yanı sıra tehditlerin içeriğinin uluslararası hukuk açısından nasıl değerlendirileceği de büyük önem arz etmektedir. Uluslararası Adalet Divanı'nın Nükleer Silahlara İlişkin Tavsiye Kararı'nda belirtildiği üzere kuvvet kullanma tehdidi ve kuvvet kullanma kavramları birbiri ile ilişkili olduğundan, kuvvet kullanma tehdidinin uluslararası hukuka aykırı olup olmadığı tehdit olarak ileri sürülen kuvvet kullanma eyleminin uluslararası hukuka uygunluğuna bağlı olarak değişecektir[123].

Siber alanda kuvvet kullanma tehdidi incelenirken, bir devletin başka bir devleti saldırgan siber operasyonlara başvurmakla tehdit etmesi yahut kuvvet kullanma teşkil edecek herhangi bir eyleme başvuracağını siber alanda mevcut kanallarla duyurması şeklinde iki farklı ihtimalden söz edilebilecektir[124]. Bir devletin kuvvet kullanma tehdidinde bulunduğunun tespiti için ilgili devletin herhangi bir şekilde uluslararası hukuka aykırı olarak bir devlete karşı kuvvet kullanacağını belirtmesi yeterli olduğundan söz konusu tehdidin siber alanda mevcut kanallar vasıtasıyla yahut farklı bir şekilde duyurulması arasında herhangi bir fark bulunmamaktadır[125]. Ayrıca bir devletin kuvvet kullanma tehdidinde bulunurken genel ifadeler kullanmasının daha olası olması dikkate alındığında, saldırgan siber operasyonların başvurulabilecek diğer kuvvet kullanma yöntemleri arasında sadece bir seçenek olarak kalacağı tespiti yapılabilecektir[126]. Kuvvet kullanma tehditlerinin uluslararası hukuk açısından yarattığı sonuçların kuvvet kullanma kavramının kendisi üzerinden incelenmesi ve tehdidin siber kanallar aracılığıyla gerçekleştirilmesinin

[122]Stürchler, **a.g.e**, ss. 263-65.
[123]*Nükleer Tavsiye Kararı*, para. 47.
[124]NATO CCD COE**, Tallinn Manual 2.0**, s. 338; Roscini, **Cyber Operations and the Use of Force in International Law**, s. 67.
[125]Delerue, **Cyber Operations and International Law**, s. 314
[126]**A.g.e**, s. 318.

ayırt edici bir sonuç yaratmaması sebebiyle çalışmanın buradan sonraki bölümünde kuvvet kullanma tehdidi ayrıca incelenmeyecektir. Zira bir siber operasyon kuvvet kullanma teşkil ettiği takdirde böyle bir siber operasyona ilişkin tehdidin de uluslararası hukuka aykırı olduğu sonucuna ulaşılabilmektedir.

2.2.3. Siber Operasyonların Kuvvet Kullanma veya Kuvvet Kullanma Tehdidi Teşkil Etmesi

Birleşmiş Milletler Şartı'nın hazırlandığı dönemde siber operasyonların öngörülmesinin mümkün olmaması siber operasyonların da kuvvet kullanma teşkil edip etmeyeceği, teşkil ettiği takdirde hangi hallerde siber operasyonların kuvvet kullanma eşiğine eriştiği hususlarının tartışılmasına yol açmıştır[127]. Zira saldırgan siber operasyonlarınn farklı hedeflere yöneltilebilmesi, söz konusu operasyonların yol açtığı olumsuz sonuçların şiddetinin değişiklik gösterebilmesi ve bu sonuçların etki sürelerinin de farklılaşabilmesi konuya ilişkin genel bir değerlendirme yapılmasını zorlaştırmaktadır[128]. Öğretide siber operasyonların kuvvet kullanma teşkil edip etmediği genel olarak siber operasyonların geleneksel silahlarla kıyaslandığı araç odaklı, hedef odaklı ve sonuç odaklı yaklaşımlar üzerinden irdelenmiştir[129]. Çalışmanın bu bölümünde, siber operasyonların kuvvet kullanma teşkil etmesine dair öğretide ileri sürülen görüşler incelenecektir[130].

---

[127]Johann-Christoph Woltag, **Cyber Warfare: Military Cross-Border Computer Network Operations under International Law**, Cambridge University Press, 2014, s. 142.

[128]Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", **Yale Journal of International Law**, vol. 36, 2011, (421-459), s. 422.

[129]Erik M. Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem", **The Air Force Law Review**, Vol. 68, 2012, (167-207) ss. 190-92; Kimi yazarlar hedef odaklı yaklaşımı sonuç odaklı yaklaşımın bir türü olarak değerlendirmiştir. (Woltag, **a.g.e**, s. 144.) Lakin bizim de katıldığımız baskın olan görüş, hedef odaklı yaklaşım ile sonuç odaklı yaklaşımın bir siber operasyonun kuvvet kullanma teşkil etmesi hususunda farklı unsurlara odaklanması sebebiyle ayrı olarak değerlendirmesini tercih etmektedir.

[130]Bu bölümde incelenen yaklaşımların kimi yazarlar tarafından saldırgan bir siber operasyonun silahlı saldırı teşkil edip etmediği değerlendirilmesinde kullanıldığı görülmüştür. Kanaatimizce bu yaklaşım, öğretide mevcut olan meşru müdafaa hakkının doğması için kuvvet kullanma yasağının ihlal edilmesinin yeterli olduğu yönündeki görüş ile silahlı saldırı kavramının kuvvet kullanma kavramından daha yüksek eşiğe haiz bir eylem olduğu şeklindeki ayrımdan kaynaklanmakta olup, her silahlı saldırının aynı zamanda kuvvet kullanma teşkil edeceği gerçeğinden hareketle, bu bölümde yaklaşımların kuvvet kullanma yasağı çerçevesinde değerlendirilmesi daha uygun görülmüştür.

2.2.3.1. Araç Odaklı Yaklaşım

Araç odaklı yaklaşımı savunanlar, bir eylemin kuvvet kullanma teşkil edip etmediği değerlendirilirken kullanılan araçların esas alındığı fikrinden hareketle, geleneksel askeri silahlarla ilişkilendirilebildiği takdirde siber operasyonların kuvvet kullanma yasağını ihlal edebileceği kanaatindedirler[131]. Bu kapsamda siber operasyonlar değerlendirilirken, bu operasyonlar aracılığıyla elde edilen sonuçlara ancak kinetik saldırılar ile erişilebileceği hallerde saldırgan bir siber operasyonun kuvvet kullanma eşiğine eriştiğinin kabul edilmesi gerektiği ileri sürülmektedir[132]. Graham bu yaklaşımı örneklendirirken, siber operasyonların günümüzdeki yetkinliklere ulaşmasından evvel bir enerji nakil şebekesinin devre dışı bırakılmasının ancak santralin bombalanması ya da diğer bir kinetik kuvvet kullanımı halinde erişilebilmesi sebebiyle, aynı eylemin bir siber operasyon aracılığıyla gerçekleştirilmesi halinde söz konusu siber operasyonun kuvvet kullanma eşiğine erişeceğini savunmuştur[133].

Birleşmiş Milletler Şartı'nın 41. maddesinde "*telgraf, radyo ve diğer iletişim ve ulaştırma araçlarının tümüyle ya da bir bölümüyle kesintiye uğratılması*" yönündeki önlemlere silahlı kuvvet kullanımı içermeyen müdahaleleri örneklendirirken yer verildiği değerlendirildiğinde, araç odaklı yaklaşımın benimsenmesi halinde siber operasyonların hiçbir koşulda askeri kuvvet kullanma teşkil etmeyeceği yorumunda bulunulabilecektir[134]. Nitekim araç odaklı yaklaşım, Birleşmiş Milletler Şartı'nın metinsel yorumuna dayanmakta olduğundan, kuvvet kullanma teşkil edecek eylemleri 1945 senesinde mevcut araçlarla sınırlayarak günümüzdeki siber alanda gerçekleştirilen eylemlerin önemini göz ardı eden dar ve tutucu bir değerlendirme olması sebebiyle eleştirilmiştir[135]. Keza Tallinn El Kitabı'nda

---

[131]Woltag, **a.g.e**, s. 142.
[132]David E. Graham, "Cyber Threats and the Law of War", **Journal of National Security Law & Policy**, Vol. 4, 2010, (87-102), s. 91.
[133]**Ibid**.
[134]Duncan B. Hollis, "Why States Need an International Law for Information Operations", **Lewis & Clark Law Review**, Vol. 11, 2007, (1023-1061), s. 1041; Sean P. Kanuck, "Information Warfare: New Challenges for Public International Law", **Harvard International Law Journal**, Vol. 37, 1996, (272-292), s. 289; Roscini, **Cyber Operations and the Use of Force in International Law**, s. 47.
[135]Nguyen, **a.g.m**, ss. 1117-19.

da bir eylemin geleneksel silahlar yerine bilgisayar sistemleri aracılığıyla gerçekleştirilmesinin söz konusu eylemin kuvvet kullanma eşiğine erişip erişmediği değerlendirmesinde herhangi bir kıstas teşkil etmeyeceği görüşü savunulmuştur[136]. Gerçekten de bu yaklaşım, kuvvet kullanma teşkil eden silahlı zorlama eylemleriyle kuvvet kullanma yasağı kapsamına girmeyen ekonomik veya politik baskı araçları arasındaki ayrımın yapılmasına olanak sağlasa da saldırgan siber operasyonların, fiziki bir yapıya sahip olmaması sebebiyle, askeri "araç" olarak değerlendirilerek kuvvet kullanma eşiğine eriştiği tespitinde bulunma imkanını oldukça sınırlamaktadır[137].

Öte yandan kanımızca araç odaklı yaklaşım değerlendirilirken kinetik saldırılarda kullanılan geleneksel silahların siber operasyonlarda kullanılmaması sebebiyle herhangi bir siber operasyonun bu yaklaşım çerçevesinde kuvvet kullanma teşkil etmeyeceği yorumunda bulunmak söz konusu yaklaşım ile hedeflenen amaç ile bağdaşmamaktadır. Burada öngörülen, siber operasyonların da tıpkı geleneksel kuvvet kullanma yöntemlerinde yapıldığı gibi kullanılan araçlar özelinde değerlendirilerek çeşitli ayrımların sağlanmasıdır. Lakin böyle bir ayrımın hangi hususlar çerçevesinde gerçekleştirileceği de bu yaklaşım açısından ayrı bir soru işareti teşkil etmektedir. Zira araç odaklı yaklaşım siber operasyonlarda kullanılan hangi araçların kuvvet kullanma teşkil edeceğine dair genel bir sınıflandırma sağlamaktan da uzaktır. Nitekim saldırgan siber operasyonlar birçok farklı araç aracılığıyla gerçekleştirilebileceği gibi bu alanda başvurulan yöntemlerin büyük bir kısmının gizlilik içerisinde yürütülmesi ve siber operasyonlarda değerlendirilebilecek araçların gelişen teknolojiyle birlikte daha da

---

[136]NATO CCD COE, **Tallinn Manual 2.0**, s. 328.

[137]Stephenie G. Handler, "New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare", **Stanford Journal of International Law**, vol. 48, no. 1, 2012, (209-238), ss. 226-27; Roscini, **Cyber Operations and the Use of Force in International Law**, s. 47; hatta Waxman silahlı saldırı kavramının dar yorumlanması halinde kinetik şiddetle özdeşleştirilebileceği ve dolayısıyla fiziki bir hasara yol açmaması sebebiyle siber operasyonların da ekonomik ve diplomatik yaptırımlar gibi değerlendirilebileceği, bu sebeple araç odaklı bir yaklaşımla yorumlandığı takdirde saldırgan siber operasyonların meşru müdafaa hakkına dayanak oluşturamayacağını ifade etmiştir. (Matthew C. Waxman, "Self Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions*"*, **International Law Studies**, Vol. 89, 2013, (109-122), s. 111) Saldırgan siber operasyonların meşru müdafaa hakkını tetiklemesi hususu ilerleyen bölümlerde incelenecektir. Ancak Waxman'ın tespitlerinin mefhum-u muhalifinden de anlaşılacağı üzere, saldırgan siber operasyonların fiziki zarara yol açma ihtimali göz önüne alındığında, birtakım siber operasyonların araç odaklı yaklaşımda dahi kuvvet kullanma olarak değerlendirme ihtimalinin mevcut olduğu kanaatindeyiz.

çeşitlenme ihtimali, söz konusu araçlar arasında hangi ilkeler çerçevesinde bir ayrım yapılabileceği hususunun da netleştirilmesini gerekmektedir.

Örneğin, Nguyen saldırgan siber operasyonları nüfuz etme saldırıları[138] (*penetration attacks*), ve hizmeti engelleme saldırıları[139] (*denial of service – "DoS" attacks)* olmak üzere iki farklı kategori altında incelemiştir[140]. Başka yazarlar tarafından ise kötücül yazılımların yayılması (*distribution of malicious software*), uzaktan izinsiz erişim ve DoS saldırıları şeklinde üçlü bir ayrım tercih etmiştir[141]. Bir an için böyle bir sınıflandırma ile her iki yaklaşımda da etkilerinin geçici olması sebebiyle daha az tehlikeli olduğu öngörülen DoS saldırılarının kuvvet kullanma eşiğine erişmediğini, kötücül yazılımların kullanılması veya sisteme izinsiz giriş sağlanmasının ise kuvvet kullanma yasağının ihlali teşkil ettiğini varsayalım. Kimi kötücül yazılımlar sadece sistem yavaşlatma veya veri hırsızlığı gibi mağdur tarafından fark edilmesi güç sonuçlar yaratabilecekken bir devletin kritik ulusal altyapısına yöneltilen uzun süreli *DoS* saldırılarının hedef devlet için çok daha ağır sonuçlara yol açabileceği düşünüldüğünde, böyle bir varsayımın yeterli bir kıstas ortaya koymadığı sonucuna kolaylıkla ulaşılabilecektir. Kaldı ki böyle bir ayrımın kabulü halinde dahi söz konusu yöntemlerin bir siber operasyonda birlikte uygulanması ihtimalinden ötürü tam anlamıyla birbirinden ayrılması mümkün gözükmemektedir[142]. Dolayısıyla Birleşmiş Milletler Genel Kurulu'nun 3814 sayılı ve 1974 tarihli Saldırının Tanımı Kararı'nda yer verildiği üzere bir devletin başka bir devletin ülkesini "bombardıman etmesi" gibi bir örneklendirme siber operasyonlar

---

[138]Nguyen'e göre, nüfuz etme saldırıları bir sistemdeki zayıflıkların kullanılarak sistem kaynaklarına erişilmesine ve böylelikle arzu edilen değişikliklerin gerçekleştirmesine olanak tanıyan saldırıların genel bir türüdür. Dolayısıyla bir sisteme doğrudan erişim sağlayan herhangi bir yöntemin kullanılması yahut *virüs*, *worm* veya *trojan* gibi zararlı kötücül yazılımlarla sisteme zarar verilmesi halinde olası yıkıcı etkisi yüksek bir nüfuz etme saldırısının gerçekleştirildiği tespit edilebilecektir. (Nguyen, **a.g.m**, ss. 1093-94)

[139]DoS saldırıları ise bir bilgisayar sisteminin değiştirilmesine veya sisteme zarar verilmesine imkan tanımayan, ancak *zombi bilgisayar*lar vasıtasıyla sistemi uzunca bir süre erişime kapatabilecek bir siber operasyon yöntemidir. (Jay P. Kesan / Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace", **Harvard Journal of Law & Technology**, Vol. 25, No. 2, 2012, (429-543), ss. 444-45; Nguyen, **a.g.e**, s. 1097)

[140]Nguyen, **a.g.m**, s. 1093.

[141]Kesan ve Hayes'in Nguyen'in nüfuz etme saldırısı olarak adlandırdığı siber operasyonları iki farklı kategoride değerlendirdiği görülmektedir. Kesan / Hayes, **a.g.m**, ss. 442-44.

[142]Kesan / Hayes, **a.g.m**, s. 442.

açısından mümkün gözükmemektedir. Sonuç olarak, araç odaklı yaklaşım benimsenerek saldırgan siber operasyonların geleneksel askeri operasyonlara kıyasla değerlendirilmesi içinde bulunduğumuz çağda etkinlikleri her geçen gün artan siber operasyonların kuvvet kullanma teşkil etmesi ihtimalini oldukça sınırladığı gibi, araç odaklı yaklaşımın kinetik saldırı araçlarıyla kıyas üzerinden şekillendilen bir kıstas yerine siber operasyonlara özgü bir yaklaşımın benimsenmeye çalışılması halinde dahi elverişli bir değerlendirme mekanizması sağlamadığı kanaatindeyiz.

2.2.3.2. Hedef Odaklı Yaklaşım

Araç odaklı yaklaşımın aksine, kusursuz sorumluluk (*strict liability*) olarak da adlandırılan hedef odaklı yaklaşım ile saldırgan bir siber operasyonun kuvvet kullanma eşiğine erişip erişmediği değerlendirilirken söz konusu siber operasyonun hedefi esas alınmakta ve siber operasyonun ulusal kritik altyapıya (*critical national infrastructure*) yönelik olması halinde kuvvet kullanma yasağını ihlal edeceği savunulmaktadır[143]. Dolayısıyla hedef odaklı yaklaşım doğrultusunda siber operasyonların kuvvet kullanma eşiğine erişip erişmediği değerlendirilirken öncelikle ulusal kritik altyapının ne olduğu ve neleri kapsadığı hususu anlaşılmalıdır.

Birleşmiş Milletler Genel Kurulu 23 Aralık 2003 tarihli kararıyla her ülkenin ulusal kritik altyapısını kendisinin belirleyeceğini ifade etmiştir[144]. Dolayısıyla devletler arasında ortak bir ulusal kritik altyapı değerlendirmesinin mevcut olduğu söylenemeyecekse de genel olarak ulusal güvenlikle ilişkilendirilebilen sektörlerin ulusal kritik altyapı çerçevesinde ele alınması yönünde bir yaklaşımın mevcut olduğu söylenebilmektedir[145]. TÜBİTAK tarafından hazırlanan Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı'nda kritik altyapı "*işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına*

---

[143]Sean M. Condron, "Getting it Right: Protecting American Critical Infrastructure in Cyberspace", **Harvard Journal of Law & Technology**, Vol. 20, No. 2, 2007, (403-422), s. 419; Handler, **a.g.e**, ss. 227-28.

[144]UNGA, Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, A/RES/58/199, s. 1.

[145]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 58.

yol açabilecek bilişim veya endüstriyel kontrol sistemlerini barındıran sistemler" olarak tanımlanmıştır[146]. Kritik altyapı sektörleri ise 20 Haziran 2013 tarih ve 2 sayılı Siber Güvenlik Kurulu kararı uyarınca kritik altyapıları barındırmakta olan elektronik haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma ve bankacılık ve finans sektörleri olarak belirlenmiştir[147]. Kıyasen incelenecek olan Amerika Birleşik Devletleri tarafından ise Kritik Altyapıların Korunması Kanunu'nda (*Critical Infrastructures Protection Act of 2001***)** kritik altyapı "*ister fiziki ister sanal olsun, yetersizliği yahut yok edilmesinin ulusal güvenlik, ulusal ekonomik güvenlik, ulusal halk sağlığı veya güvenliği ya da sayılanların herhangi bir birleşimi üzerinde zayıflatıcı etki doğurması sebebiyle hayati öneme sahip sistem ve varlıklar*" olarak tanımlanmıştır[148]. Amerika Birleşik Devletleri bu kapsamda kimya, ticari faaliyetler, iletişim, kritik üretim, barajlar, savunma sanayi üsleri, enerji, gıda ve tarım, devlet tesisleri, sağlık ve halk sağlığı, bilgi teknolojileri, nükleer reaktörler, malzemeler ve atıklar, ulaşım sistemleri ile su ve atık su sektörlerini kritik altyapı kapsamına almıştır[149]. Görüldüğü üzere her iki devletin de kritik altyapılara ilişkin benimsedikleri tanım ve dâhil ettikleri sektörler büyük oranda benzemekte ise de tamamen örtüştükleri söylenememektedir. Keza diğer birçok devletin de kendi kritik altyapı tanımlamalarını oluşturarak belirli sektörleri kritik altyapılarına dâhil ettikleri değerlendirildiğinde, gerek kritik altyapının tanımının gerekse kritik altyapı içerisinde olduğu öngörülen sektörlerin daha da farklılaşmasının olası olduğu öngörülmektedir[150].

---

[146]T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı, s. 6, *https://www.uab.gov.tr/uploads/pages/siber-guvenlik/kritik.pdf*, erişim tarihi: 11.07.2020.

[147]T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016-2019 Ulusal Siber Güvenlik Stratejisi, s. 8, *https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf*, erişim tarihi: 11.07.2020.

[148]Critical Infrastructure Protection Act of 2001, 42 U.S. Code § 5195c(e)

[149]US Department of Homeland Security, Cyber Security Strategy, 15 Mayıs 2018, s. 11, *https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf*, erişim tarihi: 11.07.2020.

[150]Birleşik Krallık (National Cyber Security Strategy 2016-2021, s. 39-40, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf*, erişim tarihi: 14.07.2020), Kanada (Angelo Gendron / Martin Rudner**, Assessing Cyber Threats to Canadian Infrastructure: Report Prepared for the Canadian Security Intelligence Service**, s. 11-12, *https://www.canada.ca/content/dam/csis-scrs/documents/publications/CyberTrheats_AO_Booklet_ENG.pdf*, erişim tarihi: 14.07.2020), Avustralya (**Critical Infrastructure Resilience Strategy: Plan**, 2015, s. 3, *https://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlan.PDF*, erişim tarihi:

Dolayısıyla hedef odaklı yaklaşım, ortak bir kritik altyapı anlayışı olmaması sebebiyle hedef alındığı halde kuvvet kullanma yasağının ihlali teşkil edecek sistemlerin net olarak tespit edilememesi, kritik altyapı olarak nitelendirilen hedeflerin geniş bir kapsama sahip olması ve saldırgan bir siber operasyonun kuvvet kullanma olarak değerlendirilmesinde siber operasyonun şiddetini göz ardı etmesi sebebiyle çok düşük bir kıstas öngördüğü yönünde eleştirilmiştir[151]. Zira hedef odaklı yaklaşım hedeften ne anlaşılması gerektiğine ilişkin net bir açıklama getirme yetisinden yoksun olduğu gibi nispeten önemsiz siber operasyonların kuvvet kullanma olarak değerlendirilmesine de olanak sağlamaktadır[152]. Nitekim Tallinn El Kitabı'nda da kritik altyapıyı hedef alan bazı saldırgan siber operasyonlar kuvvet kullanma eşiğine erişmeyeceği gibi kritik altyapıyı hedef almayan saldırgan siber operasyonların da bazı koşullarda kuvvet kullanma teşkil etmesinin mümkün olduğu savunulmuştur[153].

Elbette hedef odaklı yaklaşımın bu eksikliklerinin giderilmesi amacıyla birtakım ilave sınırlamaların öngörülmesi düşünülebilir. Örneğin Handler, kritik altyapının hedef alınmasının siber operasyonların kuvvet kullanma yasağı teşkil etmesi sonucuna ulaşmak için fazla geniş bir kapsam sağlamasını eleştirerek bunun yerine bir devletin diplomatik, askeri, ekonomik ve bilgisel olarak belirlediği kritik unsurlarının hedef alınması üzerinden bir çözümleme yapılmasını önermiştir[154]. Lakin Handler, tadil edilmiş etki odaklı yaklaşım (*modified effect based approach*) olarak adlandırdığı bu görüşünde, bu takdirde dahi hedef odaklı yaklaşımın fazla kapsayıcı olacağını öngörerek, ayrıca siber operasyonun etkisi ve zamanlamasının da göz önüne alınması gerektiğini belirtmiştir[155].

14.07.2020) ve Almanya (Federal Ministry of Interior, **National Strategy for Critical Infrastructure Protection**, 17 Haziran 2009, s. 7, *https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1*, erişim tarihi: 14.07.2020) bu kapsamda örnek olarak incelenebilir.

[151]Yaroslav Radziwill, **Cyber-Attacks and Exploitable Imperfections of International Law**, Leiden, Brill Nijhoff, 2015, s. 138; Handler, **a.g.m**, s. 228.

[152]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 47.

[153]NATO CCD COE, **Tallinn Manual 2.0**, s. 328.

[154]Handler, **a.g.m**, s. 230-31.

[155]**Ibid**. Handler, söz konusu yaklaşımı tadil edilmiş etki odaklı yaklaşım olarak nitelendirmişse de kendisinin söz konusu yaklaşımı açıklarken temel unsur olarak siber operasyonun hedefi üzerinden hareket etmesi sebebiyle çalışmanın bu kapsamında yer verilmesi tercih edilmiştir.

2.2.3.3. Etki Odaklı Yaklaşım

Sonuç odaklı yaklaşım olarak da isimlendirilen etki odaklı yaklaşım, siber operasyonların kuvvet kullanma eşiğine erişip erişmediği hususunun gerçekleştirilen siber operasyonun yarattığı etkiler üzerinden değerlendirilmesi gerektiği düşüncesi üzerine inşa edilmiştir[156]. Etki odaklı yaklaşım uyarınca, hedef odaklı yaklaşımdan farklı olarak saldırgan bir siber operasyonun kuvvet kullanma eşiğine erişip erişmediği yorumlanırken ulusal kritik altyapının hedef alınması kıstas alınmamış; hedef alınan sistem fark etmeksizin, söz konusu siber operasyon ile yıkıcı bir sonuç yaratılıp yaratılmadığı üzerinden değerlendirme yapılması gerektiği ileri sürülmüştür[157]. Zira uluslararası hukuk açısından, bir eylemin kuvvet kullanma teşkil edip etmediği değerlendirilirken kullanılan araçlardan ziyade bu araçlar vasıtasıyla elde edilen sonuç önemli olacaktır[158]. Buna göre bir devlet bilerek saldırgan bir siber operasyon aracılığıyla başka bir devletin egemenlik sahasında insanların hayatını kaybetmesi yahut yaralanmasına veya maddi varlıkların zarar görmesine yol açtığı takdirde, söz konusu siber operasyon tıpkı geleneksel bir silah gibi kuvvet kullanma yasağının ihlal edecektir[159]. Bu kapsamda örneğin, siber operasyonun bir nükleer santralde yıkıcı etkiye yol açması, bir baraja müdahale edilerek yoğun nüfuslu bir yerleşim yerinde yıkıma sebep olunması yahut hava trafik kontrol sistemine müdahale ederek uçak kazalarına sebebiyet verilmesi gibi hallerde söz konusu siber operasyonun kuvvet kullanma eşiğine eriştiği söylenebilecektir[160].

---

[156]Herpert S. Lin, "Offensive Cyber Operations and Use of Force", **Journal of National Security Law & Policy**, Vol. 4, 2010, (63-86), s. 73; Joyner / Lotrionte, **a.g.e**, s. 855; Woltag, **a.g.e**, ss. 143-44.
[157]Waxman, **Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)**, s. 435-36.
[158]Yoram Dinstein, "Computer Network Attacks and Self-Defense", **Computer Network Attack and International Law**, Ed: Michael N. Schmitt / Brian T. O'Donnell, International Law Studies, Vol. 76, 2002, (99-119), s. 103; Dimitrios Delibasis, "State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century", **Peace, Conflict & Development: An Interdisciplinary Journal**, Issue 8, 2006, s. 7.
[159]Walter G. Sharp, **CyberSpace and the Use of Force**, Aegis Research Corporation, 1999, s. 133; Delerue, **Cyber Operations and International Law**, s. 289; Daniel B. Silver, "Computer Network Attacks as a Use of Force under Article 2(4) of the United Nations Charter", **Computer Network Attack and International Law**, Ed: Michael N. Schmitt / Brian T. O'Donnell, International Law Studies, Vol. 76, 2002, (73-97), s. 92.
[160]Kriangsak Kittichaisaree, **Public International Law of Cyberspace**, Law, İsviçre, Springer International Publishing, 2017, s. 163.

Etki odaklı yaklaşım da araç odaklı yaklaşım gibi siber operasyonların kinetik askeri müdahalelere kıyasla yorumlanmasını esas alırken, kullanılan araçlar yerine sonuçlar aracılığıyla bir değerlendirme sağlaması sebebiyle askeri kuvvet kullanımının teknik evriminin de göz önünde bulundurulmasına olanak sağlamaktadır[161]. Aynı zamanda hedef odaklı yaklaşımın da birtakım hedeflere yöneltilecek siber operasyonların diğerlerine nazaran devletler için daha olumsuz sonuçlar yaratabileceği düşüncesine dayandığı dikkate alındığında her iki yaklaşımın da ilkelerini içinde barındırdığı söylenebilen etki odaklı yaklaşım günümüzde yaygın olarak kabul edilen görüş halini almıştır[162].

Öte yandan siber operasyonların yol açacağı sonuçların birçok ihtimali barındırması etki odaklı yaklaşım uyarınca genel kıstaslar öngörülebilmesinin gerçekçi olmadığı eleştirilerine yol açabilmektedir[163]. Örneğin Schmitt, saldırgan siber operasyonların uluslararası hukuk çerçevesinde tahlil edilirken siber operasyonun şiddeti (*severity*),[164] sonuçlarının yakınlığı (*immediacy*),[165] doğrudanlığı (*directness*),[166] nüfuz edilebilirliği (*invasiveness*),[167] etkilerin ölçülebilirliği (*measurability*)[168] ve varsayılan meşruiyet (*presumptive legitimacy*)[169] şeklinde altı farklı kıstas öngörmüştür[170]. Tallinn El Kitabı yazarlarınca da benzer bir yaklaşım

[161]Irene Couzigou, "The Challenges Posed by Cyber-Attacks to the Law on Self Defence", **International Law and… Select Proceedings of the European Society of International Law**, Ed: Reinisch August ve Diğerleri, Vol. 5, Hart Publishing, 2016, (245-261) s. 250.
[162]Oona A. Hathaway / Rebecca Crootof ve Diğerleri, "The Law of Cyber-Attack", **California Law Review**, Vol. 100, 2012, (817-885), s. 847.
[163]Dinniss, **a.g.e**, s. 63.
[164]En önemli kıstas olarak öngörülmüştür. Siber operasyonun şiddeti değerlendirilirken etki alanı, etki süresi ve etkisinin yoğunluğunun dikkate alınması gerektiğini açıklar. Buna göre bir siber operasyon fiziksel zarar yaratması halinde kuvvet kullanma eşiğine erişecek, böyle bir etki yaratmayan siber operasyonlar ise kuvvet kullanma olarak değerlendirilemeyecektir.
[165]Siber operasyonun olumsuz etkilerinin bir an önce gerçekleşme ihtimali arttıkça söz konusu operasyonun kuvvet kullanma olarak değerlendirilmesinin de daha olası olduğu savunulmaktadır.
[166]Siber operasyon ile söz konusu operasyonun olumsuz etkileri arasındaki illiyet bağı ne kadar güçlü olursa kuvvet kullanma yasağının ihlal edildiği sonucuna ulaşılma ihtimali de o kadar yüksek olacaktır.
[167]Siber operasyonun hedef olan devletin ne daha sıkı korunan bir sistemini hedef alması halinde kuvvet kullanma eşiğine erişmesinin daha olası olacağını ifade etmektedir.
[168]Belirli verilerle izah edilebilen bir siber operasyonun sonuçlarının belirsiz olduğu bir siber operasyona kıyasla kuvvet kullanma olarak değerlendirilmesinin daha kolay olduğu düşünülmektedir.
[169]Uluslararası hukukun temel ilkesi olarak bir eylem açıkça yasaklanmadığı takdirde meşru olduğu görüşü kapsamında elde edilecek sonuçların hukuka uygun olduğu varsayılabilen siber operasyonların kuvvet kullanma teşkil etme ihtimalinin daha düşük olduğuna inanılmaktadır.
[170]Michael N. Schmitt, **Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework**, ss. 914-15.

benimsenmiş; bu kıstaslara ilave olarak askeri karakter (*military character*)[171], devletin dahil olması (*state involvement*)[172] da öngörülmüş ve sayılan kıstasların sınırlayıcı olmadığı belirtilerek hedefin yapısı, genel politik atmosfer, saldırganın kim olduğu ve önceden de saldırgan siber operasyonlar gerçekleştirip gerçekleştirmediği, gelecekte askeri güç kullanma ihtimali gibi unsurların da devletler tarafından hesaba katılmasının mümkün olduğu belirtilmiştir[173]. Ayrıca not düşmek gerekir ki hem Schmitt hem de Tallinn El Kitabı katılımcıları sayılan kıstasların hukuki bir karakteri haiz olmadığını, daha ziyade devletlerin kuvvet kullanmaya ilişkin değerlendirmelerinde göz önüne alacağı tahmin edilen etkenler olduğunu ifade etmişlerdir[174]. Söz konusu kıstaslar kimi yazarlarca çeşitli açılardan eleştirilmiştir[175]. Roscini, Nikaragua Kararı'na atıfla silahlı örgütlerin silahlandırılması ve eğitilmesi gibi doğrudan yıkıcı etki doğurmayan eylemlerin de kuvvet kullanma olarak değerlendirilebildiği dikkate alındığında doğrudanlığın kuvvet kullanmanın esaslı bir unsuru olarak kabul edilemeyeceği ve siber operasyonların genellikle doğrudan bir etki doğurmak yerine belirli verilere müdahale ederek sistemin işlerliğini bozmak şeklinde gerçekleşmesi sebebiyle böylesi bir kıstas uyarınca değerlendirilmesinin uygun olmadığı eleştirilerinde bulunmuştur[176]. Roscini ayrıca, DoS saldırılarının sisteme erişmeksizin tahribat yaratabildiği göz önüne alındığında nüfuz edilebilirlik kıstasının; siber operasyonların etkilerinin ölçülmesinin genel olarak zor olması sebebiyle etkilerin ölçülebilirliği kıstasının; mantık bombası[177] (*logic bomb*) gibi devreye sokulması belirli bir zamana veya eylemin varlığına dayanan siber operasyon

---

[171]Siber operasyon ile askeri operasyonlar arasında sıkı bir ilişki bulunduğu takdirde ilgili siber operasyonun devletler tarafından kuvvet kullanma yasağının ihlali olarak değerlendirilmesi ihtimalinin daha yüksek olduğu düşünülmektedir.

[172]Bir devlet ile siber operasyon arasındaki bağlantının aşikar olduğu hallerde söz konusu siber operasyonun kuvvet kullanma teşkil ettiğinin benimsenmesinin daha olası olduğu belirtilmektedir.

[173]NATO CCD COE, **Tallinn Manual 2.0**, ss. 336-37.

[174]Michael N. Schmitt, "The "Use of Force" in Cyberspace: A Reply to Dr Ziolkowski", **2012 4th International Conference on Cyber Conflict**, Ed: Christian Czosseck / Rain Ottis / Katharina Ziolkowski, Tallinn, NATO CCD COE Publications, 2012, (311-317), s. 314; NATO CCD COE,**Tallinn Manual 2.0**, s. 333.

[175]Dinniss, **a.g.e**, ss. 64-65.

[176]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 48.

[177]Mantık bombası zararsız bir yazılım görünümü ile sisteme girip herhangi bir zarar verici işlemde bulunmadan çalışırken belirli bir zamanda, bir olayla veya kullanıcı tarafından gerçekleştirilen bir işlemle tetikenerek bilgisayar virüsü veya ağ solucanı gibi programları aktif hale getiren bir Truva atı türüdür. (Bayraktar, **a.g.e**, s. 85)

araçlarının mevcudiyeti sebebiyle de sonuçların yakınlığı kıstasının uygulanmasının verimli olmayacağını ifade etmiştir[178]. Keza Woltag, varsayılan meşruiyet ilkesinin bir siber operasyonun hukuki açıdan irdelenmesi sonucu değerlendirilebilecek bir husus olması sebebiyle siber operasyonun kuvvet kullanma teşkil edip etmediği meselesi incelenirken göz önüne alınabilecek bir kıstas olarak öngörülmesinin hatalı olduğu tespitinde bulunmuştur[179]. Nguyen ise öngörülen kıstasların genel olarak bir devlet tarafından kendi politik çıkarları için manipüle edilmesi riskinin yüksek olması sebebiyle amacına hizmet etmediğini ifade etmiştir[180].

Bizim de katıldığımız görüşe göre, etki odaklı yaklaşımın en büyük eksikliği kuvvet kullanma teşkil eden siber operasyonları fiziki zarara indirgeyerek günümüzde siber alan aracılığıyla faydalanılan faaliyetlerin bireylerin yaşamı ve devlet işleyişi üzerindeki etkilerini göz ardı etmesidir[181]. Örneğin bu yaklaşımın benimsenmesi halinde, bir elektrik santralini devre dışı bırakan kinetik bir saldırı aynı zamanda fiziki zarara yol açacağından kuvvet kullanma teşkil edecekken aynı etkinin saldırgan bir siber operasyonla gerçekleştirilmesi halinde eylemin kuvvet kullanma yasağı ihlal etmemesi gibi çelişkili bir sonuç ortaya çıkacaktır[182]. Nitekim günümüzde sosyal hayatın sürdürülmesinin yanı sıra ekonomik düzen ve askeri faaliyetler için de siber alanın elzem hale gelmesi dikkate alınınca, fiziksel bir zarara yol açmayan saldırgan bir siber operasyonun fiziksel zarara yol açan saldırgan bir siber operasyona kıyasla daha yıkıcı sonuçlar doğurmasının olası olduğu çıkarımında bulunulabilmektedir[183]. Dolayısıyla siber operasyonlar değerlendirilirken etki odaklı yaklaşım esas alınmakla birlikte, yukarıda işlenen diğer yaklaşımlar olan hedef odaklı yaklaşım ve araç odaklı yaklaşımın da hesaba katılarak her olayın somut özelliklerine göre bir çıkarım yapmanın en uygun çözüm olduğu kanaatindeyiz[184].

---

[178]Roscini, **Cyber Operations and the Use of Force in International Law**, ss. 48-49.
[179]Woltag, **a.g.e**, s. 151.
[180]Nguyen, **a.g.m**, s. 1124.
[181]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 48.
[182]James E. McGhee, "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy", **Journal of Law & Cyber Warfare**, Vol. 2, No. 1, 2013, (64-103), s. 73.
[183]Waxman, **Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)**, s. 436.
[184]Delerue, **Cyber Operations and International Law**, s. 290.

Sonuç olarak, fiziki zarara yol açan saldırgan siber operasyonlar kuvvet kullanma eşiğine erişebilecekken fiziki zarara yol açmayan siber operasyonların kural olarak kuvvet kullanma teşkil etmeyeceği çıkarımında bulunulabilmektedir. Lakin yukarıda belirtildiği üzere, istisnai hallerde saldırgan siber operasyonların fiziki zarara yol açmadan da kuvvet kullanma yasağını ihlal etmesinin mümkün olduğu ileri sürülmüştür. Bu kapsamda Nguyen, saldırgan bir siber operasyonun siber fiziksel sistemlere (*cyber-physical system* – "CPS")[185] fiziken zarar verilmediği hallerde dahi bu sistemlerin geri döndürülemez bir şekilde bozulmasının silahlı saldırı teşkil edebileceğini ileri sürmüştür[186]. Roscini ise ulusal kritik altyapıda yıkıcı etki yaratan saldırgan siber operasyonların da fiziki zarara yol açmasa dahi kuvvet kullanma seviyesine erişeceğini savunmuştur[187]. Bir devletin ulusal kritik altyapısını oluşturan sistemlerdeki uzun süreli aksaklıkların fiziksel bir zarar yaratmasa dahi siber operasyona maruz kalan bir devlet açısından ağır sonuçlar yaratmaya elverişli olması sebebiyle biz de bu görüşe katılmaktayız. Eklemek gerekir ki saldırgan bir siber operasyonun kuvvet kullanma veya kuvvet kullanma tehdidinde bulunma teşkil etmemesi söz konusu operasyonun uluslararası hukuka uygun olduğu anlamına gelmeyecek; 2(4) numaralı maddenin ihlali teşkil etmese dahi bir antlaşmadan kaynaklanan yükümlülüğe veya içişlerine karışma yasağı gibi uluslararası teamül hukukunun ilkelerine aykırı olması halinde de siber operasyon uluslararası hukuka aykırı kabul edilecektir[188].

---

[185]Siber-fiziksel sistem kısaca siber araçlar vasıtasıyla kontrol edilen ve çeşitli amaçlarla kullanılan fiziksel varlık olarak tanımlanabilecektir. (Networked European Software and Services Initiative, Cyber-Physical Systems: Opportunities and Challenges for Software, Services, Cloud and Data, Nessi White Paper, 2015, s. 4, *http://www.nessi-europe.com/Files/Private/NESSI_CPS_White_Paper_issue_1.pdf*, (erişim tarihi: 01.08.2020)

[186]İlerleyen bölümlerde inceleneceği üzere bir eylemin silahlı saldırı teşkil etmesinin kuvvet kullanma eşiğine erişmesine ilave olarak belirli kıstasları sağlaması gerekse de Nguyen tarafından önerilen yaklaşımın saldırgan siber operasyonların kuvvet kullanma veya kuvvet kullanma tehdidi teşkil etmesi hususunda değerlendirilebileceği kanaatindeyiz. (Nguyen, **a.g.m**, s. 1125.)

[187]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 55.

[188]Michael N. Schmitt, "The Use of Cyber Force and International Law", **The Use of Force in International Law**, Ed: Marc Weller, Oxford University Press, 2015, (1110-1130), s. 1116.

2.3. Siber Saldırı[189]: Siber Operayonların Birleşmiş Milletler Şartı 7. Bölüm ve Kolektif Güvenlik Normları Çerçevesinde Değerlendirilmesi

Kolektif güvenlik kavramı, uluslararası bir sözleşme ile taraf devletlerin olası saldırganlara karşı kuvvet kullanma yetkisini haiz uluslararası bir teşkilat oluşturması şeklinde açıklanabilir[190]. Bu kapsamda kolektif güvenlik, herhangi bir silahlı saldırıya maruz kalmayan devletlere de kuvvet kullanma yetkisi tanınmasına yol açması yönünden kolektif meşru müdafaaya benzemekle birlikte, kolektif meşru müdafaadan farklı olarak saldırganın bir dış aktör olmasından ziyade içlerinden biri olması ihtimaline karşı öngörülmüştür[191]. Birleşmiş Milletler Şartı ile de kolektif güvenlik kurumuna yer verilmiş; 24. madde uyarınca uluslararası barış ve güvenliğin korunmasında başlıca sorumluluk Birleşmiş Milletler Güvenlik Konseyi'ne bırakılmıştır. Keza yine BM Şartı'nın 25. maddesi gereğince Güvenlik Konseyi'nin kararları üye devletler açısından bağlayıcılık taşımaktadır.

Bu çerçevede, saldırgan bir siber operasyona maruz kalan bir devlet, söz konusu siber operasyon silahlı saldırı teşkil etmese dahi, Birleşmiş Milletler'in 35. maddesinden faydalanarak siber operasyonun barış ve güvenliğin korunmasını tehlikeye düşürdüğü iddiasıyla konuyu Güvenlik Konseyi'ne iletebileceği gibi Güvenlik Konseyi de gerek gördüğü takdirde VII numaralı bölümdeki yetkilerini kullanabilecektir[192]. Zira BM Şartı'nın "*Barışın Tehdidi, Bozulması ve Saldırı Durumunda Alınacak Önlemler"* başlıklı VII numaralı bölümünün ilk maddesi olan 39. madde ile Güvenlik Konseyi'nin "*barışın tehdit edildiğini, bozulduğunu ya da bir saldırı eylemi olduğunu*" saptaması halinde "*uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için*" tavsiyelerde bulunması veya 41. ve 42.

---

[189]"Siber saldırı" ile bir saldırı eylemin siber operasyonlar vasıtasıyla gerçekleştirilmesi kastedilmekte olup Birinci Bölüm'de açıklandığı üzere çalışma kapsamında siber saldırı siber operasyona alternatif bir terim olarak kullanılmamaktadır.

[190]Dinstein, **War Aggression and Self Defence**, s. 303.

[191]Volker Rittberger / Bernhard Zangl, **International Organization: Polity, Politics and Policies**, Çev: Antoinette Groom, Palgrave Macmillan, 2006, s. 127.

[192]Birleşmiş Milletler şayet söz konusu durumun barışın tehdidi, bozulması ve saldırı eylemi hali anlamına geldiğine kanaat getirmezse ayrıca BM Şartı'nın 36. maddesi doğrultusunda uyuşmazlığın çözümüne ilişkin tavsiyelerde de bulunabilecektir. (Roscini, **Cyber Operations and the Use of Force in International Law**, s. 110.)

maddelerde öngörülen önlemlere başvurması mümkün kılınmıştır. Keza Güvenlik Konseyi BM Şartı'nın 40. maddesi uyarınca durumun ağırlaşmasını önlemek amacıyla tarafları gerekli gördüğü geçici önlemleri uygulamaya çağırabilmektedir. Birleşmiş Milletler Şartı'nın 51. maddesi gereğince, Güvenlik Konseyi söz konusu yetkilerine silahlı saldırıya maruz kalan devletin hâlihazırda meşru müdafaa hakkını kullanıyor olduğu durumlarda dahi başvurabilecektir.

Çalışmanın bu bölümünde Güvenlik Konseyi'nin 41. madde ile düzenlenen silahlı kuvvet kullanımı içermeyen önlemler alması ve 42. madde ile düzenlenen kuvvet kullanma yetkisinin siber operasyonlar açısından sonuçları incelenecektir. Bu amaçla öncelikle siber operasyonların Güvenlik Konseyi tarafından barışın tehdidi yahut silahlı saldırı olarak değerlendirilme olasılığı tartışılacak; ardından Güvenlik Konseyi'nin siber operasyonlara yönelik olarak 41 veya 42. maddeler kapsamındaki önlemlere başvurma ihtimali değerlendirilecektir.

2.3.1. Siber Operasyonların Barışın Tehdidi, Bozulması veya Saldırı Teşkil Etmesi

Güvenlik Konseyi'nin Birleşmiş Milletler Şartı'nın 27. maddesinde düzenlenen karar alma mekanizmalarına ilişkin genel düzenlemeler dışında söz konusu önlemlere başvurması herhangi bir koşula bağlanmamış; "*Birleşmiş Milletler'in Amaç ve İlkeleri'ne uygun hareket etmek*" kaydıyla Güvenlik Konseyi'nin bu hususta takdir yetkisi olduğu kabul edilmiştir[193].

Birleşmiş Milletler Genel Kurulu'nun 14 Aralık 1974 tarihinde kabul ettiği 3314 sayılı Saldırının Tanımı Karar'ın 1. maddesi ile saldırı "*bir Devletin diğer bir Devletin egemenliğine, ülke bütünlüğüne veya siyasi bağımsızlığına karşı veya işbu Tanımda belirtildiği üzere, Birleşmiş Milletler Şartı ile bağdaşmayan diğer herhangi bir tarzda silahlı kuvvet kullanılması*" olarak tanımlanmış; aynı kararın 3. maddesinde

[193]Terry D. Gill, "Legal and Some Political Limitations on the Power of the UN Security Council to Exervise Its Enforcement Powers under Chapter VII of the Charter", **Netherlands Yearbook of International Law**, Vol. 26, 1995, (33-138), ss. 40-41

ise saldırı olarak kabul edilecek eylemler örneklendirilmiştir[194]. Gerek söz konusu tanımda saldırının "*herhangi bir tarzda silahlı kuvvet kullanılması*" şeklinde bir devletin egemenliğine, ülke bütünlüğüne veya siyasi bağımsızlığına yöneltilen herhangi bir eylemin saldırı olarak değerlendirileceğinin belirtilmesi gerekse önceki bölümde incelendiği üzere belirli koşullarda siber operasyonların kuvvet kullanma teşkil edebileceği göz önüne alındığında siber operasyonların da saldırı kapsamında değerlendirilmesinin mümkün olduğu kanaatindeyiz. Öte yandan Güvenlik Konseyi uygulamada barışın bozulduğunun yahut silahlı saldırının bariz olduğu durumlarda dahi yetkilerini kullanırken hemen hemen her zaman bu kararını "*uluslararası barış ve güvenliğe tehdit"* oluşmasına dayandırmıştır[195].

Birleşmiş Milletler Güvenlik Konseyi daimi üyesi Fransa açıkça, barış ve güvenliğe tehdit teşkil etmesi halinde bir kısım siber operasyonları Birleşmiş Milletler Şartı'nın VII numaralı bölümü uyarınca Güvenlik Konseyi'nde gündeme getirilebileceğini belirtmiştir[196]. Nitekim Estonya'nın Güvenlik Konseyi'ne başkanlık ettiği dönem diğer Güvenlik Konseyi üyeleri Belçika, Dominik Cumhuriyeti, Endonezya ve Kenya ile birlikte 22 Mayıs 2020 tarihinde düzenlediği uluslararası barış ve güvenliğe ilişkin Siber İstikrar, Çatışmaların Önlenmesi ve Kapasite Geliştirme (*Cyber Stability, Conflict Prevention and Capacity Building*) konulu *arria formülü toplantısı*na[197] Rusya Federasyonu hariç[198] bütün Güvenlik Konseyi üyeleri

[194]UN General Assembly, *Definition of Aggression*, 14 December 1974, A/RES/3314; 3314 sayılı Karar'ın 4. maddesinde belirtildiği üzere, 3. madde uyarınca sayılan eylemler tüketici olarak öngörülmemiştir ve dolayısıyla Güvenlik Konseyi'nin Birleşmiş Milletler Şartı hükümlerine göre başka fiillerin de saldırı teşkil ettiği tespitinde bulunma imkanı mevcuttur.

[195]Heathor H. Dinniss, **Cyber Warfare and the Laws of War**, Cambridge University Press, 2012, s. 109.

[196]Republique Française Ministère des Armées, **International Law Applied to Operations in Cyberspace**, 2019, s. 8, *https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf* (erişim tarihi: 03.06.2020)

[197]Arria-formülü toplantıları Birleşmiş Milletler Güvenlik Konseyi üyelerinin görüşlerini paylaştığı resmi olmayan toplantılardır. (United Nations Security Council, Working Methods Handbook: Background Note on the "Arria-Formula" Meetings of the Security Council Members, *https://www.un.org/securitycouncil/content/background-note*, erişim tarihi: 01.07.2020)

[198]Rusya Federasyonu Estonya, Birleşik Krallık ve Amerika Birleşik Devletleri delegasyonlarının son zamanlarda bir konuya ilişkin görüşleri fark etmeksizin bütün Güvenlik Konseyi üyelerinin aria-formülü toplantılarına katıldığı yönündeki yerleşik uygulamayı zedelemesi sebebiyle toplantıya katılmadığını bildirirek konuya ilişkin ayrı bir bildiri yayımlamış; her ne kadar çeşitli hususlarda farklı görüşlerini dile getirmişse de özetle, siber barışın gerçekçi bir hedef olduğunu ancak bu hedefe sadece Birleşmiş Milletler düzeyinde sağlanabilecek bir uzlaşı ile erişilebileceğini ifade etmiştir. (Permanent

katılmıştır[199]. Keza söz konusu toplantıya Güvenlik Konseyi üyesi olmayan 40 Birleşmiş Milletler üyesi devlet de katılmış; içlerinden Avustralya[200] Birleşmiş Milletler Şartı uyarınca Güvenlik Konseyi'nin uluslararası barış ve güvenliğin sağlanmasına ilişkin sorumluluğunu hatırlatmış, Japonya[201] ise Güvenlik Konseyi'nin siber aktivitelere ilişkin gerektiği takdirde Birleşmiş Milletler Şartı'nın 6 ve 7. bölümlerinde öngörülen yetkileri kullanmaya hazır olması gerektiği yönünde görüş bildirmiştir[202].

Saldırgan siber operasyonlar ilk kez 5 Mart 2020 tarihinde Estonya tarafından Güvenlik Konseyi'nde tartışmaya açılmış; Estonya Dışişleri Bakanı Urnas Reinsalu 2019 senesinin ekim ayında Gürcistan'a yönelik düzenlenen siber operasyonların Rusya Federasyonu askeri istihbarat birimi GRU tarafından gerçekleştirdiğini iddia ederek, "*Güvenlik Konseyi uluslararası barış ve güvenliği tehdit eden yeni meseleleri ele almalı*" temennisinde bulunmuştur[203]. Söz konusu toplantının akabinde Estonya'nın Birleşmiş Milletler Daimi temsilcisi Sven Jürgenson tarafından okunan

---

Mission of the Russian Federation to the United Nations, Statement by the Permanent Mission of Russia to the UN on its Non-participation in the UN Security Council Arria-Formula Meeting on Cyber Stability, Conflict Prevention and Capacity Building, Organized by Estonia on 22 May, 22 Mayıs 2020, *https://russiaun.ru/en/news/arria_220520*, erişim tarihi: 01.07.2020)

[199]Republic of Estonia Ministry of Foreign Affairs, Signature Event of Estonia's UNSC Presidency: Cyber Stability, Conflict Prevention and Capacity Building, *https://vm.ee/en/activities-objectives/estonia-united-nations/signature-event-estonias-unsc-presidency-cyber*, erişim tarihi: 01.07.2020.

[200]Australian Mission to the United Nations, Statement by H.E. Dr. Tobias Feakin Ambassasor for Cyber Affairs, s. 1, 22 Mayıs 2020, *https://vm.ee/sites/default/files/Estonia_for_UN/unsc_-_cyber_arria_22_may_2020_-_australian_statement_002.pdf*, erişim tarihi: 02.07.2020.

[201]Statement by Mr. Akahori Takeshi, Ambassador for Cyber Policy of the Ministry of Foreign Affairs of Japan, on the occasion of the UN Security Council Arria-Formula Meeting: Cyber Stability, Conflict Prevention and Capacity Building, s. 1, 22 Mayıs 2020, *https://vm.ee/sites/default/files/Estonia_for_UN/cyber_arria-formula_statement_of_japan.pdf*, erişim tarihi: 02.07.2020

[202]Eklemek gerekir ki diğer bir çok devlet de doğrudan Güvenlik Konseyi'nin yetkilerine atıf yapmasa dahi siber operasyonların uluslararası barış ve güvenliği tehdit edebileceği kaygısını paylaşarak söz konusu hususa ilişkin uluslararası hukukta mevcut çözümlerin uygulanmasının ehemmiyetine işaret etmiştir. Bu devletlere yazılı bildirilerinde siber saldırıların uluslararası barış, güvenlik ve istikrarı tedit ettiğinin abartı olmadığını belirten Katar (*https://vm.ee/sites/default/files/Estonia_for_UN/final_statement_at_unsc_arria_meeting_on_cyber_stability_conflict_prevention_and_capacity_building.pdf*) ve uluslararası hukukta mevcut güven arttırıcı önlemlerin uygulanmaya başlanması çağrısında bulunan Estonya (*https://vm.ee/sites/default/files/Estonia_for_UN/2020-05-22_pm_kuber-arria_sonavott_final.pdf*) örnek gösterilebilir. (erişim tarihi: 02.07.2020)

[203]Republic of Estonia Ministry of Foreign Affairs, Estonia Raised Cybersecurity for the First Time at the UN Security Council, 5 Mart 2020, *https://vm.ee/en/news/estonia-raised-cybersecurity-first-time-un-security-council*, erişim tarihi: 02.07.2020

bir bildiriyle Estonya, Birleşik Krallık ve Amerika Birleşik Devletleri'nce, 2020 senesinin şubat ayında Gürcistan daimi temsilcisinin Gürcistan hükümetine yönelik düzenlenen geniş çaplı saldırgan siber operasyonlara yönelik mektubuna atıfla, Rusya Federasyonu'nun eylemleri kınanmışsa da konuya ilişkin Güvenlik Konseyi'ne tanınan herhangi bir yetkiye başvurulması söz konusu olmamıştır[204]. Her ne kadar henüz konuya ilişkin bir karar almamış olsa da Güvenlik Konseyi'nin belirli tipteki siber operasyonların barışı tehdit ettiğini, barışı bozduğunu veya saldırı teşkil ettiğine karar verme yetkisi mevcuttur[205]. Yukarıda açıklandığı üzere Güvenlik Konseyi'nin bir hadisenin 39. madde kapsamında değerlendirilmesi hususunda takdir yetkisi olmakla birlikte kanaatimizce bir siber operasyonun fiziki zarara yol açması yahut bir devletin ulusal kritik altyapısı üzerinde hasar oluşturması halinde 41 ve 42. maddede öngörülen önlemlere başvurulması mümkündür. Hatta bir siber operasyon silahlı saldırı eşiğine erişmese dahi saldırıya maruz kalan devletin kuvvet kullanarak karşılık vermesi riskini doğurması ya da siber operasyonun siber veya kinetik şiddet olaylarının devam etmesine yol açması ihtimali yaratması halinde de Güvenlik Konseyi barışın tehdit edilmesi sebebiyle 41. ve 42. maddedeki yetkilerine başvurması beklenebilir[206]. Nitekim ilgili bölümde yer verilen siber operasyonların büyük bir kısmının silahlı saldırı teşkil etmemesi sebebiyle meşru müdafaaya yol açmadığı yönündeki tespitler ve siber operasyonların her geçen gün sıklaştığı gerçeği dikkate alındığında, bu tip bir yaklaşımın saldırgan siber operasyonların yol açabileceği olası zararların ortadan kaldırılmasında önemli bir alternatif sağladığı görüşündeyiz. Lakin Birleşmiş Milletler Şartı kapsamında öngörülen kolektif güvenlik sisteminin "sınırlı" yapısı sebebiyle, veto hakkını haiz daimi üyelerden birinin barış ve güvenliği tehdit etmesi halinde, aşağıda incelenecek uluslararası hukuk mekanizmalarının bir çözüm

[204]Permanent Mission of Estonia to the UN, Stakeout on Cyber-Attack Against Georgia by Estonia, the United Kingdom and the United States, Joint Press Stakeout, *https://un.mfa.ee/press-stakeout-by-estonia-the-united-kingdom-and-the-united-states-on-cyber-attack-against-georgia/*, erişim tarihi: 02.07.2020

[205]NATO CCD COE, **Tallinn Manual 2.0**, sf. 357.

[206]Dinniss, **a.g.e**, s. 111.

olarak tercih edilebileceği varsayımının gerçekçi olmadığını da belirtmek gerekmektedir[207].

2.3.2. Güvenlik Konseyi'nin Siber Operasyonlara Yönelik Zorlayıcı Olmayan Önlemlere Başvurması

Birleşmiş Milletler Şartı'nın 41. maddesi uyarınca Güvenlik Konseyi "*ekonomik ilişkilerin ve demiryolu, deniz, hava, posta, telgraf radyo ve diğer iletişim ve ulaştırma araçlarının tümüyle ya da bir bölümüyle kesintiye uğratılması, diplomatik ilişkilerin kesilmesi*" gibi silahlı kuvvet kullanımını içermeyen önlemler alınmasını kararlaştırarak üye devletleri bu önlemleri uygulamaya çağırabilmektedir. Güvenlik Konseyi'nin 41. madde kapsamında iletişim araçlarının tümüyle ya da bir bölümüyle kesintiye uğratılması kararı almaya yetkilendirilmiş olması, Güvenlik Konseyi'nin geniş takdir yetkisi ile birlikte değerlendirildiğinde, siber iletişimin tamamen yahut kısmen kesintiye uğratılması yönünde de karar alınabileceği şeklinde yorumlanabilmektedir[208]. Nitekim madde kapsamında sayılan önlemler sınırlayıcı nitelikte olmayıp örneklendirme amacı taşıdığından Güvenlik Konseyi'nin barışı tehdit eden, bozan yahut silahlı saldırıda bulunan bir devlete karşı siber yaptırımlar uygulaması veya internet erişimi sınırlaması önünde bir engel bulunmamaktadır[209].

Öte yandan siber iletişimin tamamen yahut kısmen kısıtlanması yönündeki bir yaptırımın özellikle teknolojiye ihtiyacı yüksek olan devletler için bir nevi abluka etkisi doğuracağı ve bu sebeple bu tip bir önlemin zorlayıcılık içermesi sebebiyle ancak 42. madde doğrultusunda uygulanabileceği görüşü de ileri sürülmüştür[210]. Kanaatimizce Birleşmiş Milletler Şartı'nın 41. maddesi kapsamında alınabilecek önlemler sayılırken iletişim araçlarının kesintiye uğratılmasının açıkça örneklendirilmesi dikkate alındığında, sadece siber iletişimin sekteye uğratılması yönündeki bir müdahale 41. madde çerçevesinde değerlendirilebilecektir. Lakin siber

---

[207]Edwin M. Smith, "Collective Security: Changing Conceptions and Institutional Adaption", **Adapting the United Nations to a Postmodern Era**, Ed: Andy W. KnighT, Global Issues Series, 2. Bası, 2005, (41-52), s. 45.
[208]NATO CCD COE, **Tallinn Manual 2.0**, s. 358.
[209]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 114.
[210]Dinniss, **a.g.e**, s. 112.

alana yönelik müdahale siber-fiziksel sistemlerin işlerliğini engelleyen bir seviyeye eriştiği takdirde bu tip önlemlerin 42. maddeye dayanılarak uygulanması gerekebilecektir.

2.3.3. Güvenlik Konseyi'nin Siber Operasyonlara Yönelik Zorlayıcı Önlemlere Başvurması

Birleşmiş Milletler Şartı'nın 42. maddesi uyarınca, 41. madde ile öngörülen önlemlerin yetersiz kalacağının düşünülmesi halinde "*gösteri, abluka ve Birleşmiş Milletler üyelerinin hava, deniz ya da kara kuvvetlerince yapılacak diğer operasyonlar*" dâhil olmak üzere gerekli gördüğü hava, deniz ya da kara kuvvetleri aracılığıyla başvurulacak her türlü girişimi uygulama konusunda Güvenlik Konseyi yetkilendirilmiştir. Güvenlik Konseyi'nin 42. madde ile düzenlenen yetkilerine başvurabilmesi için öncelikle 41. maddede öngörülen önlemleri deneme zorunluluğu bulunmamakta olduğundan 42. madde kapsamında kendisine tanınan yetkileri uygulama ve bu yetkilerin nasıl uygulanacağı konusunda da takdir yetkisini haiz olduğu tespiti yapılabilecektir[211]. Dolayısıyla Güvenlik Konseyi oylama sürecine ilişkin gereklilikleri sağladığı takdirde 42. madde doğrultusunda silahlı kuvvet kullanımı da dahil olmak üzere zorlayıcı önlemlerin uygulanması yönünde karar alabilecektir[212]. Şüphesiz Güvenlik Konseyi bu yetkilerine siber operasyonların uluslararası barışı tehdit ettiği, bozduğu veya saldırı teşkil ettiğini değerlendirdiği takdirde de başvurabilecektir. Lakin siber operasyonların en azından kuvvet kullanma seviyesine erişmediği hallerde zorlayıcı olmayan önlemlerle yetinilmesinin çok daha olası olduğunu belirtmek gerekir[213].

---

[211]Sven B. Gareis / Johannes Varwick, **The United Nations: An Introduction**, Çev: Lindsay P. Cohn, Palgrave Macmillan, 2005, s. 85; Devon Whittle, "The Limits of Legality and the United Nations Security Council: Applying the Extra-Legal Measures Model to Chapter VII Action", **The European Journal of International Law**, Vol. 26, No. 3, 2015, (671-698), s. 674.

[212]Gabriël H. Oosthuizen, "Playing the Devil's Advocate: the United Nations Security Council is Unbound by Law", **Leiden Journal of International Law**, Vol. 12, 1999, (549-563), s. 555.

[213]Brett Epstein, "The Rules of Cyber-Welfare: What Are the Issues with These Rules, How Can the United States Respond to an Attack When Applying These Rules, and Should New Rules Be Enacted", **Holy Cross Journal of Law and Public Policy**, Vol. 18, 2014, (247-304), s. 266; Dinniss, **a.g.e**, s. 112.

Güvenlik Konseyi'nin siber operasyonlara yönelik zorlayıcı önlemlere başvurma kararı aldığı takdirde bu önlemler çerçevesinde kinetik olarak kuvvet kullanabileceği gibi siber operasyonlardan da faydalanabileceği yönünde uzlaşı mevcuttur[214]. Her ne kadar 42. madde kara, hava ve deniz kuvvetleri aracılığıyla kuvvet kullanımından söz etmişse de bu yaklaşımın sebebinin Güvenlik Konseyi'nin yetkilerini sınırlamak olmadığı, aksine maddenin düzenlendiği dönemde mevcut tüm silahlı kuvvetlere yer vererek Güvenlik Konseyi'nin bu kapsamdaki yetkilerinin geniş yorumlanmasını sağlamak amacıyla böyle bir yöntemin tercih edildiği ve evrimsel yorumlama çerçevesinde siber operasyonların da madde kapsamında değerlendirilmesi gerektiği savunulmuştur[215]. Kaldı ki günümüzde siber savunma komutanlıkları bir kuvvet komutanlığı bünyesinde[216] yahut kara, deniz ve hava kuvvetleri komutanlıklarının katılımıyla müşterek bir komutanlık[217] olarak görev yapmaktadır. Keza gelecekte devletler siber savunmaya ilişkin ayrı bir kuvvet komutanlığı oluşturma yoluna gitse dahi bu durum siber alanın fiziki altyapılara bağlı bir saha olduğu gerçeğini değiştirmeyecektir. Tüm bunlar dikkate alındığında Birleşmiş Milletler Şartı'nın 39. maddesinde öngörülen koşulların vuku bulduğuna kanaat getirilmesi halinde Güvenlik Konseyi'nin 42. maddeye dayanarak uygun gördüğü siber operasyonlara da başvurabileceği görüşündeyiz. Dolayısıyla Güvenlik Konseyi'nin bu yönde bir karar alması halinde üye devletlerin 43. maddede düzenlenen her türlü yardım ve kolaylığı Güvenlik Konseyi'ne sağlaması gerekmektedir.

Güvenlik Konseyi kuvvet kullanılmasını gerektiren durumlarda 7. Bölüm uyarınca tanınan yetkilerini kullanırken kurumsal kapasiteye sahip olmaması sebebiyle, önemli bir askeri operasyonu bizzat yönetmek yerine BM Şartı'nın 48 ve

---

[214]NATO CCD COE, **Tallinn Manual 2.0**, s. 359; Roscini, **Cyber Operations and the Use of Force in International Law**, s. 114.

[215]Nils Melzer, **Cyberwarfare and International Law**, Cenevre, United Nations Institute for Disarmament Research, 2011, s. 19, *https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf*, (erişim tarihi: 04.06.2020)

[216]Örneğin Estonya, Siber Komutanlığı'nı Kara Kuvvetleri Komutanlığı bünyesi kapsamında yapılandırmıştır: *https://mil.ee/en/landforces/cyber-command/*, erişim tarihi: 02.07.2020

[217]Amerika Birleşik Devletleri'nde ise Siber Komutanlık ABD Başkanı Donald J. Trump'ın 18 Ağustos 2017 tarihindeki kararı sonrası müşterek bir komutanlık haline dönüştürülmüştür. Ayrıca her kuvvet komutanlığı bünyesinde de siber güvenliğe ilişkin görevlendirilmiş komutanlıklar bulunmaktadır: *https://www.cybercom.mil/About/History/*, erişim tarihi: 02.07.2020

53. maddeleri uyarınca üye devletleri yetkilendirmeyi tercih etmiştir[218]. Bu kapsamda Güvenlik Konseyi siber olarak kuvvet kullanılması yönünde karar alması halinde 48. madde doğrultusunda üye devletlerden yardım talep edebilecek; bu kapsamda barışı tehdit ettiği, bozduğu yahut silahlı saldırı eyleminde bulunduğu düşünülen devletlere karşı kuvvet kullanma yasağına tabi olmaksızın uygun görülen önlemlere başvurulabilecektir. Keza Güvenlik Konseyi Birleşmiş Milletler Şartı'nın 53. maddesi uyarınca ilgili önlemlerin uygulanması için bölgesel antlaşma yahut kuruluşlardan da faydalanabilecektir. Bu takdirde yetkilendirilen bölgesel kuruluş BM Şartı'nın 54. maddesi gereğince Güvenlik Konseyi'ni söz konusu siber operasyonlara ilişkin her daim bilgilendirmekle yükümlü olacaktır[219].

2.4. Siber Silahlı Saldırı: Saldırgan Siber Operasyonlarn Birleşmiş Milletler Şartı 51. Madde Uyarınca Meşru Müdafaa Hakkı Kapsamında İncelenmesi

Kuvvet kullanma yasağının bir diğer istisnası ise devletlerin meşru müdafaa amacıyla kuvvet kullanmasıdır. Nitekim Birleşmiş Milletler Şartı'nın 51. maddesi "*Bu Şart'ın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez*" hükmünü haizdir.

Bu bölümde öncelikle meşru müdafaa hakkına başvurulmasının ön koşulu olarak öngörülen silahlı saldırı kavramı tanımlanarak silahlı saldırı ile kuvvet kullanma kavramının ilişkisi tartışılacak; akabinde siber operasyonların hangi koşullarda silahlı saldırı teşkil edebileceği yorumlanacaktır. Silahlı saldırı kavramının siber operasyonlar açısından oluşturduğu sonuçlar açıklandıktan sonra takip eden bölümlerde meşru müdafaaya ilişkin genel ilkeler çerçevesinde Birleşmiş Milletler Şartı'nın 51. maddesinin siber operasyonlara nasıl uygulanabileceği tahlil edilecektir. Bu kapsamda meşru müdafaa açısından tartışmalı hususlardan henüz gerçekleşmemiş bir silahlı saldırıya yönelik meşru müdafaaya başvurulup başvurulamayacağı ve devlet

[218]Adam Roberts, "The Use of Force", **The UN Security Council: From the Cold War to the 21st Century**, Ed: David M. Malone, Londra, Lynne Rienner Publishers, 2004, (133-153) s. 136.
[219]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 115.

dışı aktörler tarafından bir silahlı saldırı gerçekleştirilmesi halinde de meşru müdafaa kapsamında kuvvet kullanılıp kullanılamayacağı meseleleri ve bunların saldırgan siber operasyonlar açısından etkileri incelenecektir. Son olarak ise kolektif meşru müdafaa hakkı ve meşru müdafaaya ilişkin Birleşmiş Milletler Güvenlik Konseyi'ni bilgilendirme yükümlülüğü saldırgan siber operasyonlar çerçevesinde değerlendirilecektir.

2.4.1. Silahlı Saldırı Kavramı

Birleşmiş Milletler Şartı meşru müdafaa hakkı kapsamında kuvvet kullanılabilmesini silahlı saldırıya maruz kalmış olma şartına bağlamışsa da silahlı saldırının tanımına ilgili madde kapsamında yer verilmemiştir[220]. Uluslararası Adalet Divanı da silahlı saldırı kavramını tanımlamaktan ziyade silahlı saldırıya ilişkin hususları kuvvet kullanma kavramı ile ilişkisi üzerinden irdelemiştir[221]. Dolayısıyla silahlı saldırı kavramını değerlendirirken kuvvet kullanma kavramı üzerinden bir inceleme gerçekleştirmek gerekmektedir[222]. Öte yandan *jus ad bellum* kapsamında gerçekleştirilen analizlerde Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesinde yer verilen kuvvet kullanma kavramı ile Birleşmiş Milletler Şartı'nın 51. maddesinde meşru müdafaaya başvurma hakkının doğmasına yol açtığı öngörülen silahlı saldırı kavramları sıklıkla karıştırılmaktadır[223].

Her ne kadar Amerika Birleşik Devletleri tarafından paylaşılan ve öğretide de kimi hukukçularca benimsenen yaklaşıma göre meşru müdafaanın her türlü hukuka aykırı kuvvet kullanımında başvurulabilecek bir hak olduğu ileri sürülmüşse[224] de Uluslararası Adalet Divanı'nın yerleşik içtihadı uyarınca kuvvet kullanma ile silahlı

---

[220]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 71.
[221]Tom Ruys, **"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice**, New York, Cambridge University Press, 2010, s. 140.
[222]James A. Green, **The International Court of Justice and Self-Defence in International Law**, Hart Publishing, 2009, s. 31.
[223]Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", **Harvard International Law Journal**, Vol. 54, 2012, (13-37), s. 18.
[224]Abraham D. Sofaer, "International Law and the Use of Force", **The National Interest**, No. 1983, 1988, (53-64), s. 54; Schmitt, **International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed**, ss. 21-22; Delerue, **Cyber Operations and International Law**, s. 330

saldırı kavramlarının denk tutulmaması gerekmektedir[225]. Nitekim Divan, Nikaragua Kararı'nda kuvvet kullanmanın silahlı saldırı teşkil eden en şiddetli biçimleriyle daha az şiddetli olanları arasında ayrım yapmak gerektiğini belirterek bir eylemin silahlı saldırı teşkil etmesi için kuvvet kullanmadan daha yüksek bir eşiğe erişmesi gerektiğini ifade etmiştir[226]. Uluslararası Adalet Divanı'nın değerlendirmeleri göz önüne alındığında, silahlı saldırı kavramının kuvvet kullanma yasağından daha yüksek bir eşiğe sahip olduğu ve her silahlı saldırı aynı zamanda kuvvet kullanma teşkil edecekse de her kuvvet kullanma yasağı ihlalinin silahlı saldırı olarak kabul edilmesinin mümkün olmadığı sonucuna ulaşılabilmektedir[227].

Bu sebeple silahlı saldırı ile meşru müdafaa hakkına dayanak teşkil etmeyen diğer kuvvet kullanma eylemleri arasında nasıl bir ayrım sağlanacağı hususu dikkatle incelenmelidir. Söz konusu ayrımın yapılmasında eylemin boyutu ve etkileri gibi objektif veya eylemi gerçekleştiren devletin niyeti ve saiki gibi subjektif faktörlerin göz önüne alınması gerektiği ileri sürülmüştür[228].

Nitekim Uluslararası Adalet Divanı kuvvet kullanma teşkil eden eylemlerin hangi koşullarda aynı zamanda silahlı saldırı eşiğine eriştiğinin kabul edilebileceğini değerlendirirken söz konusu eylemin boyutu ve etkilerinin (*scale and effects*) esas alınması gerektiğini ifade etmiştir[229]. Boyut ve etki kriterleri kümülatif olarak öngörülmüş olup; boyut ile kullanılan kuvvet, kuvvetin kullanıldığı bölge ve devam ettiği süre gibi eylemin önemi ve şiddeti, etki kıstası ile ise eylemin sonuçları kastedilmektedir[230]. Bu kapsamda örneğin, Uluslararası Adalet Divanı Nikaragua Kararı'nda kuvvet kullanma ile silahlı saldırı teşkil eden eylemler arasında öngördüğü ayrımı hatırlatarak bir ticari geminin füze ile vurulmasını tek başına bir eylemin silahlı

---

[225]Henning Lahmann, **Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution**, Cambridge University Press, 2020, s. 47-48; Dinstein, **War, Aggression and Self-Defence**, s. 193-94.
[226]*Nikaragua Davası Kararı*, para. 191.
[227]Dinstein, **War, Aggression and Self-Defence**, s. 207-08; Dinniss, **a.g.e**, s. 77-78; NATO CCD COE, **Tallinn Manual 2.0**, s. 341.
[228]Ruys, **"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice**, s. 139.
[229]*Nikaragua Davası Kararı*, para. 195.
[230]Ruys, **"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice**, s. 139; Delerue, **Cyber Operations and International Law**, s. 330.

saldırı teşkil etmesi için yeterli görmemiştir[231]. Öte yandan Divan'ın Uluslararası Petrol Platformlarına ilişkin kararında tek bir askeri geminin mayınlanmasının meşru müdafaa hakkının kullanılmasına dayanak teşkil edebileceği varsayımı[232] da dikkate alındığında kuvvet kullanma ve silahlı saldırı eşikleri arasında büyük bir uçurum olmadığı kanaatine ulaşılabilmektedir[233].

Keza *Nadelstichtaktik* olarak da adlandırılan olayların toplamı (*accumulation of events*) teorisine göre, tek başına silahlı saldırı teşkil etmemekle birlikte aynı saldırgandan kaynaklanan birden çok eylemin toplamının yarattığı etki ve sonuç silahlı saldırı eşiğine eriştiği takdirde söz konusu saldırgana karşı da meşru müdafaa yoluna başvurulabilecektir[234]. Nitekim Yargıç Schwebel de Nikaragua Kararı'ndaki ayrı görüşünde, kuvvet kullanma teşkil eden birden çok eylemin kümülatif olarak silahlı saldırı eşiğine erişebileceği yönündeki tespitine yer vermiştir[235]. Uluslararası Adalet Divanı tarafından Petrol Platformlarına İlişkin Karar'da meşru müdafaaya ilişkin değerlendirmeleri esasında uyuşmazlık konusu olayların kümülatif olarak dahi silahlı saldırı teşkil etmeyeceği[236] beyanında bulunulması söz konusu teorinin mahkeme tarafından da benimsendiği yorumlarının yapılmasına yol açmıştır[237]. Yine de devletlerin ve Birleşmiş Milletler'in henüz açıkça olayların toplamı teorisini benimsemediği değerlendirildiğinde, söz konusu yaklaşım hakkında genel bir uzlaşı bulunduğu çıkarımında bulunmak mümkün değildir[238].

Subjektif faktörler açısından ise, bir eylemin silahlı saldırı teşkil edebilmesi için niyetin de dikkate alınması gerektiği düşüncesinden hareketle kaza yoluyla silahlı saldırı eşiğine erişen bir eylemde bulunulması halinde söz konusu eylemin *animus aggressionis* yönünden eksik olacağı ve bu sebeple meşru müdafaaya dayanak teşkil

---

[231]*Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America*, International Court of Justice (ICJ), ("Petrol Platformları Kararı"), 6 November 2003, para. 64.
[232] Ibid., para. 72.
[233]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 72.
[234]Norman M. Feder, "Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack", **New York University Journal of International Law and Politics**, vol. 19, no. 2, 1987, (395-432), s. 415; NATO CCD COE, **Tallinn Manual 2.0**, s. 342.
[235]Dissenting Opinion by Judge Schewebel, para. 6.
[236]*Petrol Platformları Kararı*, para. 64.
[237]Dinstein, **War, Aggression and Self-Defence**, s. 206
[238]Lahmann, **a.g.e**, s. 50.

edemeyeceği ileri sürülmüştür[239]. Lakin bizim de katıldığımız görüşe göre, bir eylemin silahlı saldırı olarak değerlendirilmesinde niyetin herhangi bir etkisi bulunmamaktadır. Zira kazara silahlı saldırı teşkil eden bir eylemde bulunulması halinde meşru müdafaaya başvurulması düşünülse dahi, bu bölümün devamında inceleneceği üzere, bu takdirde meşru müdafaanın gerekliliği ilkesi dolayısıyla silahlı saldırıya karşı kuvvet kullanılması riski doğmayacaktır[240].

Kimi yazarlarca silahlı saldırı ile kuvvet kullanma arasında boyut ve etkiye göre ayrım yapılmasını öngören yaklaşım belirleyici bir kıstas sunmak için fazla muğlak bir yapıdadır[241]. Kanımızca silahlı saldırı kavramının netleştirilmesi hususunda bir önceki bölümde açıklanan saldırı kavramından da yararlanılması isabetli olacaktır. Nitekim Uluslararası Adalet Divanı Kongo'daki Silahlı Faaliyetler Kararı'nda silahlı saldırının mevcudiyeti meselesini incelerken Birleşmiş Milletler Genel Kurulu'nun 14 Aralık 1974 tarihinde kabul ettiği 3314 sayılı Saldırının Tanımı Kararı'na atıfta bulunmuştur[242]. Elbette silahlı saldırı (*agression armée*) kavramının saldırı (*agression*) kavramının bir alt başlığı olması sebebiyle her saldırının aynı zamanda silahlı saldırı teşkil ettiğini söylemek mümkün değildir[243]. Lakin 3314 sayılı Karar'ın 3. maddesinde örneklenen eylemlerden 3(a)[244], (b)[245], (d)[246] ve (g)[247] bentlerinde sayılan eylemlerin hem saldırı hem silahlı saldırı teşkil ettiği konusunda genel bir uzlaşı bulunmaktadır[248]. Özellikle 3(b) numaralı maddenin "*bir devletin*

[239]Lahmann, **a.g.e**, ss. 50-51
[240]NATO CCD COE, **Tallinn Manual 2.0**, s. 344.
[241]Yusuf A. Abdulqawi, "The Notion of 'Armed Attack' in the Nicaragua Judgement and Its Influence on Subsequent Case Law", **Leiden Journal of International Law**, Vol. 25, Issue 2, 2012, (461-470), s. 465.
[242]*Silahlı Aktiviteler Kararı*, para. 146.
[243]Dinstein, **Computer Network Attacks and Self-Defence**, s. 100; NATO CCD COE, **Tallinn Manual 2.0**, s. 339; Delerue, **Cyber Operations and International Law**, s. 329
[244]"*3(a)- Bir Devletin silahlı kuvvetlerinin diğer bir devleti istila etmesi veya ona hücum etmesi veya ne kadar geçici olursa olsun, böyle bir istiladan veya hücumden ileri gelen herhangi bir askeri işgal veya kuvvet yoluyla başka bir Devletin ülkesinin veya bir bölümünün ilhakı*"
[245]"*3(b)- Bir Devletin silahlı kuvvetlerinin, başka bir Devletin ülkesini bombardıman etmesi veya bir Devletin diğer bir Devletin ülkesine karşı herhangi bir şekilde silah kullanması*"
[246]"*3(d)- Bir Devletin silahlı kuvvetleriyle başka bir Devletin kara, deniz veya hava kuvvetlerine veya deniz veya hava filolarına saldırması*"
[247]*"3(g)- Bir Devlet tarafından veya bir Devlet adına diğer bir Devlete karşı yukarıda listesi verilen fiillere varan veya o ölçekte olan silahlı kuvvet fiillerini icra eden silahlı çetelerin, grupların, gayri nizami askerlerin veya paralı askerlerin gönderilmesi veya bu gibi fiillere önemli ölçüde karışılması"*
[248]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 71; Delerue, **Cyber Operations and International Law**, s. 329.

diğer bir devletin ülkesine karşı herhangi bir şekilde silah kullanması" şeklinde geniş bir kapsama sahip olacak şekilde düzenlenmesi haklı olarak saldırgan siber operasyonların da bu kapsamda değerlendirilebileceği yorumlarına yol açmıştır[249]. Gerçekten de önceki bölümlerde incelendiği üzere saldırgan bir siber operasyonun kuvvet kullanma eşiğine erişebileceği değerlendirildiğinde, söz konusu siber operasyonun aynı zamanda geniş boyutlu olması ve şiddetli sonuçlara yol açması halinde silahlı saldırı olarak kabul edilebileceği kanaatindeyiz. Lakin söz konusu boyut ve etki hususları her olay özelinde değişkenlik gösterebileceğinden silahlı saldırıya ilişkin genel geçer bir açıklamada bulunmak mümkün gözükmemektedir[250]. Bu sebeple siber operasyonların silahlı saldırı eşiğine erişip erişmediği hususu bir sonraki bölümde güncel örnekler üzerinden incelenecektir.

2.4.2. Meşru Müdafaa Kavramının İlkeleri

Uluslararası Adalet Divanı meşru müdafaa kavramına ilişkin tespitlerini içeren kararlarında bir saldırıya karşılık meşru müdafaa kapsamında gerçekleştirilen eylemlerin hukuki açıdan incelenmesinde gereklilik (*necessity*) ve ölçülülük (*proportionality*) şartları bağlamında değerlendirilmesinin uluslararası teamül hukukunun yerleşik bir kuralı olduğu açıklamasına yer vermiştir[251]. Gereklilik ve ölçülülük ilkelerinin yanı sıra meşru müdafaa hakkının kullanılmasında esas alınması gereken bir diğer ilke ise aciliyettir[252]. Çalışmanın bu kısmında meşru müdafaa kavramının sayılan ilkeleri incelenecek ve siber operasyonlar açısından doğurduğu sonuçlar örnekler üzerinden tartışılacaktır.

---

[249]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 72.
[250]Lahman, **a.g.e**, s. 49.
[251]*Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons* Z. C. J. Reports 1996 (1), ("Nükleer Silahlara İlişkin Tavsiye Kararı") p. 245, para. 41; *Military and Paramilitary Activities in and against Nicaragua* 1. C. J. Reports 1986, p. 94, para. 176
[252]Dinstein, **Computer Network Attacks and Self-Defence**, s. 109; Berdal Aral, **Uluslararası Hukukta Meşru Müdafaa Hakkı**, Ankara, Siyasal Kitabevi, 1999, s. 28.

2.4.2.1. Meşru Müdafaanın Gerekliliği

Gereklilik ilkesi uyarınca bir devlet meşru müdafaaya ancak kuvvet kullanmasından başka bir çaresi kalmadığı hallerde başvurmalıdır[253]. Dolayısıyla silahlı saldırıya maruz kalan bir devlet ancak barışçıl önlemlerin yetersiz olacağı ya da bu tedbirlerin sonuçsuz kalacağı anlaşıldığı durumlarda meşru müdafaa kapsamında silahlı mücadeleye başvurmalıdır[254]. Bu kapsamda meşru müdafaa saldırganın en kısa zamanda teslim olmasını ve saldırıyı durdurmasını sağlayıcı önlemleri almaya olanak sağlamaktadır[255].

Saldırgan siber operasyonlar açısından da meşru müdafaanın gerekliliği ilkesi uyarınca, silahlı saldırıdan mesul devlet belirlenmeli; siber operasyonun bir kaza olmadığı ve meşru müdafaaya başvuran devleti hedef aldığı teyit edilmeli ve son olarak da saldırganların hedef aldıkları bilgisayar yahut ağlardan erişiminin engellenmesi gibi pasif siber savunma sistemlerinin kullanılmasının söz konusu siber operasyonları savuşturmak için yeterli olmadığı ortaya konmalıdır[256]. Nitekim her ne kadar bir önceki bölümde tartışıldığı üzere bir eylemin silahlı saldırı teşkil etmesi saldırıyı gerçekleştiren devletin niyetine bağlı olmasa da yanlışlıkla gerçekleştirilen bir silahlı saldırıya karşı kuvvet kullanılması meşru müdafaanın gerekliliği ilkesi ile bağdaşmayacaktır. Gereklilik değerlendirmesi saldırıya maruz kalan devletin bakış açısı üzerinden değerlendirilmeli, şayet kuvvet kullanma eşiğine erişmeyen önlemlerin silahlı saldırıyı savuşturmaya elverişli olmadığı çıkarımında bulunmak makul ise söz konusu devletin meşru müdafaa kapsamında siber yahut kinetik kuvvet kullanma operasyonlarına başvurabileceği kabul edilmelidir[257].

---

[253]Ruys, **"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice,** s. 95; Gardam, **Necessity, Proportionality and the Use of Force by States**, s. 149; Mesut H. Caşın, **Modern Uluslararası Hukukun Temel Esasları**, İstanbul, Legal Yayıncılık, 2013, S. 1237.
[254]Jens D. Ohlin / Larry May, **Necessity in International Law**, New York, Oxford University Press, 2016, s. 55-56; Green, **a.g.e**, s. 78-80; Aral, **Uluslararası Hukukta Meşru Müdafaa Hakkı**, s. 26.
[255]Cassese, **International Law**, s. 355; Gardam, **Necessity, Proportionality and the Use of Force by States**, s. 155; Enver Bozkurt**, Uluslararası Hukukta Kuvvet Kullanımı**, 3. Baskı, Asil Yayın, 2007, s. 58.
[256]Marco Roscini, "World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force", **Max Planck Yearbook of United Nations Law**, Ed: Armin von Bogdandy / Rüdiger Wolfrum, Vol. 14, Brill, 2010, (85-130), s 119.
[257]NATO CCD COE, **Tallinn Manual 2.0**, s. 349.

2.4.2.2. Meşru Müdafaanın Ölçülülüğü

Bir silahlı saldırıya karşılık gerçekleştirilen meşru müdafaa yukarıda açıklanan ölçütler uyarınca gerekli görüldüğü takdirde başvurulacak meşru müdafaanın ayrıca ölçülülük açısından da denetlenmesi gerekmektedir[258]. Uluslararası Adalet Divanı içtihatları gereğince meşru müdafaa kapsamında kuvvet kullanılırken ölçülülük ilkesi uyarınca hedefin yapısı ve silahlı saldırıya karşılık gerçekleştirilen kuvvet kullanımına dair operasyonun genel boyutu dikkate alınmalıdır[259]. Zira ölçülülük ilkesi ile meşru müdafaa kapsamında kuvvet kullanılırken bu kuvvetin söz konusu silahlı saldırının savuşturulması açısından kapsam, süre ve yoğunluk açısından orantılı olması gerektiği öngörülmüştür[260]. Ölçülülük ilkesi uyarınca bir devletin meşru müdafaaya başvururken maruz kaldığı silahlı saldırı ile aynı nitelikte karşılık vermesi şart koşulmadığından siber operasyon yoluyla gerçekleştirilen bir saldırıya, orantılı olmak kaydıyla, kinetik olarak karşılık verebileceği gibi bunun tam tersi de mümkün olabilecektir[261].

2.4.2.3. Meşru Müdafaanın Aciliyeti

Aciliyet ilkesi uyarınca, bir silahlı saldırının üzerinden uzun süre geçtikten sonra meşru müdafaa hakkı kapsamında kuvvet kullanılması mümkün görülmemektedir[262]. Öte yandan aciliyet ilkesi, silahlı saldırıya maruz kalan devlete derhal meşru müdafaaya başvurma zorunluluğu getirmediğinden bu kapsamda meşru müdafaa hakkı doğrultusunda kuvvet kullanılmasına ilişkin alınacak kararın ve bu kararın uygulamaya geçirilmesinin vakit alması sebebiyle belirli bir süre sonra meşru müdafaa hakkından faydalanılması tek başına ilkenin ihlali olarak

---

[258]Judith G. Gardam, "Proportionality and Force in International Law", **The American Journal of International Law**, Vol. 87, No. 3, 1993, (391-413), ss. 403-04.
[259]*Petrol Platformları Kararı*, para. 74-77
[260]Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts", **Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy**, Washington, The National Academies Press, 2010, (151-178), s. 167.
[261]Michael N. Schmitt, **Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts**, s. 167; Roscini, **Cyber Operations and the Use of Force in International Law**, s. 90;
[262]Matthew Hoisington, "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", **Boston College International and Comparative Law Review**, vol. 32, no. 2, 2009, (439-454), s. 450.

değerlendirilmemelidir[263]. Zira aciliyet ilkesi ile amaçlanan meşru müdafaa hakkının sınırlanması değil, meşru müdafaa kapsamında kuvvet kullanımının misillemeden ayırt edilmesinin sağlanmasıdır[264].

Gerçekten de silahlı saldırıya uğrayan bir devletin meşru müdafaaya başvurabilmesi belirli bir süre gerektirebileceği gibi bu, özellikle saldırının bir devlete atfedilebilmesinin nispeten daha zor olduğu saldırgan siber operasyonlar açısından karşılaşılması oldukça olağan bir durumdur. Nitekim bir devletin silahlı saldırı eşiğine erişen siber operasyonlara maruz kalması halinde, söz konusu siber operasyonlar hedef devletin siber yapılanmaları üzerinde çeşitli düzeylerde tahribatlar yaratabilecek; silahlı saldırının tahlil edilerek sorumlu devletin belirlenmesine ilişkin delillerin toplanması ve bunu takiben siber yahut kinetik meşru müdafaa yollarına başvurulmasının zaman alabilecektir[265]. Keza silahlı saldırı teşkil eden siber operasyonların devam edeceğinin öngörülmesinin makul olduğu hallerde meşru müdafaa kapsamında siber yahut kinetik kuvvet kullanmaya devam edilmesi de misilleme olarak değerlendirilmemelidir[266].

2.4.3. Silahlı Saldırının Yakınlığı: Önleyici Meşru Müdafaa[267]

Henüz gerçekleşmemiş silahlı saldırılara karşı meşru müdafaa hakkının kullanılıp kullanılamayacağı hususu tartışmalı olup özetle, Birleşmiş Milletler

---

[263]Gardam, **Necessity, Proportionality and the Use of Force by States**, s. 152; Dinstein, **War, Aggression and Self-Defence**, s. 233.
[264]NATO CCD COE, **Tallinn Manual 2.0**, s. 353.
[265]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 91.
[266]NATO CCD COE, **Tallinn Manual 2.0**, s. 354.
[267]Önleyici meşru müdafaaya ilişkin doktrinde *interceptive*, *preventive*, *anticipatory* ve *preemptive* adlandırmalarının kullanıldığı görülmektedir. Her ne kadar söz konusu kullanımların Türkçe karşılığı olarak önleyici kelimesi yaygın olarak kullanılıyor ise de sayılan kullanımlar arasında farklılıklar mevcuttur. Bu kapsamda *interceptive* ibaresi silahlı saldırıya ilişkin girişimlere başlandığı ve tehdidin gerçekleştiği *preventive* ibaresi ise tehdidin henüz sadece bir ihtimal olduğu durumlar için kullanılmaktadır. Öte yandan bazı yazarlarca *anticipatory* ve *preemptive* şeklindeki kullanımlar arasında da ayrım yapılmakla birlikte her iki kullanımda da genel olarak yakın bir tehlikenin varlığı halinde meşru müdafaaya başvurulması kastedilmekte, ayrım yakın tehlike ölçütleri noktasında belirginleşmektedir. (Geoffrey S. DeWeese, "Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence", **2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace**, Eds: Markus Maybaum / Lauri Lindstörm, Tallinn, NATO CCD COE Publications, 2015, (81-92), ss. 85-86.) Bu çalışma kapsamında önleyici meşru müdafaa kavramı *anticipatory*, *preemptive* kullanımlarının karşılığı olarak yakın tehlike halinde meşru müdafaaya başvurulmasına anlamında kullanılmaktadır.

Şartı'nın 51. maddesini dar yorumlayan görüş silahlı saldırı ne kadar yakın yahut tehlikeli olursa olsun meşru müdafaaya ancak silahlı saldırı gerçekleştikten sonra başvurulabileceğini savunurken; meşru müdafaa hakkını geniş yorumlayan görüş ise maddede meşru müdafaanın "doğal" bir hak olarak tanımlanmasından bahisle devletlerin uluslararası teamül hukukunda tanınan önleyici meşru müdafaa hakkının kısıtlanması yönündeki yaklaşımı reddetmektedir[268]. Bu kapsamda önleyici meşru müdafaa kavramı, öğretide kimi yazarlarca meşru müdafaanın ilkelerinden sayılan silahlı saldırının yakınlığı (*imminence*) kıstası doğrultusunda[269], silahlı saldırının pek yakın olduğu ve kesin tehlike teşkil ettiği hallerde meşru müdafaaya başvurulabilmesine dayanak oluşturmaktadır[270].

Uluslararası Adalet Divanı Kongo'daki Silahlı Faaliyetlere İlişkin Karar'ında Birleşmiş Milletler Şartı'nın 51. maddesi çerçevesinde meşru müdafaaya başvurulmasının madde ile belirtilen katı sınırlar içerisinde yapılması gerektiğini belirtmiş; bir devletin söz konusu madde ile öngörülenin dışında kendi güvenlik çıkarları sebebiyle meşru müdafaa hakkından faydalanamayacağı ifade edilmiştir[271].Bu doğrultuda, önleyici meşru müdafaa teorisine karşı çıkanlar Birleşmiş Milletler Şartı'nın 51. maddesindeki düzenleme ile meşru müdafaaya başvurulabilmesi için silahlı saldırının vuku bulmuş olması gerektiğinin şart koşulduğunu ileri sürmektedirler[272]. Keza önleyici meşru müdafaa başka bir devletin niyetinden emin olamamanın yanı sıra silahlı saldırı gerçekleştirilmeden evvel her an vazgeçilme ihtimali olması sebebiyle silahlı saldırının kesinliğinin sağlanamaması ve henüz gerçekleşmemiş olan bir silahlı saldırıya karşı meşru müdafaaya başvurulduğu takdirde ölçülülük ilkesinin nasıl sağlanacağının belirsiz olması hususları yönünden eleştirilmiştir[273]. Dolayısıyla devletlerin kendi değerlendirmeleriyle bir silahlı saldırı

---

[268]Stephen M. Schwebel, "Aggression, Intervention, and Self-Defense in Modern International Law", **Justice in International Law: Selected Writings**, Cambridge, Cambridge University Press, 1994, (530-592), s. 580-81; Aslan Gündüz, **Milletlerarası Hukuk**, Ed: Reşat Volkan Günel, 6. Baskı, Beta, 2013, s. 148; Aksar, **a.g.e**, s. 118.

[269]Kenneth Watkin, **Fighting at the Legal Boundaries: Controlling the Use of Force in Contemporary Conflict**, New York, Oxford University Press, 2016, s. 56

[270]Brownlie, **International Law and the Use of Force by States**, ss. 275-76; Sur, **a.g.e**, s. 265.

[271]*Silahlı Faaliyetler Kararı*, para. 148.

[272]Gray, **International Law and the Use of Force**, s. 160

[273]Ian Brownlie, "*The Use of Force in Self-Defense*", **British Year Book of International Law**, Vol. 37, 1961, (183-268), s. 227.

tehdidine dayanarak meşru müdafaaya başvurmasının Birleşmiş Milletler Şartı'nın amacıyla çelişeceği, bunun yerine böyle bir durumda hedef olduğunu düşünen devletin konuyu Birleşmiş Milletler Güvenlik Konseyi'ne taşıması gerektiği ileri sürülmüştür[274].

Öte yandan bazı devletler tarafından, özellikle teknolojik gelişmelerin günümüz silahları üzerindeki etkileri esas alınarak, devletlerin önleyici meşru müdafaa hakkını haiz olduğunun kabul edilmesi elzem görülmüştür[275]. Önleyici meşru müdafaa hakkının uluslararası hukuk tarafından tanındığını savunan görüş, maddenin yakın tehlikeye karşı meşru müdafaaya başvurulmasına olanak tanınmayacak şekilde dar yorumlanmasının amacıyla çelişeceğini belirtmiştir[276]. Zira madde kapsamında her ne kadar önleyici meşru müdafaa hakkına açıkça yer verilmemişse dahi, maddenin aynı zamanda silahlı saldırının tanımı veya meşru müdafaanın ilkelerine ilişkin de herhangi bir hüküm içermediği göz önüne alındığında, meşru müdafaaya ilişkin tüm hususlara Birleşmiş Milletler Şartı çerçevesinde yer verilmesine gerek duyulmadığı sonucuna ulaşılabilmektedir[277]. Viyana Antlaşmalar Hukuku Sözleşmesi'nin 32. maddesi uyarınca 31. maddede yer verilen yorumlara ilişkin genel kuralların bir sözleşmeye uygulanması neticesinde "*çok açık bir şekilde saçma"* veya "*makul olmayan*" sonuçlara ulaşılması halinde tamamlayıcı yorum araçlarına başvurulması öngörülmektedir[278]. Bu kapsamda devletlerin yakın bir silahlı saldırı tehdidiyle karşılaşması halinde herhangi bir karşılık vermemesini mantığa aykırı bulan yazarlarca devletlerin önleyici meşru müdafaa hakkı kapsamında kendilerini savunmak için gerekli önlemleri alabileceği savunulmuştur[279].

---

[274]David Kretzmer, "The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum", **The European Journal of International Law**, Vol. 24, No. 1, 2013, (235-282), s. 248.
[275]Carlo Focarelli, "Self-Defence in Cyberspace", **Research Handbook on International Law and Cyberspace**, Ed: Nicholas Tsagourias / Russell Buchan, Edward Elgar Publishing, 2015, (255-284), s. 270.
[276]Lahmann, **a.g.e**, ss. 55-56.
[277]Dinniss, **a.g.e**, s. 85.
[278]United Nations, Vienna Convention on the Law of Treaties, 23 May 1969, United Nations, Treaty Series, vol. 1155, Art. 32.
[279]Alexandrov A. Stanimir, **Self-Defense Against the Use of Force in International Law**, Developments in International Law, Vol. 23, Klumet Law International, 1996, s. 149; Roscini, **Cyber Operations and the Use of Force in International Law**, s. 78.

Yakın bir tehlike halinde silahlı saldırıya başvurulabileceğini savunan hukukçular ayrıca, *Caroline Olayı*nı[280] örnek göstererek önleyici meşru müdafaanın uluslararası teamül hukukunun bir parçası olduğunu belirtmiştir[281]. Nitekim Caroline Olayı çerçevesinde meşru müdafaa hakkı tartışılmış; dönemin ABD Dışişleri Bakanı'nın "*ortaya çıkan tehdidin ani, karşı konulamaz ve başka yollarla giderilemez olması ve müzakere etmek için zaman bırakmaması*"[282] halinde önleyici meşru müdafaaya başvurulabileceği yönündeki tespiti günümüze değin herhangi bir uluslararası mahkeme veya Güvenlik Konseyi kararıyla yanlışlanmamıştır[283].

Nitekim İsrail'in Altı Gün Savaşları sırasında yakın bir silahlı saldırı tehdidinin varlığına dayanarak Mısır ordusuna ait taarruz uçaklarını imha etmesi de önleyici meşru müdafaanın halen uluslararası teamül hukukunun bir parçası olarak görüldüğünün örneği olarak sunulmaktadır[284]. Keza İsrail'in Tuwaitha Araştırma Merkezi ve Bağdat yakınlarındaki Osarik Nükleer Reaktörü'nü imha etmesinin Güvenlik Konseyi tarafından şiddetle kınanmasının sebebi, önleyici meşru müdafaa yaklaşımının uluslararası hukuka aykırı bulunmasından ziyade, İsrail'in uluslararası toplumu yakın bir tehdit ile karşı karşıya olduğuna ikna edememesi olarak görülmektedir[285].

Institut de Droit International de Uluslararası Hukukta Silahlı Kuvvet Kullanımına İlişkin Mevcut Sorunlar başlıklı raporunun meşru müdafaaya ilişkin bölümünde, meşru müdafaa hakkının bir devletin açıkça yakın bir silahlı saldırı

---

[280]Söz konusu olay, Kanada'nın Birleşik Krallık'a karşı bağımsızlık mücadelesinde kullanılan ABD bandıralı Caroline isimli geminin 1837 senesinde Birleşik Krallık askerleri tarafından Niagara Şelalesi'nden atılıp yok edilerek 2 kişinin ölümüne yol açması olarak özetlenebilir. (Martin A. Rogoff / Edward Collins, "The Caroline Incident and the Development of International Law", **Brooklyn Journal of International Law**, vol. 16, no. 3, 1990, (493-528), s. 495)

[281]Terry D. Gill / Paul A. L. Ducheine, "Anticipatory Self-Defense in the Cyber Context", **International Law Studies**, Vol. 89, 2013, (438-471), ss. 454-54; Dinniss, **a.g.e**, s. 88.

[282]Rogoff / Ducheine, **a.g.m**, ss. 499-500.

[283]Gill / Ducheine, **a.g.m**, s. 457; Hatta Webster'in yukarıda alıntılanan sözleriyle özdeşleşen yaklaşıma Uluslararası Askeri Ceza Mahkemesi tarafından Nüremberg Kararları çerçevesinde atıfta bulunulmuştur. (*The Trial of German Major War Criminals. Proceedings of the International Military Tribunal sitting at Nuremberg, Germany*, Part 22 (22nd August ,1946 to 1st October, 1946), s. 435)

[284]Franck, **a.g.e**, s. 103; Lahmann, **a.g.e**, s. 56; Gray ise söz konusu operasyonların İsrail tarafından önleyici meşru müdafaa teorisine dayandırılmadığı görüşündedir. (Gray, **International Law and the Use of Force**, s. 161)

[285]Dinniss**, a.g.e**, s. 87.

tehdidiyle karşılaştığı hallerde de doğabileceği ve söz konusu silahlı saldırıyı durdurmak veya savuşturmak için başka bir yöntem bulunmadığı takdirde Güvenlik Konseyi gerekli önlemleri alıncaya kadar meşru müdafaa kapsamında kuvvet kullanılabileceği yönünde görüş bildirmiştir[286]. Benzer bir şekilde Birleşmiş Milletler nezdinde hazırlanan Tehditler, Zorluklar ve Değişim başlıklı Yüksek Düzey Panel'in Raporu'nda da uluslararası hukuktaki yerleşik normlara göre, bir devletin yakın bir silahlı saldırı tehdidiyle karşılaştığı takdirde, söz konusu saldırıya yönelik başka bir çözüm mümkün olmadığında orantılı olarak meşru müdafaa kapsamında kuvvet kullanabileceği belirtilmiştir[287].

Sonuç olarak, önleyici meşru müdafaa hakkı uluslararası toplum tarafından sürekli başvurulabilecek bir yaklaşım olarak benimsenmese dahi bu kapsamda yapılan müdahalelerin olay özelinde yapılan değerlendirmelere göre uluslararası hukuka uygun görülebileceği söylenebilmektedir[288]. Dolayısıyla bir devletin kendisini savunma imkanı varken meşru müdafaa hakkına başvurabilmesi için silahlı saldırının gerçekleşmesini beklemenin gerçeklikten uzak olması sebebiyle, bir silahlı saldırının hedefi olan devletin silahlı saldırıya maruz kalacağının neredeyse kesin olduğu hallerde ("*the last window*") söz konusu silahlı saldırıya karşılık meşru müdafaaya başvurabilmesinin mümkün olduğu savunulmaktadır[289]. Yakın tehlikeye ilişkin değerlendirmeler iyi niyetle ve mümkün olan tüm bilgiler değerlendirilerek yapılmalı; devletler bu konuda açık ve ikna edici delillere dayanmalıdır[290].

Saldırgan siber operasyonlar açısından da önleyici meşru müdafaaya başvurulması uluslararası hukuka uygunluk açısından geleneksel askeri

---

[286]Institute de Droit International, **Present Problems of the Use of Armed Force in International Law: Self-Defence**, 10A Resolution EN, Tenth Commission, Rap: M. Emmanuel Roucounas, Session de Santiago, 27 Ekim 2007, para. 3, *https://www.idi-iil.org/app/uploads/2017/06/2007_san_02_en.pdf*, (erişim tarihi: 04.08.2020)

[287]United Nations General Assembly, **A more Secure World: Our Shared Responsibility**, Report of the High-level Panel on Threats, Challenges and Change, A/59/565, 2 Aralık 2004, s. 54, para. 188

[288]Franck, **a.g.e**, s. 105; Eric Myjer, "Some Thoughts on Cyber Deterrence and Public International Law", **Research Handbook on International Law and Cyberspace**, Ed: Nicholas Tsagourias / Russell Buchan, Edward Elgar Publishing, 2015, (284-307), s. 272.

[289]Michael N. Schmitt, "Preemptive Strategies in International Law", **Michigan Journal of International Law**, Volume 24, Issue 2, 2003, (513-548), s. 535.

[290]Roscini, **Cyber Operations and the Use of Force in International Law**, ss. 79-80.

operasyonlardan farklı değildir[291]. Örneğin, yukarıda incelenen Altı Gün Savaşı sırasında İsrail aynı operasyonu radar ve kumanda sistemlerine yönlendireceği bir siber operasyonla gerçekleştirseydi bu değişiklik eylemin meşruiyetinde bir farklılık yaratmazdı[292]. Hatta saldırgan siber operasyonların etkilerini gösterme hızı ve olası yıkıcı sonuçları göz önüne alınınca önleyici meşru müdafaanın etkili bir savunma için elzem olduğu çıkarımında bulunulabilmektedir[293]. Tallinn El Kitabı yazarlarının çoğunluğu da bu görüşü benimsemiş; bir devletin kendisine yöneltilmekte olan bir siber operasyona yönelik makul bir şekilde kendisini savunmak için son anda önleyici meşru müdafaaya başvurabileceği görüşünü bildirmiştir[294]. Keza 2012 senesinin Eylül ayında Amerika Birleşik Devletleri Dışişleri Bakanlığında yasal danışmanlık görevini sürdüren Harold Koh da yapmış olduğu bir konuşmada "*Birleşmiş Milletler Şartı'nın 51. maddesi ile tanınan bir devletin ulusal meşru müdafaa hakkı silahlı saldırı yahut muhtemel tehdit (imminent threat) oluşturan bilgisayar ağı aktiviteleri tarafından da tetiklenebilecektir*" beyanında bulunmuştur[295].

Nitekim saldırgan siber operasyonlar geleneksel yöntemlerle gerçekleştirilecek bir silahlı saldırının yaklaştığına dair yakın tehdidin varlığına işaret edebileceği gibi silahlı saldırı eşiğine erişen bir siber operasyonun kendisinin de yakın tehdit teşkil etmesi mümkündür[296]. Zira saldırgan siber operasyonlar geleneksel saldırı yöntemlerine eşlik edebileceği gibi 2007 yılında İsrail'in *Operation Orchard* kapsamında Suriye'nin hava savunma sistemlerini siber operasyonlar aracılığıyla etkisiz hale getirerek bir nükleer tesisi bombalaması veya Rusya'nın 2008'de Gürcistan'a yönelik gerçekleştirdiği saldırılar öncesi *DoS* saldırıları vasıtasıyla uydu ve radar sistemleri ile askeri iletişim kanallarını devredışı bırakması böyle bir ihtimalin mümkün olduğuna dair yakın geçmişte mevcut örneklerdir[297]. Bir an için Suriye'nin İsrail tarafından siber operasyonlar aracılığıyla hava savunma sistemlerinin devre dışı bırakıldığını fark ettiğini varsayarsak; bunun bir saldırının başlangıcına dair işaret

[291]Gill / Ducheine, **a.g.m**, s. 465.
[292]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 79.
[293]Focarelli, **a.g.m**, s. 273.
[294]NATO CCD COE, **Tallinn Manual 2.0**, s. 351.
[295] Koh, **a.g.m**, s. 4.
[296]Dinniss, **a.g.e**, s. 88.
[297]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 79; Dinniss, **a.g.e**, s. 82.

olarak kabul edilip yakın tehdide karşı önleyici meşru müdafaaya başvurulması düşünülebilir[298]. Öte yandan bir sisteme sonradan kullanılmak üzere kötücül yazılım yerleştirilmesi halinde söz konusu kötücül yazılımın sadece veri toplama gibi bir amaç için kullanılması ihtimali de dikkate alınınca aynı sonuca ulaşmak makul gözükmemektedir[299].

Ancak herhangi bir kinetik operasyonun parçası olarak yürütülmeyen saldırgan siber operasyonların açık bir istihbarat olmaksızın yakın tehdit oluşturacağını öngörmek mümkün olmadığından saldırgan siber operasyonlar açısından önleyici meşru müdafaaya başvurulabilmesinin daha düşük bir olasılık olduğu yorumunda bulunulabilir[300]. Siber operasyonların gerçekleştirildikten sonra dahi kaynağının tespit edilebilmesinin güç olduğu dikkate alınınca henüz gerçekleşmemiş bir saldırgan siber operasyonun yakın tehlike teşkil ettiğinin öngörülebilmesi uygulamada zor gözükmektedir[301]. Dolayısıyla siber alanda yetkin devletlerin önleyici meşru müdafaaya ilişkin daha istekli bir tutum sergilemeleri ve siber alanda daha geride kalmış devletlerin ise önleyici meşru müdafaaya ilişkin daha tutucu bir yaklaşım benimsemeleri beklenebilir[302].

2.4.4. Silahlı Saldırının Kaynağı: Devlet Dışı Aktörlere Karşı Meşru Müdafaaya Başvurulması

Birleşmiş Milletler Şartı'nın 51. maddesi uyarınca meşru müdafaa hakkının kullanılmasının üyelerden birinin silahlı saldırıya uğraması şartına bağlanması devlet dışı aktörlerin saldırılarına karşı meşru müdafaa hakkının kullanılıp kullanılamayacağına ilişkin tartışmalara yol açmıştır[303]. Uluslararası Adalet Divanı Nikaragua kararında, silahlı saldırının bir devletin düzenli ordusu tarafından gerçekleştirilen saldırılarla sınırlı olmadığını belirterek bir devlet tarafından

[298]Dinniss, **a.g.e**, s. 88.
[299]Dinniss, **a.g.e**, s. 90.
[300]Gill / Ducheine, **a.g.m**, ss. 468-69.
[301]Focarelli, **a.g.m**, s. 272.
[302]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 80.
[303]Gray, **International Law and the Use of Force**, s. 202; Ruys, **'Armed Attack' and the Article 51 of the UN Charter**, s. 490; Ceren Zeynep Pirim, "Devletlere Atfedilemeyen Silahlı Saldırılara Karşı Meşru Müdafaa: Uluslararası Hukukta Sınır Ötesi Operasyonların Hukuki Zemini", **Türkiye Adalet Akademisi Dergisi**, Sayı: 40, 2019, (245-303), s. 247; Lahmann, **a.g.e**, s. 51; Aksar, **a.g.e**, ss. 120-21.

gönderilen yahut bir devlet adına hareket eden silahlı örgütlerin, grupların yahut paralı askerlerin başka bir devlete yönelik gerçekleştirdikleri saldırıların da düzenli ordu tarafından gerçekleştirilen saldırıların seviyesine eriştiği takdirde silahlı saldırı kapsamında değerlendirilebileceğini belirtmiştir[304]. Görüldüğü üzere Uluslararası Adalet Divanı silahlı saldırının bizzat bir devlet tarafından gerçekleştirilmesini bir zorunluluk olarak değerlendirmemiş; ancak herhangi bir devletin dahli söz konusu olmaksızın devlet dışı bir aktör tarafından gerçekleştirilen eylemlerin silahlı saldırı teşkil edip etmeyeceği ve dolayısıyla bu tip eylemlere karşı meşru müdafaaya başvurulup başvurulamayacağına ilişkin bir açıklama yapmaktan kaçınmıştır[305].

Her ne kadar uzunca bir süre Birleşmiş Milletler Şartı'nın 51. maddesi lafzi yorumlanarak bir eylemin silahlı saldırı olarak değerlendirilebilmesi için bir devlet tarafından gerçekleştirilmesi yahut bir devlete atfedilebiliyor olması gerektiği yaygın kanaat olarak benimsenmişse de kimi yazarlarca bu yaklaşımın ilerleyen süreçte değişim gösterdiği ileri sürülmüş[306]; bu hususun başlıca dayanağı olarak da Amerika Birleşik Devletleri'ni hedef alan 11 Eylül saldırıları sonrası Birleşmiş Milletler Güvenlik Konseyi'nin 12 Eylül 2001 tarihinde almış olduğu 1368 sayılı ve 28 Eylül 2001 tarihinde almış olduğu 1373 sayılı kararlarında meşru müdafaa hakkına atıfta bulunulması gösterilmiştir[307]. Nitekim NATO da 11 Eylül saldırılarının silahlı saldırı olduğunu tespit ederek tarihinde ilk defa kolektif meşru müdafaaya ilişkin NATO Antlaşması'nın 5. maddesini devreye sokmuştur[308]. Keza Avrupa Birliği ve Avrupa Güvenlik ve İşbirliği Teşkilatı (*Organization for Security and Cooperation in Europe* – "OSCE") da 11 Eylül saldırılarını silahlı saldırı olarak nitelendirerek Amerika Birleşik Devletleri'nin meşru müdafaa hakkını kullanabileceğini belirtmişlerdir[309]. Bu

---

[304]*Nikaragua Davası Kararı*, para. 195.
[305]Gray, **International Law and the Use of Force**, s. 80.
[306]Sean D. Murphy, "Terrorism and the Concept of Armed Attack in Article 51 of the U.N. Charter", **Harvard International Law Journal**, vol. 43, no. 1, 2002, (41-52), s. 48; Gray, **International Law and the Use of Force**, s. 199; Ruys, **'Armed Attack' and the Article 51 of the UN Charter**, s. 486-87; Franck, **a.g.e**, s. 54; Pirim, **a.g.m**, ss. 265-66.
[307]Resolution 1368 (2001) Adopted by the Security Council at its 4370th meeting, on 12 September 2001, S/RES/1368 (2001); Resolution 1373 (2001) Adopted by the Security Council at its 4385th meeting, on 28 September 2001, S/RES/1373 (2001)
[308]Natalino Ronzitti, "The Expanding Law of Self-Defence", **Journal of Conflict and Security Law**, Vol. 11, 2006, (343-359), s. 348
[309]Ibid.

kapsamda Ruys, devlet uygulamasında terör örgütlerince gerçekleştirilen birtakım eylemlerin de silahlı saldırı olarak değerlendirildiği ve söz konusu silahlı saldırılara karşılık meşru müdafaa hakkının herhangi bir devlete değil doğrudan devlet dışı aktöre yöneltildiğini dikkate alarak günümüzde uluslararası teamül hukukunun, istisnai durumlarda, devlet dışı aktörlerin eylemlerinin de silahlı saldırı kabul edilecek şekilde değişim geçirdiğini savunmuştur[310].

Öte yandan Uluslararası Adalet Divanı ise İşgal Altındaki Filistin Topraklarında Duvar İnşa Edilmesinin Hukuki Sonuçlarına İlişkin Tavsiye Karar'da, Birleşmiş Milletler Şartı'nın 51. maddesi ile meşru müdafaa hakkının bir devlet tarafından gerçekleştirilen veya bir devlete atfedilebilen bir silahlı saldırının mevcudiyeti halinde tanındığı tespitinde bulunmuştur[311]. Keza bu yaklaşım daha sonra devletler tarafından da benimsenmiş; örneğin Fransa, Suriye'de faaliyet gösteren DAEŞ (IŞİD) terör örgütüne yönelik müdahalelerini "*quasi-state*" bir oluşumun silahlı saldırılarına yönelik meşru müdafaa hakkının kullanılması olarak açıklayarak, Uluslararası Adalet Divanı içtihatlarına atıfla, bu yaklaşımın Fransa tarafından meşru müdafaa hakkının genişletilerek bir devlete atfedilmeyen devlet dışı aktörlerin saldırılarına yönelik meşru müdafaa hakkının tanındığı anlamına gelmediği ifade edilmiştir[312]. Gerçekten de Birleşmiş Milletler Şartı'nın 51. maddesinde yer verilen meşru müdafaa hakkı ile 2(4) numaralı maddede düzenlenen kuvvet kullanma yasağına bir istisna getirilmek istendiği ve söz konusu kuvvet kullanma yasağının bir

---

[310]Ruys, **'Armed Attack' and the Article 51 of the UN Charter**, s. 493; aynı yönde bkz: Pirim, **a.g.m**, s. 273.

[311]International Court of Justice (ICJ), *Advisory Opinion Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 9 Temmuz 2004, para. 139; Lakin söz konusu kararda Yargıç Higgins ayrı görüşünde, Birleşmiş Milletler Şartı'nın 51. maddesinde meşru müdafaanın sadece bir devlet tarafından silahlı saldırı gerçekleştirilmesi halinde söz konusu olacağına dair bir düzenleme bulunmadığını belirtmiş (Separate opinion by Judge Higgins para 33); aynı doğrultuda Yargıç Kooijmans'ın ayrı görüşünde ve Yargıç Buergenthal'in ayrı bildirisinde de her ne kadar 50 yılı aşkın süredir meşru müdafaa hakkının kullanımının başka bir devlet tarafından gerçekleştirilen bir silahlı saldırının mevcudiyetine dayanması gerektiği şeklinde bir uygulama benimsenmiş olsa da Birleşmiş Milletler Güvenlik Konseyi'nin 12 Eylül 2001 tarih ve 1368 sayılı Kararı'na atıfla meşru müdafaa kavramına ilişkin yeni bir yaklaşımın doğduğuna dikkat çekilmiş; Uluslararası Adalet Divanı'nın bu yeni unsuru göz önüne almadığı eleştirisinde bulunulmuştur. (Separate opinion by Judje Kooijmans para. 35; Separate declaration of Judge Buergenthal para. 133)

[312]Délégation à l'information et à la Communication de la Defense, **International Law Applied to Operations in Cyberspace**, *https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf*, s. 8-9, (erişim tarihi: 20.05.2020)

devletin başka bir devlete karşı kuvvet kullanmasına dair olduğu dikkate alındığında, devlet dışı aktörlere karşı kuvvet kullanılmasına ilişkin bir yasak bulunmadığı, dolayısıyla da bu kapsamda gerçekleştirilecek eylemlerin meşru müdafaa hakkına dayandırılmasının gerekmediği sonucuna ulaşılabilecektir[313].

Devlet dışı aktörlerin de yıkıcı etki doğurmaya elverişli saldırgan siber operasyonlara başvurabileceği değerlendirildiğinde konunun siber operasyonlar açısından da mühim olduğu söylenebilmektedir[314]. Yine de devlet dışı aktörlerce gerçekleştirilen saldırgan siber operasyonlar yorumlanırken yukarıda özetlenen ilkeler çerçevesinde hareket edilmelidir. Bu kapsamda bizim de katıldığımız çoğunluk görüşüne göre herhangi bir devletin desteği olmaksızın devlet dışı aktörlerce gerçekleştirilen siber operasyonlar uluslararası hukuk kapsamında silahlı saldırı teşkil etmeyecektir[315]. Dolayısıyla devlet dışı bir aktör tarafından gerçekleştirilen siber operasyon kapsamında meşru müdafaa hakkının kullanılması ancak söz konusu siber operasyonun bir devlete atfedilebilmesi halinde mümkün olacaktır[316].

2.4.5. Saldırgan Siber Operasyonlar ve Kolektif Meşru Müdafaa

Birleşmiş Milletler Şartı'nın 51. maddesi açıkça, devletlerin sadece bireysel değil kolektif olarak da meşru müdafaa haklarını kullanabileceklerini belirtmiştir. Kolektif meşru müdafaanın yukarıda özetlenen ilkeler doğrultusunda

---

[313]Olivier Corten, "The Unwilling or Unable" Test: Has it Been, and Could it be Accepted?", **Leiden Journal of International Law**, Vol. 29, 2016, (777–799), s. 795; Elbette bu kapsamda bir yaklaşım uygulamada bir devletin bölgesi üzerinden başka bir devlete saldırı gerçekleştiren devlet dışı aktörlerle nasıl mücadele edeceğine yönelik tartışmalara da yol açabilecektir. Bu kapsamda Deeks, "isteksiz ya da aciz devlet" görüşü uyarınca bir devletin başka bir devletin bölgesinde yapılanmış bir devlet dışı aktörün saldırısına uğraması ve saldırının kaynaklandığı devletin söz konusu tehdidi ortadan kaldırmaya gücünün yetmemesi yahut isteksiz olması durumunda meşru müdafaa kapsamında kuvvet kullanılabileceğini ileri sürmektedir. (Ashley S. Deeks, "Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-Defense", **Virginia Journal of International Law**, vol. 52, no. 3, 2012, (483-550), s. 487) Nitekim bu yaklaşımın birçok devlet tarafından da benimsendiği gözlemlenmektedir. (Pirim, **a.g.m**, ss. 285-86)

[314]Lahmann, **a.g.e**, s. 61-62.

[315]Delerue, **Cyber Operations and International Law**, s. 338-39; Öte yandan Schmitt, devletlerin devlet dışı aktörlerin dahil olduğu eylemlerde silahlı saldırı kavramına başvurma yatkınlığı sebebiyle devlet dışı aktörlerce gerçekleştirilen siber operasyonların silahlı saldırı eşiğine erişmesi halinde saldırıya maruz kalan devlet tarafında meşru müdafaa hakkı kapsamında karşılık verilmesinin oldukça olası olduğunu savunmuştur. (Michael N. Schmitt, "Cyber Operations and the Jus ad Bellum Revisited", **Villanova Law Review**, vol. 56, issue 3, 2011, (569-606) s. 601.

[316]Devlet dışı aktörlerin gerçekleştirdiği saldırgan siber operasyonların devlete atfedilmesi hususu çalışmanın 3. bölümünde incelenecektir.

gerçekleştirilmesi gerektiği hususu net olmakla birlikte, bir devletin hangi koşullarda kolektif meşru müdafaa kapsamında başka bir devlete yardım edebileceği hususu nispeten daha tartışmalıdır[317].

Teorik olarak kolektif meşru müdafaa ile bir devletin başka bir devletin hükümeti tarafından herhangi bir dış müdahaleye karşı destek sağlaması amacıyla davet edilmesi arasında fark bulunsa dahi uygulamada ikisi arasındaki ayrımı yapmak her zaman kolay olmamaktadır[318]. Uluslararası Adalet Divanı Nikaragua Kararı'nda, saldırıya maruz kalan devletin talebi olmaksızın kolektif meşru müdafaa kapsamında kuvvet kullanılmasına izin veren bir kuralın mevcut olmamasına dayanarak, üçüncü bir devletin kolektif meşru müdafaa amacıyla kuvvet kullanmasının mağdur devletin silahlı saldırıya uğradığını ilan etmesi ve söz konusu devletten yardım talep etmesi şartlarına bağlı olduğunu açıklamıştır[319]. Yargıç Jennings ise muhalefet şerhinde, kolektif meşru müdafaanın bir devleti koruma bahanesiyle kuvvet kullanılması gibi kötüye kullanımlara açık olması sebebiyle çeşitli sınırlamalar öngörülmesinin isabetli olduğuna katılmakla birlikte Uluslararası Adalet Divanı'nın sergilediği şekilci yaklaşımı eleştirmiş; saldırıya maruz kalan devletin kendisini bir saldırının mağduru "ilan etmesi" ve üçüncü devletin yardımı için resmi olarak talepte bulunmasının "zorunluluk" olarak şart koşulmasının bazı koşullarda gerçekçi bir beklenti olmayacağı tespitinde bulunmuştur[320]. Benzer eleştiriler doktrinde de ileri sürülmüş; hatta kolektif meşru müdafaa hakkının esasında yardımda bulunan devlet lehine bir hak olarak yorumlanması gerektiği dahi ileri sürülmüştür[321]. Öte yandan UAD'nin yaklaşımının saldırıya maruz kalan bir devletin rızası hilafına kuvvet kullanılması ihtimalini önlemek açısından gerekli olduğu ve eleştirilerin aksine söz konusu

[317]Ronald St. J. Macdonald, "The Nicaragua Case: New Answers to Old Questions?", **The Canadian Yearbook of International Law**, vol. 124, 1986, (127-160), s. 146.
[318]Gray, **International Law and the Use of Force**, s. 168.
[319]*Nikaragua Davası Kararı*, para. 196-99, 232.
[320]Dissenting Opinion of Judge Sir Robert Jennings, ss. 544-45; Yargıç Schwebel de benzer bir şekilde, kolektif meşru müdafaa kapsamında üçüncü bir devletten destek edinmek için bir devletin silahlı saldırıya uğradığını ilan etmesi ve resmi olarak yardım talep etmesine yönelik bir sınırlama bulunmadığını ve meşru müdafaa kapsamında gerçekleştirilen eylemlere ilişkin derhal Birleşmiş Milletler Güvenlik Konseyi'ni bilgilendirme yükümlülüğünün de tek başına böylesi bir sınırlamaya sebep teşkil etmek için yeterli olmadığı eleştirisinde bulunmuştur. (Dissenting Opinion of Judge Schwebel, para. 191.)
[321]Macdonald, **a.g.m**, s. 151.

yaklaşımın katı bir şekilcilikle mağdur devletten saldırıya uğradığının ilanı ile üçüncü bir devletten resmi olarak kolektif meşru müdafaa için destek talebinde bulunulması gerektiği olarak yorumlanması gerekmediği tespitinde bulunulabilecektir[322].

Kolektif meşru müdafaa hakkının kullanılabilmesinin, saldırıya maruz kalan devlet ile yardımda bulunan devlet arasında önceden mevcut bir antlaşmanın varlığına bağlı olup olmadığı da tartışılmış; devlet uygulaması ise böyle bir antlaşmanın varlığının kolektif meşru müdafaanın uygulanması için bir kıstas olarak öngörülmediğini, tarafların *ad hoc* bir uzlaşı ile de kolektif meşru müdafaaya başvurabileceğinin benimsendiğini göstermiştir[323]. Dolayısıyla bir devletin başka bir devlete silahlı saldırıda bulunması halinde saldırıya maruz kaldığı kanaatinde olan devlet, yukarıda incelenen meşru müdafaanın genel ilkeleriyle uyumlu bir şekilde, meşru müdafaa hakkını üçüncü bir devlet veya devletlerle birlikte kullanabilecektir.

Belirli özellikleri haiz siber operasyonların silahlı saldırı eşiğine erişebildiği dikkate alındığında, devletlerin saldırgan bir siber operasyona yönelik bireysel meşru müdafaanın yanı sıra kolektif meşru müdafaaya da başvurabileceği kanaatindeyiz. Zira kolektif meşru müdafaa hakkı tanınırken saldırıda kullanılan yöntemlere ilişkin bir ayrımda bulunulmamıştır[324]. Nitekim aktif olarak varlığını sürdüren en büyük askeri ittifak olan NATO da saldırgan siber operasyonlara yönelik olarak kolektif meşru müdafaaya başvurulabileceğini beyan etmiştir[325]. Dolayısıyla saldırgan bir siber operasyonun üye devletlerden birine yönelik bir silahlı saldırı teşkil edip etmediği her olay özelinde incelenecek; bir müttefiğin bu kapsamda talebi halinde ve diğer üye devletlerin konuya ilişkin oybirliğiyle karar alması durumunda söz konusu siber operasyona yönelik kolektif meşru müdafaaya başvurulabilecektir[326].

---

[322]Gray, **International Law and the Use of Force**, ss. 185-86.
[323]Dinstein, **War, Aggression and Self Defence**, ss. 281-82; NATO CCD COE, **Tallinn Manual 2.0**, s. 355.
[324]Dinstein, **Computer Network Attacks and Self-Defense**, s. 112
[325]North Atlantic Treaty Organization, **NATO Summit Guide**, Brüksel, 11-12 Temmuz 2018, s. 35, *https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180718_180711-summit-guide-brussels.pdf*, (erişim tarihi: 04.08.2020)
[326]Katharina Ziolkowski, "NATO and Cyber Defence", **Research Handbook on International Law and Cyberspace**, Ed: Nicholas Tsagourias / Russell Buchan, Edward Elgar Publishing, 2015, (426-446), s. 435.

2.4.6. Meşru Müdafaaya İlişkin Birleşmiş Milletler Güvenlik Konseyi'ni Bilgilendirme Yükümlülüğü

Birleşmiş Milletler Şartı'nın 51. maddesi uyarınca, meşru müdafaa hakkını kullanan devletler bu kapsamda aldıkları önlemleri hemen Güvenlik Konseyi'ne bildirmelidir. Söz konusu düzenlemenin devletlere bir zorunluluk mu yüklediği yoksa Güvenlik Konseyi'nin silahlı saldırıya yönelik etkili önlemler alarak çatışma ortamının bir an önce sonlandırılması niyetiyle yer verilen usuli bir düzenleme mi olduğu hususu tartışmalıdır[327].

Dinstein, saldırgan bir siber operasyona karşı meşru müdafaa hakkı kapsamında kuvvet kullanan bir devletin Güvenlik Konseyi'ni konuya ilişkin bilgilendirmemesinin meşru müdafaa hakkına başvurmasının engellenmesi gibi vahim sonuçları olabileceğini belirtmiştir[328]. Öte yandan baskın olan görüşe göre, saldırıya uğrayan bir devletin Güvenlik Konseyi'ne bildirim yükümlülüğünü ihlal etmiş olması tek başına meşru müdafaa hakkından yoksun bırakılmasına dayanak teşkil etmeyecektir[329]. Zira Yargıç Schwebel'in Nikaragua Davası Kararı'ndaki ayrı görüşünde isabetli bir şekilde açıkladığı üzere; söz konusu düzenleme Güvenlik Konseyi'nin yetkilerini zamanında kullanabilmesi açısından öngörülmüş olup her ne kadar ihlali önem taşısa dahi, ilgili hükmün usuli bir nitelik taşıması sebebiyle, bir devleti meşru müdafaa hakkı doğrultusunda hareket etmekten alıkoymayacaktır[330].

2.5. Saldırgan Siber Operasyonların Güncel Örnekler Üzerinden *Jus ad Bellum* Kapsamında Değerlendirilmesi

Çalışmanın önceki bölümlerinde saldırgan siber operasyonlar jus ad bellum çerçevesinde genel olarak incelenmiştir. Bu bölümde ise saldırgan siber operasyonlar güncel örnekler üzerinden gerçekleştiriliş amaçlarına göre incelenecektir. Bu kapsamda sırasıyla gizli verilere izinsiz erişimin sağlanmasıyla gerçekleştirilen siber

---

[327]Donald W. Greig, "Self-Defence and the Security Council: What Does Article 51 Require?", **The International and Comparative Law Quarterly**, vol. 40, no. 2, 1991, (366-402), s. 367.
[328]Dinstein, **Computer Network Attacks and Self-Defense**, s. 113
[329]Roscini, **Cyber Operations and the Use of Force in International Law**, ss. 103-04; NATO CCDCOE, **Tallinn Manual 2.0**, s. 356.
[330]Dissenting Opinion of Judge Schwebel, s. 376, para. 227.

casusluk (*cyber espionage*); siber casusluk ile elde edilen verilerin paylaşılmasıyla işlenen siber faydalanma (*cyber exploitation*); özellikle bir devletin seçmenlerini etkileyerek siyasi seçimlerinin sonucuna müdahale etme gibi amaçlarla gerçekleştirildiği deneyimlenen siber sosyal mühendislik; bir siber sistemin işlerliğini bozan siber operasyonlar ve son olarak da fiziksel zarara yol açan siber operasyonlar incelenecektir. Yukarıda sayılan saldırgan siber operasyonlar değerlendirilirken öncelikle çalışmanın önceki bölümlerinde açıklanan yaklaşımlar uyarınca söz konusu siber operasyon yönteminin kuvvet kullanma veya kuvvet kullanma tehdidinde bulunma yasağını ihlal edip etmediği tartışılacak; kuvet kullanma eşiğine erişen saldırgan siber operasyonlar ise ayrıca silahlı saldırı teşkil edip etmemesi açısından incelenecektir. Kuvvet kullanma eşiğine erişmeyen siber operasyonların ise içişlerine karışma yasağını ihlal edip etmediği değerlendirilecektir. Söz konusu incelemeler yapılırken yakın geçmişte karşılaşılmış örnekler üzerinden hareket edilecektir.

2.5.1. Siber Operasyonlar Aracılığıyla Gizli Verilere İzinsiz Erişim (Siber Casusluk)

Çalışma kapsamında siber operasyonlar *jus ad bellum* açısından incelendiğinden bu kısımda barış zamanı siber casusluk faaliyetleri incelenecektir. Keza siber casusluk terimi ile kastedilen devlet destekli siber casusluk faaliyetleri olup atfedilebilirlik hususu ilerleyen bölümlerde inceleneceğinden, bu başlık altında ayrıca atfedilebilmeye ilişkin tartışmalara yer verilmeyecektir. Aynı şekilde çalışmanın kapsamı *jus ad bellum* ile sınırlı olduğundan, siber casusluk faaliyetlerinin özel şahıs veya şirketler açısından yaratabileceği fikri ve sınai hak ihlalleri ile başta kişisel verilerin korunması ve özel hayatın gizliliği olmak üzere, olası insan hakları ihlalleri tartışılmayacak olup bunun amacı siber casusluk faaliyetlerinin söz konusu alanlarda ihlallere yol açabileceğini reddetmek değil, çalışmanın amaçlarına erişebilmesi için esas konusunu teşkil eden alanların derinlemesine incelenmesinin tercih edilmesidir.

Siber casusluk "*bilgi toplamak amacıyla başka bilgisayarlara, bilgisayar sistemlerine yahut şebekelere, erişilen sistemin işlerliğine yahut içerdiği verilere zarar*

vermeksizin sağlanan izinsiz erişim" olarak tanımlanabilir[331]. Siber casusluk elektronik olarak iletilen yahut depolanan iletişim, veri ve diğer bilgilerin siber sistemler aracılığıyla gizlice denetlenmesi, gözlenmesi veya elde edilmesine yönelik her türlü faaliyeti kapsamaktadır[332]. Keza siber casusluk faaliyetlerinin daha büyük ölçekli bir operasyon için modern keşif yöntemi olarak değerlendirilmesi ihtimali de mevcuttur[333].

Siber casusluğun en bilinen örnekleri olarak *Moonlight Maze* (Mehtap Labirenti) ve *Titan Rain* (Titan Yağmuru) olarak isimlendirilen operasyonlar sayılabilir[334]. Bu operasyonların ilki olan Moonlight Maze'in Rusya Federasyonu'nun desteğiyle icra edilen bir istihbarat operasyonu olduğu iddia edilmiş; o zamana dek gerçekleştirilen en kapsamlı siber casusluk faaliyeti olan operasyon ile ABD Savunma Bakanlığı, ABD Enerji Bakanlığı, ABD Ulusal Havacılık ve Uzay Dairesi (*National Aeronautics and Space Administration* – "NASA"), askeri yükleniciler ve askeri bağlantılı sivil üniversitelerden bir yılı aşkın süre boyunca yüklü miktarda hassas veri ele geçirilmiştir[335]. Benzer bir şekilde Titan Rain, 2002'de başlayan ve ABD Savunma Bakanlığı'nı hedef alan siber casusluk faaliyetleri için kullanılan gayrı resmi adlandırmadır[336]. Titan Rain olarak adlandırılan siber casusluk faaliyetleri sonucunda da askeri laboratuvarlardan elde edinilenleri de içeren, hükümete ait pek çok bilgi elde edilmiştir[337]. Görüldüğü üzere, siber operasyonlar diğer yöntemlere kıyasla çok daha az riskle çok daha etkili casusluk faaliyetlerinin gerçekleştirilmesine olanak

---

[331] Roscini, **Cyber Operations and the Use of Force in International Law** s. 65.
[332]NATO CCD COE, **Tallinn Manual 2.0**, s. 168.
[333]Michael Gervais, "Cyber Attacks and the Laws of War", **Berkeley Journal of International Law**, Vol. 30, 2012, (525-579), s. 535.
[334]Arie J. Schaap, "Cyber Warfare Operations: Development and Use under International Law", **Air Force Law Review**, Volume 64, 2009, (121-173), s. 141.
[335]Joyner / Lotrionte, **a.g.e**, ss. 840-841
[336]Jeffrey Carr, **Inside Cyber Warfare: Mapping the Cyber Underworld**, ABD, 2. Bası, O'Reilly, 2011, s. 4; Her ne kadar söz konusu siber casusluk faaliyetleri NATO'nun 1999'da yanlışlıkla Çin Halk Cumhuriyeti'nin ("ÇHC") Belgrad büyükelçiliğini bombalaması ile ilişkilendirilmişse de ÇHC hükümeti saldırının kendisine atfedilmesini kabul etmeyerek herhangi bir şekilde bahsi geçen siber operasyonlara dahil olmadıklarını iddia etmiştir. (Ralph D. Berenger, "Cyber Warfare", **Encyclopedia of Research on Cyber Behavior**, Ed: Zheng Yan, Volume I, IGI Global, 2012, (1074-1088), s. 1079)
[337]Alexander Melnitzky, "Defending America against Chinese Cyber Espionage Through the Use of Active Defenses", **Cardozo Journal of International and Comparative Law**, Vol. 20, No. 2, 2012, (537-570), s 544.

tanımaktadır[338]. Öte yandan öğretide kimi yazarlar tarafından, geleneksel casusluk faaliyetleri istihbarat ajanlarının gizli bilgilere erişmek amacıyla başka bir devletin egemenlik sahasına girmesini gerektirmekteyken, siber casusluk faaliyetlerinin siber alanda gerçekleştirilmesi sebebiyle başka bir devletin egemenlik sahasına girilmesi gerekmediğinden, bunların farklı bir değerlendirmeye tabi tutulması lüzumu ileri sürülmüştür[339]. Her ne kadar siber casusluk için, geleneksel anlayışla bir sınır ihlali zorunlu olmasa dahi yukarıda açıklandığı üzere siber alan, fiziki de dahil olmak üzere, üç farklı katmandan oluştuğundan ve devletlerin siber alanda faydalandıkları varlıklar üzerinde de egemenlik hakları bulunduğundan böyle bir ayrıma ihtiyaç olmadığı kanaatindeyiz.

Öğretide kimi yazarlarca, siber casusluk amacıyla kullanılan kötücül yazılımların sonradan kolaylıkla daha yıkıcı sonuçlar için kullanılabileceği gibi siber casusluk faaliyetlerinin de tek başına ağır sonuçları olduğu göz önünde bulundurularak bu tip siber operasyonların olası bir silahlı saldırı olarak değerlendirilip meşru müdafaaya yol açabileceği iddia edilmiştir[340]. Bu kapsamda özellikle hedef odaklı yaklaşım uyarınca, bir devlet için büyük öneme sahip gizli bilgiler ile her türlü askeri nitelikteki bilgiye yönelik siber casusluk faaliyetlerinin kuvvet kullanma yasağını ihlal edeceği; hatta siber casusluk operasyonunun bir devletin ulusal kritik altyapısını hedef alması halinde silahlı saldırı dahi teşkil edebileceği savunulmuştur[341]. Lakin yukarıda yer verilen siber casusluk tanımdan da anlaşılacağı üzere, siber casusluk operasyonları sırasında hedef verilere erişim sağlanmasının yeterli olması ve bu amacın yıkıcı bir etki yaratılmaksızın gerçekleştirilebilmesi sebebiyle baskın olan görüş siber casusluğun diğer saldırgan siber operasyonlardan ayrıldığı yönündedir[342]. Zira etki

---

[338]Philip Pool, "War of the Cyber World: The Law of Cyber Warfare", **The International Lawyer**, Vol. 47, No. 2, 2013, (299-323), s. 306.
[339]Russell Buchan, "Cyber Espionage and International Law", **Research Handbook on International Law and Cyberspace**, Ed: Nicholas Tsagourias & Russell Buchan, Edward Elgar Publishing, 2015, (168-190), s. 181.
[340]Melnitzky, **Defending America against Chinese Cyber Espionage Through the Use of Active Defenses**, ss. 565-66.
[341]Katharina Ziolkowski, "Peacetime Cyber Espionage – New Tendencies in Public International Law", **Peacetime Regime for State Activities in Cyberspace**, Ed: Katharina Ziolkowski, Tallinn, NATO CCD COE Publications, 2013, (425-465), s. 454
[342]Herbert S. Lin, "Offensive Cyber Operations and the Use of Force", **Journal of National Security Law & Policy**, Vol. 4, 2010, (63-86), s. 64; Marco Roscini, "*Cyber Operations as a Use of Force*",

odaklı yaklaşım uyarınca siber casusluk operasyonları değerlendirildiğinde, bu tip siber operasyonların fiziksel bir zarara yol açmadığından kuvvet kullanma eşiğine erişmediği tespitinde bulunulabilecektir[343]. Keza siber casusluk operasyonlarının, ulusal kritik altyapıya yöneltilse bile, kural olarak bu sistemler üzerinde herhangi bir aksamaya yol açmayacağı düşünüldüğünde sonuç odaklı yaklaşımın diğer yaklaşımlarla birlikte değerlendirilmesi halinde de siber casusluk operasyonlarının tek başına kuvvet kullanma yasağını ihlal etmediği sonucuna ulaşılabilmektedir[344]. Siber casusluk operasyonlarının kuvvet kullanma eşiğine erişmediği dikkate alındığında bu tip operasyonların saldırı yahut silahlı saldırı da teşkil etmeyeceği kabul edilmelidir. Her ne kadar çalışma kapsamında siber operasyonların *jus ad bellum* açısından incelenmesi hedeflenmişse de siber operasyonların kuvvet kullanma eşiğine erişmesi tek başına söz konusu siber operasyonun uluslararası hukuka uygun olduğu anlamına gelmemektedir. Zira içişlerine karışma yasağı, devletin ülkesel bütünlüğünün yanı sıra politik bütünlüğünü de koruduğundan, devletin müdahalede bulunulan konuya ilişkin münhasır bir yetkisi bulunduğu ve müdahalenin zorlayıcılık unsurunu haiz olduğu takdirde siber casusluğun yasağın ihlali olduğu düşünülebilecektir.

Öncelikle belirtmek gerekir ki siber casusluk faaliyetleri uluslararası hukukun içişlerine karışma yasağı kapsamı dışında bir normunun ihlali niteliği taşıdığı durumda doğal olarak uluslararası hukuka aykırı hale gelecektir. Nitekim herhangi bir sözleşme ile güvence altına alınmış bir veriye yönelik gerçekleştirilen siber casusluk operasyonu, söz konusu sözleşme hükümlerinin ihlali anlamına geleceğinden

---

Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, Ed: Katharina Ziolkowski, Tallinn, NATO CCD COE Publication, 2013, (233-255), s. 241

[343]Ziolkowski, **Peacetime Cyber Espionage – New Tendencies in Public International Law**, ss. 451-52; Elbette siber casusluk operasyonları sırasında yürütülen faaliyetlerin gizli verilere izinsiz erişimin ötesinde bir etkiye yol açması halinde, söz konusu operasyonun gerçekleştirilişi sebebiyle ortaya çıkan diğer etkilerin kuvvet kullanma teşkil etmesi sonucu doğabilecektir. (NATO CCD COE, **Tallinn Manual 2.0**, s. 355.)

[344]Siber casusluk operasyonları araç odaklı yaklaşım uyarınca incelendiğinde de casusluğa ilişkin kullanılan araçların silah olmaması sebebiyle söz konusu operasyonların kuvvet kullanma eşiğine erişmediği sonucuna ulaşılabilmektedir. Her ne kadar hedef odaklı yaklaşım açısından mesele değerlendirildiğinde, bir devletin ulusal kritik altyapısına yöneltilen siber casusluk faaliyetlerinin kuvvet kullanma eşiğine eriştiği söylenebilecekse de ilgili bölümde açıklandığı üzere böyle bir yaklaşım siber operasyonların uluslararası hukuk açısından durumunu tahlil etmek için fazla kapsayıcı olduğundan reddedilmiştir.

uluslararası hukuka aykırılık teşkil edecektir[345]. Eklemek gerekir ki siber casusluğun yukarıda örneklendirildiği üzere uluslararası hukuk sözleşmelerinin açık hükmü uyarınca yasaklandığı hallerin yanı sıra yerleşmiş genel ilkelerle çatıştığı durumlarda da uluslararası hukuka aykırılık iddiaları gündeme gelebilecektir[346]. Lakin siber casusluk faaliyetlerinin uluslararası hukuk tarafından korunan herhangi bir ilkeyi ihlal etmediği hallerde de uluslararası hukuka aykırılık teşkil edip etmeyeceği hususu tartışılmalıdır[347]. Nitekim casusluk faaliyetlerinin, gerçekleştiriliş araçlarına ilişkin bir ayrım yapmaksızın, yerel yasalarla cezalandırılsa dahi uluslararası teamül hukuku

[345]Örneğin, uluslararası teamül hukukunun bir parçası haline gelen 1967 tarihli Diplomatik İlişkiler Hakkında Viyana Sözleşmesi'nin 24. maddesi uyarınca, diplomatik misyonun arşivleri ve evraklarının nerede bulunursa bulunsun her zaman dokunulmazlığı haiz olduğu öngörülmüş; 27(2) maddesi uyarınca da diplomatik misyona ve görevlerine ait her türlü yazışmanın ihlali yasaklanmıştır. (United Nations, Vienna Convention on Consular Relations, 24 April 1963) Doktrinde sözleşme kapsamında yer verilen yasağın sadece kabul eden devlet tarafından gönderen devletin diplomatik misyonuna karşın gerçekleştirilebilecek operasyonlar açısından bağlayıcılık taşıdığı öne sürülerek üçüncü devletler tarafından gerçekleştirilecek siber casusluk faaliyetlerinin bu kapsamda değerlendirilemeyeceği görüşü de savunulmuştur. (Ziolkowski, **Peacetime Cyber Espionage – New Tendencies in Public International Law**, s. 444.) Keza benzer bir şekilde 1982 tarihli Birleşmiş Milletler Deniz Hukuku Sözleşmesi'nin 19 (2) numaralı maddesinin c bendinde karasularında zararsız geçiş sırasında kıyı devletinin savunma ve güvenliğinin zararına olarak bilgi toplamayı amaçlayan her türlü hareket yasaklanmıştır. (UN General Assembly, Convention on the Law of the Sea, 10 December 1982) Söz konusu yasağın bilgi toplama faaliyetlerinin gerçekleştirme yöntemine ilişkin bir sınırlamaya yer vermeksizin her türlü hareketi yasak kapsamına aldığı değerlendirildiğinde, zararsız geçiş hakkını kullanan bir devletin bu sırada siber casusluk girişiminde bulunmasının ilgili maddenin ihlali anlamına geleceği tespit edilebilecektir.

[346]Örneğin Uluslararası Adalet Divanı, Avustralya'nın temsilcileri tarafından Doğu Timor'a ait uluslararası hukuk kapsamında korunduğu iddia edilen belgeler, veri ve diğer mülkiyete 3 Aralık 2013 tarihinde el koyulmasından kaynaklanan uyuşmazlığa dair verdiği Belirli Belgelere ve Verilere El Koyulması ve Tutulmasına İlişkin Sorular kararında, Doğu Timor'un Avustralya'nın müdahalesi olmaksızın tahkim süreci ve müzakerelerini yürütme ve yasal danışmanlarıyla gizlilik içerisinde iletişim kurma haklarının ihlali iddialarını makul bularak Avustralya'nın Doğu Timor'un yasal danışmanları ile devam etmekte olan tahkim sürecine ilişkin iletişimine müdahil olmaması gerektiğini belirtmiştir. (*Questions relating to the Seizure and Detention of Certain Documents and Data, Timor-Leste v Australia*, Order on Provisional Measures, ICGJ 472 (ICJ 2014), 3rd March 2014, United Nations [UN]; International Court of Justice [ICJ] , para 1, 28, 55.) Bu kapsamda benzer bir sonuca siber casusluk açısından da ulaşmak mümkün olup Avustralya tarafından söz konusu belgelere siber operasyonlar aracılığıyla erişildiği takdirde de uluslararası hukuk ihlalinin vuku bulacağı savunulabilecektir.

[347]Doktrinde bir görüş tarafından, uluslararası hukukun savaş sırasında casusluk faaliyetlerine açıkça izin verirken barış zamanında gerçekleştirilen casusluk faaliyetleri hususunda sessiz kaldığı dikkate alınarak barış zamanında casusluk faaliyetlerinin uluslararası hukuka aykırı olduğu ileri sürülmüştür. (Jared Beim, "Enforcing a Prohibition on International Espionage", **Chicago Journal of International Law**, Vol. 18, 2018, (647-672), s. 653) Uluslararası Daimi Adalet Divanı'nın S.S. Lotus Davası'nda verdiği karar ile devletlerin gerçekleştirdiği faaliyetlerin uluslararası hukuka uygun olarak değerlendirilebilmesi için açıkça onaylanması gerekmediği, aksine devletlerin uluslararası hukuk tarafından yasaklanmayan hususlarda irade serbestisi bulunduğu yönündeki tespiti dikkate alındığında bu görüşe katılmak mümkün gözükmemektedir. (*Lotus (France v Turkey)* [1927] PCIJ Rep, Series A, No 10, s. 18)

tarafından yasaklanmadığı görüşü geniş anlamda kabul görmüştür[348]. Hatta birçok devlet mevzuatında güvenlik güçlerini, siber casusluk da dahil olmak üzere, casusluk faaliyetlerine başvurulması hususunda yetkilendirmiştir[349]. Kaldı ki casusluk faaliyetinin gerçekleşmesi için gizli bilginin edinilmesi yahut bir şekilde gizli bilgiye erişilmesi yeterli olup, elde edilen bilginin nasıl değerlendirildiği faaliyetin casusluk olarak kabulünde bir etken olmadığından, siber casusluğun tek başına bir devlet üzerinde baskı aracı olmadığı tespiti yapılabilecek; dolayısıyla içişlerine karışma yasağının zorlayıcılık unsurunun mevcut olmaması nedeniyle de salt siber casusluk faaliyetleri ile ilgili yasağın ihlal edilmediği sonucuna ulaşılabilecektir[350]. Nitekim devletlerin, başta siber alanda yürütülenler olmak üzere, casusluk faaliyetlerine kendilerine avantaj sağlama ihtimali olan bilgileri gizlice edinme amacıyla başvurduğu düşünüldüğünde, siber casusluk ile hedef devlet üzerinde baskı kurmanın hedeflenmediği, aksine hedef devletin bu durumdan haberdar olmamasının tercih edileceği çıkarımında bulunulabilir[351]. Elbette siber casusluk faaliyetleri her ne kadar uluslararası hukuka aykırı olmasa da devletler bu tip faaliyetlerin dostça olmaması sebebiyle, siber casusluk operasyonlarını gerçekleştiren devletin diplomatının sınır dışı edilmesi gibi yine hukuka uygun ancak dostça olmayan bir şekilde karşılık verebilecektir[352].

---

[348]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 66; Öte yandan Wright, barış döneminde gerçekleştirilen casusluk faaliyetlerinin bir devlet ajanının başka bir devletin bölgesine yerel yasalara aykırı bir şekilde sızması anlamına geldiğinden, uluslararası hukukun diğer devletlerin bölgesel bütünlük ve politik bağımsızlığına saygı duyma görevinin de ihlalini oluşturduğunu savunmuştur. (Quincy Wright, "Espionage and the Doctrine of Non-Intervention in Internal Affairs", **Essays on Espionage and International Law**, Ed: Roland J. Stanger, Ohio State University Press, 1962, (3-28) s. 12) Delupis de benzer bir şekilde barış zamanı gerçekleştirilen casusluk faaliyetlerinin yabancı bir güç tarafından gönderilen ajanların gizlice başka bir devletin bölgesinde bulunması halinde uluslararası hukuka aykırı olacağını ifade etmiştir. (Ingrid Delupis, "Foreign Warships and Immunity for Espionage", **The American Journal of International Law**, Vol. 78, No. 1, 1984, (53-75), s. 67.) Her iki yazar da casusluğu geleneksel yöntemler açısından değerlendirirken, Pun siber casusluk faaliyetlerinin başka bir devletin egemenlik sahasına girilmeksizin elektronik ortamda uzaktan gerçekleştirilebilmesi sebebiyle birtakım belirsizliklere yol açabileceğini belirtmiştir. (Darien Pun, "Rethinking Espionage in the Modern Era", **Chicago Journal of International Law**, Vol. 18 No. 1, 2017, (353-391), s. 384.) Ancak yukarıda açıklanan sebeplerle biz bu yönde bir ayrım yapılması gerektiğini düşünmemekteyiz.

[349]NATO CCD COE, **Tallinn Manual 2.0**, s. 169

[350]Russell Buchan, "The International Legal Regulation of State-Sponsored Cyber Espionage", **International Cyber Norms: Legal, Policy & Industry Perspectives**, Ed: Anna-Maria Osula / Henry Roigas, Tallinn, NATO CCD COE Publications, 2016, (65-86) s. 80

[351]Ziolkowski, **Peacetime Cyber Espionage – New Tendencies in Public International Law**, s. 454.

[352]Dinstein, **Computer Network Attacks and Self-Defense**, s. 101.

2.5.2. Siber Casusluk ile Edilen Verilerin İfşası (Siber Faydalanma)

Siber alanda ele geçirilen bilgilerin bir çeşit "şantaj" amacıyla kullanılması oldukça yaygın olup bu kapsamda siber casusluk faaliyetleri gerçekleştirilen siber operasyonun hazırlık hareketi yahut bileşik eylemin ayrılmaz parçası olarak değerlendirilebileceğinden ayrıca incelenmesi gereketiği kanaati hâsıl olmuştur[353].

Bu tip saldırgan siber operasyonların en bilinen örneği, 24 Kasım 2014 tarihinde kendilerini *Guardians of Peace* "GoP" olarak adlandıran bir grubun Amerika Birleşik Devletleri'nde yerleşik Sony Pictures Entartainment ("Sony PE") isimli bir özel şirketi *hack*leyerek[354] içlerinde film, şirket içi yazışma, finansal kayıt, film sözleşmeleri, ünlü oyuncular hakkında kişisel bilgi ve çalışanların sağlık verileri de bulunan pek çok bilgiyi sızdırmasıdır[355]. ABD Federal Soruşturma Bürosu ("FBI") 19 Aralık 2014 tarihinde yayımlamış olduğu bildiriyle veri silmek için kullanılan kötü amaçlı yazılımın teknik analizi, siber saldırıda kullanılan altyapı ve diğer araçları değerlendirerek saldırıdan KDHC'nin sorumlu olduğu sonucuna ulaştıklarını duyurmuştur[356]. Aynı gün ABD İç Güvenlik Bakanlığı saldırının hedefinin sadece özel bir firma ve çalışanları olmadığını, ifade özgürlüğü ve yaşam tarzının hedef alındığı yorumunu paylaşmış[357]; dönemin ABD Başkanı Barack Hussein Obama ise orantılı

---

[353]Delerue, **Cyber Operations and the Use of Force in International Law**, s. 258.

[354]*Hack*, internet sitelerine saldırılarak web sayfalarının içeriğinin silinmesi, değiştirilmesi veya başka bir adrese yönlendirilmesi gibi siber saldırılar için kullanılan bir terimdir. (Gökhan Bayraktar, **Siber Savaş ve Ulusal Güvenlik Stratejisi**, Yeniyüzyıl Yayınları, 2015, s. 92.)

[355]Stephan Haggard / Jon R. Lindsay, "North Korea and the Sony Hack: Exporting Instability Through Cyberspace", **Analysis from East-West Center**, No. 117, 2015, s. 2; 8 Aralık 2014'te ise GoP, the Interview isimli filme atıfla, bölgesel barışı bozup savaşa yol açabilecek olan terör filmi olarak tanımladıkları yapımın gösteriminin acilen durdurulması çağrısında bulunmuş; bunun üzerine ertesi gün Sony PE filmin planlanan yayın tarihini iptal ettiğini açıklamıştır. (Clare Sullivan, "The 2014 Sony Hack and the Role of International Law", **Journal of National Security Law & Policy**, Vol. 8, 2016, (437-468), ss. 440-41.); Sony PE ayrıca 31 Mart 2015 tarihinde sona eren hesap dönemi için yayınlamış olduğu konsolide finansal sonuçlar raporunda, 2014 yılının kasım ayında gerçekleşen siber saldırılara ilişkin yürütülen soruşturma ve iyileştirme faaliyetleri kapsamında yapılan harcamaların yaklaşık 41 milyon ABD doları tutarında masrafa neden olduğunu açıklamıştır. (Sony Corporation, Consolidated Financial Results for the Fiscal Year Ended March 31, 2015, Tokyo, April 30, 2015, No. 15-039E, s. 5.)

[356]FBI National Press Office, Update on Sony Investigation, *https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation*, Washington, D.C, 19 Aralık 2014, (erişim tarihi: 09.03.2020)

[357]DHS Press Office, Statement By Secretary Johnson On Cyber Attack On Sony Pictures Entertainment, *https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment*, 19 Aralık 2014, (erişim tarihi: 09.03.2020) Zira söz konusu olayda, 11 Haziran 2014 tarihinde Japon Sony Şirketi'nin Amerika Birleşik Devletleri'nde yerleşik iştiraki Sony PE,

bir şekilde karşılık verileceğini ifade etmiştir[358]. Lakin KDCH söz konusu siber operasyonlardan sorumlu olduğu yönündeki iddiaları reddetmiştir[359]. Bütün bu gelişmeler sonucu Sony PE'nin maruz kaldığı siber ifşa operasyonlarının uluslararası hukuk açısından niteliği tartışma konusu olmuştur.

Her ne kadar siber sömürü operasyonlarının ekonomik olarak ağır sonuçları olabilcekse de bu tip operasyonların siber casusluktan tek farkı elde edilen verilerin kamuyla paylaşılmasıdır. Dolayısıyla siber sömürü operasyonlarının başarıya ulaşması fiziksel bir zarara yol açmasını gerektirmediğinden, etki odaklı yaklaşım uyarınca bu tip saldırgan siber operasyonların kuvvet kullanma eşiğine erişmediği, dolayısıyla silahlı saldırı teşkil etmeyeceği yorumunda bulunulabilir. Keza siber sömürü operasyonları bir devletin ulusal kritik altyapısı üzerinde ciddi hasar oluşturacak elektronik aksamalara da yol açmamaktadır. Öte yandan her ne kadar bir devletin siber alanda gizli verilere izinsiz erişim amacıyla gerçekleştirdiği kendisine atfedilebilen faaliyetler siber casusluk olarak tanımlanıp bu kapsamda gerçekleştirilen siber operasyonların içişlerine karışma yasağının zorlayıcılık unsurunu haiz olmadığından ihlal niteliği taşımadığı değerlendirilmişse de söz konusu verilerin ifşası söz konusu olduğu takdirde hedef devlet üzerinde baskı oluşturulması ihtimali doğacağından, bu hususun da ayrıca incelenmesi önem arz etmektedir.

---

yapımcılığını üstlendiği ve konu olarak Kore Demokratik Halk Cumhuriyeti ("KDHC") liderinin hayranı olduğu eğlence programının yapımcısı ve sunucusu ile temasa geçen ABD Merkezi İstihbarat Teşkilatı'nın ("CIA") bu kişilerden KDHC lideri Kim Jong-un suikasti için işbirliği talep etmesini işleyen *the Interview* (Röportaj) adlı bir mizah filmini duyurmuştur. (Arthur Charles, **Cyber Wars: Hacks that Shocked the Business World**, Kogan Page, 2018, s. 27.) Bunun üzerine KKDC Birleşmiş Milletler Daimi Temsilcisi 27 Haziran 2014 tarihinde Birleşmiş Milletler Güvenlik Konseyi'nde Birleşmiş Milletler Genel Sekreteri'ne sunmuş olduğu bir mektupla, Amerika Birleşik Devletleri'nde çekilen filmin KDHC liderinin suikastine ilişkin bölümler içerdiği; başka bir egemen devletin liderinin suikasti üzerine bir filmin yapımı ve dağıtımının terörizmin sponsorluğu ve savaş nedeni olduğunu belirterek ABD otoritelerinin filmin yapımı ve dağıtımını yasaklamak için gerekli önlemleri alması gerektiğini belirtmiştir. (United Nations, General Assembly Security Council, "Letter Dated 27 June 2014 from the Permanent Representative of the Democratic People's Republic of Korea to the United Nations Addressed to the Secretary-General," A/68/934–S/2014/451, June 27, 2014)

[358]The White House Office of the Press Secretary, Remarks by the President in Year-End Press Conference, *https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference*, 19 Aralık 2014, (erişim tarihi: 09.03.2020)

[359]Antonio DeSimone / Nicholas Horton, "Sony's Nightmare Before Christmas The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyber Space", **The Johns Hopkins University Applied Physics Laboratory LLC**, 2017, s. 14

Siber operasyonların KDHC'ne atfedilebilir olduğu varsayımından hareket edilmesi halinde, öncelikle özel bir şirket olan Sony PE'ye karşı gerçekleştirilen siber saldırının devletin ülkesel yetkisi kapsamında korunan haklarına müdahale teşkil edip etmediği tahlil edilmelidir. ABD yetkilileri saldırının hedefinin sadece özel bir şirket ve çalışanları olmadığını, ifade özgürlüğünün de saldırıdan etkilendiğini ifade etmiştir. Keza saldırının yarattığı ekonomik sonuçlar şirketin yanı sıra şirketin faaliyet gösterdiği ekonomik düzeni de etkileyebilecek seviyededir. 1965 tarihli Devletlerin İç İlişkilerine Müdahalenin Kabul Edilemezliği ile Devletlerin Bağımsızlıkları ve Egemenliklerinin Korunması Bildirisi, devletin politik, ekonomik, kültürel unsurlarına karşı gerçekleştirilen tehdit ve teşebbüsleri kınarken; 1970 tarihli BM Şartı'na Uygun Olarak Devletler Arasında İşbirliğine ve Dostça İlişkilere İlişkin Uluslararası Hukuk İlkeleri Bildirisi, herhangi bir menfaat temin etmek amacıyla zorlayıcı ekonomik, siyasi veya diğer herhangi tipteki tedbirlerin kullanılmasını veya kullanılmasının teşvik edilmesini yasaklamıştır. Sony PE örneğinde, ifade özgürlüğünün ABD'nin kültürel unsurları arasında olduğu ve siyasi saiklerle gerçekleştirilen siber operasyonlar sonucu ciddi ekonomik kayba maruz kalındığı değerlendirildiğinde, söz konusu saldırıların bu kapsamda kabul edilmesi mümkündür. Lakin siber saldırıların ABD üzerinde doğrudan yahut dolaylı olarak zorlayıcı bir etki oluşturmadığı da göz önüne alındığında gerçekleştirilen siber sömürü operasyonlarının içişlerine karışma yasağının ihlali olmadığı tespiti yapılabilecektir[360]. Sonuç olarak, siber casusluk ile elde edilen verilerin ifşa edilmesi amacıyla gerçekleştirilen siber operasyonlar kural olarak içişlerine karışma yasağı teşkil edebilmekle birlikte, bu yönde bir değerlendirmenin kabul edilebilmesi için siber operasyonların yabancı bir devletin üzerinde özgürce tasarruf edebileceği bir hususta zorlayıcı bir etki yaratacak seviyeye ulaşması gerektiği söylenebilmektedir.

2.5.3. Siber Sosyal Mühendislik

Siber sosyal mühendislik bireylerin iletişim, düşünce tarzı, güven gibi insani zaaflarından faydalanılarak güvenilir bir kaynak olarak tanıtılan kanallar aracılığıyla

[360]Delerue, **Cyber Operations and International Law**, s. 240.

çeşitli yalanlar ve sahte senaryolar üretilmesi olarak özetlenebilir[361]. Bu sayede, siber operasyonlardan faydalanılarak hedef kitlenin davranışlarının etkilenmesi amaçlanmaktadır[362]. Söz konusu siber operasyonlar, yukarıda açıklanan yöntemlerden siber casusluk ve siber casusluk aracılığıyla edinilen bilgilerin ifşasından yararlanılarak gerçekleştirilebileceği gibi siber alanda gerçekleştirilen yoğun propaganda faaliyetleri şeklinde de vuku bulabilmektedir. Öte yandan sosyal mühendislik, paylaşılan bilgilerin çarpıtılması yönüyle siber sömürü operasyonlarından ayrılmaktadır.

Siber sosyal mühendislik operasyonlarıyla her geçen gün daha çok karşılaşılmaya başlanmış; henüz 2012 senesinde Azerbaycan Birleşmiş Milletler Daimi Temsilcisi BM Genel Sekreterliği'ne sunmuş olduğu bir mektupla *Armenian Cyber Army* ("Ermeni Siber Ordusu") isimli bir grubun Ermenistan hükümetinin direktifleri ve kontrolü doğrultusunda etnik ve dini kökenli nefret, ayrımcılık ve şiddete yönlendiren siber operasyonlarından şikayetçi olmuştur[363]. Keza en büyük sosyal medya ağlarından biri olan Twitter'ın güvenlik birimi tarafından yapılan; Honduras, Suudi Arabistan ve Sırbistan hükümetlerinin direktifleri doğrultusunda hareket eden ve kendi lehlerine veya başka devletler aleyhine propaganda yapan binlerce hesabın ortadan kaldırılmasına ilişkin 2 Nisan 2020 tarihli duyurusu da daha güncel bir örnek olarak gösterilebilir[364]. Bu tip operasyonların en çok ses getiren örneği ise 2016 senesinde Amerika Birleşik Devletleri'nin başkanlık seçimlerine yönelik gerçekleştirilen ve Rusya Federasyonuna atfedilen operasyonlardır[365]. Her ne

---

[361]Ulusal Siber Olaylara Müdahale Merkezi (USOM-TRCERT), Siber Güvenliğe İlişkin Temel Bigiler, 2014, s. 12, *https://www.usom.gov.tr/dosya/1418807122-USOM-SGFF-001-Siber%20Guvenlige%20Giris%20ve%20Temel%20Kavramlar.pdf*, erişim tarihi: 05.08.2020

[362]Pascal Brangetto / Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyber Attacks in Support of Cyber Operations", **2016 8th International Conference on Cyber Conflict: Cyber Power**, Eds: Nikolaos Pissanidis / Henry Rõigas / Matthijs Veenendaal, Tallinn, NATO CCD COE Publications, 2016, (113-126), s. 115.

[363]Letter dated 6 September 2012 from the Charge d'affaires a.i. of the Permanent Mission of Azerbaijan to the United Nations addressed to the Secretary-General, UN Doc A/66/897-S/2012/687, 7 September 2012, s. 1.

[364]Twitter Safety, *https://twitter.com/TwitterSafety/status/1245682439969792005*, (erişim tarihi: 05.04.2020)

[365]Mueller iddianamesine konu olan olaya göre, 2016 ABD Başkanlık Seçimleri'ne müdahale etmek amacıyla, seçimlerde görev alan ABD kişilerinin ve kurumlarının bilgisayarlarına izinsiz olarak erişilerek gizli belgeler çalınmış ve ifşa edilmiştir. (U.S. District Court, District of Columbia, *United States v. Victor Borisovich Netyksho and Others*, 13 July 2018, para. 20,

kadar Rusya tarafından sürece dâhil olduğu inkâr edilmişse de Amerika Birleşik Devletleri istihbaratı yayınlamış olduğu rapor ile siber operasyonlar sonucu ele geçirilen belgelerin takip eden süreçte *WikiLeaks* benzeri platformlarda yayınlanmasından GRU'nun sorumlu olduğunu tespit ettiklerini beyan etmiştir[366].

Tıpkı siber casusluk ve siber sömürü operasyonları gibi siber sosyal mühendislik operasyonlarında da herhangi bir fiziksel zarara yol açılmamakta yahut bir devletin ulusal kritik altyapı sistemlerine erişim engellenmemektedir. Dolayısıyla siber sosyal mühendislik operasyonları da kuvvet kullanma eşiğine erişmeyeceği gibi saldırı veya silahlı saldırı da teşkil etmeyecek; lakin özellikle seçimlere müdahale amacıyla gerçekleştirildiğine içişlerine karışma yasağının ihlali gündeme gelebilecektir[367].

Zira seçimlerin yürütülmesinin *domaine réservé* kapsamında bir faaliyet olması sebebiyle, devletler başka devletlerin seçimlerinin yürütülüş sürecine ya da sonuçlarına ilişkin zorlayıcı müdahalelerden kaçınmak zorundadır[368]. Gerçekten de Birleşmiş Milletler nezdinde alınan birçok kararla seçimlere yönelik dışarıdan müdahaleler kınanmıştır[369]. Öte yandan her ne kadar içişlerine karışma yasağını ihlal

---

https://d3i6fh83elv35t.cloudfront.net/static/2018/07/Muellerindictment.pdf, (erişim tarihi: 27.03.2020) Bu kapsamda, Rusya Federasyonu'nun Genel İstihbarat Genel Müdürlüğü ("*Main Intelligence Directorate of the General Staff* - "GRU"), Mart 2016'nın başında dönemin ABD başkan adayı Hillary Clinton adına yürütülen Clinton Kampanyası'nı destekleyen organizasyonlar, çalışanlar ve gönüllülerin bilgisayarlarına ve e-postalarına izinsiz olarak erişmiş; Nisan 2016'da ise ABD Demokratik Kongre Kampanya Komitesi ve Demokratik Ulusal Komite'nin bilgisayar ağlarına giriş sağlayarak yüz binlerce dokümanı ele geçirmiştir. (Robert S. Mueller, Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Washington D.C, U.S. Department of Justice, Volume I of II, 2019, s. 36.)

[366]U.S. Office of the Director of National Intelligence, Assessing Russian Activities and Intentions in Recent US Elections, 6 Ocak 2017, s.3, *https://www.dni.gov/files/documents/ICA_2017_01.pdf*, (erişim tarihi: 27.03.2020)

[367]NATO CCD COE, **Tallinn Manual 2.0**, s. 318 / 331

[368]Michael N. Schmitt, ""Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*",* **Chicago Journal of International Law**, Vol. 19, No. 1, Article 2, 2018, (30-67), s.49.

[369]Resolution adopted by the General Assembly on 16 December 2005, Respect for the principles of national sovereignty and diversity of democratic systems in electoral processes as an important element for the promotion and protection of human rights, A/RES/60/164, 6 Aralık 2005; Benzer bir şekilde Birleşik Krallık ve Amerika Birleşik Devleti yetkilileri, başka bir devletin seçim yapma yetkinliğine müdahale eden yahut seçim sistemlerini manipüle ederek sonuçlarda değişiklik yaşanmasına sebep olan saldırgan siber operasyonların içişlerine karışma yasağı teşkil edeceğini beyan etmiştirler. (Jeremy Wright, Cyber and International Law in the 21st Century, 23 Mayıs 2018, *https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century*; Brian J.

eden müdahalelerde amaç yabancı bir devletin normal şartlarda hareket etmeyeceği şekilde etmesini sağlamak olsa da bir seçime yönelik yapılan bu yönde bir müdahalenin devlete yapılmış sayılıp sayılmayacağı ve bir hareketin zorlayıcı olması ile demokrasinin olağan işlevini yıpratıcı olması arasındaki farkın nasıl çizileceği tartışılmalıdır[370]. Kanımızca milletler arasındaki artan işbirliğinin kuvvet kullanmaksızın müdahaleyi mümkün hale getirdiği de dikkate alındığında yeni ve daha geniş kapsamlı bir içişlerine karışma anlayışının gerekli olduğu savunulabilecektir[371]. Kaldı ki gerek 1976 tarihli Devletlerin İçişlerine Müdahale Etmeme Bildirisi gerekse 1981 tarihli Devletlerin İçişlerine Karışma ve İç İlişkilerine Müdahale Etmenin Kabul Edilemezliği Bildirisi düşmanca propaganda ve iftira eylemlerini kınamaktadır[372]. Dolayısıyla demokratik kurumların hedef alındığı ve sosyal mühendislik aracılığıyla bir devletin herhangi bir doğrultuda başka bir devletin işleyişine ilişkin kamuoyu yaratma amacıyla gerçekleştirdiği siber operasyonların içişlerine karışma yasağını ihlal ettiği tespitinde bulunulabilecektir. Sonuç olarak, benzer siber operasyonların

---

Egan, Remarks on International Law and Stability in Cyberspace, 10 Kasım 2016, *https://2009-2017.state.gov/s/l/releases/remarks/264303.htm* erişim tarihi: 27.03.2020) Lakin çalışmanın bu bölümünde seçim sistemlerine yönelik saldırgan siber operasyonlar değil, sosyal mühendislik amacıyla siber casusluk ile elde edilen bilgilerin ifşası ve bu bilgilerden faydalanarak gerçekleştirilen propaganda faaliyetleri aracılığıyla gerçekleştirilen siber operasyonlar incelenmektedir.

[370]David J. Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?", **Texas Law Review**, Vol. 95, 2017, (1579-1598), s. 1593; Nitekim bir görüşe göre, her ne kadar ifşa edilen veriler ve zamanlaması söz konusu siber operasyonların baskı unsuru olarak değerlendirilmesine olanak sağlıyorsa da ne tehdit edilen sonuçlar ne de siber operasyonların hedefini net olarak tespit etmek mümkün gözükmemektedir. (Duncan Hollis, "The Influence of War; the War for Influence", **Temple International & Comparative Law Journal**, Vol. 32, 2018, (31-46), s. 41.) Tsagourias ise söz konusu saldırıları değerlendirirken, içişlerine karışma ya1sağının yorumunda bireylerin dışarıdan müdahale olmaksızın politik durumlarına özgürce karar verebilmesi hakkını koruyan *self-determinasyon* ilkesine de yer vermiş; içişlerine karışma yasağının sadece devletin bütünlüğünü ve bağımsızlığını korumadığını ve hükümetin oluşum kaynağı olan halka yönelik müdahalelerin de içişlerine karışma yasağı teşkil edebileceğini iddia etmiştir. (Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination and The Principle of Non-Intervention in Cyberspace", 2019, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3438567*, (erişim tarihi: 02.04.2020)) Bunun yanı sıra bir görüş tarafından, içişlerine karışma yasağının zorlayıcılık kıstasının miadını doldurduğu kanaatiyle, teknik olarak zorlayıcı olmamakla birlikte karmaşa yaratan siber operasyonların da içişlerine karışma yasağı kapsamında değerlendirilmesi gerektiği öne sürülmüştür. (Christopher T. Stein, "Hacking the Electorate: a Non-Intervention Violation Maybe, But Not an "Act of War"", **Arizona Journal of International & Comparative Law**, Vol. 37, No. 1, 2020, (29-48), s. 45.) Yine bu yönde öğretide, kasıtlı olarak ve ayrılık yaratma veya asileri cesaretlendirme amacıyla gerçekleştirilen yayınların içişlerine karışma yasağının ihlali teşkil etme ihtimalinin yüksek olduğu değerlendirmesinde bulunulmuştur. (Jamnejad / Wood, **a.g.m**, s. 374.)

[371]Philip Kunig, "Intervention, Prohibition of", **Max Planck Encylopedia of Public International Law**, Vol VI, Brill, 2012, s. 290

[372]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 65.

uluslararası hukuk açısından oluşturduğu durum değerlendirilirken de her vaka bazında somut durumun koşulları dikkate alınmalı ve siber operasyonların hedef aldığı olgu ile kapsamı göz önünde bulundurularak içişlerine karışma yasağının ihlali olup olmadığı tahlil edilmelidir.

2.5.4. Sistemlerin Çalışırlığını Etkileyen Saldırgan Siber Operasyonlar

Çalışmanın bu bölümünde, yöneltildiği sistemde çeşitli aksaklıklara yol açan, hedef sistemi yavaşlatan veya tamamen erişilmez kılan ancak fiziksel olarak herhangi bir zarara yol açmayan saldırgan siber operasyonlar incelenecektir. Saldırgan bir siber operasyonun hangi koşullarda kuvvet kullanma eşiğine eriştiğine dair görüşlerin açıklandığı bölümde değinildiği üzere, etki odaklı yaklaşım uyarınca fiziksel zarara yol açan siber operasyonların kuvvet kullanma eşiğine eriştiği kabul edilmekteyken fiziksel zarara yol açmamakla birlikte sistemlerin çalışırlığını etkileyenlerin durumu tartışmalıdır[373]. Lakin sistemlerin çalışırlığını etkileyen saldırgan siber operasyonların bir devletin güvenliğine yönelik ciddi sonuçlara yol açması halinde, bu tip saldırıların da kuvvet kullanma yasağının ihlali teşkil edeceği görüşü gittikçe popülerleşmektedir[374]. Bu kapsamda, yakın tarihimizde gerçekleşen ve sistemlerin çalışırlığını etkileyen saldırgan siber operasyonlar üzerinden bu görüş tartışılacak; bu tip siber operasyonların kuvvet kullanma eşiğine eriştiği sonucuna ulaşıldığı takdirde mesele ayrıca silahlı saldırı kavramı üzerinden incelenecektir.

Estonya'nın 2007 senesinde maruz kaldığı saldırgan siber operasyonlar fiziksel bir zarara yol açmamakla birlikte, siber alan sayesinde var olan pek çok hizmetin devre dışı kalmasına yol açması sebebiyle bu kapsamda incelenebilecektir[375]. Nitekim bahsi

---

[373]NATO CCD COE, **Tallinn Manual 2.0**, s. 342.

[374]Robin Geiss / Henning Lahmann, "Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention", **Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy**, Ed: Katharina Ziolkowski, Tallinn, NATO CCD COE Publication, 2013, (621-657), ss. 622-23; Sheng Li, "When Does Internet Denial Trigger the Right of Armed Self-Defense?", **The Yale Journal of International Law**, Vol. 38, 2013, (179-216), s. 214; Roscini, **Cyber Operations and the Use of Force in International Law**, s. 55; Delerue, **Cyber Operations and International Law**, s. 304

[375]Söz konusu saldırgan siber operasyonlar Estonya Hükümeti'nin Sovyet dönemine ait bir İkinci Dünya Savaşı anıtını kaldırma kararına yönelik eylemler sonrası başlamış; Rusya Federasyonu kaynaklı *DoS* saldırıları ile üç haftadan uzun bir süre boyunca Estonya'nın kamu kurumlarına ve haber portallarına ait internet sitelerine erişim sıkıntısı yaşanmıştır. (Tikk Eneken / Kadri Kaska / Liis Vihul**,**

geçen olayda Estonya Hükümeti'nin bütün bakanlıklarına ait olanlar ile iki büyük bankanınkiler de dahil olmak üzere pek çok internet sitesine erişim engellenmiş; hatta Estonya parlamentosunun e-posta sunucuları dahi devre dışı bırakılmıştır[376]. Söz konusu saldırgan siber operasyonların sonucu olarak Estonya'nın ambulans ve itfaiye acil yardım hatlarına bir saati aşkın bir süre boyunca ulaşılamamış; siber operasyonların ciddi etkileri olmasından dolayı *jus ad bellum* açısından yarattığı durum yoğun bir şekilde tartışılmıştır[377]. Sadece bir sene sonra benzer bir tartışma, Gürcistan'ı hedef alan ve Rusya Federasyonu'na atfedilen saldırgan siber operasyonlar sonucu tekrar gündeme gelmiştir[378]. Zira 2008 senesinin Ağustos ayında gerçekleştirilen saldırgan siber operasyonlar Gürcistan devlet başkanının yanı sıra dışişleri bakanlığı ve savunma bakanlığının internet sitelerini ilaveten, ülkenin en büyük ticari bankasını ve haber portallarını hedef almış; saldırıların sonucu olarak Gürcisten Dışişleri Bakanlığı'nın sunucuları Estonya'ya taşınırken Gürcü yetkililer resmi duyurularını Polonya Cumhuriyeti devlet başkanının internet sitesinde sağladığı bir bölüm üzerinden gerçekleştirmek durumunda kalmıştır[379]. Keza daha güncel bir örnek olarak, yine Rusya Federasyonu kaynaklı olduğu düşünülen ve *BlackEnergy* olarak adlandırılan bir kötücül yazılımın Ukrayna'nın elektronik dağıtım şirketlerinin sistemlerine yüklenmesi sonucu 23 Aralık 2015'te geniş çapta elektrik kesintilerine yol açan saldırgan siber operasyonlar da bu kapsamda değerlendirilebilir[380].

International Cyber Incidents: Legal Considerations, Tallinn, NATO CCD COE Publications, 2010, ss. 15-16.)

[376]Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", **Journal of Strategic Security**, Vol. 4, No. 2, 2011, (49-60), s. 51.

[377]Jeffrey T. G. Kelsey, "Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", **Michigan Law Review**, Vol. 106, 2008, (1427-1451), s. 1429.

[378]Constantine Antonopoulos, "State Responsibility in Cyberspace", **Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy**, Ed: Katharina Ziolkowski, Tallinn, NATO CCD COE Publication, 2013, (55-72), s. 56; Tsagourias, **Cyber Attacks Self,defence and the Problem of Attribution**, s. 232.

[379]Eneken / Kaska / Vihul, **a.g.e**, ss. 69-70.

[380]FireEye, **Cyber Attacks on the Ukrainian Grid: What You Should Know**, FireEye Industry Intelligence Report, s. 1-2, *https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf*, erişim tarihi: 06.08.2020; Electricity Information Sharing and Analysis Center, **Analysis of the Cyber Attack on the Ukrainian Power Grid**, Washington, 18 Mart 2017, s. iv, *https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf*, erişim tarihi: 06.08.2020

Murphy, verinin (*data*) günümüzdeki önemini de dikkate alarak, bir çeşit eşya olarak değerlendirilmesi halinde geniş çapta veri kaybına yol açan saldırgan siber operasyonların silahlı saldırı gibi değerlendirilebileceği yorumunda bulunmuştur[381]. Bu yaklaşımın kabul edilmesi halinde, sistemlerin çalışırlığını etkileyen saldırgan siber operasyonların da esasında belirli verilerin çarpıtılması yahut yok edilmesi aracılığıyla gerçekleştirilmesi sebebiyle silahlı saldırı eşiğine eriştiği sonucuna ulaştırmaktadır. Yine de sistemlerin çalışırlığını etkileyen saldırgan siber operasyonların kuvvet kullama ve silahlı saldırı teşkil edip etmediği değerlendirilirken tek başına bu yaklaşım doğrultusunda bir çıkarımda bulunulmasının isabetli olmadığı görüşündeyiz[382]. Ancak bu tespit, yukarıda incelenen örneklerde de görüldüğü üzere, saldırgan bir siber operasyonun doğrudan fiziksel bir zarara yol açmadığı hallerde de devlet için ciddi sonuçlar doğurabileceği; dolayısıyla kuvvet kullanma yahut silahlı saldırı teşkil etme ihtimalinin mevcut olduğu yönündeki görüşlerin tamamen reddedildiği anlamına gelmemektedir.

Bu kapsamda bir devletin kritik altyapısına yöneltilen saldırgan siber operasyonların kuvvet kullanma teşkil edebileceği; hatta söz konusu saldırgan siber operasyonların bu sistemler üzerindeki etkisinin ciddi olduğu hallerde fiziksel bir zarara yol açılmasa dahi silahı saldırı eşiğine eriştiği tespitinde bulunulabileceği ileri sürülmüştür[383]. Roscini de sistemlerin çalışırlığını etkileyen ve acil yardım ve kurtarma hizmetleri, enerji, halk sağlığı, ulaşım, yemek ve su temini gibi ulusal kritik altyapıyı oluşturan sektörlerde ciddi aksaklıklara yol açan saldırgan siber operasyonların dolaylı olarak fiziksel zarara yol açmasının çok yüksek bir ihtimal olduğunu belirterek; bu tip siber operasyonların kuvvet kullanma eşiğine eriştiğinin kabul edilmesi gerektiğini savunmuştur[384]. Keza Roscini, yine fiziksel bir zarar doğmadığı hallerde de bir devletin bankacılık ve finans ile kamu hizmetleri ve iletişim sektörlerine yöneltilen saldırgan siber operasyonların kuvvet kullanma yasağını ihlal

---

[381]John F. Murphy, "Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S.Vital Interests", **International Law Studies**, vol. 89, 2013, (309-340), s. 325.
[382]Roscini, **Cyber Operations as a Use of Force**, s. 244.
[383]National Research Council, **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities**, Ed: William A. Owens / Kenneth W. Dam / Herbert S. Lin, The National Academy Press, Washington, 2005, ss. 253-54
[384]Roscini Marco, **Cyber Operations as a Use of Force**, s. 246.

edebileceğini ifade etmiştir[385]. Tsagouiras ve Melzer ise, bir devletin kritik altyapısını durduran yahut ciddi bir şekilde aksaklığa yol açan saldırgan siber operasyonların fiziksel zarara yol açmasa dahi silahlı saldırı eşiğine eriştiğinin kabul edilmesi gerektiğini savunmuşlardır[386]. Nitekim Amerika Birleşik Devletleri de belirli koşullar altında sistemlerin çalışırlığını etkileyen saldırgan siber operasyonların doğrudan fiziksel bir zarara yol açmasa dahi silahlı saldırı olarak değerlendirilmesinin mümkün olduğu yönünde görüş bildirmiştir[387].

Öte yandan kimi yazarlarca, ulusal kritik altyapının ekonomik altyapılardan soyutlanamayacağından ve dolayısıyla ulusal kritik altyapının işlerliğini bozan saldırgan siber operasyonların kuvvet kullanma olarak değerlendirilmesinin istenmeyen olumsuz hukuki sonuçları söz konusu olacağından, bu tip saldırgan siber operasyonların kuvvet kullanma kavramı yerine içişlerine karışma yasağı üzerinden değerlendirilmesi gerektiği eleştirisinde bulunulmuştur[388]. Lakin belirtmek gerekir ki bir devletin kritik altyapısını hedef alan saldırgan siber operasyonlar, sonuçlarını doğurduğu kritik altyapı ekonomik dahi olsa tespit edilebilir bir hedefe yöneltilmesi ve ambargo gibi bir baskı aracının kullanılmasının yerine doğrudan sistemin işlerliğini hedef alması sebebiyle ekonomik baskı mekanizmalarından ayrılmaktadır[389]. Yine belirtmek gerekir ki söz konusu saldırgan siber operasyonların kuvvet kullanma

---

[385]Ibid.

[386]Tsagourias, **Cyber Attacks Self-defence and the Problem of Attribution**, s. 231; Melzer, **a.g.e**, s. 16.

[387]United Nations General Assembly, Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General, A/66/152, 15 Temmuz 2011, s. 18; Keza Amerika Birleşik Devletleri Savunma Bakanlığı da konuya ilişkin değerlendirmelerinde, bir ülkenin bilgisayar sistemlerine erişip verilerinde değişiklik yaparak, yakıt yönetimi, yedek parça veya tıbbi malzeme yönetiminin yahut ulaşım ve birliklerin naklini ciddi şekilde etkileyen bir siber operasyonun askeri operasyon gerçekleştirme yetisine müdahale teşkil edeceğinden kuvvet kullanma olarak kabul edilebileceği yorumunda bulunmuştur. (US Department of Defense Office of General Counsel, "An Assessment of International Legal Issues in Information Operations", **Computer Network Attack and International Law**, Ed: Michael N. Schmitt / Brian T. O'Donnell, 2. Bası, International Law Studies, Vol. 76, 2002, (459-529), s. 483.)

[388]Vida M. Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places", **Naval Law Review**, vol. 51, 2005, (132-174), s. 135; Antonio Segura-Serrano, "Internet Regulation and the Role of International Law", **Max Planck Yearbook of United Nations Law**, Vol. 10, Ed: Armin von Bogdandy / Rüdiger Wolfrum / Christiane E. Philipp, Brill, Hollanda, 2006, (191-272), s. 225.

[389]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 62; Woltag, **a.g.e**, s. 154.

yasağını ihlal ettiği kabul edildiği takdirde, bu tek başına meşru müdafaa hakkına başvurulmasına yetmeyeceğinden, böyle bir yaklaşım siber operasyonlardan kaynaklı çatışmaların doğmasına yol açmayacak ve fakat bu tip saldırgan siber operasyonlara gelecekte daha az rastlanılmasına sebep olabilecektir. Zira saldırgan bir siber operasyon silahlı saldırı eşiğine erişmediği takdirde meşru müdafaa hakkına başvurulamayacaksa da kuvvet kullanma veya kuvvet kullanma tehdidi yahut içişlerine karışma yasağının ihlali teşkil eden saldırgan siber operasyonlara kuvvet kullanma teşkil etmeyen siber operasyonlarla karşılık verilebileceği gibi ekonomik baskı gibi karşı önlemlere de başvurulabilecektir[390].

Sonuç olarak, şayet saldırgan bir siber operasyon devletin kritik altyapısının bir parçasını teşkil eden sistemlerin işlerliğini ciddi şekilde bozuyorsa, söz konusu siber operasyonun kuvvet kullanma eşiğine eriştiği değerlendirmesinde bulunulabileceği kanaatindeyiz[391]. Bu doğrultuda belirtmek gerekir ki bir devletin kritik altyapısına yöneltilmemiş yahut kritik altyapısına yöneltilse dahi etkileri şiddetli olmayan saldırgan siber operasyonların içişlerine karışma yasağı kapsamında değerlendirilmesi daha isabetli olacaktır[392]. Ayrıca ilgili bölümde açıklandığı üzere, silahlı saldırı kavramı değerlendirilirken en vahim kuvvet kullanma eylemlerinin silahlı saldırı eşiğine eriştiğinin kabul edildiği göz önüne alındığında, kanımızca sistemlerin işlerliğini etkileyen saldırgan siber operasyonların silahlı saldırı olarak nitelenmesi kavramı fazla genişleten bir yaklaşım olacaktır[393].

2.5.5. Fiziksel Zarara Yol Açan Saldırgan Siber Operasyonlar

Saldırgan siber operasyonlar önce yöneltildikleri bilgisayar sistemi üzerinde, ardından bu bilgisayar sisteminin yönettiği altyapı üzerinde etki doğurarak söz konusu altyapıda yaşanan aksaklıkların bir sonucu olarak fiziksel eşyaların zarar görmesine,

---

[390]François Delerue, **State Responses to Cyber Operations**, Global Relations Forum Young Academics Program Policy Paper Series No. 5, İstanbul, 2017, ss. 13-14; Roscini, **Cyber Operations and the Use of Force in International Law**, s. 63; Anthony Aust, **Handbook of International Law**, New York, Cambridge University Press, 2005, s. 425.
[391]Delerue, **Cyber Operations and International Law**, s. 304
[392]Roscini, **Cyber Operations as a Use of Force**, s. 244; Delerue, **Cyber Operations and International Law**, s. 304
[393]NATO CCD COE, **Tallinn Manual**, ss. 57-58.

hatta insanların yaralanmasına veya ölmesine yol açabilecektir[394]. İlgili bölümde açıklandığı üzere, bu tip fiziksel zarara yol açan saldırgan siber operasyonların kuvvet kullanma eşiğine eriştiği yönünde öğretide büyük oranda görüş birliği olduğu gibi devletler de konuya ilişkin açıklamalarında genel olarak bu yaklaşımla örtüşen bir tutum sergilemiştir[395]. Hatta bu tip siber operasyonların aynı zamanda silahlı saldırı eşiğine de eriştiği dolayısıyla saldırının isnat edildiği devlete karşı meşru müdafaa hakkı kapsamında kuvvet kullanılmasına imkan tanıyacağı da ileri sürülmüştür[396]. Çalışmanın bu bölümünde saldırgan siber operasyonların fiziksel zarara yol açması halinde silahlı saldırı eşiğine erişip erişmeyeceği meselesi güncel örnekler üzerinden tartışılarak irdelenecektir.

Saldırgan bir siber operasyonun silahlı saldırı eşiğine erişilebileceği kanaatinde olan hukukçular, bu varsayımlarını temellendirirken sıklıkla *Stuxnet* olayı üzerinden değerlendirmelerde bulunmaktadır[397]. Zira söz konusu saldırgan siber operasyon kapsamında, 2010 senesinin Haziran ayında İran İslam Cumhuriyeti'nin ("İran") Natanz'daki uranyum zenginleştirme tesisinin Merkezi Kontrol ve Veri Toplama Sistemi'ne (*Supervisory Control And Data Acquisition* – "SCADA") yüklenen kötücül bir yazılım aracılığıyla, Siemens S7-300 isimli sisteme müdahale edilerek tesiste fiziksel zarara yol açılmıştır[398]. Stuxnet birçokları tarafından Amerika Birleşik

---

[394]Roscini, **Cyber Operations and the Use of Force in International Law**, ss. 52-53.

[395]Roscini, **Cyber Operations as a Use of Force**, s. 239; Woltag, **a.g.e**, s. 174; Delerue, **Cyber Operations and International Law**, s. 296-97; Roscini, **World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force**, ss. 108-09; Michael N. Schmitt, ""Attack" as a Term of Art in International Law: The Cyber Operations Context", **2012 4th International Conference on Cyber Conflict**, Ed: Christian Czosseck / Rain Ottis / Katharina Ziolkowski, Tallinn, NATO CCD COE Publications, 2012, (283-293), s. 286

[396]NATO CCD COE, **Tallinn Manual 2.0**, s. 341; Dinstein, **Computer Network Attacks and Self-Defense**, s. 103.

[397]Kimi yazarlarca fiziksel zarara yol açan saldırgan siber operasyonların geçmişi 1982 senesinde Sibirya'daki Urengoy-Surgut-Chelyabinsk boru hattında meydana gelen ve CIA tarafından gerçekleştirildiği iddia edilen bir siber operasyona dayandırılsa da söz konusu siber operasyonun gerçekten yaşandığına dair kesin delil bulunmamaktadır. (Thomas Rid, **Cyber War will not Take Place**, New York, Oxford University Press, 2013, s. 4)

[398]Scott D. Applegate, "The Dawn of Kinetic Cyber", **2013 5th International Conference On Cyber Conflict (CYCON 2013)**, Ed: Karlis Podins / Jans Stinissen / Markus Maybaum, Tallinn, NATO CCD COE Publications, 2013, (163-181), ss. 170-71; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", **Security Studies**, vol. 22, 2013, (365-404), ss. 365-66; Hatta kimi kaynaklarda merkezkaçlarda meydana gelen patlamadan dolayı bir işçinin hayatını kaybettiği iddia edilmektedir. (Neil C. Rowe, "Distinctive Ethical Challenges of Cyberweapons", **Research Handbook on International Law and Cyberspace**, Ed: Nicholas Tsagourias / Russell Buchan, Edward Elgar Publishing, 2015, (307-326), s. 310.)

Devletleri ve İsrail'e isnat edilmiş; her iki devlet de bu iddiaları reddetmediği gibi İran da SCADA'ya ilişkin bilgilerin Amerika Birleşik Devletleri ve İsrail'e sağlanması sebebiyle Alman mühendislik şirketi Siemens'i suçlamıştır[399].

Tallinn El Kitabı'nı hazırlayan hukukçular tarafından da Stuxnet'in kuvvet kullanma eşiğine eriştiği yönünde görüş birliğine ulaşılmış; katılımcıların bir kısmı söz konusu siber operasyonun aynı zamanda silahlı saldırı da teşkil ettiği yönünde görüş bildirmiştir[400]. Birçok hukukçu tarafından *Stuxnet* örneğinin kuvvet kullanma eşiğine eriştiği kabul edilse de muhtemelen karşılaşılan fiziksel zararın sadece birkaç merkezkaç ile sınırlı olması ve bütün nükleer santrali etkilememesi yahut siyasi tercihler sebebiyle İran saldırgan siber operasyonlara yönelik gerekli önleyici önlemleri alacağını duyurmakla yetinmiştir[401]. Lahmann, Stuxnet'e ilişkin tartışmaların yanı sıra konuyu benzer bir örnek olan 5 Ağustos 2008 tarihinde Bakü-Tiflis-Ceyhan boru hattının Refahiye kısmında gerçekleşen patlama açısından değerlendirmiş;[402] Stuxnet örneğinde yıkıcı etki sadece sınırlı bir alanda görülürken

---

[399]Shaun Roberts, "Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors", **Northern Kentucky Law Review**, vol. 41, no. 3, 2014, (535-572), ss. 544-45; Delerue, **State Responses to Cyber Operations**, ss. 5-6; Focarelli, **a.g.e**, s. 261.

[400]NATO CCD COE, **Tallinn Manual 2.0**, s. 342; Keza *Stuxnet* kuvvet kullanma yasağını ihlal etmesi sebebiyle doğal olarak içişlerine karışma yasağının da ihlali anlamına gelmektedir. (Gill, **Non-Intervention in the Cyber Context**, s. 235)

[401]Delerue, **Cyber Operations and International Law**, s. 297; Dinniss, **a.g.e**, s. 57; Katharina Ziolkowski, **Stuxnet – Legal Considerations**, Tallinn, NATO CCD COE Publications, 2012, s. 11; Dieter Fleck, "Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual", **Journal of Conflict & Security Law**, vol. 18, no. 2, 2013, (331-351), ss. 332-33; Her ne kadar İran İslam Cumhuriyeti yetkileri Stuxnet olayının kuvvet kullanma yahut silahlı saldırı teşkil ettiği yönünde bir beyanda bulunmamışsa da İran Genelkurmay Başkanlığı tarafından yakın bir dönemde gerçekleştirilen açıklama ile bireyler yahut maddi eşyalar üzerinde ciddi ve geniş çaplı fiziksel zarara yol açan siber operasyonların kuvvet kullanma yasağını ihlal edeceği; İran Silahlı Kuvvetleri'nin kritik altyapılarına yöneltilen şiddetli siber operasyonlara karşılık meşru müdafaa hakkına başvurabileceğini duyurmuştur. (Nour News, General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat, 18 Ağustos 2020, *https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat*, erişim tarihi: 19.08.2020)

[402]Söz konusu patlamada alarm sistemlerinin basıncın yükselmesine ilişkin herhangi bir uyarıda bulunmaması sonucu boru hattını devamlı kontrol eden birimlerin patlamayı gerçekleştikten 40 dakika sonra fark edebilmesi ve güvenlik kamerası sisteminin *hack*lenerek 60 saatlik görüntü kayıtlarının silinmesi patlamanın bir siber operasyondan kaynaklandığı yönünde tahminlerde bulunulmasına yol açmıştır. (Alper Başaran, "Turkey Under Cyber Fire", **Turkish Policy Quarterly**, vol. 16, no. 1, 2017, (95-102), s. 97; s. 14; Can Kasapoğlu, **Turkey's Future Cyber Defense Landscape**, A Primer on Cyber Security in Turkey and the Case of Nuclear Power, s. 14, *https://edam.org.tr/document/CyberNuclear/edam_cyber_security_ch1.pdf*, (erişim tarihi: 08.08.2020); Robert M. Lee / Michael J. Assante / Tim Conway, **ICS CP/PE (Cyber-to-Physical or Process Effects) Case Study Paper: Media Report of the Baku-Tbilisi-Ceyhan (BTC) Pipeline**

ikinci örnekte, 30.000 varil ham petrolün Anadolu'da çevreye verdiği zararı da göz önüne alarak, söz konusu eylemin tıpkı bir füze saldırısı gibi silahlı saldırı kabul edilebileceğini ifade etmiştir[403].

Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesi uyarınca kullanılan kuvvetin büyüklüğüne ve süresine göre bir ayrım yapılmaksızın her türlü tek taraflı kuvvet kullanma eylemi yasaklanmıştır[404]. Dolayısıyla etki odaklı yaklaşım tarafından da benimsendiği üzere, fiziksel bir zarara yol açan saldırgan bir siber operasyonun kuvvet kullanma yasağını ihlal ettiği tespitinde bulunulabilecektir. Lakin silahlı saldırı eşiğinin kuvvet kullanmadan daha yüksek olması ve sadece etki ve boyut olarak belirli bir şiddete erişen kuvvet kullanma eylemlerinin silahlı saldırı olması sebebiyle, fiziksel zarara yol açan her türlü siber operasyonun aynı zamanda silahlı saldırı teşkil ettiğini savunmak isabetli olmayacaktır. Örneğin, Amerika Birleşik Devletleri Savunma Bakanlığı da yayımlamış olduğu bir raporda siber operasyonları değerlendirirken; bir ülkenin hava trafik kontrol sistemini, banka ve finans sistemini veya kamu hizmet kurumlarını devre dışı bırakarak sivil ölümlerin yahut mülk zararlarının önünü açan bir siber operasyonun silahlı saldırı olarak kabul edilmesinin mümkün olabileceğini savunmuştur[405]. Gerçekten de saldırgan bir siber operasyonun yol açtığı fiziksel zarar tek bir bilgisayarın devre dışı bırakılmasının ötesinde, geniş çaplı ve maruz kalan devleti ciddi anlamda olumsuz etkileyecek sonuçlara yol açtığı hallerde mağdur devletin silahlı saldırıya uğradığını kabul etmek makul gözükmektedir. Nitekim saldırgan siber operasyonların şimdiden fiziksel zarara yol açan örnekleri mevcut olduğu gibi ilerleyen süreçte söz konusu teknolojilerin gelişmesi ile bu tip siber operasyonların daha yıkıcı etki doğuran türleriyle de karşılaşılmasının mümkün olduğu unutulmamalıdır.

Cyber Attack, SANS Industrial Control Systems, 20 Aralık 2014, ss. 1-2, *https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf*, (erişim tarihi: 08.08.2020)

[403]Lahmann, **a.g.e**, s. 65.

[404]Melzer, **a.g.e**, s. 8.

[405]US Department of Defense Office of General Counsel, **An Assessment of International Legal Issues in Information Operations**, s. 483.

ÜÇÜNCÜ BÖLÜM:

SİBER OPERASYONLARIN ATFEDİLEBİLİRLİĞİ

Çalışmanın bu bölümünde siber operasyonların hangi koşullarda bir devlete atfedilebileceği değerlendirilecektir. Zira uluslararası hukukta sorumluluğa ilişkin normlar devletler arası ilişkiler temel alınarak oluşturulmuş; keza Birleşmiş Milletler Şartı'nın 51. maddesi uyarınca düzenlenen meşru müdafaa hakkı da bir devletin başka bir devlete silahlı saldırı gerçekleştirmiş olması şartına bağlanmıştır. Dolayısıyla önceki bölümde incelenen hususların uluslararası hukuk kapsamında bir sonuç doğurabilmesi ancak inceleme konusu eylemin bir devlete atfedilebilmesi halinde mümkün olacaktır. Nitekim saldırgan bir siber operasyona karşı meşru müdafaaya başvurulabilmesi için şüphesiz öncelikle söz konusu saldırı sorumlu olan devlete atfedilebiliyor olmalıdır[406]. Hatta saldırgan bir siber operasyonun silahlı saldırı teşkil etmemekle birlikte uluslararası hukuku ihlal ettiği hallerde de bir devletin karşı önlemlere başvurabilmesi uluslararası hukuku ihlal eden siber operasyonun devletin sorumluluğu kapsamında bir devlete atfedilebiliyor olması halinde mümkün olacaktır[407].

Devletlerin gerçekleştirilen uluslararası hukuka aykırı bir eylemden sorumlu tutulabilmesine dair kurallar uluslararası teamül hukuku kapsamında mevcut olup bu kurallar Uluslararası Hukuk Komisyonu tarafından Uluslararası Hukuka Aykırı Eylemlerden Dolayı Devletlerin Sorumluluğuna İlişkin Metin (*Articles on Responsibility of States for Internationally Wrongful Acts* – "ARSIWA") kapsamında tedvin edilmiştir[408]. Birleşmiş Milletler Hükümet Uzmanları Grubu, 22 Temmuz 2015 tarihinde yayımladığı rapor ile devletlerin kendilerine atfedilebilen haksız fiillere

---

[406]Nicholas Tsagourias, "Cyber Attacks Self-defence and the Problem of Attribution", **Journal of Conflict & Security Law**, Vol. 17, No. 2, 2012, (229-244) s. 233.
[407]Michael N. Schmitt, "Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law", **Virginia Journal of International Law**, Vol. 54, No. 3, 2014, (697-732), s. 707
[408]Michael N. Schmitt / Liis Vihul, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution", **Fletcher Security Review**, Vol. 1, No. 2, 2014, (53-72), ss. 56-57

ilişkin uluslararası yükümlülüklerini yerine getirmeleri gerektiğini belirtmiş; ardından bir siber aktivitenin belirli bir ülkenin bölgesinden kaynaklanıyor olmasının söz konusu aktiviteyi ilgili devlete isnat etmek için yeterli olmadığını ifade ederek devletlerin iddialarının gerekçelerini açıklamalarını tavsiye etmiştir[409]. Bu bölümde öncelikle devletlerin siber alanda gerçekleştirdikleri eylemlerden doğan uluslararası hukuk sorumlulukları siber alanın kendisine özgü özellikleri de göz önünde bulundurularak mevcut devlet uygulaması kapsamında incelenecek; ardından ARSIWA'nın 4 ila 11. maddeleri uyarınca bir siber operasyonun sorumlu devlete ne koşullarda atfedilebileceği hususu tartışılacaktır.

3. 1. Genel Olarak

Devlet soyut bir hukuki kurum olması nedeniyle "kendi başına" herhangi bir eylemde bulunamamakta, dolayısıyla devletler kendileri için çalışan bireyler yahut gruplar aracılığıyla faaliyet göstermekte ve doğal olarak bu kapsamda kendilerine isnat edilebilen hukuka aykırı fiillerinden sorumlu tutulabilmektedir[410]. Zira Uluslararası Adalet Divanı tarafından Korfu Boğazı Davası'nda belirtildiği üzere devletlerin kontrol ettikleri bölgelerde gerçekleşen her haksız eylemi yahut faillerini bildiği, bilmesi gerektiği sonucuna ulaşmak mümkün değildir[411]. Benzer bir şekilde bir siber operasyonun kaynaklandığı altyapının başka bir devletin egemenlik sahası içerisinde bulunmasının tek başına söz konusu siber operasyonun ilgili devlete atfedilmesi için yeterli olmadığı yorumunda bulunulabilecektir[412]. Kaldı ki siber alanda mevcut anonimlik dolayısıyla saldırgan bir siber operasyonun kaynağı olan devletin tespit edilebilmesinin karşılaşılabilecek teknik sorunlar sebebiyle daha güç olduğu söylenebilmektedir[413]. Gerçekten de saldırgan siber operasyonlarda sıklıkla *botnetler* kullanıldığı ve IP kandırmacası (*IP Spoofing*) yöntemi aracılığıyla saldırının kaynağı gizlendiği gibi bu yöntemlerle bilinçli olarak saldırıya maruz kalan devletin saldırının

[409]UN GGE Report 2015, UN Doc. A/70/174, 22 Temmuz 2015, s. 13, para. 28(f).
[410]Shaw, **a.g.e**, s. 701.
[411]*Corfu Channel Case (United Kingdom v. Albania)*; Merits, International Court of Justice (ICJ), 9 April 1949, s. 18.
[412]Carr Jeffrey, "Responsible Attribution: A Prerequisite for Accountability", **Tallinn Paper No. 6**, Tallinn, CCD COE Publications, 2014, s. 7.
[413]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 33.

kaynağına ilişkin yanıltılması da sağlanabilecektir[414]. Bu takdirde meşru müdafaa yahut karşı önlem kapsamında gerçekleştirilen eylemlerin saldırgan siber operasyondan sorumlu olmayan bir devlete yöneltilmesi riskiyle karşılaşılabilecektir. Ancak yine de bir siber operasyondan sorumlu kimselerin tespit edilmesi imkansız olmayıp her ne kadar özerk bir saldırı teşkil eden siber operasyonlar açısından süreç daha çok vakit alabilse de bir grup saldırıyla birlikte gerçekleştirilen siber operasyonlarda bu konuda daha süratli ve daha kolay bir şekilde sonuç alınabilmektedir[415]. Örneğin, Birleşik Krallık 28 Ekim 2019 tarihinde Gürcü web sağlayıcılarına karşı gerçekleştirilen siber operasyonlardan "mümkün olan en yüksek seviyede" ve "neredeyse kesin olarak" (%95'ten yüksek ihtimalle) Rusya Federasyonu'nun istihbarat teşkilatı GRU'nun sorumlu olduğunu duyurmuştur[416]. Keza Avrupa Birliği Yüksek Temsilcisi Josep Borell Avrupa Birliği adına gerçekleştirdiği bir duyuruyla siber alanda uluslararası güvenlik ve barışın sağlanmasına yönelik Birleşmiş Milletler nezdinde alınan kararları hatırlatarak "kötücül davranış" sergileyen altı birey ve üç kuruluşa Avrupa Birliği ve üye devletlerini tehdit eden siber operasyonlar sebebiyle seyahat yasağı ve malvarlığının dondurulması yaptırımlarının uygulanmasına karar verildiğini açıklamıştır[417]. Avrupa Birliği Konseyi konuya ilişkin 2020/1127 sayılı kararında *WannaCry* ve *NotPetya* isimli saldırıların ciddi ekonomik zarara yol açtığını ve Hollanda merkezli Kimyasal

---

[414]Dinniss, **Computer Network Attacks and Self-Defense**, ss. 99-100.

[415]Dinstein, Yoram, "Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference", **U.S. Naval War College International Law Studies**, Vol. 89, 2013, (276-287), s. 282

[416]Keza aynı açıklama ile Birleşik Krallık 2015 senesinin aralık ayında gerçekleşen ve Ukrayna'da 230.000 insanın 1 ila 6 saat arasında elektriksiz kalmasına yol açan *BlackEnergy* saldırısının, 2016 senesinin aralık ayında gerçekleşen ve Kiev'in beşte birlik bölümünün elektriksiz kalmasına yol açan *Industroyer* saldırısının, 2017 senesinin temmuz ayında gerçekleşen ve Ukrayna'nın finans, enerji ve kamu sektörünü etkileyen *NotPetya* saldırısının ve yine 2017 senesinin ekim ayında gerçekleşip Kiev metrosu ve Odessa Havalimanı'nda aksamalara yol açan *BadRabbit* saldırısının da "Birim 74455" (*Unit 74455*) olarak da bilinen GRU Özel Teknolojiler Merkezi (*GRU Main Center for Special Technologies* – "GTsST") tarafından gerçekleştirildiğini düşündüklerini ifade etmiştir. (Foreign & Commonwealth Office / National Cyber Security Center / The Rt Hon Dominic Raab MP, UK Condemns Russia's GRU over Georgia Cyber-Attacks, Press Release, 20 Şubat 2020, *https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks*, erişim tarihi: 26.06.2020)

[417]Council of the European Union, Declaration by the High Representative Josep Borrell on behalf of the EU: European Union Response to Promote International Security and Stability in Cyberspace, Press Release, 30 Temmuz 2020, *https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-eu-european-union-response-to-promote-international-security-and-stability-in-cyberspace/*, erişim tarihi: 01.08.2020

Silahların Yasaklanması Örgütü'nü hedef alan (*Organisation for the Prohibition of Chemical Weapons* – "OPCW") ve *Operation Cloud Hopper* olarak adlandırılan siber operasyonun OPCW'nin amacına yönelik "saldırgan bir eylem" olduğunu ifade etmiştir[418]. Karar ile yaptırımların, söz konusu siber operasyonları gerçekleştirdiği tespit edilen Qiang Gao ve Shilong Zang isimli Çin Halk Cumhuriyeti (ÇHC) vatandaşları; Alexey Valeryevich Minin, Aleksei Sergeyvich Morenets, Evgenii Mikhaylovich Serebriakov, Oleg Mikhaylovich Sotnikov isimli Rusya Federasyonu Askeri İstihbarat Teşkilatı "GRU" personeli; Tianjin Huaying Haitai Science and Technology Development Co. Ltd isimli ve ÇHC merkezli şirket; Chosun Expo isimli ve Kore Demokratik Halk Cumhuriyeti (KDHC) merkezli ortak girişim; GRU'nun Özel Teknolojiler Merkezi'ne ("GTsST") uygulanacağı açıklanmıştır[419]. Öte yandan her ne kadar yaptırıma tabi tutulanlar arasında Rusya Federasyonu'nun bir organı ve bu organın personelleri yer alsa da Rusya Federasyonu'nun uluslararası hukuktan doğan sorumluluğuna ilişkin herhangi bir beyana karar çerçevesinde yer verilmemiştir.

Nitekim Hollanda Dışişleri Bakanlığı 5 Temmuz 2019 tarihinde Hollanda Parlamentosu'na yazmış olduğu mektup ile siber alanda uluslararası hukuk düzenini açıklamış; atfedilebilirlik meselesini teknik, politik ve hukuki olarak üç ayrı aşamada incelemiştir[420]. Bu kapsamda teknik isnat siber operasyonun muhtemel sorumlularının tespitine ilişkin teknik soruşturma ve bu kapsamda elde edilen bilgiler, politik isnat belirli bir siber operasyonun sorumluya atfedilmesine ilişkin siyasi tercih, hukuki isnat ise bir devletin gerçekleştirmiş olduğu eylemin yahut ihmalinin uluslararası hukuk yükümlülüklerinin ihlali teşkil etmesi sebebiyle hukuken sorumlu tutulması olarak özetlenebilir[421]. Zira bir siber operasyonun sorumlusu olan birey yahut birimin

---

[418]Official Journal of the European Union**,** Council Decision (CFSP) 2020/1127: Amending Decision (CFSP) 2019/97 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States, L 246/12, 30 Temmuz 2020

[419]Official Journal of the European Union, Council Implementing Regulation (EU) 2020/1125: Implementing Regulation (EU) 2019/796 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States, L 246/4, 30 Temmuz 2020

[420]Government of the Netherlands Ministry of Foreign Affairs**,** Letter to the Parliament on the International Legal Order in Cyberspace Appendix: International Law in Cyberspace, 5 Temmuz 2019, s. 6, *https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace*, (erişim tarihi: 24.06.2020)

[421]Ibid.

eylemlerinin devlete atfedilebilmesi için öncelikle siber operasyonun hangi bilgisayar veya sunuculardan kaynaklandığı belirlenmeli ve ardından söz konusu operasyonu gerçekleştiren kimseler tespit edilmelidir[422]. Çalışma kapsamında teknik ve politik isnat hususları derinlemesine incelenmeyecek, hukuki isnat meselesi uluslararası hukukun mevcut normları ışığında tartışılacaktır.

3. 2. Siber Operasyondan Sorumlu Devletin Tespit Edilmesi

Her ne kadar bir siber operasyonun kim yahut kimler tarafından gerçekleştirildiği maddi bir sorun ise de söz konusu tespitin bağlı olacağı ispat standardı hukuki bir meseleyi de kapsamasına yol açmaktadır[423]. Uluslararası Adalet Divanı tarafından Nikaragua Kararı'nda belirtildiği üzere uluslararası hukuk kapsamında sorumluluğa ilişkin bir inceleme yapılabilmesi için öncelikle maddi deliller toplanmalı ve fail tespit edilmelidir[424]. Uluslararası hukuk devletlerin eylemlerini dayandırmaları gereken bir kanıt düzeyi öngörmese de uygulamada bir saldırıya karşı meşru müdafaaya başvurulabilmesi için saldırının kaynağı ve saldırganın kimliğinin belirlenmesine ilişkin yeterli kesinliğe sahip olunması aranmıştır[425].

Almanya, Amerika Birleşik Devletleri, Avustralya, Belçika, Birleşik Krallık, Çek Cumhuriyeti, Danimarka, Estonya, Finlandiya, Fransa, Güney Kore, Hollanda, İspanya, İsveç, İtalya, İzlanda, Japonya, Kanada, Kolombiya, Letonya, Litvanya, Macaristan, Norveç, Polonya, Romanya, Slovakya ve Yeni Zelanda yayınlamış oldukları ortak bildiri ile siber alanda devletlerin hesap verilebilirliğinin sağlanması adına birlikte çalışacaklarını beyan etmiş; siber alandaki "kötü davranışların" sonuçları

---

[422]Marco Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations", **Texas International Law Journal**, Vol. 50, Issue 2, 2015, (233-273), s. 240.
[423]Robin Geiss / Henning Lahmann, "Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses towards Non-forcible Countermeasures and Collective Threat-prevention", **Peacetime Regime for State Activities in Cyberspace**, Ed: Ziolkowski Katharina, Tallinn, NATO CCD COE Publications, 2013, (621-657) s. 623.
[424]*Nikaragua Davası Kararı*, para. 57.
[425]Advisory Council on International Affairs / Advisory Committee on Issues of Public International Law, **Cyber Warfare**, No 77, AIV / No 22, CAVV, 2011, s. 22, *https://www.advisorycouncilinternationalaffairs.nl/binaries/advisorycouncilinternationalaffairs/documents/publications/2011/12/16/cyber-warfare/Cyber_Warfare_AIV-Advisory-report-77_CAVV-Advisory-report-22_ENG_201112.pdf*, (erişim tarihi: 25.06.2020)

olacağını açıklamışlardır[426]. Lakin devletler saldırgan siber operasyonları sorumlu devlete atfettikleri açıklamalarda dahi uluslararası hukukun hangi normunun ihlal edildiğine dair tespitlerde bulunmak yerine genel kınama ifadeleri kullanmakla yetinmişlerdir[427]. Gerçekten de Gürcistan'da hükümete ait olanlar da dahil olmak üzere birçok internet sitesine yöneltilen ve Rusya Federasyonu'nun istihbarat teşkilatı GRU'ya atfedilen siber operasyonlar ortak bildiride katılımcı olarak yer alan devletler tarafından çeşitli beyanlarla eleştirilmişse de devletler genel olarak açıklamalarında söz konusu siber operasyonların belirli bir uluslararası hukuk normunu ihlal etmesi sebebiyle Rusya Federasyonu açısından yaratacağı sonuçlara ilişkin detaylı bir analize yer vermemiştir[428].

Meşru müdafaaya kuvvet kullanma yasağının bir istisnası olarak yer verildiği dikkate alındığında, devletlerin meşru müdafaaya başvurabilmesi için "açık ve inandırıcı" bir delile dayanmasının beklenmesi söz konusu kuralın amacına ulaşılabilmesi için elzem gözükmektedir[429]. Öte yandan uluslararası hukukta adli olmayan süreçlerde ispat mekanizmalarına ilişkin herhangi bir kural öngörülmediği gibi devletlerarası yargılamalarda dahi görevli mahkemelerin yaklaşımlarının farklılık gösterebileceği de dikkate alındığında devletlerin siber operasyonlara ilişkin

---

[426]U.S. Department of State, Joint Statement on Advancing Responsible State Behavior in Cyberspace, 23 Eylül 2019, *https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/*, (erişim tarihi: 26.06.2020)

[427]Dennis Broeders / Els De Busser / Patryk Pawlak, **Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates**, The Hague Program for Cyber Norms Policy Brief, 2020, s. 8

[428]Hollanda açıklamasında "*siber operasyonların Birleşmiş Milletler tarafından kabul edilen siber alandaki sorumlu devlet davranışına ilişkin normları ihlal ettiğini*" (Government of the Netherlands, The Netherlands Considers Russia's GRU Responsible for Cyber Attacks Against Georgia, Diplomatic Statement, 20 Şubat 2020, *https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia%E2%80%99s-gru-responsible-for-cyber-attacks-against-georgia*, erişim tarihi: 26.06.2020); Polonya "*söz konusu siber operasyonların uluslararası istikrara ve devletlerin egemenliğine zarar verdiğini*" (Ministry of Foreign Affairs Republic of Poland, Statement of Polish MFA on Cyberattacks Against Georgia, 20 Şubat 2020, *https://www.gov.pl/web/diplomacy/statement-of-the-polish-mfa-on-cyberattacks-against-georgia*, erişim tarihi: 26.06.2020); Estonya ise Rusya Federasyonu'nun "*mevcut uluslararası normlar ve antlaşmalar kapsamında sorumlu tutulması*" gerektiğini açıklamıştır. (Republic of Estonia Ministry of Foreign Affairs, Statement of the Foreign Minister of the Republic of Estonia Urmas Reinsalu, 20 Şubat 2020, *https://vm.ee/en/news/statement-foreign-minister-republic-estonia-urmas-reinsalu*, erişim tarihi: 26.06.2020)

[429]Marry Ellen O'Connell, "Lawful Self-Defense to Terrorism", **University of Pittsburgh Law Review**, Vol. 63, 2002, (889-908), s. 899.

soruşturmalarının "karmaşık" bir mesele olduğu tespit edilebilecektir[430]. Her ne kadar kimi yazarlarca çözüm olarak saldırgan siber operasyonların atfedilmesine ilişkin uluslararası bir mekanizma oluşturulması önerilmişse de[431] bu takdirde dahi bu tip hizmet sağlayan bir kuruluşun şeffaflığı, hükümetlerle olan ilişkisi yahut ticari çıkarları üzerinden doğabilecek tartışmalar dikkate alındığında böyle bir oluşumun da atfedilebilirlik meselesine ilişkin bir uzlaşı sağlamaktan uzak olduğu tespit edilebilecektir[432]. Dolayısıyla saldırgan bir siber operasyonun sorumlu devlete atfedilmesi hususunun büyük oranda devletler tarafından gerçekleştirilecek girişimler sonucu mümkün olacağı kanaatindeyiz.

Bu kapsamda örneğin Avustralya, hukuka aykırı bir siber operasyonu belirli bir devlete atfederken kendi emniyet güçleri, istihbarat teşkilatlarının değerlendirmeleri[433] ve uluslararası ortaklarıyla gerçekleştirecekleri istişarelere göre hareket edeceklerini açıklamıştır[434]. Amerika Birleşik Devletleri ise yayımlamış olduğu Siber Atfedilebilirlik Raporu ile yöntem (*tradecraft*), altyapı (*infrastructure*), kötücül yazılım (*malware*), niyet ve dış kaynaklar kıstas alınarak yapılan değerlendirmeler uyarınca 2017 senesinin mayıs ayında gerçekleşen *WannaCry* saldırılarından Kore Demokratik Halk Cumhuriyeti'nden, *NotPetya* saldırılarından ise

---

[430]Roscini, **Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations**, s. 242.

[431]Tomohiro Mikanagi / Kubo Macak, "Attribution of Cyber Operations: An International Law Perspective on the Park Jin Hyok Case", **Cambridge International Law Journal**, Vol. 9, No. 1, 2020, (51-75), ss. 68-71.

[432]Yuval Shany / Michael N. Schmitt, "An International Attribution Mechanism for Hostile Cyber Operations", **International Law Studies**, Vol. 96, 2020, (196-222), s. 215.

[433]Uluslararası Adalet Divanı Kongo'nun Bölgesindeki Silahlı Hareketlere İlişkin Karar'ında askeri istihbarata dayanan delillerin imzasız, tarihsiz olmasını gerekçe göstererek herhangi bir iddiayı ispat için tek başına yeterli olmadığını beyan etmiştir. (Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Rwanda), International Court of Justice (ICJ), 18 September 2002, para 127-28.) Dolayısıyla bir siber operasyona ilişkin uluslararası hukuk sorumluluğuna dair bir mesele Uluslararası Adalet Divanı'na taşındığı takdirde istihbarat raporları kapsamındaki delillerin ispata elverişliliği söz konusu raporların içeriğine göre değişkenlik gösterebilecektir.

[434]Australian Government, Australia's International Cyber Engagement Strategy 2019 International Law Supplement Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace, *https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html*, (erişim tarihi: 24.06.2020)

Rusya Federasyonu'nun sorumlu olduğuna dair yeterli delile ulaşıldığını ifade etmiştir[435].

Sonuç olarak, devletler saldırgan bir siber operasyonun kaynağını tespit ederken kendilerince uygun gördükleri kıstaslar doğrultusunda çeşitli tespitlerde bulunmuş; fakat henüz konuya ilişkin belirgin bir devlet uygulaması oluşmamıştır. Ancak Roguski tarafından önerildiği üzere, siber alanda uluslararası hukuk sorumluluğa ilişkin ilkelerin gereğince uygulanabilmesi için devletlerin siber operasyonun isnadında dayandıkları kullanılan altyapı, operasyon yöntemi, operasyonun boyutu ve hedeflenen sonuçlar gibi teknik işaretlere, devletlerin siyasi uyuşmazlıkları gibi politik işaretlere ve olayların kronolojisi gibi davranışsal kalıplara ilişkin görüşlerini paylaşmaları bu alanda normların oluşması adına büyük ehemmiyet taşımaktadır[436].

3. 3. Devletlerin Uluslararası Hukuka Aykırı Eylemlerden Sorumluluğuna İlişkin Normların Siber Operasyonlara Uygulanması

Devletler saldırgan siber operasyonlara başvururken kendi organları veya kamu gücü yetkilerini kullanan kişi ya da birimler aracılığıyla hareket edebileceği gibi devlet dışı aktörlerden de faydalanabilecektir. Bu bölümde her iki ihtimal de ARSIWA'nın ilgili maddeleri uyarınca incelenecek, hangi koşullarda bir siber operasyonun devlete atfedilebileceği güncel örneklerden de destek alınarak açıklanmaya çalışılacaktır.

3.3.1. Devlet Organlarının veya Kamu Gücü Yetkilerini Kullanan Bir Kişi ya da Birimin Tasarrufu

Devletlerin silahlı kuvvetleri, emniyet güçleri veya istihbarat teşkilatları kapsamında siber güvenlik alanında çalışan personel istihdam ettikleri düşünüldüğünde bu kişi veya birimlerin saldırgan bir siber operasyon amacıyla da

---

[435]The US Office of the Director of National Intelligence, **A Guide to Cyber Attribution**, 14 Eylül 2018, s. 5, *https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf*, (erişim tarihi: 10.08.2020)

[436]Przemyslaw Roguski, **Application of International Law to Cyber Operations: A Comparative Analysis of States' Views**, The Hague Program for Cyber Norms Policy Brief, 2020, s. 17.

görevlendirilmesinin mümkün olduğu söylenebilecektir. Keza herhangi bir devlet organı olmamakla birlikte devlet çalışanı olarak kamu gücü yetkileriyle donatılan kimselere de aynı amaçla görevlendirme yapılabilecektir. Keza devletler kendi aralarında hayata geçirdikleri çeşitli işbirliği mekanizmaları doğrultusunda başka bir devletin organından bu amaçla faydalanabilecek veya faydalandırabilecektir. Bu bölümde yukarıda sayılan ihtimaller uluslararası hukuk kapsamında irdelenecek; ayrıca bu hallerde gerçekleşebilecek yetki aşımlarının hukuki sorumluluk açısından sonuçlarına yer verilecektir.

3.3.1.1. Devlet Organlarının Gerçekleştirmiş Olduğu Siber Operasyonlar

ARSIWA'nın 4. maddesi uyarınca ne tür bir fonksiyon üstlendiğine ve devlet yapısında hangi konuma sahip olduğuna bakılmaksızın bütün devlet organlarının gerçekleştirmiş olduğu eylemler ilgili devlet tarafından gerçekleştirilmiş kabul edilecektir[437]. Keza aynı maddenin ikinci fıkrasında devletin iç hukukuna göre bu statüyü haiz her kişi veya kuruluşun bu kapsama dâhil olduğu belirtilmiştir[438]. Öte yandan söz konusu düzenlemede "dâhil olma" (*includes*) kelimesinin tercih edilmesinden anlaşılacağı üzere, ilgili fıkra ile devlet organı sıfatı iç hukuka göre belirli bir statüye sahip kişi veya kuruluşlarla sınırlanmamakta, aksine devletlerin iç hukuka dayanarak organlarının haksız eylemlerinden kaynaklanan sorumluluklarından kaçınmasını önlemek amacıyla uygulamadaki durumun da dikkate alınması gerekli kılınmaktadır[439]. Nitekim Uluslararası Adalet Divanı Soykırım Kararı'nda, istisnai hallerde, iç hukuka göre devlet organı statüsü taşımamakla birlikte büyük ölçüde devletin kontrolü altında olduğu ispatlanabilen kişi, grup veya kurumların da devlet organıymış gibi değerlendirilebileceğini beyan etmiştir[440]. Uluslararası Adalet Divanı'nın yaklaşımı ile hukuki olarak devlet organı statüsünü haiz olmamakla birlikte devletle arasında "tamamen bağlılık" ilişkisi olan kişi, grup ve kurumların araç olarak

---

[437]International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1, Art. 4.
[438]Ibid.
[439]Commentary to the Articles on State Responsibility, 2 Yearbook of the International Law Commission, Part II, 31, 40, Commentary to Art. 4, para. 11
[440]*Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia)*, International Court of Justice (ICJ), 26 Şubat 2007, para. 393.

kullanılarak uluslararası sorumluluklardan kaçınılmasının önüne geçilmesi amaçlanmaktadır[441].

Bir devletin organlarınca gerçekleştirilen eylemlerle bağlı olmasının bir sonucu olarak bir devletin ordusu, istihbarat yahut emniyet teşkilatı gibi yapılanmaları tarafından gerçekleştirilen uluslararası hukuka aykırı bir siber operasyon devletin uluslararası hukuk açısından söz konusu ihlalden sorumlu olmasına yol açacaktır[442]. Örneğin, Türk Silahlı Kuvvetleri bünyesinde Genelkurmay Başkanlığı'na bağlı olarak görev yapan Siber Savunma Komutanlığı'nın gerçekleştirmiş olduğu eylemler Türkiye Cumhuriyeti'ne atfedilebilecek ve bu kapsamda Türkiye Cumhuriyeti'nin bir organı olan bu kuruluşun personelleri tarafından gerçekleştirilecek siber operasyonlar sonucu uluslararası hukuk sorumluluğu oluşabilecektir. Nitekim yakın tarihimizde saldırgan siber operasyonların bir devletin askeri ve istihbarat birimlerine atfedildiği örneklere rastlanmış; Avustralya Dışişleri Bakanlığı 4 Ekim 2018 tarihinde gerçekleştirmiş olduğu bir basın duyurusuyla, başta 2017 senesinin Ekim ayında Ukrayna ve Rusya'da enerji ve ulaşım sektörü gibi kritik ulusal altyapıyı olumsuz etkileyen *BadRabbit* isimli fidye yazılımı olmak üzere çeşitli siber operasyonlardan Rus ordusu ve istihbarat teşkilatı GRU'nun sorumlu olduğunu açıklamıştır[443].

Keza hem kamu kuruluşu hem de özel kuruluş olarak rastlanabilen bilgisayar acil müdahale ekiplerinin (*computer emergency response teams – "CERTs"*) de bir devlet organı olarak hizmet vermesi halinde söz konusu kuruluşun eylemleri 4. madde uyarınca bağlı bulundukları devlete atfedilebilecektir[444]. Örneğin Türkiye, Siber Güvenlik Kurulu tarafından 21 Aralık 2012 tarihli toplantıda kabul edilen ve Bakanlar Kurulu'nun 20 Haziran 2013 tarihli ve 28683 sayılı kararı ile Resmi Gazete'de

---

[441]**Ibid**, para 392.
[442]NATO CCD COE, **Tallinn Manual 2.0**, s. 87.
[443]Avustralya söz konusu basın açıklamasında ayrıca uluslararası hukuk normlarının ihlali teşkil eden eylemlerin sonuçları olacağını ifade ederek ilgili eylemlerin sorumlu devlete atfedilmesini bunun ilk adımı olarak duyurmuşsa da duyuruda siber operasyonlar dolayısıyla uygulanacak herhangi bir yaptırıma ilişkin bilgi vermemiştir. (Department of Foreign Affairs and Trade, Attribution of a Pattern of Malicious Cyber Activity to Russia, Joint Media Release, 4 Ekim 2018, *https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-pattern-malicious-cyber-activity-russia*, erişim tarihi: 25.06.2020)
[444]Delerue, **Cyber Operations and International Law**, ss. 116-17.

yayımlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ile siber tehditlere karşı Ulusal Siber Olaylara Müdahale Merkezi'nin ("USOM") kurulmasını kararlaştırmıştır[445]. USOM'un kurulmasında sorumlu kuruluşun Ulaştırma Denizcilik ve Haberleşme Bakanlığı; ilgili kuruluşların ise İçişleri Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Telekomünikasyon İletişim Başkanlığı, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Tübitak olarak sayıldığı[446] da dikkate alındığında, USOM'un bir devlet organı olduğu ve dolayısıyla USOM tarafından gerçekleştirilecek siber operasyonların Türkiye Cumhuriyeti'ne atfedilebileceği tespiti yapılabilecektir.

3.3.1.2. Kamu Gücü ve Yetkilerini Kullanan Bir Kişi ya da Birimin Tasarrufu

ARSIWA'nın 5. maddesi uyarınca devlet organı olmasa dahi devletin hukuku tarafından kamu gücü yetkilerini kullanmak için yetkilendirilmiş olan kişi ya da grupların davranışlarının da uluslararası hukuk açısından devlet fiili olarak kabul edilmesi öngörülmüştür[447]. Bir kuruluşun 5. madde kapsamında değerlendirilmesi kendisine bahşedilen yetki, bu yetkinin bahşediliş şekli, amacı ve kuruluşun yetkinin kullanımına ilişkin hükümete ne ölçüde hesap verdiği kıstasları üzerinden gerçekleştirilmelidir[448]. Kamu gücü kullanan kişi veya kurumun tasarrufları değerlendirirken bağımsız bir takdir yetkisine sahip olması söz konusu eylemlerin devlete atfedilebilir olmasında bir fark yaratmadığından bu kişi veya kurumların devletin kontrolü altında gerçekleştirmediği eylemlerden dahi uluslararası hukuk sorumluluğunun doğması mümkün olacaktır[449].

Kamu gücünün kullanımına yönelik kişi ve kurumların yetkilendirilmesinin uluslararası hukuk açısından sonuçları son dönemde özellikle özel askeri şirketler

---

[445]Türkiye Cumhuriyeti Ulaştırma Denizcilik ve Haberleşme Bakanlığı, **Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı**, 2013, s. 19, *https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf,* erişim tarihi: 15.06.2020
[446]**A.g.e**, s. 26.
[447]International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Art. 5.
[448]Commentary to the Articles on State Responsibility, Commentary to Art. 5, para. 6.
[449]Commentary to the Articles on State Responsibility, Commentary to Art 5, para. 7.

açısından gündeme gelmiştir[450]. Benzer bir şekilde bir devletin özel bir şirkete kamu gücü bahşederek şirketi başka bir devlete siber operasyon gerçekleştirilmesi hususunda yetkilendirmesi halinde 5. madde kapsamında ilgili devletin uluslararası hukuk sorumluluğunun doğacağı sonucuna ulaşılabilecektir[451].

3.3.1.3. Bir Devlet Tarafından Bir Başka Devletin Emrine Verilmiş Bir Organın Tasarrufu

ARSIWA'nın 6. maddesine göre, bir devletin organının başka bir devletin emrine verilmesi halinde bu organ kamu gücü yetkilerini kullandığı sürece, söz konusu organın gerçekleştirmiş olduğu eylemler emri altında bulunduğu devlete atfedilecektir[452]. Bu madde kapsamında uluslararası hukuka aykırı bir eylemin gönderilen devlete atfedilebilmesi gönderen devletin emir altına vermiş olduğu birimin organ statüsünü haiz olmasına ve bu birimin gönderildiği devlette kamu gücü kullanmasına bağlıdır. Ayrıca madde kapsamındaki "emir altına verme" şartının gerçekleştiğinin kabulü için söz konusu organın, gönderen devletin değil, gönderilen devletin münhasır kontrolü ve talimatları altında faaliyet göstermesi gerekmektedir[453]. Lakin emir altına verilen organın halen gönderen devletten ödenek yahut kaynak ediniyor olması organ gönderilen devlet yararına faaliyet gösterdiği sürece atfedilebilirlik açısından herhangi bir değişiklik yaratmayacaktır[454].

Bir devletin başka bir devlete kolektif meşru müdafaa kapsamında askeri destek sağlaması gibi işbirliği amacıyla birtakım organların yeterliliklerinden faydalandırması, bu durumda söz konusu organın halen gönderen devlete bağlı olarak faaliyet göstermesi sebebiyle, gönderilen askeri kuvvetlerin eylemlerinin 6. madde uyarınca gönderilen devlete atfedilmesine olanak sağlamayacaktır[455]. Örneğin, Gürcistan'ın 2008 yılında siber saldırılara uğraması sonucu Estonya'nın yardım amaçlı

---

[450]James Crawford, **State Responsibility: the General Part**, New York, Cambridge University Press, 2013, s. 127.
[451]NATO CCD COE, **Tallinn Manual**, s. 31.
[452]International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Art. 6.
[453]Commentary to the Articles on State Responsibility, Commentary to Art. 6, para. 2.
[454]NATO CCD COE, **Tallinn Manual 2.0**, s. 93.
[455]Commentary to the Articles on State Responsibility, Commentary to Art. 6, para. 3.

iki bilgi teknoloji uzman göndermesi örneğinde görüldüğü gibi gönderilen devletin emrine verilmeyip sadece siber savunma çalışmalarına destek olma amacıyla gönderilmesi halinde 6. maddede atfedilebilirliğe ilişkin öngörülen şartlar sağlanmamaktadır[456]. Keza bir devletin teknik yardım sağlama gibi çeşitli sebeplerle uzmanlarını yahut danışmanlarını başka bir devletin emrine vermesi çoğu zaman uzman ve danışmanların organ statüsünü haiz olmaması nedeniyle 6. maddeye kapsamında değerlendirilemeyecektir[457].

Devletlerin saldırgan siber operasyonlara karşı kırılganlıkları gibi bu tip siber operasyonlara karşılık verebilme yeterlilikleri de değişiklik gösterebilmektedir. Dolayısıyla bir devletin şiddetli saldırgan siber operasyonlara maruz kalması halinde başka bir devletin, siber savunma faaliyetleri yürüten bir organını bir süreliğine saldırıya uğrayan devletin emrine vermesi durumuyla karşılaşılması olası olup bu takdirde yukarıda özetlenen kurallar çerçevesinde söz konusu organın faaliyetlerinden dolayı gönderilen devletin uluslararası hukuk sorumluluğu doğacaktır[458]. Üstelik siber savunma amacıyla başka bir devletin emri altına verilen organın 6. madde kapsamında atfedilebilirlik hususunda değişiklik yaratması için fiziken yer değiştirmesine dahi gerek duyulmayacaktır[459]. Ancak saldırgan siber operasyonların hem gönderen devleti hem gönderilen devleti etkilediği hallerde gönderen devletin bilgisayar acil müdahale ekiplerinin her iki devlet yararına gerçekleştirdiği eylemlere ilişkin 6. maddeye başvurulması mümkün gözükmemektedir[460].

3.3.1.4. Yetki Aşımı ya da Talimatlara Aykırı Davranış

ARSIWA'nın 7. maddesi uyarınca bir devlet organı veya kamu gücü yetkilerini kullanmakla yetkilendirilmiş bir kişi ya da birim resmi görevleri kapsamında hareket ederken kendilerine tanınan yetkileri aşarsa yahut talimatlara aykırı hareket ederse dahi söz konusu eylem uluslararası hukuka göre devletin fiili kabul edilecektir[461]. İlgili

[456]Eneken / Kaska / Vihul, **a.g.e**, s. 70
[457]Commentary to the Articles on State Responsibility, Commentary to Art. 6, para. 5
[458]Delerue, **Cyber Operations and International Law**, s. 126.
[459]Ibid.
[460]NATO CCD COE, **Tallinn Manual 2.0**, s. 94.
[461]International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Art. 7.

madde ile devletin uluslararası haksız bir fiilin sorumluluğundan kaçınması için iç hukuk düzenlemelerine veya verilen talimatlar ile uygulama arasındaki farklılıklara başvurmasının önlenmesi amaçlanmış olup aynı zamanda resmi görevini hukuka aykırı kullanan yahut bilerek yetkisini aşan kimselerin eylemlerinin de devlete atfedilmesi sağlanmıştır[462]. Lakin her halükarda resmi görev kapsamında yürütülen ve yetki aşımı teşkil eden eylemler ile hükümet çalışanlarının resmi görevleri dışında gerçekleştirmiş olduğu özel eylemler arasında ayrım yapılmalı, kişi veya grupların hususi eylem veya ihmallerinin devletin sorumluluğuna yol açmayacağı hususuna dikkat edilmelidir[463]. 7. maddedeki düzenlemenin devlet organlarının veya kamu gücü yetkilerini kullanan kişi ya da birimin tasarrufu ile bir devlet tarafından bir başka devletin emrine verilmiş bir organın tasarrufu açısından geçerli olması öngörülmüş olup devletin uluslararası hukuk sorumluluğunun doğduğu her ihtimali kapsamamaktadır[464].

Yetki aşımı ya da talimatlara aykırı davranışla uluslararası haksız fiilin işlenmesi ile siber alanda da karşılaşılması mümkündür. Siber operasyonlar gibi gizli yürütülen süreçlerde *ultra vires* ile hususi davranış arasında ayrım yapmak daha da zor olacağından eylemin devlete atfedilebilmesi için devlet organının görünen değil fiili olarak yürüttüğü resmi görevin dikkate alınması daha isabetli olacaktır[465]. Bir askerin siber savunma komutanlığının emirlerine aykırı hareket ederek hukuka aykırı bir siber operasyon gerçekleştirmesi halinde bağlı bulunduğu devletin uluslararası hukuk sorumluluğunun doğması siber alanda *ultra vires*e ilişkin akla ilk gelen örneklerdendir[466]. Benzer bir şekilde, kritik altyapısına karşı gerçekleştirilen düşmanca siber operasyonlara karşı bir devletin özel bir siber güvenlik firması ile anlaşması[467] yahut başka bir devlet tarafından bir organının siber savunma amacıyla saldırıya maruz kalan devletin emrine verilmesi[468] halinde, söz konusu birimlerce

[462]Commentary to the Articles on State Responsibility, Commentary to Art. 7, para. 2.
[463]Commentary to the Articles on State Responsibility, Commentary to Art. 7, para. 8.
[464]Commentary to the Articles on State Responsibility, Commentary toArt. 7, para. 9.
[465]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 36.
[466]Schmitt, **Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law**, s. 709.
[467]NATO CCD COE, **Tallinn Manual 2.0**, s. 90
[468]**A.g.e**, s. 94.

hack-back[469] eylemi gerçekleştirilmesi gibi *ultra vires* teşkil edecek bir eyleme başvurulması halinde de ilgili eylem devlete atfedilebilecektir. Öte yandan, ister bir devlet organı olarak çalışsın ister ise devlet organı olmamakla birlikte kendisine kamu gücü tahsis edilmiş olsun veya başka bir devletin organı olmakla birlikte söz konusu devletin emrine verilmiş olsun, herhangi bir kişi ya da birimin safi kendi çıkarları için gerçekleştirdiği bir siber operasyondan dolayı devletin uluslararası hukuk sorumluluğu doğmayacaktır.

3.3.2. Devlet Dışı Aktörlerin Tasarrufu

Yukarıda bahsedildiği üzere bir devletin siber operasyonlardan doğan hukuki sorumluluğu devlet organları veya kamu gücü kullanan kişi yahut birimlerin gerçekleştirdiği eylemlerle sınırlı değildir. Nitekim devletler saldırgan siber operasyonlardan kaçınmak için *hacktivist*ler[470] gibi devlet dışı aktörlerden de faydalanabilecektir. Örneğin Kanada, 28 Ekim 2019 tarihinde içlerinde hükümete ait olanların da bulunduğu 15.000 civarı internet sitesine yöneltilen siber operasyonların Rusya Federasyonu'nun askeri istihbarat birimi GRU'nun gözetimindeki *Sandworm Team* olarak adlandırılan bir birim tarafından gerçekleştirildiğini değerlendirdiklerini beyan etmiştir[471].

Bu bölümde öncelikle devlet tarafından yönlendirilen veya kontrol edilen eylemler, mevcut uluslararası hukuk içtihadı da göz önünde bulundurularak

---

[469]Hack-back aktif siber savunma olarak da adlandırılmakta olup saldırgan bir siber operasyonun önlenmesiyle yetinilmeyerek saldırının kaynağına saldırgan bir siber operasyonla karşılık verilmesi olarak özetlenebilir. (Patrick Lin, **Ethics of Hacking Back: Six Arguments from Armed Conflicts to Zombies**, A Policy Paper on Cyber Security, 2016, s. 3, *http://ethics.calpoly.edu/hackingback.pdf*, erişim tarihi: 01.08.2020)

[470]Hacktivist çoğunlukla yasa dışı yöntemlerle çeşitli siber araçları kullanarak eylemlerde bulunan kişi veya gruplar için kullanılan genel bir adlandırma olarak özetlenebilir. (Dorothy E. Denning, "Activism, Hacktivism, and Cyber Terrorism: The Internet as a Tool for Influencing Foreign Policy", **Networks and Netwars: The Future of Terror, Crime and Militancy**, Ed: John Arquilla / David Ronfeldt, RAND Corporation, 2001, (239-288), s. 263.

[471]Global Affairs Canada, Canada Condemns Russia's Malicious Cyber-Activity Targeting Georgia, Ottowa, 20 Şubat 2020, *https://www.canada.ca/en/global-affairs/news/2020/02/canada-condemns-russias-malicious-cyber-activity-targeting-georgia.html*, erişim tarihi: 26.06.2020; Öte yandan aynı siber operasyonlara yönelik Amerika Birleşik Devletleri doğrudan GRU'yu sorumlu tutmuş; açıklamada *Sandworm*'e GTsST'nin (GRU Özel Teknolojiler Merkezi) diğer bir ismi olarak yer verilmiştir. (U.S. Department of State, The United States Condemns Russian Cyber Attack Against the Country of Georgia, 20 Şubat 2020, *https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/*, erişim tarihi: 26.06.2020)

değerlendirilecek; akabinde ARSIWA'nın konuya ilişkin diğer düzenlemeleri olan "resmi makamların yokluğunda yahut yetersizliğinde gerçekleştirilen tasarruf" ile "isyancı hareket veya bir başka hareketin tasarrufu" incelenecektir. Son olarak da normal şartlarda devlet tarafından kendisinin olduğu onaylanıp kabul edilen eylemler siber operasyonlar açısından değerlendirilecektir.

3.3.2.1. Devlet Tarafından Yönlendirilen veya Kontrol Edilen Eylemler

ARSIWA'nın 8. maddesi gereğince bir kişi veya grubun belirli bir devletin talimatları, yönetimi yahut kontrolü altında gerçekleştirdiği eylemler uluslararası hukuk açısından ilgili devlete atfedilebilecektir[472]. Madde 8 özel kişilerin devletin talimatları doğrultusunda haksız fiil işlemeleri ve daha genel olarak devletin yönetimi ya da kontrolü altında haksız fiil işlemeleri şeklinde iki farklı hususu düzenlemekte olup bunlardan her ikisi açısından da esas unsur eylemi gerçekleştiren kişi veya grupla devlet mekanizması arasındaki gerçek bağlantıdır[473]. Bu anlamda "talimat", "yönetim" ve "kontrol" kelimeleri birbirine alternatif olarak kullanılmış olup içlerinden herhangi birinin uluslararası haksız fiil teşkil eden eylemi gerçekleştiren özel kişilerle devlet arasındaki ilişkiyi açıklıyor olması söz konusu madde uyarınca uluslararası sorumluluğun doğması için yeterlidir[474].

Devlet dışı aktörlerin eylemlerinin devlet tarafından kontrol edildiği hallerde ilgili devletin uluslararası hukuk sorumluluğunun doğacağı belirtilirken kastedilen

---

[472]International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Art. 8.

[473]Commentary to the Articles on State Responsibility, Commentary to Art. 8, para. 1.

[474]Commentary to the Articles on State Responsibility, Commentary to Art. 8, para. 7; Cassese devletin talimatı yahut yönetimi altında olma kavramlarının belirli bir eylemin gerçekleştirilmesi için devletin emir vermesi olarak özetlenebilmesi sebebiyle daha açık olduğu, buna kıyasla devletin kontrolü altında olma kriterinin ise önceki iki kritere göre daha gevşek olduğu eleştirisinde bulunmuştur. (Antonio Cassese, "The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia", **European Journal of International Law**, Vol. 18, No. 4, 2007, (649-668), s. 663) Öte yandan uluslararası mahkeme ve tahkimler tarafından devletin yönetimi altında olma ve devletin kontrolü altındaolma kriterlerinin tek bir standart olarak birlikte kullanıldığı gözlemlenmiştir. (Crawford, **State Responsibility: the General Part**, s. 146) Gerçekten de bir devletin talimatı altında olma kriterinin devlet organlarının resmi kanallar yerine "yardımcı" olarak kullandıkları özel kişiler aracılığıyla eylemlerini gerçekleştirdiği hallerde sağlanmış olacağı, yönetim veya kontrol altında olma kriterinin ise devletin yönettiği yahut kontrol ettiği bir operasyonun ayrılmaz parçası olan eylemlerin ilgili devlete atfedilmesinde başvurulabileceği yorumu yapılabilir. (Commentary to the Articles on State Responsibility, Commentary to Art. 8, para. 2-3)

kontrolün standardına ilişkin bir açıklık getirilmemesi, Uluslararası Adalet Divanı'nın Nikaragua ve Bosna Soykırımı kararları ile Eski Yugoslavya Uluslararası Ceza Mahkemesi'nin Tadic kararında görüldüğü üzere, uygulamada yaklaşım farklılıklarının oluşmasına yol açmıştır[475]. Uluslararası Adalet Divanı özel kişi veya grupların eylemlerinin devlete atfedilebilmesi hususunu incelerken etkin kontrol (*effective control*) değerlendirmesine göre hareket etmiş; Nikaragua Kararı'nda Amerika Birleşik Devletleri'nin hukuki sorumluluğunun askeri ve paramiliter güçler üzerinde etkin kontrolü olduğunun ispat edilmesi halinde söz konusu olabileceğini beyan etmiştir[476].

Eski Yugoslavya Uluslararası Ceza Mahkemesi Temyiz Kurulu ("EYUCM") ise Tadic Kararı'nda Nikaragua Kararı'nda uygulanan kıstasların uluslararası hukuktaki devlet sorumluluğu sisteminin mantığına aykırı olduğu eleştirisinde bulunmuş[477]; devlet dışı aktörlerin eylemlerinin devlete atfedilebilmesi için devletin bu kimseler üzerinde sahip olması beklenen kontrol seviyesinin her durumda değişiklik gösterebileceğini belirterek her seferinde yüksek bir kontrol kriterinin öngörülmesini eleştirmiştir[478]. Buna göre EYUCM bir devletin bireyler aracılığıyla uluslararası hukuka aykırı bir eylem gerçekleştirmesi halinde, etkin kontrol testinde önerildiği gibi, söz konusu bireylerin devlet talimatlarıyla hareket etmesi halinde ilgili eylemin devlete atfedilebileceğini ve devletin birey üzerindeki genel kontrolünün uluslararası hukuk sorumluluğunun oluşması için tek başına yeterli olmadığını belirtmiş;[479] devletin organize ve hiyerarşik olarak örgütlenmiş bir grup aracılığıyla hareket ettiği hallerde ise Nikaragua Kararı'ndan farklı olarak, eylemlerin devlete

---

[475]Crawford, **State Responsibility: the General Part**, s. 144.

[476]*Nikaragua Davası Kararı*, para. 115. Söz konusu kararda Uluslararsı Adalet Divanı, Amerika Birleşik Devletleri'nin her ne kadar operasyonlara doğdudan katıldığına dair bir delil mevcut olmasa da ABD yetkililerinin operasyonların planlamasında, yönetiminde ve desteklenmesinde yer aldığı tespitinde bulunmuştur. Lakin *kontra*lar tarafından gerçekleştirilen uluslararası insancıl hukuka aykırı eylemlerin Amerika Birleşik Devletleri'nin kontrolü olmadan da işlenebileceğini belirterek, Amerika Birleşik Devletleri'nin *kontra*ları finanse etmesi, örgütlemesi, eğitmesi, teçhizat sağlaması, askeri ve paramiliter hedefleri seçmesi ve operasyonları planlamasının *kontra*lar tarafından gerçekleştirilen uluslararası insancıl hukuka aykırı eylemerin ABD'ye atfedilebilmesi için tek başına yeterli olmadığı sonucunu ulaşmıştır. (*Nikaragua Davası Kararı*, para. 86, 115-16)

[477]*Prosecutor v. Dusko Tadic* (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999, ("Tadic Kararı") para. 116.

[478]*Tadic Kararı*, para. 117.

[479]*Tadic Kararı*, para. 118-19

atfedilebilmesi için devletin grup üzerinde genel kontrolü (*overall control*) bulunmasını yeterli bulmuştur[480].

Uluslararası Adalet Divanı Soykırım Kararı'nda EYUCM'nin yargı yetkisinin ceza hukukuna yönelik olduğunu ve bu kapsamda sadece bireyleri kapsadığını, dolayısıyla da genel uluslararası hukuk meselelerinde bu yaklaşımın benimsenmesinin gerekli olmadığını;[481] Tadic Kararı'nda açıklanan genel kontrol testinin bir silahlı çatışmanın uluslararası nitelikte olup olmadığını değerlendirmek için uygulandığını[482] ve devletin başka bir ülkenin bölgesindeki silahlı çatışmalara dahil olması ile devlete belirli eylemlerin atfedilebilmesinin farklı hususlar olması sebebiyle iki farklı yaklaşım belirlenmesinin mantığa da aykırı düşmeyeceğini belirtmiştir[483]. Sonuç olarak Uluslararası Adalet Divanı, etkin kontrol testinin ARSIWA'nın uluslararası teamül hukukunu yansıtan 8. maddesiyle uyumlu bir düzenleme olduğunu açıklayarak, genel kontrol testinin devletin uluslararası hukuktan doğan sorumluluğunun kapsamını uluslararası sorumluluğun temel ilkelerine kıyasla çok fazla genişletmesi sebebiyle genel kontrol testini kararında uygulamayacağını beyan etmiştir[484]. Cassese, Uluslararası Adalet Divanı'nın Soykırım Kararı'na eleştiri getirerek devlet uygulamaları ve içtihatların "genel kontrol" standardını desteklediğini ifade etmiş; organize silahlı grupların ve askeri birimlerin eylemleri söz konusu olduğunda, ilgili eylemin devlete atfedilebilmesi için her operasyona yönelik belirli talimatların verilip verilmediği yönünde bir incelemeye gerek duyulmadığını savunmuştur[485]. Crawford ise, Tadic Kararı'nda uygulanan genel kontrol kriterinin kabul edilmesi durumunda bir devletin tek bir teröriste yahut bir gruba yönelik finans, eğitim, danışmanlık sağlama

---

[480] *Tadic Kararı*, para. 120.

[481] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007, ("Soykırım Kararı"), para. 403.

[482] *Soykırım Kararı*, para. 404.

[483] *Soykırım Kararı*, para 405.

[484] *Soykırım Kararı*, para. 406-07

[485] Cassese, **The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia**, s. 657; Keza öğretide kimi yazarlarca bu yaklaşım daha da genişletilmiş; bir silahlı saldırının devlete atfedilebilirliği hususunda uluslararası teamül hukukunun "barındırma kriterine" doğru evrildiği ve bu kapsamda devlet dışı aktörlerin eylemlerine pasif yaklaşılarak söz konusu eylemlerin gerçekleştirilmesinin kolaylaştırılmasının da devletin hukuki sorumluluğunun doğmasına yol açabileceği ileri sürülmüştür. (Pirim, **a.g.m**, s. 268)

veya eylemlerini planlama gibi yardımlarının sonuçları açısından ayrım yapmanın zor olacağı gerekçesiyle Uluslararası Hukuk Komisyonu'nun söz konusu yaklaşımının benimsenmesi gerektiğini belirtmiştir[486].

Saldırgan siber operasyonların büyük bir kısmının devlet dışı aktörler tarafından gerçekleştirildiği dikkate alındığında devletin uluslararası hukuk sorumluluğunun siber alanda da uygulanmasının elzem olduğu aşikardır[487]. Kimi yazarlarca, saldırgan siber operasyonların etkin kontrol kriterlerine göre değerlendirilmesinin devletlerin söz konusu eylemlerin kendilerine atfedilmesinden kurtulmasına olanak sağlayacağından, siber operasyonların uluslararası hukuk açısından sonuçları incelenirken genel kontrol kriterinin uygulanması gerektiği savunulmuştur[488]. Keza etkin kontrol ve genel kontrol testlerinin siber alanın karakteristik özelliklerine uygun olmadığı öne sürülerek alternatif bir standardın oluşturulması gerektiği yönünde görüşler de ileri sürülmüştür[489]. Örneğin Margulies, siber operasyonların atfedilmesi hususunda dar bir yaklaşımın da geniş bir yaklaşımın da kendi içerisinde riskler taşıdığını belirterek "sanal kontrol" (*virtual control*) olarak isimlendirdiği bir yaklaşım tavsiye etmiştir[490]. Margulies sanal kontrol standardı ile özetle, saldırgan bir siber operasyon halinde ispat yükümlülüğünün yer değiştirmesini önermiş; söz konusu saldırının kaynaklandığı devletin mağdur devlete sağlayacağı açıklamalarla siber operasyondan sorumlu olmadığını kanıtlayamaması halinde uluslararası hukuk sorumluluğunun doğacağını ve eylem silahlı saldırı teşkil ettiği takdirde saldırıya maruz kalan devlete meşru müdafaa hakkının tanınması gerektiğini savunmuştur[491]. Siber alana özgü bir isnat kriterinin atfedilebilirlik meselesine katkılar sağlayabileceğini kabul etmekle birlikte, bu tip bir yaklaşımın ancak devlet uygulaması yahut uluslararası mahkemelerin içtihatları aracılığıyla geçerli

[486]Crawford, **State Responsibility: the General Part**, ss. 153-54.
[487]Delerue, **Cyber Operations and International Law**, s. 144.
[488]Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", **Berkeley Journal of International Law**, Vol. 27, No. 1, 2009, (192-252), s. 235.
[489]Bradley Raboin, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", **Journal of the National Association of Administrative Law Judiciary**, Vol. 31, No. 2, 2011, (602-666), s. 659.
[490]Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", **Melbourne Journal of International Law**, Vol. 14, No. 2, 2013, (469-519), ss. 500-501
[491]Margulies, **a.g.e**, ss. 514-15

sayılabileceği ve henüz bu yönde bir gelişmeye rastlanmaması sebebiyle bu tip çözüm önerilerinin uluslararası hukuk açısından herhangi bir geçerliliği bulunmayacağı kanaatindeyiz. Bizim de katıldığımız görüş, siber operasyonların isnat edilmesinin daha zor olması sebebiyle yanlış bir devlete siber operasyonların atfedilerek meşru müdafaaya başvurulması ihtimalinden dolayı etkin kontrol kriterinin daha uygun olduğunu savunmaktadır[492]. Dolayısıyla örneğin, herhangi bir devletin, özel bir şirketle girmiş olduğu sözleşmesel ilişki kapsamında üçüncü bir devletin Merkezi Kontrol ve Veri Toplama Sistemi'ne (*Supervisory Control And Data Acquisition* – "SCADA") yıkıcı bir *logic bomb* yüklenerek fiziki zarar verilmesini emretmesi halinde, söz konusu şirketin gerçekleştirmiş olduğu eylem devlete atfedilebilecektir[493]. Ancak 2007'de Estonya'ya karşı gerçekleştirilen siber operasyonlarda deneyimlendiği üzere, bir devletin devlet dışı aktörlerin gerçekleştirmiş olduğu eylemleri sessizce onaylaması yahut sorumluların cezalandırılması hususunda işbirliğinden kaçınması tek başına etkin kontrol kriterini karşılamadığından söz konusu saldırıların herhangi bir devlete atfedilmesi için yeterli görülmeyecektir[494].

Son olarak belirtmek gerekir ki Uluslararası Adalet Divanı, madde 8 kapsamında doğan hukuki sorumluluğu devletin *de facto* organının gerçekleştirmiş olduğu eylemden doğan sorumluluktan ayırmış; bir eylemi gerçekleştiren birimin devletin *de facto* organı olmamakla birlikte devletin talimatları, yönetimi veya kontrolü altında hareket ettiği anlaşıldığı takdirde, sadece bu kapsamda gerçekleştirilen eylemler yönünden ilgili devletin sorumluluğu doğabileceğini belirtmiştir[495]. Bu yaklaşımın bir sonucu olarak, devlet dışı bir aktörün gerçekleştirmiş olduğu siber operasyonun *ultra vires* teşkil etmesi halinde, *de facto* organın eylemlerinden farklı olarak ancak *ultra vires* olarak değerlendirilen eylemlerin görevin ayrılmaz bir parçası olması halinde ilgili eylem devlete atfedilebilecektir[496].

---

[492]Roscini, **Cyber Operations and the Use of Force in International Law**, s. 100.
[493]NATO CCD COE, **Tallinn Manual 2.0**, ss. 97-98.
[494]Schmitt / Vihul, **Proxy Wars in Cyberspace: The Evolving International Law of Attribution**, s. 63.
[495]*Soykırım Kararı*, para. 397.
[496]NATO CCD COE, **Tallinn Manual 2.0**, s. 98.

3.3.2.2. Resmi Makamların Yokluğunda veya Yetersizliğinde Bulunulan Tasarruf

ARSIWA'nın 9. maddesi gereğince resmi makamların yokluğunda veya yetersizliğinde ve şartların bu güç unsurlarının kullanılmasını gerektirdiği hallerde kamu gücü kullanan unsurların tasarrufları uluslararası hukuka göre devlete atfedilebilecektir[497]. Siber operasyonların kamu gücünün kullanılması teşkil edebileceği de dikkate alındığında, bir devletin resmi makamlarının yokluğunda veya yetersizliğinde devlet dışı aktörlerce başka bir devlete yöneltilen siber operasyonlar söz konusu devletin uluslararası hukuk sorumluluğunun doğmasına yol açabilecektir[498].

3.3.2.3. İsyancı Hareketin veya Bir Diğer Hareketin Tasarrufu

ARSIWA'nın 10. maddesine göre isyancı hareket yahut başka türlü bir hareketin daha sonra devletin yeni hükümetini oluşturması veya önceki devletin bölgesinde yeni bir devlet oluşturması halinde söz konusu hareketin eylemleri bu yeni (?) devletin uluslararası hukuk sorumluluğunun doğmasına yol açabilecektir[499]. Burada belirtmek gerekir ki isyancı grup devlete karşı hareket ettiği takdirde devletin iyi niyete aykırı bir tutumla ihmali olmaması halinde söz konusu hareketin eylemlerinden devlet sorumlu tutulmayacak; lakin hareketin hükümet olmayı başarması veya yeni bir devlet kurması durumunda hareketin üyelerinin isyan sırasında gerçekleştirmiş olduğu davranışlar kurulan yeni devlete yüklenebilecektir[500]. İlgili madde isyancı hareketin eylemlerini devlete atfederken önceki devletin yönetiminin başarılı bir şekilde ele geçirilmesi veya yeni bir devlet kurulmasını yeterli görerek eylemin niteliğine göre bir ayrım gerçekleştirmediğinden siber operasyonların

[497]International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Art. 9.
[498]Delerue, **Cyber Operations and International Law**, s. 151.
[499]International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Art. 10.
[500]Hakkı Hakan Erkiner, **Devletin Haksız Fiilden Kaynaklanan Uluslararası Sorumluluğu**, 1. Baskı, İstanbul, On İki Levha Yayıncılık, 2010, s. 144.

da 10. madde kapsamında bir devletin uluslararası hukuk sorumluluğunun doğmasına yol açması mümkündür[501].

3.3.2.4. Devlet Tarafından Kendisinin Olduğu Onaylanan ve Kabul Edilen Tasarruf

Bir özel kişi veya grubun gerçekleştirdiği haksız fiil yukarıda değinilen maddeler kapsamında devlete atfedilemiyor olsa dahi herhangi bir devlet bu kimselerce gerçekleştirilen bir eylemi kendisinin olarak onaylayıp kabul ettiği takdirde ARSIWA'nın 11. maddesi sebebiyle uluslararası sorumluluğu doğabilecektir[502]. Devletin devlet dışı bir aktör tarafından sergilenen eylemin tamamını kendisinin olarak onaylayıp kabul etmesi gerekmemektedir; lakin devletin eylemlerin bir kısmını kendisinin olarak onaylayıp kabul etmesi halinde devletin uluslararası hukuk sorumluluğu sadece kendisinin olarak onaylayıp kabul ettiği kısım açısından geçerli olacaktır[503].

Roscini devletlerin siber alanın alanın kendilerine sunduğu gizli operasyon yapma imkanından faydalanma yatkınlığı dikkate alındığında böylesi bir yaklaşımın siber operasyonlar açısından gerçekleşme olasılığının düşük olduğu yorumunda bulunmuştur[504]. Her ne kadar ilgili madde ile onaylama ve kabul etme kriterleri kümülatif olarak öngörülerek devletin yalnızca bir eylemin varlığını kabul etmesinin yahut destek gösteren açıklamalarda bulunmasının eylemin devlete atfedilebilmesi için yeterli olmadığı belirtilmişse de söz konusu onaylama ve kabulün açık olarak gerçekleştirilmesi şart koşulmamış, devletin eylemlerinden de bu sonuca ulaşılabileceği kabul edilmiştir[505]. Nitekim Uluslararası Adalet Divanı Amerika Birleşik Devletleri'nin Tahran'daki Diplomatik ve Konsolosluk Çalışanlarına İlişkin Karar'ında her ne kadar haksız fiili gerçekleştiren kimselerin devletin organı yahut çalışanı olduğuna veya devlet adına hareket ettiklerine dair yeterli delil bulunmasa

[501]Delerue, **Cyber Operations and Interational Law**, s. 157.
[502]International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Art. 11.
[503]Commentary to the Articles on State Responsibility, Commentary to Art. 11 para. 7.
[504]Roscini, **Cyber Operations and the Use of Force in International Law**, ss. 39-40.
[505]Commentary to the Articles on State Responsibility, Commentary to Art. 11 para. 6-9.

dahi Ayetullah Humeyni'nin ve diğer İran devlet organlarının ABD Hükümeti'ne baskı yapabilmek amacıyla elçiliğin işgaline ve rehinelerin tutukluluğunun devamına yönelik onay vermeleri sebebiyle eylemi gerçekleştirenlerin devletin çalışanları haline geldiğini ve eylemlerin devlete atfedilebilir olduğunu beyan etmiştir[506]. Uluslararası Adalet Divanı'nın yukarıda özetlenen kararı siber operasyonlar açısından da uygulanabilecektir[507]. Dolayısıyla bir devletin devlet dışı aktörlerce gerçekleştirilen bir siber saldırıyı tasvip ettiğini açıklaması tek başına söz konusu eylemi devlete atfedilebilir kılmayacak; ancak devletin siber yeterliliklerini bilerek eylemi gerçekleştiren devlet dışı aktörleri karşı siber operasyonlara karşı koruması gibi girişimlerde bulunarak siber operasyonların devamını sağlaması halinde haksız fiilin devlet tarafından benimsendiği söylenebilecek ve uluslararası hukuk kapsamında sorumluluğu doğabilecektir[508].

[506]*Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*; Order, 12 V 81, International Court of Justice (ICJ), 12 May 1981, para. 58 -74.
[507]Scott J. Shackelford / Richard B. Andres, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem", **Georgetown Journal of International Law**, Vol. 42, No, 4, 2011, (971-1016), s. 989.
[508]NATO CCD COE, **Tallinn Manual 2.0**, s. 99.

SONUÇ

Çalışmamızda, siber operasyonlar mevcut uluslararası hukuk normları uyarınca incelenerek siber operasyonların hangi koşullarda uluslararası haksız fiil, kuvvet kullanma eylemi veya kuvvet kullanma tehdidi, saldırı yahut silahlı saldırı olarak değerlendirilebileceği ve nasıl sorumlu devlete atfedilebileceği meseleleri ele alınmıştır.

Yakın geçmişimizde pek çok saldırgan siber operasyona tanıklık edilmiştir. Siber alanın öneminin her geçen gün artması sebebiyle gelecekte saldırgan siber operasyonların olası etkilerinin devletler için daha da yıkıcı olması ihtimali söz konusudur. Keza yeni teknolojik gelişmeler siber güvenliğe ilişkin daha nitelikli önlemler alınabilmesine olanak tanısa da bu durum aynı zamanda ileride gerçekleştirilecek siber operasyonların daha etkili bir askeri harekat yöntemine dönüşmesine de yol açabilecektir. Kaldı ki şimdiye kadar karşılaşılan siber operasyonlar kapsamında mevcut yetkinliklerin ne denli kullanıldığından emin olmak mümkün olmasa dahi devletlerin bu alanda uzman personelleri aracılığıyla daha ciddi siber operasyonlar gerçekleştirme imkanları bulunduğu tahmin edilebilmektedir.

Öte yandan siber alan devletlerin kurallardan bağımsız olduğu yeni bir muharebe alanı olarak yorumlanmamalıdır. Nitekim her ne kadar henüz doğrudan siber operasyonları düzenleyen bir uluslararası sözleşme bulunmasa da mevcut uluslararası sözleşmeler uygun düştüğü ölçüde siber operasyonlara uygulanabilecektir. Ayrıca devletlerin son dönemde ilan ettikleri siber güvenlik planlamaları yahut resmi kanallar aracılığıyla duyurdukları bildiriler aracılığıyla konuya ilişkin yaklaşımlarını her fırsatta kamuoyuna açıkladıkları dikkate alındığında, bu alandaki uluslararası teamül hukuku kurallarının da yakın bir gelecekte oluşmaya başlayacağı öngörülebilmektedir.

Siber operasyonların uluslararası hukuka tabi olmasının en önemli sonucu, şüphesiz bu çalışmanın da esas odak noktasını oluşturan kuvvet kullanma yasağının siber alanda gerçekleştirilecek eylemler açısından da bağlayıcılık taşımasıdır. Elbette

bu tespit şimdiye değin devletlerin vuku bulan herhangi bir siber operasyonu açık bir şekilde kuvvet kullanma yahut kuvvet kullanma tehdidinde bulunma yasağının ihlali olarak değerlendirmediği gerçeğiyle birlikte yorumlanmalıdır. Gerçekten de siber operasyonların büyük bir kısmının kuvvet kullanma eşiğine erişmemesi beklenmektedir. Öte yandan bu takdirde dahi söz konusu eylemlerin uluslararası haksız fiil teşkil etme ihtimali mevcuttur. Nitekim uluslararası hukuk, egemen devletlerin eşitliği düşüncesini temel almaktadır. Dolayısıyla bir devletin başka bir devletin içişlerine ilişkin bir mesele hakkında baskı oluşturarak bir şeyi yapma veya bir şeyi yapmaktan kaçınma hususunda zorlaması uluslararası hukuka aykırılık teşkil edecektir. Siber operasyonlar ise nispeten gizli yürütülebiliyor olması, farklı şekillerde yürütülebiliyor olması ve diğer yöntemlere nazaran daha kolay gerçekleştirilebiliyor olması gibi sebeplerle bu yöndeki girişimler için önemli bir alternatif oluşturmaktadır. Lakin devletlerin son dönemdeki hasmane siber aktivitelere karşı gösterdiği hassasiyet dikkate alındığında, gelecekte kuvvet kullanma eşiğine erişmeyen ancak uluslararası haksız fiil teşkil eden siber operasyonlara ilişkin de uluslararası toplumda mevcut normlara riayet edilmesine daha büyük önem atfedileceği umudunu taşımak mümkündür.

Çalışma kapsamında siber operasyonlar *jus ad bellum* çerçevesinde incelenirken mevcut görüşlerin öncelikle kuvvet kullanma kavramı üzerinden değerlendirilmesi tercih edilmiştir. Zira kuvvet kullanma veya kuvvet kullanma tehdidinde bulunma yasağı sadece Birleşmiş Milletler Şartı'nın 2(4) numaralı maddesinde yer verildiği şekliyle önem arz etmemektedir. Nitekim Birleşmiş Milletler Genel Kurulu'nun 3314 sayılı Saldırı'nın Tanımına İlişkin Karar'da saldırı kavramı netleştirilirken kuvvet kullanma kavramı üzerinden hareket edilmiş; yine Uluslararası Adalet Divanı'nın içtihatlarında da silahlı saldırı kavramının kapsamı kuvvet kullanma eylemleri aracılığıyla netleştirilmeye çalışılmıştır. Bunun bir sonucu olarak, saldırgan bir siber operasyona yönelik uluslararası hukuka uygun bir şekilde tek taraflı kuvvete başvurulabilmesi için öncelikle söz konusu operasyonun kuvvet kullanma eşiğine erişip erişmediği değerlendirilmelidir.

Öğretide bu husus tartışılırken araç odaklı yaklaşım, hedef odaklı yaklaşım ve etki odaklı yaklaşım olmak üzere üç farklı görüş üzerinden hareket edildiği gözlemlenmiştir. Araç odaklı yaklaşım siber operasyonları kuvvet kullanma yasağı kapsamında değerlendirirken, söz konusu operasyonda kullanılan araçlara odaklanmakta ve bu araçların geleneksel silahlarla kıyaslanabilir olması halinde eylemin kuvvet kullanma eşiğine eriştiğinin kabul edilmesi gerektiğini savunmaktadır. Her ne kadar bu yaklaşım, ekonomik baskı mekanizmaları ile kuvvet kullanma teşkil eden eylemler arasında bir ayrımın sağlanması açısından işlevsel olsa da içinde bulunduğumuz çağın temel özelliklerini göz ardı etmektedir.

Hedef odaklı yaklaşım ise siber operasyonların kuvvet kullanma yasağını ihlal edip etmediğini değerlendirirken söz konusu operasyonun ulusal kritik altyapıya yöneltilmiş olmasını kıstas almaktadır. Bu yaklaşımın temel noktası ulusal kritik altyapının bir parçası olan sistemlerin devletler için daha önemli olduğu ve bu sistemlere yöneltilen siber operasyonların daha büyük bir tehdit teşkil etmesi sebebiyle kuvvet kullanma eşiğine eriştiğinin kabul edilmesi gerektiği yönündedir. Lakin bu yaklaşım ulusal kritik altyapıya yöneltilen siber operasyonlar arasında herhangi bir ayrım öngörmediğinden düşük tesirli siber operasyonların dahi kuvvet kullanma eylemi olarak değerlendirilmesine olanak tanımaktadır. Keza hedef odaklı yaklaşım uyarınca ulusal kritik altyapıya yöneltilmeyen ancak vatandaşların hayatını kaybetmesi gibi bir devlet için önemli görülebilecek zaiyata yol açan siber operasyonların nasıl değerlendirileceği de ayrı bir soru işaretidir. Kaldı ki ulusal kritik altyapıya dair genel geçer bir tanımlamaya ulaşmak dahi mümkün değildir. Dolayısıyla ulusal kritik altyapıya ilişkin devletler arasında farklı yaklaşımlar olabileceği gibi devletlerin herhangi bir sistemi ulusal kritik altyapının bir parçası kabul edebiliyor olması hedef odaklı yaklaşım uyarınca gerçekçi bir sonuca ulaşılmasını güçleştirmektedir. Böyle bir yaklaşımın benimsenmesi halinde ufak çaplı siber operasyonlar sonucunda dahi devletler arasındaki çatışma ortamının şiddetlenmesi riski ortaya çıkabilecektir.

Günümüzde yaygın olarak kabul edilen etki odaklı yaklaşım, saldırgan siber operasyonların kuvvet kullanma eşiğine erişip erişmediğinin değerlendirilmesinde söz

konusu siber operasyonun yol açtığı etkilerin esas alınması gerektiğini ileri sürmektedir. Gerçekten de devletlerin bir eylemin kuvvet kullanma olarak değerlendirilmesinde kullanılan araçlar veya yöneltilen hedeften ziyade karşılaşılan sonuçlarla ilgilenmesi daha olasıdır. Zira bir tesisin havaya uçurulmasında taarruz uçaklarının kullanılması yahut siber-fiziksel sistemlere yüklenen kötücül yazılımlara başvurulması arasında ayrım yapmak makul gözükmemektedir. Etki odaklı yaklaşımı savunanlar tarafından bir siber operasyonun kuvvet kullanma olarak kabul edilebilmesi fiziksel bir zarara yol açılmış olması şartına bağlanmıştır. Bu kapsamda hukukçular arasında maddi hasar yahut can kaybı gibi fiziksel bir zarara yol açan bir siber operasyonun kuvvet kullanma eşiğine eriştiği yönünde büyük bir uzlaşı mevcuttur. Lakin kuvvet kullanma olarak değerlendirilebilecek saldırgan siber operasyonları fiziksel zarara yol açma koşulu ile sınırlamak günümüzde siber alana duyulan bağımlılığı ve siber alan aracılığıyla gerçekleştirilecek ve fiziksel zarara yol açmayacak siber operasyonlar sonucu yaratabilecek zaiyatı göz ardı etmek anlamına gelmektedir. Bu doğrultuda son dönemde etki odaklı yaklaşımın tadil edilerek fiziksel zarara yol açanların yanı sıra bir devlet için kritik öneme sahip sistemlerin çalışırlığını uzun süreliğine etkileyen saldırgan siber operasyonların da kuvvet kullanma eylemi olarak değerlendirilmesi gerektiği öne sürülmektedir. Zira bir devletin enerji santrallerini devre dışı bırakıp günler süren elektrik sıkıntısına yol açan bir siber operasyonun etkileri bakımından aynı enerji santralinde ortaya çıkan yerel düzeyde bir patlamadan daha vahim olacağı çıkarımında bulunulabilmektedir.

Çalışma kapsamında kuvvet kullanma yasağının ilk istisnası olarak Birleşmiş Milletler Şartı'nın 7. Bölümünde yer verilen kolektif güvenlik normlarına yer verilmiştir. Nitekim Birleşmiş Milletler Güvenlik Konseyi Birleşmiş Milletler Şartı'nın 39. maddesi uyarınca barışın tehdit edildiğini, bozulduğunu ya da bir saldırı eyleminin vuku bulduğunu saptadığı takdirde Birleşmiş Milletler Şartı'nın 41. maddesinde yer verilen zorlayıcı olmayan önlemlere veya 42. maddede düzenleme bulan zorlayıcı önlemlere başvurabilmektedir. Saldırgan siber operasyonların belirli koşullarda kuvvet kullanma eşiğine erişebildiği dikkate alındığında bir siber operasyonun saldırı eylemi olarak da değerlendirilebileceği sonucuna ulaşılabilmektedir. Kaldı ki Birleşmiş Milletler Güvenlik Konseyi barışın tehdit

edildiği, bozulduğu ya da saldırı eyleminin vuku bulduğu yönündeki değerlendirmelerinde takdir yetkisine sahiptir. Hâlihazırda birçok devlet de siber operasyonların da bu kapsamda değerlendirilerek konunun gerektiği takdirde Güvenlik Konseyi'nin yetkileri çerçevesinde gerekli yaptırımlarla çözümlenmesi gerektiği yönünde görüş beyan etmiştir. Gerçekten de Birleşmiş Milletler Güvenlik Konseyi'nin söz konusu yetkilerini kullanması siber alanda hasmane aktivitelerin önlenmesi açısından elverişli bir mekanizma olarak değerlendirilebilecektir. Öte yandan nispeten daha ivedi meselelerde dahi Birleşmiş Milletler Güvenlik Konseyi'nin daimi üyeleri arasındaki politik anlaşmazlıklar sebebiyle veto hakkı aracılığıyla karar süreçlerinin tıkandığı dikkate alındığında böyle bir çözümün uygulamada sonuç vermesi ihtimalinin düşük olduğu öngörüsünde bulunulabilinir.

Tek taraflı kuvvet kullanma yasağının bir diğer istisnası ise meşru müdafaa hakkı kapsamında kuvvet kullanılmasıdır. Nitekim Birleşmiş Milletler Şartı'nın 51. maddesi uyarınca bir devletin silahlı saldırıya uğraması halinde meşru müdafaa hakkına başvurabileceği hususu güvence altına alınmıştır. Uluslararası Adalet Divanı içtihatlarında en şiddetli kuvvet kullanma eylemlerinin silahlı saldırı olarak değerlendirildiği görülmektedir. Uluslararası Adalet Divanı farklı kararlarında istikrarlı olarak söz konusu ayrımın yapılmasında gerçekleştirilen eylemin boyutu ve etkilerinin esas alınması gerektiğini ifade etmiştir. Dolayısıyla etki ve boyutları açısından en şiddetli kuvvet kullanma eylemleri arasında olduğu kabul edilebilen siber operasyonların aynı zamanda silahlı saldırı teşkil ettiği sonucuna ulaşılabilmektedir. Öte yandan kuvvet kullanma ile silahlı saldırı eşikleri arasında açıkça ayrım yapıldığı dikkate alındığında ancak ciddi fiziksel zarara yol açan saldırgan siber operasyonların meşru müdafaa hakkının kullanılmasına yol açabileceği kanaatindeyiz.

Saldırgan bir siber operasyona maruz kalan devlet meşru müdafaa hakkı kapsamında başka bir siber operasyonla karşılık verebileceği gibi geleneksel askeri yöntemler aracılığıyla da kuvvet kullanabilecektir. Zira meşru müdafaa hakkı kapsamında maruz kalınan saldırıyla aynı yöntemin kullanıldığı bir saldırı ile karşılık verilmesi yönünde bir sınırlama öngörülmemiştir. Saldırgan bir siber operasyona karşılık kinetik kuvvete başvurulması fikri ilk bakışta çatışma ortamının daha da

şiddetlenmesine yol açabileceği yönünde eleştirilere maruz kalabilir. Lakin meşru müdafaa hakkı gereklilik, ölçülülük ve aciliyet ilkeleri doğrultusunda sınırlandırmıştır. Dolayısıyla bir devlet saldırı eşiğine erişen bir siber operasyona karşılık verirken hangi yöntemi benimserse benimsesin silahlı saldırıyı defetmek amacıyla ve gerektiği ölçüde kuvvete başvurabilecektir. Devletler saldırgan siber operasyonlara ilişkin de meşru müdafaa hakkını bireysel yahut kolektif olarak kullanabilecektir. Nitekim NATO da üye devletlerden birinin silahlı saldırı eşiğine erişen bir siber operasyona maruz kalması halinde kolektif meşru müdafaaya başvurulabileceğini beyan etmiştir. Son olarak ifade etmek gerekir ki meşru müdafaa hakkı kapsamında kuvvet kullanan devlet bu kapsamda aldığı önlemlere ilişkin derhal Birleşmiş Milletler Güvenlik Konseyi'ni bilgilendirmelidir.

Çalışma kapsamında incelenen hususların uluslararası hukuk açısından bir sonuç doğurabilmesi büyük oranda siber operasyonların sorumlu devlete atfedilebilmesine bağlıdır. Zira devletler tüzel kişilik olması sebebiyle kendileri adına hareket eden kişi yahut birimler aracılığıyla eylemlerini gerçekleştirmektedirler. Öte yandan bir siber operasyonun belirli bir devletin ülkesinden kaynaklanması tek başına söz konusu operasyonun o devlete isnat edilebileceği anlamına gelmemektedir. Nitekim siber operasyonlar herhangi bir devletin bilgisi olmadan gerçekleştirilebileceği gibi bir devlet bilinçli olarak teknik araçlardan faydalanarak siber operasyonun yöneltildiği devleti saldırının kaynağı konusunda yanıltabilecektir. Lakin siber operasyonun sorumlu devlete isnat edilebilmesi teknik olarak imkansız değildir. Birçok devlet şimdiden uluslararası hukuka aykırı olduğunu iddia ettiği siber operasyonlara ilişkin başka devletleri itham etmiştir. Her ne kadar mevcut örnekler şimdilik sınırlı sayıda olsa da siber operasyonların nicelik ve nitelik olarak etkisinin artmasıyla birlikte söz konusu operasyonların sorumlulara atfedilmesine gösteren ehemmiyetin de artması beklenmektedir.

Tıpkı kuvvet kullanma yasağı ve tek taraflı kuvvete başvurulabilen hallerde görüldüğü gibi siber operasyonların atfedilmesi hususu da uluslararası hukukun mevcut normları çerçevesinde çözümlenebilecektir. Bu kapsamda bir devletin ordusu veya istihbarat güçleri gibi devlet organlarınca veya kamu gücü yetkilerini kullanan

kişi ya da birimlerce gerçekleştirilen siber operasyonların, söz konusu eylemler bir yetki aşımı sonucu gerçekleştirilmiş olsa dahi, bağlı bulundukları devletin uluslararası hukuk sorumluluğunun doğmasına yol açabilecektir. Keza siber alanda devlet dışı aktörlerin de yoğun bir şekilde faaliyet gösterdiği dikkate alındığında, devletlerin siber operasyonların gerçekleştirilmesi için özel siber güvenlik firmaları gibi devlet dışı aktörlerden de faydalanması olasıdır. Bu takdirde de bir devletin talimatları, yönetimi yahut kontrolü altında gerçekleştirilen siber opreasyonlar devlet dışı aktörü yönlendiren veya kontrol eden devlete atfedilebilecektir. Böylelikle siber operasyondan sorumlu olan devlete karşı, siber operasyonun niteliğine göre, karşı önlemlere başvurulabilecek hatta meşru müdafaa hakkı kapsamında kuvvet kullanılabilecektir.

Sonuç olarak, siber operasyonların nispeten yeni bir kavram olduğu dikkate alındığında, meselenin uluslararası hukuk açısından yorumlanmasında kısa sürece ciddi aşama kat edildiği söylenebilmektedir. Lakin siber alanın kendine özgü özellikleri dikkate alındığında, uluslararası hukuk normlarının meseleye nasıl uygulanacağı hususunda halen gelişim gösteren devlet uygulamalarının yakından takip edilmesi büyük önem arz etmektedir. Zira doğrudan siber operasyonları düzenleyen bir uluslararası sözleşmeye erişilmediği yahut uluslararası bir yargı makamı tarafından siber operasyonlara yönelik kapsamlı bir inceleme gerçekleştirilmediği takdirde, tartışma konusu hususların devletlerin yaklaşımları ve öğretide mevcut görüşler çerçevesinde incelenmesi isabetli bir değerlendirmeye erişilebilmesi için elzemdir.

KAYNAKÇA

BASILI KAYNAKLAR

Abdulqawi, Yusuf A., "The Notion of 'Armed Attack' in the Nicaragua Judgement and Its Influence on Subsequent Case Law", **Leiden Journal of International Law**, Vol. 25, Issue 2, 2012, (461-470)

Acer, Yücel / Kaya, İbrahim, **Uluslararası Hukuk**, Ankara: Seçkin, 2014.

Aksar, Yusuf, **Teoride ve Uygulamada Uluslararası Hukuk – II**, Ankara: Seçkin Yayınları, 2017.

Antolin-Jenkins, Vida M., "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places", **Naval Law Review**, Vol. 51, 2005, (132-174)

Antonopoulos, Constantine, "State Responsibility in Cyberspace", **Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy**, Ed: Ziolkowski, Katharina, Tallinn: NATO CCD COE Publications, 2013, (55-72)

Applegate, Scott D, "The Dawn of Kinetic Cyber", **2013 5th International Conference on Cyber Conflict (CYCON 2013)**, Ed: Podins, Karlis, Jans Stinissen ve Markus Maybaum, Tallinn: NATO CCD COE Publications, 2013. (163-181.)

Aust, Anthony, **Handbook of International Law**, New York: Cambridge University Press, 2005.

Baker, Roozbeh B., "Customary International Law in the 21st Century: Old Challenges and New Debates", **The European Journal of International Law**, vol. 21, no.1, 2010, (173-204)

Başaran, Alper, "Turkey under Cyber Fire", **Turkish Policy Quarterly**, Vol. 16, No. 1, 2017, (95-102)

Bayraktar, Gökhan, **Siber Savaş ve Ulusal Güvenlik Stratejisi**, Yeniyüzyıl Yayınları, 2015.

Beim, Jared, "Enforcing a Prohibition on International Espionage", **Chicago Journal of International Law**, Vol. 18, 2018, (647-672)

Berdal, Aral, **Uluslararası Hukukta Meşru Müdafaa Hakkı**, Ankara: Siyasal Kitabevi, 1999.

Berenger, Ralph D, "Cyber Warfare", *Encyclo***pedia of Research on Cyber Behavior**, Vol. I, Ed: Yan, Zheng, ABD: IGI Global, 2012, (1074-1088)

Bozkurt, Enver, **Uluslararası Hukukta Kuvvet Kullanımı**, 3. Baskı: Asil Yayın, 2007.

Brangetto, Pascal / Veenendaal Matthijs A, "Influence Cyber Operations: The Use of Cyber Attacks in Support of Cyber Operations", **2016 8th International Conference on Cyber Conflict: Cyber Power**, Ed: Pissanidis, Nikolaos, Henry Roigas ve Matthijs Veenendaal, Tallinn: NATO CCD COE Publications, 2016, (113-126.)

Broeders, Dennis / Busser Els de / Pawlak Patryk, "Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates", **The Hague Program for Cyber Norms Policy Brief**, 2020.

Brown, Garry / Poellet Keira, "The Customary International Law of Cyberspace", **Strategic Studies Quarterly**, 2012, (126-145)

Brownlie, Ian, **International Law and the Use of Force by States**, New York: Oxford University Press, 1963.

Brownlie, Ian, **Principles of Public International Law**, New York: Oxford University Press, 1990

Brownlie Ian, "The Use of Force in Self-Defense", **British Year Book of International Law**, Vol. 37, 1961, (183-268)

Brownlie, Ian / Apperley C.J., "Kosovo Crisis Inquiry: Memorandum on the International Law Aspects", **International and Comparative Law Quarterly**, vol. 49, 2000, (878-906)

Buchan, Russell, "Cyber Espionage and International Law", **Research Handbook on International Law and Cyberspace**, Ed: Buchan Russell / Tsagourias Nicholas, Edward Elgar Publishing, 2015, (168-190)

Buchan, Russell, "The International Legal Regulation of State-Sponsored Cyber Espionage", **International Cyber Norms: Legal, Policy & Industry Perspectives**, Ed: Osula, Anna-Maria / Roigas Henry, Tallinn: NATO CCD COE Publications, 2016, (65-86)

Carr, Jeffrey, **Inside Cyber Warfare: Mapping the Cyber Underworld**, 2. Bası, ABD: O'Reilly, 2011.

Casey-Maslen, Stuart, **Jus ad Bellum: The Law on Inter-State Use of Force**, Hart Publishing, 2020.

Cassese, Antonio, **International Law**, 2. Bası: Oxford University Press, 2005.

Cassese, Antonio, "The Nicaragua and Tadic Test Revisited in Light of the ICJ Judgment on Genocide in Bosnia", **European Journal of International Law**, Vol. 18, No. 4, 2007, (649-688)

Caşın, Mesut H, **Modern Uluslararası Hukukun Temel Esasları**, İstanbul: Legal Yayıncılık, 2013.

Charles, Arthur, **Cyber Wars: Hacks that Shocked the Business World**, Kogan Page, 2018.

Condron, Sean M, "Getting it Right: Protecting American Critical Infrastructure in Cyberspace", **Harvard Journal of Law & Technology**, Vol. 20, No. 2, 2007, (403-422)

Corn, Gary P. / Taylor Robert, "Sovereignty in the Age of Cyber", **American Journal of International Law**, Vol. 111, 2017, (207-212)

Corten, Olivier, ""The Unwilling or Unable" Test: Has it Been, and Could it be Accepted?", **Leiden Journal of International Law**, Vol. 29, 2016, (777-799)

Couzigou, Irene, "The Challenges Posed by Cyber-Attacks to the Law on Self Defence", **International Law and... Select Proceedings of the European Society of International Law**, Ed: Reinisch August ve Diğerleri, Hart Publishing, 2016, (245-261)

Crawford, James, **Brownlie's Principles of Public International Law**, Oxford University Press, 2012.

Crawford, James, **State Responsibility: the General Part**, New York: Cambridge University Press, 2013.

Çiftçi, Hasan, **Her Yönüyle Siber Savaş**, Ankara: TÜBİTAK Popüler Bilim Kitapları, 2013.

D'amato, Anthony, "The Invasion of Panama was a Lawful Response to Tyranny", **Faculty Working Papers**, 1990.

Deeks, Ashley S., "Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-Defense", **Virginia Jounal of International Law**, Vol. 52, 2012, (483-550)

Delerue, François, **Cyber Operations and International Law**, Cambridge: Cambridge University Press, 2020.

Delerue, François, "State Responses to Cyber Operations", **Global Relations Forum Young Academics Program Policy Paper Series No. 5**, 2017.

Delibasis, Dimitrios, "State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century", **Peace, Conflict & Development: An Interdisciplinary Journal**, 2006.

Delupis, Ingrid, "Foreign Warships and Immunity for Espionage", **The American Journal of International Law**, Vol. 78, No. 1, 1984, (53-75)

Denning, Dorothy E., "Activism, Hacktivism, and Cyber Terrorism: The Internet as a Tool for Influencing Foreign Policy", **Networks and Netwars: The Future of Terror, Crime and Militancy**, Ed: Arquilla, John / Ronfeldt David, RAND Corporation, 2001, (239-288)

DeSimone, Antonio / Horton Nicholas, "Sony's Nightmare Before Christmas The 2014 North Korean Cyber Attack on Sony and Lessons for the US Government Actions in Cyber Space", **The Johns Hopkins University Applied Physics Laboratory LLC**, 2017.

DeWeese, Geoffrey S, "Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence", **2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace**, Ed: Maybaum, Markus / Lindstörm Lauri, Tallinn: NATO CCD COE Publications, 2015, (81-92)

Dinniss, Heather H, **Cyber Warfare and the Laws of War**, Cambridge University Press, 2012.

Dinstein, Yoram, "Computer Network Attacks and Self-Defense", **Computer Network Attack and International Law**, Ed: Schmitt, Michael N. / O'Donnell Brian, International Law Studies, 2002, (99-109)

Dinstein, Yoram, "Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference", **U.S. Naval War College International Law Studies**, Vol. 89, 2013, (276-287)

Dinstein, Yoram, War, Aggression and Self-Defence, Cambridge: Cambridge University Press, 2011.

Dixon, Martin / McCorquodale Robert, **Cases & Materials on International Law**, New York: Oxford University Press, 2003.

Egan, Brian J., "International Law and Stability in Cyberspace", Vol. 35 **Berkeley Journal of International Law**, 2017, (169-180)

Eneken, Tikk / Kaska Kadri / Vihul Liis, **International Cyber Incidents: Legal Considerations**, Tallinn: NATO CCD COE Publications, 2010.

Epstein, Brett, "The Rules of Cyber-Welfare: What Are the Issues with These Rules, How Can the United States Respond to an Attack When Applying These Rules, and Should New Rules Be Enacted", **Holy Cross Journal of Law and Public Policy**, Vol. 18 (2014): 247-304.

Erkiner, Hakkı Hakan, **Devletin Haksız Fiilden Kaynaklanan Uluslararası Sorumluluğu**, İstanbul: On İki Levha Yayıncılık, 2010.

Etienne, Henry, "The Falklands/Malvinas War – 1982", Ruys, Tom / Corten Olivier, **The Use of Force in International Law: A Case-based Approach**, Oxford: Oxford University Press, 2018, (361-379)

Feder, Norman M., "Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack", **New York University Journal of International Law and Politics**, Vol. 19, No. 2, 1987, (395-432)

Fleck, Dieter, "Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual", **Journal of Conflict & Security Law**, Vol. 18, No. 2, 2013, (331-351)

Focarelli, Carlo, "Self-Defence in Cyberspace", **Research Handbook on International Law and Cyberspace**, Ed: Tsagourias, Nicholas / Russell Buchan, Edward Elgar Publishing, 2015, (255-284)

Franck, Thomas M., **Recourse to Force: State Action Against Threats and Armed Attacks**, Cambridge: Cambridge University Press, 2002.

Franzese, Patrick W, "Sovereignty in Cyberspace: Can it Exist?", **Air Force Law Review**, Vol. 64, 2009, (1-42)

Frimen, Johanna, **Revisiting the Concept of Defence in the Jus ad Bellum: The Dual Face of Defence**, Hart Publishing, 2007.

Gardam, Judith, "Proportionality and Force in International Law", **The American Journal of International Law**, Vol. 87, No. 3, 1993, (391-413)

Gardam, Judith, **Necessity, Proportionality and the Use of Force by States**, New York: Cambridge University Press, 2004.

Gareis, Sven B. / Varwick Johannes, **The United Nations: An Introduction**, Palgrave Macmillan, 2005.

Geiss, Robin / Lahmann Henning, "Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention", **Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy**, Ed: Ziolkowski, Katharina, Tallinn: NATO CCD COE Publications, 2013, (621-657)

Geiss, Robin / Lahmann Henning, "Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses towards Non-forcible Countermeasures and Collective Threat-prevention", **Peacetime Regime for State Activities in Cyberspace**, Ed: Katharina, Ziolkowski, Tallinn: NATO CCD COE Publications, 2013, (621-657)

Gervais, Michael, "Cyber Attacks and the Laws of War", **Berkeley Journal of International Law**, Vol. 30, 2012, (525-579)

Gill, Terry D., "Legal and Some Political Limitations on the Power of the UN Security Council to Exervise Its Enforcement Powers under Chapter VII of the Charter", **Netherlands Yearbook of International Law**, Vol. 26, 1995, (33-138)

Gill, Terry D., "Non-Intervention in the Cyber Context", **Peacetime Regime for State Activities in Cyberspace**, Ed: Ziolkowski, Katharina, Tallinn: NATO CCD COE Publications, 2013, (217-238)

Gill, Terry D. / Ducheine Paul A. L., "Anticipatory Self-Defense in the Cyber Context", **International Law Studies**, Vol. 89, 2013, (438-471)

Glahn, Gerhard Von, **Law Among Nations an Introduction to Public International Law**, 7. Baskı, Longman, 1996.

Graham, David E., "Cyber Threats and the Law of War", **Journal of National Security Law & Policy**, Vol. 4, 2010, (87-102)

Gray, Christine, **International Law and the Use of Force**, New York: Oxford University Press, 2008.

Gray, Christine, "The Use of Force and the International Legal Order**", International Law**, Ed: Malcolm, Evans D., New York: Oxford University Press, 2003, (589-620)

Green, James A, **The International Court of Justice and Self-Defence in International Law**, Hart Publishing, 2009.

Greig, Donald W., "Self-Defence and the Security Council: What Does Article 51 Require?", **The International and Comparative Law Quarterly**, Vol. 40, No. 2, 1991, (366-402)

Gündüz, Aslan, **Milletlerarası Hukuk**, Dü: Günel Reşat Volkan, 6. Baskı, Beta, 2013.

Haggard, Stephan / Lindsay Jon R., "North Korea and the Sony Hack: Exporting Instability Through Cyberspace", **Analysis from East-West Center**, 2015.

Handler, Stephenie G. "New Cyber Face of Battle: Developing a Legal Approach to Accomodate Emerging Trends in Warfare", **Stanford Journal of International Law**, Vol. 48, No. 1, 2012, (209-238)

Hathaway, Oona A. / Crootof Rebecca Crootof ve Diğerleri, "The Law of Cyber-Attack", **California Law Review**, Vol. 100, 2012, (817-885)

Herzog, Stephen, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", **Journal of Strategic Security**, Vol. 4, No. 2, 2011, (49-60)

Hoisington, Matthew, "Cyberwarfare and the Use of Force Giving Rise to the Right to Self-Defense", **Boston College International and Comparative Law Review**, Vol. 32, No. 2 (2009): 439-454.

Hollis, Duncan B., "Why States Need an International Law for Information Operations", **Lewis & Clark Law Review**, Vol. 11, 2007, (1023-1061)

Hollis, Duncan, "The Influence of War; the War for Influence", **Temple International and Comparative Law Journal**, Vol. 32, 2018, (31-46)

Jamnejad, Maziar / Wood, Michael, "The Principle of Non-Intervention", **Leiden Journal of International Law**, Vol. 22, 2009, (345–381)

Jeffrey, Carr, "Responsible Attribution: A Prerequisite for Accountability", **Tallinn Paper No. 6**, NATO CCD COE Publications, 2014.

Joyner, Christopher C. / Lotrionte Catherine, "Information Warfare as International Coercion: Elements of a Legal Framework", **European Journal of International Law**, 2001, (825-865)

Kaljurand, Marina, "United Nations Group of Governmental Experts: the Estonian Perspective", **International Cyber Norms: Legal, Policy & Industrial Perspectives**, Ed: Osula, Anna-Maria / Rõigas Henry, Tallinn: NATO CCD COE Publications, 2016, (111-127)

Kanuck, Sean P., "Information Warfare: New Challenges for Public International Law", **Harvard International Law Journal**, Vol. 37, 1996, 272-292.

Kelsey, Jeffrey T.G. "Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", **Michigan Law Review**, Vol. 106, 2008, (1427-1451)

Kesan, Jay P. / Hayes Carol M., "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace", **Harvard Journal of Law & Technology**, Vol. 25, No. 2, 2012, (429-543)

Kilovaty, Ido, "Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare", **National Security Law Brief 5**, No. 1, 2004, (91-124)

Kittichaisaree, Kriangsak, **Public International Law of Cyberspace**, İsviçre: Springer International Publishing, 2017.

Koh, Harold H., "International Law in Cyberspace", **Harvard International Law Journal**, vol. 54, 2012, (1-12)

Kolb, Robert, **An Introduction the the International Law of Armed Conflicts**, Oxford: Hart Publishing, 2008.

Krasner, Stephen D., **Sovereignty: Organized Hypocrisy**, New Jersey: Princeton University Press, 1999.

Kretzmer, David, "The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum", **The European Journal of International Law**, Vol. 24, No. 1, 2013, (235-282)

Kunig, Philip, "Intervention, Prohibition of", **Max Planck Encylopedia of Public International Law**, Vol VI, Brill, 2012

Lahmann, Henning, **Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution**, Cambridge University Press, 2020.

Li, Sheng, "When Does Internet Denial Trigger the Right of Armed Self-Defence?", **The Yale Journal of International Law**, Vol. 38, 2013, (179-216)

Libicki, Martin C., **Cyberdeterrence and Cyber War**, RAND Corporation, 2009.

Lin, Herbert S., "Offensive Cyber Operations and the Use of Force", **Journal of National Security Law & Policy**, Vol. 4, 2010, (63-86)

Lindsay, Jon R., "Stuxnet and the Limits of Cyber Warfare", **Security Studies**, Vol. 22, 2013, (365-404)

Lowe, Vaughan, "Jurisdiction - The Scopeof Sovereignty", **International Law**, Ed: Evans, Malcolm D., New York: Oxford University Press, 2003, (329-357)

Macdonald, Ronald St. J., "The Nicaragua Case: New Answers to Old Questions?", **The Canadian Yearbook of International Law**, Vol. 124, 1986, (127-160)

Margulies, Peter, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", **Melbourne Journal of International Law**, Vol. 14, No. 2, 2013, (469-519)

Mazanec, Brian M., **The Evolution of Cyber War: International Norms for Emerging-Technology Weapons**, University of Nebraska Press, 2015

McGhee, James E., "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy", **Journal of Law & Cyber Warfare**, Vol. 2, No. 1, 2013, (64-103)

Melnitzky, Alexander, "Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses", **Cardozo Journal of International and Comparative Law**, Vol. 20, No. 2, 2012, (537-570)

Melzer, Nils, **Cyberwarfare and International Law**, Cenevre: United Nations Institute for Disarmament Research, 2011.

Metcalf, Katrin N., "A Legal View on Outer Space and Cyber Space: Similarities and Differences.", **Tallinn Paper No. 10**, NATO CCD COE Publications, 2018.

Mikanagi, Tomohiro / Macak Kubo, "Attribution of Cyber Operations: An International Law Perspective on the Park Jin Hyok Case", **Cambridge International Law Journal**, Vol. 9, No. 1, 2020, (51-75)

Moir, Lindsay, **Reappraising the Resort to Force: International Law, Jus ad Bellum and the War on Terror**, Hart Publishing, 2010.

Mudrinich, Erik M., "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem", **The Air Force Law Review**, Vol. 68, 2012, (167-207)

Mueller, Benjamin, "The Laws of War and Cyberspace On the Need for a Treaty Concerning Cyber Conflict", **LSE Ideas Strategic Update 14.2**, 2014

Murphy, John F., "Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S.Vital Interests", **International Law Studies**, Vol. 89, 2013, (309-340)

Murphy, Sean D., **Humanitarian Intervention: The United Nations in an Evolving World Order**, Philadelphia: University of Pennsylvania Press, 1996.

Murphy, Sean D., "Terrorism and the Concept of Armed Attack in Article 51 of the U.N. Charter", **Harvard International Law Journal**, Vol. 43, No. 1, 2002, (41-52)

National Research Council, **Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities**, Ed: Owens, William A. / Dam Kenneth W. / Lin Herbert., Washington: National Academy Press, 2005.

NATO Müşterek Siber Savunma Mükemmeliyet Merkezi, **Tallinn Manual on the International Law Applicable to Cyber Warfare**, Ed: Michael N. Schmitt, Cambridge University Press, 2013.

NATO Müşterek Siber Savunma Mükemmeliyet Merkezi, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, Ed: Michael N. Schmitt, Cambridge University Press, 2017

Nguyen, Reese, "Navigating "Jus Ad Bellum" in the Age of Cyber Warfare", **California Law Review**, Vol. 101, No. 4, 2013, (1079-1129)

O'Connell, Marry Ellen, "Lawful Self-Defense to Terrorism", **University of Pittsburgh Law Review**, Vol. 63, 2002, (889-908)

Ohlin, David J. "Did Russian Cyber Interference in the 2016 Election Violate International Law?", **Texas Law Review**, Vol. 95, 2017, (1579-1598)

Ohlin, Jens D. / May Larry, **Necessity in International Law**, New York: Oxford University Press, 2016.

Oosthuizen, Gabriel H., "Playing the Devil's Advocate: the United Nations Security Council is Unbound by Law", **Leiden Journal of International Law**, 1999, (549-563)

Oppenheim, Lassa F. L., **International Law a Treatise, Vol. I. – Peace**, Ed: Hersch Lauterpacht, Londra: Longmans, 1955.

Oppenheim, Lassa F. L., **International Law a Treatise Vol. II Disputes, War and Neutrality**, Longmans, Seventh Edition, Ed: H. Lauterpacht, 1952.

Pazarcı Hüseyin, **Uluslararası Hukuk**, 7. Bası, Ankara, Turhan Kitabevi Yayınları, 2008.

Pirim, Ceren Zeynep, "Devletlere Atfedilemeyen Silahlı Saldırılara Karşı Meşru Müdafaa: Uluslararası Hukukta Sınır Ötesi Operasyonların Hukuki Zemini", **Türkiye Adalet Akademisi Dergisi**, Sayı: 40, 2019, (245-303)

Pool, Philip., "War of the Cyber World: The Law of Cyber Warfare", **The International Lawyer**, Vol. 47, No. 2 2013, (299-323)

Pun, Darien, "Rethinking Espionage in the Modern Era", **Chicago Journal of International Law**, Vol. 18, No. 1, 2017, (353-391)

Raboin, Bradley, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", **Journal of the National Association of Administrative Law Judiciary**, Vol. 31, No. 2, 2011, (602-666)

Radziwill, Yaroslav, **Cyber-Attacks and Exploitable Imperfections of International Law**, Leiden: Brill Nijhoff, 2015.

Ratner, Steve R., **The Thin Justice of International Law: A Moral Reckoning of the Law of Nations**, New York: Oxford University Press, 2015.

Rid, Thomas, **Cyber War will not Take Place**, New York: Oxford University Press, 2013.

Rittberger, Volker / Bernhard Zangl, **International Organization: Polity, Politics and Policies**, Palgrave Macmillan, 2006.

Roberts, Adam, "The Use of Force", **The UN Security Council: From the Cold War to the 21st Century**, Ed: Malone, David M., Londra: Lynne Rienner Publishers, 2004. (133-153)

Roberts, Shaun, "Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors", **Northern Kentucky Law Review**, Vol. 41, No. 3, 2014, (535-572)

Rogoff, Martin A. / Collins Edward, “The Caroline Incident and the Developments of International Law”, **Brooklyn Journal of International Law**, Vol. 16, No. 3, 1990, (493-528)

Roguski, Przemyslaw, “Application of International Law to Cyber Operations: A Comparative Analysis of States' Views”, **The Hague Program for Cyber Norms Policy Brief**, 2020.

Ronzitti, Natalino, “The Expanding Law of Self-Defence”, **Journal of Conflict and Security Law**, Vol. 11, 2006, 343-359.

Roscini, Marco, **Cyber Operations and the Use of Force in International Law**, New York: Oxford University Press, 2014.

Roscini, Marco, “Cyber Operations as a Use of Force” **Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy**, Ed: Ziolkowski, Katharina, Tallinn: NATO CCD COE Publications, 2013, (233-255)

Roscini Marco, “Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations”, **Texas International Law Journal**, Vol. 50, 2015, (233-273)

Roscini, Marco, “Threats of Armed Force and Contemporary International Law”, **Netherlands International Law Review**, 2007, (229-277)

Roscini, Marco, “World Wide Warfare - Jus Ad Bellum and the Use of Cyber Force”, **Max Planck Yearbook of United Nations Law**, Ed: Bogdandy, Armin von / Wolfrum Rüdiger, Brill, 2010, (85-130)

Rowe, Neil C., “Distinctive Ethical Challenges of Cyberweapons”, **Research Handbook on International Law and Cyberspace**, Ed: Tsagourias, Nicholas / Buchan Russell, Edward Elgar Publishing, 2015, (307-326)

Ruys, Tom, **"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice**, New York: Cambridge University Press, 2010.

Ruys, Tom, “The Meaning of "Force" and the Boundaries of Jus ad Bellum: Are Minimal Uses of Force Excluded from UN Charter Article 2(4)?”, **The American Journal of International Law**, Vol. 108, No. 2, 2014, (159-210)

Sadurska, Romana, “Threats of Force”, **The American Journal of International Law**, Vol. 82, No. 2, 1988, (239-268)

Schaap, Arie J., “Cyber Warfare Operations: Development and Use under International Law”, **Air Force Law Review**, Vol. 30, 2009, (525-579)

Schachter, Oscar, **International Law in Theory and Practice**, Hollanda: Martinus Nijhoff Publishers, 1991.

Schachter, Oscar, "The Lawful Resort to Unilateral Use of Force", **Yale Journal of International Law**, vol. 10, no. 2, 1985, (291-294)

Schmitt, Michael N., ""Attack" as a Term of Art in International Law: The Cyber Operations Context", **2012 4th International Conference on Cyber Conflict**, Ed: Czosseck, Christian / Ottis Rain Ottis / Ziolkowski Katharina, Tallinn: NATO CCD COE Publications, 2012, (283-293)

Schmitt, Michael N., ""Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law", **Chicago Journal of International Law**,Vol. 19, No. 1, 2018, (30-67)

Schmitt, Michael N., "Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law", **Virginia Journal of International Law**, Vol. 54, No. 3, 2014, (697-732)

Schmitt, Michael N., "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", **Columbia Journal of Transnational Law**, Vol. 37, 1999, (885-937)

Schmitt, Michael N., "Cyber Operations and the Jus ad Bellum Revisited", **Villanova Law Review**, Vol. 56, Issue 3, 2011, (569-606)

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

Schmitt, Michael N., "Preemptive Strategies in International Law", **Michigan Journal of International Law**, Vol. 24, Issue 2, 2003, (513-548)

Schmitt, Michael N., "The Law of Cyber Warfare: Quo Vadis", **Stanford Law & Policy Review**, Vol. 15, (269-299)

Schmitt, Michael N., "The "Use of Force" in Cyberspace: A Reply to Dr Ziolkowski", **2012 4th International Conference on Cyber Conflict**, Ed: Czosseck, Christian / Ottis Rain / Ziolkowski Katharina, Tallinn: NATO CCD COE Publications, 2012, (311-317)

Schmitt, Michael N., "The Use of Cyber Force and International Law", **The Use of Force in International Law**, Ed: Weller, Marc, Oxford University Press, 2015, (1110-1130)

Schmitt, Michael N. / Vihul Liis, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution", **Fletcher Security Review**, Vol. 1, No. 2, 2014, (53-72)

Schmitt, Michael N. / Vihul Liis, "The Nature of International Law Cyber Norms", **Tallinn Paper No. 5 Special Expanded Issue**, Tallinn: CCDCOE Publications, 2014.

Schmitt, Micheal N., "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts", **Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy**, Washington: The National Academic Press, 2010, (151-178)

Schwebel, Stephen M., "Aggression, Intervention, and Self-Defense in Modern International Law", **Justice in International Law: Selected Writings**, Cambridge: Cambridge University Press, 1994, (530-592)

Segura-Serrano, Antonio, "Internet Regulation and the Role of International Law", **Max Planck Yearbook of United Nations Law**, Ed: Bogdandy, Armin von / Wolfrum Rüdiger Philipp Christiane E., Vol. 10, Hollanda: Brill, 2006, (191-272)

Shackelford, Scott J., "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", **Berkeley Journal of International Law**, Vol. 27, No. 1, 2009, (192-252)

Shackelford, Scott J. / Andres Richard B., "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem", **Georgetown Journal of International Law**, Vol. 42, No. 4, 2011, (971-1016)

Shany, Yuval / Schmitt Michael N., "An International Attribution Mechanism for Hostile Cyber Operations", **International Law Studies**, Vol. 96, 2020, (196-222)

Sharp, Walter G., **CyberSpace and the Use of Force**, Aegis Research Corporation, 1999.

Shaw, Malcolm N., **International Law**, Cambridge: Cambridge University Press, 2003.

Silver, Daniel B., "Computer Network Attacks as a Use of Force under Article 2(4) of the United Nations Charter", **Computer Network Attacks and International Law**, Ed: Schmitt, Michael N. / O'Donnell Brian T., International Law Studies, 2002, (73-97)

Singer, Peter W. / Friedman Allan, **Cybersecurity and Cyberwar: What Everyone Needs to Know**, Oxford University Press, 2014.

Smith, Edwin M., "Collective Security: Changing Conceptions and Institutional Adaption", **Adapting the United Nations to a Postmodern Era**, Ed: Knight, Andy W., Global Issues Series, 2005, (41-52)

Sofaer, Abraham D., "International Law and the Use of Force", **The National Interest**, No. 1983, 1988, (53-64)

Sony Corporation, **Consolidated Financial Results for the Fiscal Year Ended March 31, 2015**, Tokyo, 2015.

Stanimir, Alexandrov A., **Self-Defense Against the Use of Force in International Law**, Klumet Law International, 1996.

Stein, Christopher T., "Hacking the Electorate: a Non-Intervention Violation Maybe, But not an "Act of War"", **Arizona Journal of International & Comparative Law**, Vol. 37, No. 1, 2020, (29-48)

Stockburger, Peter Z., "Known Unknowns: State Cyber Operations, Cyber Warfare and the Jus Ad Bellum", **American University International Law Review**, Vol. 31, Issue 4, Article 2, 2016, (545-591)

Sur Melda, **Uluslararası Hukukun Esasları**, İstanbul: Beta, 2014

Stürchler, Nikolas, **The Threat of Force in International Law**, New York: Cambridge University Press, 2007.

Sullivan, Clare, "The 2014 Sony Hack and the Role of International Law", **Journal of National Security Law & Policy**, Vol. 8, 2016, (437-468)

Thirlway Hugh, "The Sources of International Law", **International Law**, Ed: Evans D. Malcolm, Oxford University Press, 2010, (117-145)

Tsagourias, Nicholas, "Cyber Attacks, Self-defence and the Problem of Attribution", **Journal of Conflict & Security Law**, Vol. 17, No. 2, 2012, 229-244.

Ulutaş, Güzin, "Siber Güvenlik", **Siber Güvenlik ve Savunma, Farkındalık ve Caydırıcılık**, Ed: Şeref Sağıroğlu / Mustafa Alkan, Ankara: BGD Siber Güvenlik ve Savunma Kitap Serisi, 2018.

US Department of Defense Office of General Counsel, "An Assessment of International Legal Issues in Information Operations", **Computer Network Attack and International Law**, Ed: Schmitt, Michael N. / O'Donnell Brian T., International Law Studies, 2002, (459-529)

Valek, Peter, "Legality versus Legitimacy and the Use of Force", **Progress in International Law**, Ed: Miller Russell A. / Bratspies Rebecca M., Martinus Nijhoff Publishers, 2008, (615-633)

Watkin, Kenneth, **Fighting at the Legal Boundaries: Controlling the Use of Force in Contemporary Conflict**, New York: Oxford University Press, 2016.

Waxman, Matthew C., "Self Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions", **International Law Studies**, Vol. 89, 2013, (109-122)

Waxman, Matthew C., "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", **Yale Journal of International Law**, vol. 36, 2011, (421-459)

Whittle, Devon, "The Limits of Legality and the United Nations Security Council: Applying the Extra-Legal Measures Model to Chapter VII Action", **The European Journal of International Law**, Vol. 26, No. 3, 2015, (671-698)

Woltag, Johann-Christoph**, Cyber Warfare: Military Cross-Border Computer Network Operations under International Law**, Cambridge University Press, 2014.

Wright, Quincy, "Espionage and the Doctrine of Non-Intervention in Internal Affairs", **Essays on Espionage and International Law**, Ed: Stanger, Roland J., Ohio State University Press, 1962, (3-28)

Ziolkowski, Katharina, "Peacetime Cyber Espionage – New Tendencies in Public International Law", **Peacetime Regime for State Activities in Cyberspace**, Ed: Katharina Ziolkowski, Tallinn, NATO CCD COE Publications, 2013, (425-465)

Ziolkowski, Katharina, "NATO and Cyber Defence", **Research Handbook on International Law and Cyberspace**, Ed: Tsagourias, Nicholas / Buchan Russell, Edward Elgar Publishing, 2015, (426-446)

Ziolkowski, Katharina, **Stuxnet - Legal Considerations**, Tallinn: NATO CCD COE Publications, 2012

ELEKTRONİK KAYNAKLAR

Advisory Council on International Affairs / Advisory Committee Issues of Public International Law, **Cyber Warfare**, No 77, AIV / No 22, CAVV, 2011, https://www.advisorycouncilinternationalaffairs.nl/binaries/advisorycouncilinternationalaffairs/documents/publications/2011/12/16/cyber-warfare/Cyber_Warfare_AIV-Advisory-report-77_CAVV-Advisory-report-22_ENG_201112.pdf.

Egan, Brian J., **Remarks on International Law and Stability in Cyberspace**, 10 Kasım 2016, https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.

Electricity Information Sharing and Analysis Center, **Analysis of the Cyber Attack on the Ukrainian Power Grid**, 18 Mart 2017, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

FireEye, "Cyber Attacks on the Ukrainian Grid: What You Should Know", **FireEye Industry Intelligence** Report, https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf.

International Committee of the Red Cross, **International Humanitarian Law: Answers to Your Questions**, ICRC Publications, https://shop.icrc.org/droit-international-humanitaire-reponses-a-vos-questions-2616.html.

Institute de Droit International, **Present Problems of the Use of Armed Force in International Law: Self-Defence**, 2007, https://www.idi-iil.org/app/uploads/2017/06/2007_san_02_en.pdf.

International Law Association Use of Force Committee, **Final Report on Aggression and the Use of Force**, 2018, https://ila.vettoreweb.com/Storage/Download.aspx?DbStorageId=11391&StorageFileGuid=6a499340-074d-4d4b-851b-7a56871175d6.

Kasapoğlu, Can. "Turkey's Future Cyber Defense Landscape", **A Primer on Cyber Security in Turkey and the Case of Nuclear Power**,. https://edam.org.tr/document/CyberNuclear/edam_cyber_security_ch1.pdf.

Lee, Robert M. / Assante Michael J. / Conway Tim**, ICS CP/PE (Cyber-to-Physical or Process Effects) Case Study Paper: Media Report of the Baku-Tblisi-Ceyhan (BTC) Pipeline Cyber Attack**, SANS Industrial Control Systems, 20 Aralık 2014, https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf.

Lin, Patrick, "Ethics of Hacking Back: Six Arguements from Armed Conflicts to Zombies", **A Policy Paper on Cyber Security**, 2016, http://ethics.calpoly.edu/hackingback.pdf.

Microsoft, **A Digital Geneva Convention to Protect Cyber Space**, Microsoft Policy Papers, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH.

Networked European Software and Services Initiative, "Cyber-Physical Systems: Opportunities and Challenges for Software, Services, Cloud and Data", **Nessi White Paper**, 2015, http://www.nessi-europe.com/Files/Private/NESSI_CPS_White_Paper_issue_1.pdf.

Nour News, General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat, 18 Ağustos 2020, https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat

Schmitt, Michael N., "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace", **Texas National Security Review**, 2020, https://tnsr.org/2020/07/taming-the-lawless-void-tracking-the-evolution-of-international-law-rules-for-cyberspace/

Schreier, Fred, "On Cyberwarfare", **DCAF Horizon 2015 Working Paper No. 7**, *https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf*

Tsagourias, Nicholas, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace", 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3438567.

Twitter Safety, 5 Nisan 2020, https://twitter.com/TwitterSafety/status/1245682439969792005.

Wright, Jeremy, **Cyber and International Law in the 21st Century**, 23 Mayıs 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

https://mil.ee/en/landforces/cyber-command

https://www.cybercom.mil/About/History/

https://dictionary.cambridge.org/tr/sözlük/ingilizce/cyberspace

YARGI KARARLARI

Advisory Opinion Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, International Court of Justice (ICJ), 9 Temmuz 2004.

Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons, International Court of Justice, 1996.

Advisory Opinion No. 4, Nationality Decrees Issued in Tunis and Morocco, 4, Permanent Court of International Justice, 7 February 1923

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), International Court of Justice (ICJ), 2007.

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Rwanda). International Court of Justice (ICJ), 18 Eylül 2002.

Corfu Channel Case (United Kingdom v. Albania); Merits, International Court of Justice (ICJ), 9 Nisan 1949.

Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua), International Court of Justice, (ICJ), 13 July 2009.

Island of Palmas Case (or Miangas), United States v Netherlands, Award, (1928) II RIAA 829, ICGJ 392 (PCA 1928), Permanent Court of Arbitration (PCA), 4th April 1928

Lotus (France v Turkey), No. Series A, No 10, Permanent Court of International Justice, 1927.

Military and Paramilitary Activities in and against Nicaragua, International Court of Justice (ICJ), 1986.

North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. Netherlands), International Court of Justice (ICJ), 20 February 1969

Oil Platforms (Islamic Republic of Iran v. United States of America, International Court of Justice (ICJ), 6 Kasım 2003.

Prosecutor v. Dusko Tadic (Appeal Judgement), No. IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 Temmuz 1999.

Questions relating to the Seizure and Detention of Certain Documents and Data, Timor-Leste v Australia, Order on Provisional Measures, No. ICGJ 472 (ICJ 2014), International Court of Justice (ICJ), 3 Mart 2014.

The Trial of German Major War Criminals Part 22 (22nd August ,1946 to 1st October, 1946), Proceedings of the International Military Tribunal sitting at Nuremberg, Germany.

United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), No. 12 V 81, International Court of Justice (ICJ), 12 Mayıs 1981.

United States v. Victor Borisovich Netyksho and Others. U.S. District Court, District of Columbia, 13 Temmuz 2018.

ULUSLARARASI ANTLAŞMALAR

United Nations, Charter of the United Nations, 1 UNTS XVI, 24 October 1945.

United Nations, Statute of the International Court of Justice, 18 April 1946

United Nations, Vieanna Convention on the Law of Treaties, UNTS. 1115, 23 May 1969

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001

United Nations, Vienna Convention on Consular Relations, 24 April 1963

United Nations, Convention on the Law of the Sea, 10 December 1982

Montevideo Convention on Rights and Duties of States, opened for signature 26 December 1933, 165 LNTS 19

KARARNAMELER VE DİĞER RESMİ BELGELER

Birleşmiş Milletler

UN General Assembly, **Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty**, 21 December 1965, A/RES/2131(XX)

UN General Assembly, **Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations**, 24 October 1970, A/RES/2625(XXV)

UN General Assembly, **Non-interference in the internal affairs of States**, 14 December 1976, A/RES/31/91

UN General Assembly, **Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States**, 9 December 1981, A/RES/36/103

UN General Assembly, **A more Secure World: Our Shared Responsibility**, Report of the High-level Panel on Threats, Challenges and Change, A/59/565, 2 Aralık 2004

UN General Assembly, **Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures**, A/RES/58/199

UN General Assembly, **Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General**, A/66/152, 15 Temmuz 2011.

UN General Assembly, **Definition of Aggression**, A/RES/3314, 14 Aralık 1974.

UN General Assembly, **Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures**, A/RES/58/199.

UN General Assembly, **Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General**, A/66/152, 15 Temmuz 2011

UN General Assembly, **Respect for the principles of national sovereignty and diversity of democratic systems in electoral processes as an important element for the promotion and protection of human rights**, A/RES/60/164, 16 Aralık 2005

Resolution adopted by the General Assembly on 22 December 2018, A/RES/73/266

Resolution adopted by the General Assembly on 5 December 2018, A/RES/73/27

UN GGE, **Developments in the Field of Information and Telecommunications in the Context of International Security**, A68/98, 24 Haziran 2013

UN GGE Report 2015, UN Doc. A/70/174, 22 Temmuz 2015

Resolution 1368 (2001) Adopted by the Security Council at its 4370th meeting, on 12 September 2001, S/RES/1368 (2001); Resolution 1373 (2001) Adopted by the Security Council at its 4385th meeting, on 28 September 2001, S/RES/1373 (2001)

United Nations, General Assembly Security Council, Letter Dated 27 June 2014 from the Permanent Representative of the Democratic People's Republic of Korea to the United Nations Addressed to the Secretary-General, A/68/934–S/2014/451, 27 Haziran 2014.

Resolution 1368 (2001) Adopted by the Security Council at its 4370th meeting, on 12 September 2001, S/RES/1368 (2001)

Resolution 1373 (2001) Adopted by the Security Council at its 4385th meeting, on 28 September 2001, S/RES/1373 (2001)

Letter dated 6 September 2012 from the Charge d'affaires a.i. of the Permanent Mission of Azerbaijan to the United Nations addressed to the Secretary-General.» UN Doc A/66/897-S/2012/687, 7 Eylül 2012.

United Nations Security Council, Working Methods Handbook: Background Note on the "Arria-Formula" Meetings of the Security Council Members, https://www.un.org/securitycouncil/content/background-note.

Amerika Birleşik Devletleri

DHS Press Office, Statement by Secretary Johnson on Cyber Attack on Sony Pictures Entertainment, 19 Aralık 2014, https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment.

FBI National Press Office, Update on Sony Investigation, 19 Aralık 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

U.S. Office of the Director of National Intelligence, Assessing Russian Activities and Intentions in Recent US Elections, 6 Ocak 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

US Department of Defense, **DOD Dictionary of Military and Associated Terms**, Washington DC, 2020

Mueller, Robert S., **Report on the Investigation Into Russian Interference in the 2016 Presidential Election**, Washington D.C.: U.S. Department of Justice, 2019.

Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates, **Joint Terminology for Cyberspace Operations**, 2010, http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

The US Office of the Director of National Intelligence, A Guide to Cyber Attribution, 14 Eylül 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

The White House Office of the Press Secretary. Remarks by the President in Year-End Press Conference, 19 Aralık 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

U.S. Department of State, Joint Statement on Advancing Responsible State Behavior in Cyberspace, 23 Eylül 2013, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

U.S. Department of State, The United States Condemns Russian Cyber Attack Against the Country of Georgia, 20 Şubat 2020, https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.

US Department of Homeland Security, Cyber Security Strategy, 15 Mayıs 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

Avrupa Birliği

Council of the European Union, Declaration by the High Representative Josep Borrell on behalf of the EU: European Union Response to Promote International Security and Stability in Cyberspace, Press Release, 30 Temmuz 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-eu-european-union-response-to-promote-international-security-and-stability-in-cyberspace/.

Official Journal of the European Union, Council Implementing Regulation (EU) 2020/1125: Implementing Regulation (EU) 2019/796 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States, L 246/4, 30 Temmuz 2020.

Official Journal of the European Union, Council Decision (CFSP) 2020/1127: Amending Decision (CFSP) 2019/97 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States, L 246/12, 30 Temmuz 2020.

Avustralya

Australian Department of Foreign Affairs and Trade, Attribution of a Pattern of Malicious Cyber Activity to Russia, Joint Media Release, 4 Ekim 2018, https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-pattern-malicious-cyber-activity-russia.

Australian Government, Australia's International Cyber Engagement Strategy 2019 International Law Supplement Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace, https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html.

Australian Government, Critical Infrastructure Resilience Strategy: Plan, 2015, https://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlan.PDF.

Australian Mission to the United Nations. Statement by H.E. Dr. Tobias Feakin Ambassador for Cyber Affairs, 22 Mayıs 2020, https://vm.ee/sites/default/files/Estonia_for_UN/unsc_-_cyber_arria_22_may_2020_-_australian_statement_002.pdf.

Birleşik Krallık

Foreign & Commonwealth Office / National Cyber Security Center / The Rt Hon Dominic Raab MP., UK Condemns Russia's GRU over Georgia Cyber Attacks, Press Release, 20 Şubat 2020, https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

UK Cabinet Office, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, Birleşik Krallık Hükümeti, 2011, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

UK Government, National Cyber Security Strategy 2016-2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Estonya

Republic of Estonia Ministry of Foreign Affairs, Estonia Raised Cybersecurity for the First Time at the UN Security Council, 5 Mart 2020, https://vm.ee/en/news/estonia-raised-cybersecurity-first-time-un-security-council.

Republic of Estonia Ministry of Foreign Affairs, Signature Event of Estonia's UNSC Presidency: Cyber Stability, Conflict Prevention and Capacity Building, https://vm.ee/en/activities-objectives/estonia-united-nations/signature-event-estonias-unsc-presidency-cyber.

Republic of Estonia Ministry of Foreign Affairs, Statement of the Foreign Minister of the Republic of Estonia Urmas Reinsalu, 20 Şubat 2020, https://vm.ee/en/news/statement-foreign-minister-republic-estonia-urmas-reinsalu.

Federal Almanya Cumhuriyeti

Federal Ministry of Interior, National Strategy for Critical Infrastructure Protection, 17 Haziran 2009, https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1.

Fransa

Délégation à l'information et à la communication de la défense, International Law Applied to Operations in Cyberspace, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

République Française Ministère des Armées, International Law Applied to Operations in Cyberspace, 2019,

https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

Permanent Mission of Estonia to the UN, Stakeout on Cyber-Attack Against Georgia by Estonia, https://un.mfa.ee/press-stakeout-by-estonia-the-united-kingdom-and-the-united-states-on-cyber-attack-against-georgia/.

Hollanda

Government of the Netherlands Ministry of Foreign Affairs, Letter to the Parliament on the International Legal Order in Cyberspace Appendix: International Law in Cyberspace, 5 Temmuz 2019, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

Government of the Netherlands, The Netherlands Considers Russia's GRU Responsible for Cyber Attacks Against Georgia, Diplomatic Statement, 20 Şubat 2020, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia%E2%80%99s-gru-responsible-for-cyber-attacks-against-georgia.

Japonya

Mr. Akahori Takeshi, Ambassador for Cyber Policy of Foreign Affairs of Japan, The UN Security Council Arria-Formula Meeting: Cyber Stability, Conflict Prevention and Capacity Building, 22 Mayıs 2020, https://vm.ee/sites/default/files/Estonia_for_UN/cyber_arria-formula_statement_of_japan.pdf.

Kanada

Global Affairs Canada, Canada Condemns Russia's Malicious Cyber-Activity Targeting Georgia, 20 Şubat 2020, https://www.canada.ca/en/global-affairs/news/2020/02/canada-condemns-russias-malicious-cyber-activity-targeting-georgia.html.

Gendron, Angelo ve Martin Rudner, Assessing Cyber Threats to Canadian Infrastructure: Report Prepared for the Canadian Security Intelligence Service, https://www.canada.ca/content/dam/csis-scrs/documents/publications/CyberTrheats_AO_Booklet_ENG.pdf.

Kuzey Atlantik Antlaşması Örgütü (NATO)

North Atlantic Treaty Organization, NATO Summit Guide, 2018, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180718_180711-summit-guide-brussels.pdf.

Polonya

Republic of Poland Ministry of Foreign Affairs, Statement of Polish MFA on Cyberattacks Against Georgia, 20 Şubat 2020, https://www.gov.pl/web/diplomacy/statement-of-the-polish-mfa-on-cyberattacks-against-georgia.

Rusya Federasyonu

Permanent Mission of the Russian Federation to the United Nations. Statement by the Permanent Mission of Russia to the UN on its Non-participation in the UN Security Council Arria-Formula Meeting on Cyber Stability, Conflict Prevention and Capacity Building, Organized by Estonia on 22 May, 22 Mayıs 2020, https://russiaun.ru/en/news/arria_220520.

Türkiye Cumhuriyeti

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016-2019 Ulusal Siber Güvenlik Stratejisi, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/kritik.pdf.

Türkiye Cumhuriyeti Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf.

Ulusal Siber Olaylara Müdahale Merkezi (USOM-TRCERT), Siber Güvenliğe İlişkin Temel Bilgiler, 2014, https://www.usom.gov.tr/dosya/1418807122-USOM-SGFF-001-Siber%20Guvenlige%20Giris%20ve%20Temel%20Kavramlar.pdf

ÖZGEÇMİŞ

Kaan Erdoğan, 1994 senesinde İstanbul'da doğmuştur. 2013'te Ankara Gölbaşı Anadolu Lisesi'nden mezun olup aynı sene Çankaya Üniversitesi Hukuk Fakültesi'ne başlamıştır. 2017'de ise Çankaya Üniversitesi Hukuk Fakültesi'ni tamamlamasını müteakip eğitimine Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü'nde Kamu Hukuku Yüksek Lisans programı ile devam etmiştir. 2018-2020 seneleri arasında İstanbul Barosu'nun bir mensubu olarak avukatlık mesleğini icra etmiş; 2020 senesinin temmuz ayından itibaren ise İzmir Demokrasi Üniversitesi Hukuk Fakültesi Uluslararası Hukuk Anabilim Dalı bünyesinde araştırma görevlisi olarak çalışmaya başlamıştır.

TEZ ONAY SAYFASI

Üniversite	: T.C. GALATASARAY ÜNİVERSİTESİ
Enstitü	: SOSYAL BİLİMLER ENSTİTÜSÜ
Hazırlayanın Adı Soyadı	: KAAN ERDOĞAN
Tez Başlığı	: SİBER OPERASYONLAR VE JUS AD BELLUM
Savunma Tarihi	: 08 / 09 / 2020
Danışmanı	: DR. ÖĞR. ÜYESİ BLEDA RIZA KURTDARCAN

JÜRİ ÜYELERİ

Unvanı, Adı Soyadı	İmza
Dr. Öğr. Üyesi Bleda Rıza KURTDARCAN	
Doç. Dr. Ceren Zeynep PİRİM KIZILCA	
Dr. Öğr. Üyesi Dolunay ÖZBEK	

Prof. Dr. M. Yaman ÖZTEK
Enstitü Müdürü