T.C.
ÖZYEĞİN ÜNİVERİSTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU YÜKSEK LİSANS PROGRAMI

ULUSLARARASI HUKUK BAĞLAMINDA NÜKLEER SANTRALLERİN SİBER GÜVENLİĞİ

Cihad Furkan Eliaçık

Haziran 2018

T.C.
ÖZYEĞİN ÜNİVERİSTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU YÜKSEK LİSANS PROGRAMI

ULUSLARARASI HUKUK BAĞLAMINDA NÜKLEER SANTRALLERİN SİBER GÜVENLİĞİ

Cihad Furkan Eliaçık

Tez Danışmanı: Dr.Öğr.Üye. Özge YÜCEL DERİCİLER
Tez Eş Danışmanı: Prof. Dr. Mesut Hakkı CAŞIN

Haziran 2018

ÖZYEĞİN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ ONAY FORMU

"Özyeğin Üniversitesi SBE Kamu Hukuku
Anabilim Dalı ..... Kamu Hukuku Tezli .....
yüksek lisans programı S007719 numaralı öğrencisi Cihat Furkan Elmacık
Uluslararası Hukuk Bağlamında Nükleer
Santrallerin Siber Güvenliği"
başlıklı tez çalışması jürimiz tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

TEZ DANIŞMANI	: Dr. Öğr. Üy. Özge Yücel Dereler	
İKİNCİ TEZ DANIŞMANI	: PROF. DR. MEHMET HAKKI CASIN	
JÜRİ ÜYESİ	: Prof. Dr. A. Lerzan Yılmaz	
JÜRİ ÜYESİ	: Prof. Dr. Mustafa TOPALOĞLU	
JÜRİ ÜYESİ	: Dr. Öğr. Üy. Ali Hulki Cilan	

Özyeğin Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun 19./06./2018 Tarih, 2018./17 sayılı kararı ile onaylanmıştır.

İÇİNDEKİLER

İKİNCİ BÖLÜM

ULUSLARARASI NÜKLEER HUKUK ve GÜNCEL GELİŞMELER

ÜÇÜNCÜ BÖLÜM

NÜKLEER SANTRALLERİN SİBER GÜVENLİĞİ ve ULUSLARARASI HUKUKİ ESASLARI

ÖNSÖZ

Bu tezin konusu uluslararası hukuk bağlamında nükleer santrallerin siber güvenliğidir. Tezin amacı, nükleer enerji kaynağının insani amaçla kullanımına, değişen ve gelişen teknolojiyle birlikte nükleer santrallerin siber güvenliğine dair uluslararası hukuk rejimi oluşturma çabalarını irdeleyerek saptanan sorunsala dair bir hipotez geliştirmektir.

Uluslararası hukuk ve ilişkilerin temelini özellikle soğuk savaş ve sonrasındaki dönemde enerji sektörü oluşturmuştur. II. Dünya savaşında Hiroşima ve Nagazaki'ye atılan atom bombaları, nükleer enerjinin tahrip edici gücünü ortaya koyarken, "Atom for Peace" yani Barış için Atom projesiyle birlikte nükleer enerjinin insani amaçla kullanımına dair uluslararası kamuoyu oluşturma çabaları başlamıştır. Bu gelişmeler ışığında paradoksal olarak UAEA ve BM nezdinde nükleer enerjinin insani amaçla kullanımı, nükleer silahların yayılmasını ve olası nükleer savaşa yol açabileceği kaygısını da beraberinde getirmiştir. Güçlenen bu kaygıyla birlikte ulusal ve uluslararası nükleer güvenlik tedbirlerin öngörülmesini gerekli kılmıştır.

Nükleer santrallerin güvenliğine dair özellikle UAEA ve BM Genel Kurulu ve Güvenlik Konseyi'nin uluslararası hukuki düzenlemeleri diğer devletler nezdinde bağlayıcı hükümler içerirken, hukuki araçların yetersiz kaldığı ve hukuki boşluk oluşturduğu alanlar da olmuştur. Nükleer santrallerin siber güvenliği bu boşlukların başında gelmektedir. NPT Antlaşması, BM Güvenlik Konseyi Kararları ve OCED-NEA bu konuya dair genel bir çerçeve çizmiş, ancak uluslararası hukuki boşluğu tam anlamıyla doldurmada yetersiz kalmıştır. NTI, WNA ve daha birçok bağımsız kuruluş nükleer santrallerin siber güvenli hakkında çalışmalar yapsa da bu metinlerin hukuki bağlayıcılığı yoktur. Birçok tartışmayı bünyesinde bulunduran nükleer santrallerin siber güvenliğinin hukuki boyutu, bu çalışmada ilgili alanlarda literatür taraması yapılarak tekrar irdelenmiştir. Tez'in Milletlerarası Hukuk tezi olması ve Türkçe literatürde konuya ilişkin doğrudan

alakalı kaynakların yok denecek kadar az olması, çalışmanın büyük bir kısmının yabancı kaynaklar kullanılarak oluşmasına vesile olmuştur. Bu tez oluşturulurken yararlanılan internet kaynaklarının fazla olmasının sebebi ise ilgili alanda yapılan çalışmaların genellikle BM nezdinde ya da bağımsız kuruluşlar tarafından yürütülmesiyle ilgilidir. Bazı kısımlardaki detaylı açıklamalar "EKLER" kısmında sunulmuştur. Bu çalışma, özellikle Akkuyu Nükleer Santral projesinin başlamasına paralel olarak, nükleer santralin siber güvenliğinin hukuki altyapısı hususunda Türkiye Cumhuriyetine de referans olmasını temenni ediyorum.

Cihad Furkan ELİAÇIK
İstanbul, 2018

TEŞEKKÜR

Öncelikle tez konusunu belirleme, süre zarfında sürekli takip etme ve hiçbir desteği benden esirgemeyen Prof. Dr. Mesut Hakkı CAŞIN hocama şükranlarımı sunuyorum. Aynı şekilde, Dr. Öğr. Üye. Özge Yücel DERİCİLER hocama, her konuda yapıcı ve samimi bir yaklaşımla bana sunduğu desteklerden ötürü teşekkürlerimi sunuyorum. Bununla birlikte, Özyeğin Üniversitesi Hukuk Fakültesi Dekanımız Prof. Dr. Dr. h. c. Yener ÜNVER hocamızın süre zarfında bilgilendirme konusunda yardım ve desteğini esirgemediğinden ötürü teşekkür ediyorum. Ayrıca, Özyeğin Üniversitesi Sosyal Bilimler Enstitüsü Direktör Yardımcısı Prof. Dr. Özlem Yenerer ÇAKMUT hocama bana sağladığı her türlü içten yardım için can-ı gönülden teşekkür ediyorum. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dekan Yardımcımız Prof. Dr. Ahmet Hamdi TOPAL hocama ise süre zarfındaki teşvik edici yaklaşımından dolayı teşekkürü bir borç bilirim. En önemli teşekkürü ise, bu çalışmanın başından sonuna kadar en büyük motivasyonum olan sevgili eşim Cansu Yurdakul ELİAÇIK' a bir borç bilirim. Tez yazım sürecinde, hamile olmasına rağmen hiçbir desteğini benden esirgemeyerek bu çalışmanın oluşmasında büyük emekleri olmuştur.

KISALTMALAR

µSv : Microsievert
a.e : aynı eser
a.g.e : adı geçen eser
a.g.k : adı geçen kaynak
a.g.t : adı geçen tez
AAET : Avrupa Atom Enerjisi Topluluğu
ABD : Amerika Birleşik Devletleri
AGECC : The Secretary-General's Advisory Group on Energy and Climate Change
AHW : Asymmetrical Hybrid Warfare
AMACAD : American Academy of Arts & Sciences
AOLTUNW : Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons
APAC : Asia-Pacific
APT : Advanced Persistent Threat
ARENA : Australian Government – Australia Renewable Energy Agency
ASN : Authorite De Surete Nucleaire
BBC : British Broadcasting Service
Bkz. : bakınız
BM : Birleşmiş Milletler
BP : Beyond Petroleum
CBM : Confidence Building Measures
CCDCOE **:** NATO Cooperative Cyber Defence Center of Excellence
CD : The Conference of Disarmament
CE : Council of Europe
CEF : Conserve Energy Future

CIA	: Central Intelligence Agency
CIL	: Centre for International Law
CISAC	: Center for International Security and Cooperation
Cm	: santimetre
CNA	: Computer Network Attack
CPPNM	: Convention on the Physical Protection of Nuclear Material
CPS	: The Crown Prosecution Service
CPU	: Central Processing Unit
CSC	: Coal and Steel Community
CTBT	: Comprehensive Test Ban treaty
CTBTO	: Comprehensive Nuclear Test Ban Treaty
Çev.	: Çeviren
DNS	: Domain Name System
DoD	: The U.S. Department of Defense
DRC	: Democratic Republic of the Congo
E.T	: Erişim Tarihi
EC	: European Council
EDAM	: Ekonomi ve Dış Politika Araştırmalar Merkezi
EF	: Energy Fundamental
EIA	: The US Energy Information Administration
EMEA	: Europe, the Middle East and Africa
ERDA	: United States Energy Research and Development Administration
et al.	: et alia (and others: ve diğerleri/arkadaşları)
EURATOM	: European Atomic Energy Community
FAS	: Federation of American Scientist
FBI	: Federal Bureau of Investigation
GCI	: Global Cybersecurity Index
GICNT	: The Global Inititative to Combat Nuclear Terrorism
Gmbh	: Gesellschaft mit beschränkter Haftung (Company with Limited Liability)

GP	: The G8 Global Partnership
GW	: GigaWatt
HEU	: Highly Enriched Uranium
HS	: US Department of Homeland Security
I&C	: Instrumentation and Control
IAE	: International Atomic Energy
IAEA	: International Atomic Energy Agency
IATA	: International Air Transport Association
ICAN	: International Campaign to Abolish Nuclear Weapons
ICAO	: International Civil Aviation Organization
ICJ	: International Court of Justice
ICRC	: International Commitee of the Red Cross
ICSANT	: International Convention on Suppression of Acts of Terrorism
ICSTB	: The International Convention for the Suppression of Terrorist Bombings
IMCO	: The Inter-Governmental Maritime Consultative Organization
IMS	: The International Monitoring System
INLEX	: International expert Group on Nuclear Liability
INTERPOL	: The International Criminal Police Organization
IO	: Information Operation
ITU	: the International Telecommunication Union
IW	: Information Warfare
JAEA	: Japan Atomic Energy Agency
Km	: kilometre
kWh	: Kilo Watt Hour
md.	: Madde
MFA	: Republic of Turkey Ministry of Foreign Affairs
MFAPRC	: Ministry of Foreign Affairs, the People's Republic of China
MSC	**:** The Maritime Safety Committee

MW : MegaWatt

NASA : Natioanal Aeronautics and Space Administration

NATO : Notrh Atlantic Treaty Organization

NCIRC : The NATO Computer Incident Response Capability

NGS : Nükleer Güç Santrali

NMSSM : NATO Müşterek Siber Savunma Merkezi

No. : Number

Npps : Nuclear Power Plants

NPS : Nuclear Power Source

NPT **:** Non-Proliferation Treaty

NSA : National Security Agency

NSGEG : the Nuclear Security Governance Experts Group

NSS : Nuclear Security Summit

NTI : Nuclear Threat Initiative

OAS : Organization of American States

OECD – NEA : OECD Nuclear Energy Agency

OECD : The Organization for Economic Cooperation and Development

OSI : On-Site Inspections

p. : Page

pp. : Pages

PPC : Plant Process Computer

PUI : Peaceful Uses Initiative

PWC : PricewaterhouseCoopers

RDD : Radiological Dispersal Device

Res. : Resolution

RFID : Radio Frequency Identification

SALT II : Strategic Arms Limitation Talks

SCADA : Supervisory Control And Data Acquisition

SCO : the Shanghai Cooperation Organization

SDR : Special Drawing Rights

SPDS : Safety Parameter Display System

SSS : Siber Suçlar Sözleşmesi

SUA : Supprassion of Unlawful Acts

ŞİÖ : Şangay İşbirliği Örgütü

TBMM : Türkiye Büyük Millet Meclisi

TDK : Türk Dil Kurumu

TEİAŞ : Türkiye Elektrik İletim A.Ş.

TETAŞ : Türkiye Elektrik Ticaret ve Taahüt A.Ş.

TMI : Three Mile Island

TNT : Trinitroluen

UAD : Uluslararası Adalet Divanı

UDHB : Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

UN : United Nations

UNAEC : United Nations Atomic Energy Comission

UNCLOS : The 1982 United Nations Convention on the Law of the Sea

UNGA : United Nations General Assemby

UNIDIR : The United Nations Institute for Disarmament Research

UNIS : United Nations Information Service

UNODA : United Nations for Disarmament Affairs

UNODC : United Nations Office on Drugs and Crime

UNOOSA : United Nations Office for Outer Space Affairs

UNSC : United Nations Security Council

UNSCR : United Nations Security Council Resolutions

UNTC : United Nations Treaty Collection

USAF : United States Air Force

USCC : U.S.-China Economic and Security Review Commission

USNRC : United States Nuclear Regulatory Comission

USOM : Ulusal Siber Olaylara Müdahale Merkezi

UTB : Uluslararası Telekomünikasyon Birliği

VCDNP : Vienna Center for Disarmament and Non-Proliferation

Vol. : Volume

vs. : versus (mukabil/karşı)

WHO	: World Health Organization
WISE	: World Information System on Energy
WNA	: World Nuclear Association
WSIS	: World Summit on the Information Society
yy	: yüzyıl

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

ULUSLARARASI HUKUK BAĞLAMINDA NÜKLEER SANTRALLERİN SİBER GÜVENLİĞİ

CİHAD FURKAN ELİAÇIK

Bu çalışmada, Aristoteles'e kadar mazhar olan maddenin en küçük yapı taşı olan 'atom'dan nükleer enerjinin ilk kullanım alanlarına, nükleer enerjinin diğer enerji kaynaklarındaki yerinden uluslararası hukukta ne anlama geldiğine; insani ve askeri kullanım amaçlarından temel ilkelerine kadarki süreç bütünsel bir yaklaşımla irdelenmiştir. Nükleer enerjinin kullanım sahaları, günümüzde hangi amaçlarla kullanıldığı, dünyadaki toplam nükleer santral ünitesi ve neden önemli olduğu mukayeseli bir şekilde izah edilmeye çalışılmıştır. Uluslararası kamuoyu nezdinde nükleer enerjinin ucuz olması ve karbon salınımın olmaması bir avantaj olarak görülürken, nükleer santrallerin emniyet ve güvenliği noktasında ciddi kaygılar ortaya çıkmıştır. Bu kaygıların başında, son zamanlarda gelişen teknolojiyle birlikte terör örgütlerinin daha kırılgan ve büyük facialara yol açabilecek nükleer santraller gibi hedeflere yönelme eğilimleri gelmektedir. Nükleer santrallerin güvenliği ve barışçıl amaçlarla kullanılması yönünde UAEA, BM ve UAD gibi önemli uluslararası kuruluşlar Paris Sözleşmesi, Viyana Sözleşmesi ve NPT gibi hem bağlayıcı hem de tavsiye niteliğinde çalışmalar yürütmüşlerdir. Nükleer santrallerin siber güvenliği ise son zamanlarda gittikçe önem kazanmaktadır ve uluslararası hukukun tam anlamıyla yasal çerçeve oluşturamadığı bir sahadır. Bu durum da uluslararası camiada, bu boşluğu doldurmak üzere yeni hukuki düzenlemeler gerçekleştirmeye sebebiyet vermiştir. Üç bölümden oluşan bu çalışmada, nükleer enerjinin gelişimi, uluslararası hukuki esasları ve nükleer santrallerin siber güvenliği konularını irdeleyerek, bu konu hakkında bir hipotez geliştirilmeye çalışılacaktır.

Anahtar Kelimeler: Nükleer Enerji, Nükleer Santraller, Nükleer Hukuk, NPT, Viyana Sözleşmesi, Paris Sözleşmesi, Siber Güvenlik, Nükleer Güvenlik

ABSTRACT

CYBER SECURITY OF NUCLEAR POWER PLANTS IN THE CONTEXT OF INTERNATIONAL LAW

CİHAD FURKAN ELİAÇIK

In this study, the processes from the "Atom", which is the smallest building block of the material that was even mentioned by Aristotle, to the first uses of nuclear energy; from what the nuclear energy means in international law to the importance of nuclear energy compared to other energy sources and from humanitarian and military use to basic principles have been examined with a holistic approach. The use of nuclear energy in various areas, for what purposes it is used today and the total nuclear power plants in the world have been tried to be explained in a comparative way. While the international public opinion regards nuclear energy's being cheap and not emitting carbon as an advantage, there have been a serious concerns for the safety and security of nuclear power plants. Among these concerns, with the latest technology, the tendencies of the terrorists to target nuclear power plants that are vulnerable and can cause massive disasters have been the leading reasons. Prominent international organizations such as IAEA, UN and ICJ have been working for the safety and peaceful use of nuclear power plants that are both binding and advisory, such as the Paris Convention, the Vienna Convention and the NPT. Cybersecurity of nuclear power plants has become increasingly important in recent times and is an area where international law couldn't fully form a legal framework. This study, consisting of three parts, examines the development of nuclear energy, international legal principles and cyber security of nuclear power plants, and tries to develop a hypothesis on this subject.

Keywords: Nuclear Energy, Nuclear Power Plants, Nuclear Law, NPT, Vienna Convention, Paris Convention, Cyber Security, Nuclear Security

GİRİŞ

Enerji, kavramsal olarak bilinenin aksine İngilizce kökenli olmayıp Aristoteles'in "Enérgeia" olarak tanımladığı ve geliştirdiği Yunanca kökenli bir kelimedir. [1] Günlük hayatta ihtiyaç duyduğumuz gereksinimlerinin büyük bir kısmı enerji tarafından tedarik edilmektedir. Yenilenebilir ve yenilenemez olmak üzere bu enerji kaynaklarını karşılamak için yaygın olan iki yöntem vardır. Günümüzde petrol ve kömür kaynaklarının elektrik üretmek için önemli bir parametre olduğu gerçeği ışığında, yenilemez enerji kaynakların önemli bir kısmı hala bu fosil yakıtlarından tedarik edilmektedir. Bu kaynakların kıt olup bir gün biteceği gerçeği, [2] Kyoto Protokolünde de vurgulandığı üzere karbon salınımlarından dolayı ekosistemde ciddi tahribata yol açarak ozon tabakasına zarar vermesi, ülkelerin küreselleşen dünyada artan enerji ihtiyacını karşılamak üzere alternatif enerji kaynaklarına yönelmesine sebep olmuştur. Sanayileşmenin tetiklediği artan enerji talebi ise enerjiye bağımlılığı artar hale getirmiştir. Özellikle 11 Eylül 2001 terör saldırıları ve devam eden çalkantılı uluslararası gündemlerin bir sonucu olarak petrolde artan fiyatların ardından, ülkeler petrol ve doğalgazda dışa bağlamlılıklarını azaltıp kendi enerji ihtiyaçlarını karşılamak üzere yeni enerji kaynaklarına yönelme eğilimi göstermişlerdir. Yönelimin bir diğer ana unsuru ise küresel ısınmadır. Konu ile ilgili en geniş kamuoyu 23 Eylül 2014 te BM nezdinde gerçekleşen İklim Zirvesinde oluşmuştur. BM'nin sekizinci Genel Sekreteri Ban Ki Moon da bu zirvede özellikle karbon salınımından kaynaklanan çevre sorunlarına dikkat çekerek tüm üye devletlerden konuya ilişkin hassasiyet beklemiştir. [3] Son zamanlarda uluslararası kamuoyunda artan farkındalığın da bir sonucu olarak ülkeler için daha temiz ve ucuz enerji kaynakları, bir seçenekten ziyade zorunluluk haline gelmiştir. Nükleer enerji ise ucuz ve çevre dostu olması hasebiyle bu seçeneklerin başında gelmektedir. Ancak

[1] EF, Historical Development of the Word "Energy" : http://home.uni-eipzig.de/energy/ef/01.htm (E.T: 05.04.18).
[2] Hubbert, M. King, Nuclear Energy and Fossil Fuels, Houston, Texas: Shell Development Company Exploration and Production Research Division, No. 95, June 1956, p.23.
[3] UN, UN Climate Summit 2014: https://www.un.org/climatechange/summit/ (E.T: 05.04.18).

bu durumda da nükleer enerjinin hangi amaçlarla kullanılacağı sorunsalı ortaya çıkmıştır ve böylelikle uluslararası kamuoyunun gündemini önemli ölçüde meşgul etmiştir.

Bu sorunsalın ortaya çıkma sebebi ise nükleer enerjinin hem insani hem de askeri amaçlı kullanabileceği gerçeğidir. Özellikle II. Dünya Savaşında Hiroşima ve Nagazaki'ye atılan atom bombaları ve yıkıcı etkisi tüm dünyada nükleer enerjinin tahrip edici etkisini gözler önüne sermiştir. Bu gibi girişimlerin önüne geçmek ve nükleer enerjinin insani amaçla kullanımı sağlamak üzere BM Genel Kurulu 8 Aralık 1953 te toplanmıştır ve dönemin ABD Başkanı Dwight Eisenhower "Barış için Atom – Atom for Peace" konuşmasıyla nükleer enerji olgusunu dünyaya tanıtarak barışçıl amaçlarla kullanılmasının ilk yolunu açmıştır. Nükleer enerjinin insani amaçla kullanılması çabalarının ilk somut sonucu olarak BM nezdinde UAEA'nın kurulması olmuştur. Böylelikle nükleer enerji ile ilgili kurumsal bir oluşum kurulmuştur. Nükleer enerjinin bahsi geçen sebeplerden ötürü ikiyüzlü olmasından dolayı nükleer silahların gelişiminin önlenmesi konusunda da aynı ivmede çalışmalar olmuştur. Bu çabaların ilki Nükleer Silâhların Yayılmasının Önlenmesi Antlaşması (NPT) olmuştur. Bu Antlaşmanın amacı ise nükleer silahların dünya çapında yayılmasını önleyerek bu enerji kaynağının insani amaçla kullanımını teşvik etmektir. Egemen bir devletin nükleer enerjiyi insani amaçlı kullanmasında herhangi katı bir sınırlama yokken, nükleer silah geliştirme amaçlı kullanımı UAD tarafından da meşru olmayan eylem olarak tanımlanmıştır. NPT Antlaşmasının nükleer mühimmatı olan devletler nezdinde ne anlama geldiği ya da ne kadar önemi haiz olduğu ise Antlaşmasının tartışmalı kısımlarının başında gelmektedir. Askeri amaçla ilgili uluslararası kuruluşlarca bir dizi uluslararası hukuki rejim oluşturma çabaları sürerken insani amaçla kullanım alanlarının başında gelen nükleer santrallerin güvenliği ve işletilmesine dair hukuki rejim oluşturma çabaları da aynı hızda ilerlemiştir. Bunun sebebi ise nükleer santrallerin kırılgan yapıda olmalarından dolayı kasti ya da kazara herhangi bir aksama ya da saldırı durumunda olası felaketleri önleme arzusudur. Three Mile Island, Çernobil ve Fukuşima kazaları bu savı destekler nitelikteki somut örneklerdir. Özellikle Paris ve Viyana

Sözleşmeleri nükleer santrallerin çalışma esaslarına dair önemli hükümler içermektedir. Kurucu işletmelerin sorumluluğu, nükleer kaza, nükleer atık yönetimi ve tazminat bedeli gibi bir dizi parametreye dair açıklayıcı hükümler bu iki sözleşmede çerçeve halinde sunulmuştur. Akademik konferanslar sonucunda bu iki Sözleşemeye ek maddeler ilave edilerek yeni protokoller oluşturulmuştur ve böylelikle Sözleşmeler güncel tutulmaya çalışılmıştır. 1964 Tarihli Paris Sözleşmesini Yenileyen Brüksel Ek Sözleşmesi, Nükleer Enerji Alanında Üçüncü Şahıslara Karşı Hukuki Sorumluluğa ilişkin Paris Sözleşmesi'ni Yenileyen 1982 Ek Protokolü ve Paris ve Viyana Sözleşmelerinin Ortak Uygulanmasına İlişkin 21.10.1988 Tarihli Ortak Protokol, bahsi geçen konuya örnek olacak düzenlemelerden sadece birkaçıdır. Nükleer santrallerin güvenliğinin uluslararası hukuki çerçeve çalışmaları devam ederken, nükleer güvenlik noktasında uluslararası kamuoyu nükleer terörizm olgusuna dair hukuki çerçeve oluşturma çabası içerisinde olmuştur. 1373 (2001), 1540 (2004) ve 1735 (2006) Sayılı BM Güvenlik Konseyi kararları ve diğer 13 küresel antlaşma bu gayretlerin Uluslararası İnsan Hakları yükümlülükleriyle uyumlu bir şekilde uygulanması gereken nükleer terörizme karşı evrensel hukuki çerçeve çizmiştir. Temel olarak, bu 13 antlaşma ve 1373 sayılı karar, Uluslararası Ceza Hukuku araçlarıdır. Nükleer terörizme karşı bu uluslararası hukuki çerçevenin oluşmasında, 1540 sayılı karar ile oluşturulan çerçeve, 1987 yılında yürürlüğe giren Nükleer Maddelerin Fiziki Korunması Sözleşmesi (CPPNM) ve 2001 yılından bu yana yürürlükte olan Terörist Bombalamaların Önlenmesine Dair Uluslararası Sözleşme (ICSTB) kilit öneme haizdir. Nükleer terörizmle mücadele konusunda uluslararası kuruluşlarca uluslararası hukuki çerçeve oluşturma sürecinde sürekli içtihat çalışmaları olmuştur ve Nükleer Güvenlik Zirvelerinde de dünya liderleri tarafından ele alınmaktadır. Bu konuda uluslararası kamuoyunu teyakkuz halinde tutan gerekçe ise nükleer santrallerin kırılgan bir yapıda olması ve nükleer santrallerin siber güvenliğinin olası bir siber saldırı durumunda oluşacak muhtemel felakettir. Bu konuda çeşitli uluslararası kurum ve kuruluşlarca çalışmalar yapılsa da gelişen teknolojiyle birlikte siber saldırılar daha karmaşık bir hale gelmiştir. Nükleer santrallere karşı gerçekleşebilecek en basit siber saldırıları SCADA sistemlerine yapılan Stuxtnet ve DDoS saldırılarıdır. Yaygın olan bu

saldırılarla birlikte ve genel olarak siber saldırıların uluslararası hukukta herhangi bir savaş suçu sayılıp sayılmayacağı *jus ad bellum* ve *jus in bello* kavramlarıyla tanımlanmaya çalışılsa da, yapılan çalışmalar devletler ve kurucu işletmelerin uluslararası hukuki çerçevede mukabil tedbirler uygularken hangi kaynağa dayanak göstererek müdafaa gösterecekleri noktasında yetersiz kalmıştır. Hâlihazırda kırılgan bir yapıda olan nükleer santrallerin siber güvenliği de bu yüzden 11 Eylül terör saldırılarından itibaren uluslararası kamuoyunda yoğun bir şekilde odak noktası olmuştur. UAEA, BM Genel Kurul ve Güvenlik Konseyi, UDÖ gibi uluslararası kuruluşlar bu alanda nükleer terörizm ve nükleer santrallerin emniyet ve fiziki güvenliği başlığı altında bağlayıcı ve tavsiye niteliğinde düzenlemelere gitmişlerdir. UAEA nezdinde Nükleer Malzemelerin Fiziksel Korunması Sözleşmesi ve 2005 tarihli Değişiklik, Nükleer Kazaların Erken Bildirimi Sözleşmesi ve Acil Nükleer ve Radyolojik Kaza Durumunda Yardım Sözleşmesi, olası bir terör saldırısı ya da kaza durumunda alınması gereken tedbirler noktasında bağlayıcı hükümler içermektedir. BM nezdinde ise BM Güvenlik Konseyinin 1373 (2001) ve 1540 (2004) Sayılı Kararları, Terörist Bombalamalarının Engellenmesine Dair Uluslararası Sözleşme ve Nükleer Terör Faaliyetlerinin Önlenmesine Dair Uluslararası Sözleşme bağlayıcı hükümler içeren bir dizi uluslararası hukuki düzenlemeler bulunmaktadır. Bu hükümler bağlayıcı nitelikte olup hem üye devletler için önemli bir hukuki çerçeve çizmekte hem de nükleer santrali olmayıp yeniden inşa edecek devletler için bir yol haritası çizmektedir. UDÖ nezdinde de bağlayıcı hükümler içeren düzenlemeler bulunmaktadır. Bunların başında ise Deniz Ulaştırması Güvenliğine Karşı Yasadışı Eylemlerin Önlenmesine İlişkin Sözleşme (1988 SUA Sözleşmesi) ve SUA (Yasadışı Eylemlerin Önlenmesi) Sözleşmesinin 2005 Protokolleri uluslararası deniz taşımacılığı esnasında gerçekleşebilecek terör saldırıları ve nükleer terörizm ile ilgili önemli bağlayıcı hükümler içermektedir. Euratom un yapmış olduğu çalışmalar da aynı şekilde uluslararası hukuki açıdan emsal teşkil edecek bir dizi düzenlemeleri içermektedir. Euratom Anlaşmasının 103. maddesinin Uygulanmasına İlişkin Komisyon Tavsiyesi, üye devletler arasında nükleer enerji ile ilgili düzenlemeler içermektedir ancak bu düzenleme bağlayıcı olmayıp tavsiye niteliğindedir. Bu bilgiler ışığında, uluslararası hukuk araçlarında

nükleer santrallerin siber güvenliğine dair doğrudan düzenlemeler olmamakla birlikte, ilgili konu hakkında nükleer terörizm ve nükleer santrallerin emniyet ve fiziki güvenliği başlığı altında genel bir çerçeve çizilmiştir. Buna ek olarak nükleer santrallerin siber güvenliğini ele alırken dikkat edilmesi gereken diğer bir husus da kritik altyapılardır. Kritik altyapılar ve nükleer santrallerin siber güvenliği arasında kuvvetli bir bağ vardır. Nükleer santrallere gerçekleştirilen siber saldırılar sadece SCADA sistemine karşı değil, kontrol odalarına giden elektrik hatları ve diğer teknik akşamlara da gerçekleştirilebilmektedir. Bu yüzden siber saldırıların bütünsel ele alınabilmeleri için nükleer santrallerin kritik altyapılarının da sürece dâhil edilerek değerlendirilmeleri gerekmektedir. Nükleer santrallerin kritik altyapılar dâhilinde siber güvenliğini doğrudan düzenleyen uluslararası hukuki bir düzenleme olmamakla birlikte konu ile ilgili bağlayıcı olmayan EIA, UAEA ve OECD-NEA' nın bilimsel yayınları vardır. Uluslararası kamuoyu nezdinde bu konu ile ilgili farkındalık düzeyi ve çalışmalar günden güne artarken, uluslararası hukuki çerçeve oluşturma konusunda da ülkeler yeni rejim oluşturma çabaları içerisindedirler. Bu girişimler düzenli olarak Nükleer Güvenlik Zirvesinde dile getirilmektedir ve uluslararası camiada kamuoyu oluşturulmaya çalışılmaktadır. Sonuç olarak, ucuz ve çevre dostu olması hasebiyle nükleer enerjiye olan ilgi 'Barış için Atom' süreciyle başlayan girişimlerle artmış olsa da, nükleer enerjinin ikiyüzlü olması sebebiyle uluslararası kamuoyunu oldukça meşgul etmiştir. Nükleer santraller insani amaçla kullanırlarken dahi kırılgan bir yapıda olmalarından dolayı oldukça sıkı denetim dâhilinde işletilmesi gerekmektedir. Nükleer santraller ve santrallerin güvenliğine dair uluslararası hukuki rejimler kapsamında ele alınıp bağlayıcı hükümler içeren noktalar olsa dahi tam anlamıyla nükleer santrallerin siber güvenliği gibi cevaplanamayan alanlar vardır. Doğrudan bu konu ile ilgili uluslararası camiada çeşitli kurum ve kuruluşlar çalışmalar yürütse de, bunlar genellikle tavsiye niteliğinde olup önleyici tedbirler içermeyen ve caydırıcı nitelikte olmayan çalışmalardır. Bu da, ülkeleri bu uluslararası hukuki boşluğu doldurmaya yönelik yeni rejim oluşturma girişimlerine sevk etmiştir ancak çalışmalar yetersiz düzeydedir.

Tüm bu bilgiler ışığında, çalışmamızın birinci bölümünde günlük hayatımızın en önemli yapı taşını teşkil eden 'Enerji'nin tarihi gelişimi incelenmiştir. Yenilenebilir ve sürdürülebilir enerji kapsamında nükleer enerjinin yeri saptanarak günümüzde önemi ve kullanım alanları ayrıntılı bir şekilde izah edilmiştir. Nükleer enerjinin kullanım amacı olarak askeri ve insani amaçlı kullanımları ve uluslararası camiada etkisi kavramsal olarak açıklanarak lehteki ve aleyhteki görüşler açıklanmıştır. Üçüncü bölümde ayrıntılı bir şekilde ele alınacak olan siber güvenlik ve nükleer santrallerin siber güvenliği olgusu da bu kısımda ön bilgi niteliğinde sunulmuştur.

İkinci bölümde ise UAEA, BM ve UAD ve diğer uluslararası kurum ve kuruluşların nükleer santrallerin çalışma esaslarına dair uluslararası hukuki düzenlemeleri incelenmiştir. Kurucu işletmenin hukuki sorumlulukları, sorumluluk rejimi, nükleer kaza halinde hukuki sorumluluğun kime ait olduğu, lisanslama süreci ve NPT gibi uluslararası hukuki düzenlemeler bu kısımda konu başlıkları altında incelenmiştir. Düzenlemelerdeki boşluklar irdelenerek değerlendirme kısmında da paylaşılmıştır. Ulusal düzenleme kapsamında TAEK'in çalışmalarının da dâhil edildiği ikinci kısımda, genel olarak nükleer santrallerin uluslararası hukuki esasları incelenmiştir.

Üçüncü bölümde ise nükleer güvenlik başlığı altında nükleer santrallerin siber güvenliği ve uluslararası kurum ve kuruluşların çalışmalarına yer verilmiştir. Uluslararası hukuk nezdinde nükleer santrallerin siber güvenliğine dair doğrudan bir çalışma olmadığı gerçeği ise mevcut uluslararası düzenlemelerdeki boşluklar ele alınarak izah edilmeye çalışılmıştır. Aynı şekilde nükleer güvenlik ve uluslararası hukuki esasları bu bölümde ayrıntılı bir şekilde ele alınarak gelişen teknoloji ile birlikte 'nükleer terörizm' olgusu ve siber saldırılar bağıntısı uluslararası hukuk düzenlemeleriyle ele alınmıştır. Nükleer santrallere karşı gerçekleşen siber saldırılar bu kısımda paylaşılarak konu ile ilgili örnekler sunulmuştur. Bununla birlikte uluslararası hukuktaki boşluk ve devletlerin hukuki rejim oluşturma çabaları incelenmiştir.

BİRİNCİ BÖLÜM

NÜKLEER ENERJİNİN TEMEL ESASLARI ve GELİŞİMİ

1. Enerji ve Enerjinin Temel Esasları

Nükleer santralleri konusunun hukuki boyutlarını analiz etmeden önce, yenilenemez enerji kaynaklarından olan nükleer enerji ve daha temel kaynak olarak enerji kavramı açıklanmaya çalışılacaktır. Enerji ve hukuk bağıntısı kavramsal olarak açıklandıktan sonra enerjinin gelişimi hukuk bağlamında ele alınacaktır.

1.1. Enerji Tanımı, Türleri ve Hukuk Bağıntısı

Enerji kavramını açıklamadan önce bilimsel bağlamda ilk kullanımlarını saptamak, enerji ve nükleer enerji bağıntısını ilişkilendirme yolunda isabetli olacaktır. Bu bağlamda, enerji kelimesi ilk olarak 1807 yılında İngiliz araştırmacı Thomas Young tarafından bilimsel bir bağlamda kullanılmıştır ve 1852 yılında William Thomson tarafından (daha sonra Lord Kelvin olarak bilinmiştir) modern bilimsel anlamını almıştır. Thomson' ın bu katkısına paralel olarak 1847 deki bir dersinde fizikçi James Joule enerjiyi 'yaşayan kuvvet' olarak tanımlamıştır. [4] Üretim yöntemlerinin farklılık göstermesiyle birlikte enerji kaynakları yenilenebilir ve yenilenemez enerji olarak esasında iki kategoriye ayrılmaktadır. [5] Yenilemez fosil yakıtların aksine yenilenebilir enerji tekrar kullanılabilen enerji anlamına gelirken, kısa bir süre içerisinde oluşup tekrar yenilemeyen enerji

[4] Morris, Andrew, "Energy." Why Icebergs Float: Exploring Science in Everyday Life, 1st ed., London, UCL Press, 2016, p. 139.

[5] Uyar, Fatih, Enerji Kaynakları Nelerdir? Kaça Ayrılır?, Enerji Beş Temiz Enerji Portalı, 1 Ocak 2017: http://www.enerjibes.com/enerji-kaynaklari/ (E.T: 11.03.18).

kaynakları ise yenilenemez enerji olarak tanımlanmaktadır. [6] Bu bilgiler ışığında, sanayi devrimi ile başlayan enerji ihtiyacı ve girişimcilik inovasyonu ekseninde özellikle 1840'ların sonlarında ve 1850'lerin başlarında kömür ve diğer hidrokarbonların bu ihtiyaçlara cevap vermeye başlaması, [7] enerji olgusunun ekonomik yönünün önemini ortaya koymuştur. Günümüzde ise, politik-stratejik öneme haiz olaylar ve ekonomik gelişmeler, dünya ülkelerinin enerji politikalarındaki değişimler için önemli katalizörler olmuştur. [8] Bu gerekçe ile sürdürülebilir ekonomik büyüme ve gelişmiş insan refahı için enerji vazgeçilmez bir hale gelmiştir[9] ve birçok yöntemle farklı amaçlar çerçevesinde orta düzeyde günlük ihtiyaçlarımızı karşılamada enerji önemli bir parametredir. [10] Bu ihtiyaçları karşılarken elektrik enerjisi, gündelik hayatta ihtiyaç duyduğumuz birçok malzeme ve aygıt için önemli bir unsurdur. Enerji dâhilinde elektrik enerjisinin hukuk bağıntısı ulusal mevzuatta 6446 Sayılı Elektrik Piyasası Kanunu'nda amaç, kapsam ve tanımlamalarla açıklığa kavuşturulmuştur. Bu bağlamda:

Madde 1: "Bu Kanunun amacı; elektriğin yeterli, kaliteli, sürekli, düşük maliyetli ve çevreyle uyumlu bir şekilde tüketicilerin kullanımına sunulması için, rekabet ortamında özel hukuk hükümlerine göre faaliyet gösteren, mali açıdan güçlü, istikrarlı ve şeffaf bir elektrik enerjisi piyasasının oluşturulması ve bu piyasada bağımsız bir düzenleme ve denetimin yapılmasının sağlanmasıdır." [11]

---

[6] EIA, Nonrenewable and Renewable Energy Sources, February 9, 2017: https://www.eia.gov/energyexplained/index.php?page=nonrenewable_home (11.03.18).

[7] Yergin, Daniel, The Prize: The Epic Quest for Oil, Money, & Power, New York: Simon & Schuster, 1991, p.23.

[8] Janardhanan, Nandakumar, Transition to Energy Secure Future: Policies Enabling Energy Transition in India, Report, Institute for Global Environmental Strategies, 2012, p.4.

[9] UAEK: https://www.iaea.org/topics/energy (E.T: 10.03.18).

[10] Keeney, Spurgeon M. Jr. Chmn., Nuclear Power Issues and Choices, the USA, Nuclear Energy Policy Research Group, Sponsored by the Ford Foundation and Administered by the MITRE Corporation, 1977, p.44.

[11] Elektrik Piyasası Kanunu, Resmî Gazete, 30.03.2013, Sayı: 28603 : http://www.resmigazete.gov.tr/eskiler/2013/03/20130330-14.htm (12.03.18).

Enerjinin özellikle elektrik üretimi dâhilinde "TEİAŞ Şubat 2016 verilerine[12] göre 31 Ocak 2016 itibariyle Türkiye Cumhuriyeti elektrik üretimi kurulu gücü 73.427 MW olmuştur." [13] Enerjiye artan taleple birlikte hem ulusal hem de uluslararası kamuoyunda alternatif enerji kaynakları oluşturma ve enerjiyi daha verimli kullanma yönünde girişimler olmuştur ve hala devam etmektedir. [14] Bu kavramsal tanımlamalara paralel olarak yenilenebilir, yenilenemez ve son zamanlarda üzerinde durulan sürdürülebilir enerji başlıklarını ayrı başlıklar altında incelemek, farklarının kavranması açısından isabetli olacaktır.

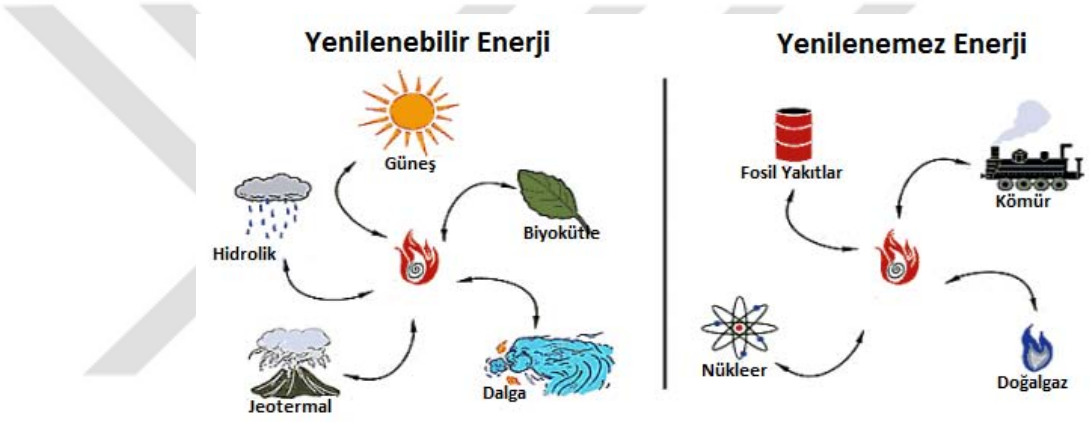
1.1.1. Yenilenebilir Enerji

Bir önceki başlıkta yenilenebilir enerji ile ilgili özet niteliğinde tanımlama yapılmıştır. Bu düzlemde, enerji ihtiyacı sürekli artarken, yeni enerji kaynaklarının araştırılması da yoğunlaşmıştır ve bu çalışmaların sonucunda son yüzyılda kömürden petrole ve petrolden doğal gaza kademeli bir değişim olmuştur[15]. Bu bağlamda, yenilenebilir enerji teknolojileri de bir dizi avantaj sağlamaktadır ve teknolojiler sürdürülebilir ve adil ekonomik kalkınma, enerji erişimi, güvenli enerji tedariki, çevresel ve sağlık etkilerini ele alabilmektedir. [16] Buna ilaveten, 2012 yılında dünya, toplam birincil enerji kaynağının yaklaşık % 13,2'si için yenilenebilir kaynaklara dayanmaktaydı. 2013 yılında yenilenebilir enerji kaynakları, küresel elektrik üretiminin yaklaşık % 22' sini oluştururken,

[12] TEİAŞ, Türkiye Kurulu Gücünün Yıllar İtibariyle Gelişimi, https://www.teias.gov.tr/tr/i-kurulu-guc (12.03.18).
[13] PWC, Elektrik Piyasasında Kaynakların Kullanımına İlişkin bir Değerlendirme, https://www.pwc.com.tr/tr/sektorler/enerji-altyapi-madencilik/enerji-spotlights/elektrik-piyasasinda-kaynaklarin-kullanimina-iliskin.html (13.03.18).
[14] Ozturk, Ilhan, Energy Dependency and Security: The Role of Efciency and Renewable Energy Sources, IGC, April 2014, p.2.
[15] Kilinc Ata, N., An Exploration of Renewable Energy Policies with an Econometric Approach, University of Stirling, Yayınlanmamış Doktora Tezi, 2015, s.14.
[16] Lee, C. [李卓穎], 发展可再生能源行业的风险管理和投资战略。[Development of Risk Management and Investment Strategies in Renewable Energy Industry] , University of Hong Kong, Pokfulam, Hong Kong SAR, Yayınlanmamış Doktora Tezi, 2016, s.1.

2015 UEA (IEA) Orta Vadeli Yenilenebilir Enerji Raporuna göre, [17] 2020 yılında payının en az % 26' ya yükseleceğini öngörmektedir. [18] Pek çok doğal enerji kaynağı olduğu gibi, birçok yenilenebilir enerji teknolojisi vardır. Güneş en bilinenlerinden biri, rüzgâr enerjisi en yaygın olanı ve hidroelektrik en eskilerinden biridir ve diğer yenilenebilir teknolojiler, ısı veya elektrik üretmek için jeotermal enerji, biyoenerji veya okyanus enerjisinden yararlanmaktadır. [19]

Şekil 1: Enerji Kaynakları ve Çeşitleri



Kaynak: Uyar, 2017.

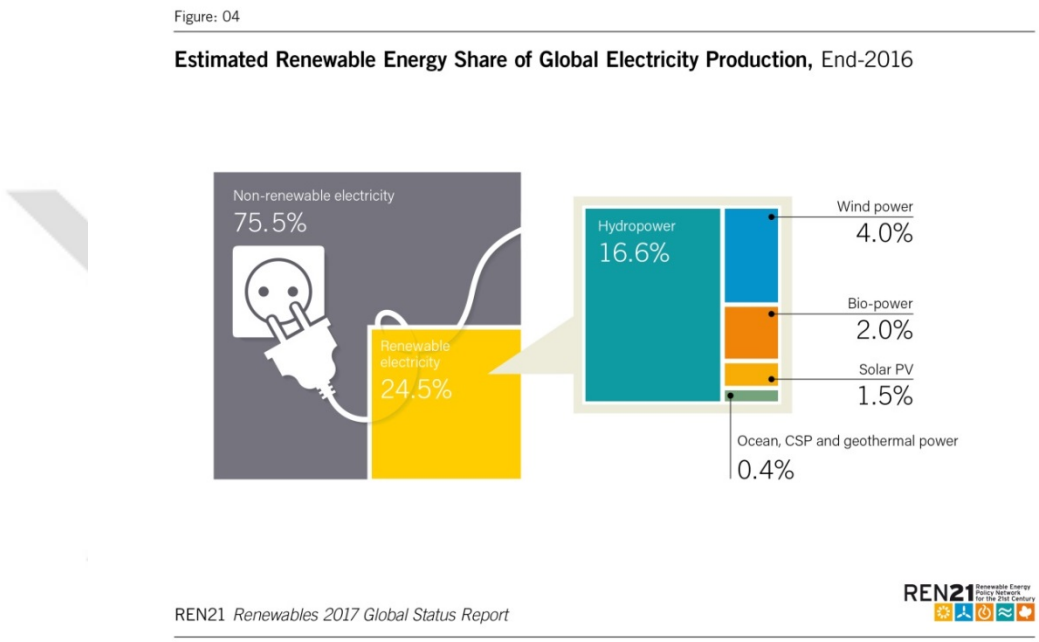
1.1.2. Yenilenemez Enerji

Yenilenemez enerji kaynakları, yüzyıllar boyunca biriken fosil rezervlerini tüketen kaynaklardır. Bu durum ise, bu enerji rezervlerinin tükenmesine neden

[17] Bkz: http://www.iea.org/newsroom/news/2015/october/renewables-to-lead-world-power-market-growth-to-2020.html (E.T: 11.03.18).
[18] Uluslararası Enerji Ajansı, Renewable Energy, https://www.iea.org/about/faqs/renewableenergy/ (E.T: 11.03.18).
[19] ARENA, What is Renewable Energy?, https://arena.gov.au/about/what-is-renewable-energy/ (E.T: 13.03.18).

olmaktadır. [20] Fosil yakıtlar (petrol, doğal gaz ve kömür gibi) ve radyoaktif yakıt (uranyum) en yaygın yenilenemeyen enerji kaynaklarıdır. Bu kaynaklar esasında yenilenebilir olmasına rağmen, üretmesi binlerce yıl sürmesi, onları sürdürülebilir olmayan ve dolayısıyla yenilenemez hale getirmektedir. [21]

Şekil 2: Küresel Yenilenebilir-Yenilemez Enerji İstatistiği



Kaynak: REN21, 2017.[22]

Yenilenebilir ve yenilemez enerji kaynakları enerji tedarikinde iki kategoriye ayrılırken, bu tedarik zincirinin sürdürülebilirliği konusunda da uluslararası kamuoyunda çalımalar yürütülmektedir. Bu yüzden, sürüdürülebilir enerji başlığını genel hatlarıyla ayrıca incelemek, yenilenebilir ve yenilenemez enerji kaynaklarının devamlılığı ilkesini kavramada önem arz etmektedir.

[20] CEF, What are Non-Renewable Sources of Energy? : https://www.conserve-energy-future.com/nonrenewableenergysources.php (E.T: 11.03.18).
[21] Maehlum, Mathias Aarre, Non-Renewable Energy Resources, Energy Informative, May 3, 2013 : http://energyinformative.org/non-renewable-energy-resources/ (E.T: 14.03.18).
[22] REN21, Global Status Report, 2017: http://www.ren21.net/status-of-renewables/global-status-report/ http://energyinformative.org/non-renewable-energy-resources/ (E.T: 14.03.18).

1.1.3. Sürdürülebilir Enerji

Kavramsal olarak sürdürülebilir enerji, enerji politikasının nasıl geliştirildiğini ve uygulandığını ve bu alandaki zorlukları ile ilgili stratejiler geliştirmekle birlikte [23] tam anlamıyla, belli bir süre boyunca sürdürülebilen sürdürülebilir enerji, öngörülebilir bir gelecek için enerji üretimi anlamına gelmektedir ve sürdürülebilir enerji uygulamaları, ihtiyaçlarımızı karşılamaya devam edebilecek kaynaklara dayanması gerekliliğini savunmaktadır. [24] Sürdürülebilir enerji ile alakalı politikalar esasında Sanayi Devriminin ortaya çıkmasına paralel olarak ortaya çıkmıştır ve tartışmalar Sanayi Devrimine kadar gitmektedir. Bu kaynakların, kullanılmayacakları, tükenmeyecekleri veya başka bir şekilde kullanılamaz hale gelmeleri için dikkatli bir şekilde kullanılması gerekmektedir. Bu gerekçeyle, enerjiye erişim konusu son zamanlarda küresel politika gündeminde önemli bir yere sahip olmaktadır ve şu anda uluslararası kalkınma politikalarının oluşturulmasında merkezi bir tema haline gelmiştir. [25] Bu gelişmeler ışında, BM Genel Kurulu, 2014-2024'ü 'Herkes için Sürdürülebilir Enerji'nin on yılı olarak ilan etmiştir. [26] Sürdürülebilir enerjinin önemine binaen BM, mevcut enerji üretimi ve tüketimi modelleri sürdürülemez ve çevreyi hem yerel hem de küresel ölçekte tehdit etmekte olduğunu ve fosil yakıtların yakılmasından kaynaklanan emisyonlar, iklim değişikliğinin öngörülemeyen etkilerine ve kentsel hava kirliliğine ve toprak ve suyun asitlendirilmesine büyük katkıda bulunduna dikaat çekmiştir. Aynı şekilde BM, enerjinin karbon

[23] Corporate Knights Inc., Back Matter, Corporate Knights, Vol. 9, No. 1, 2010, p.2.
[24] Jenden, James/ Ellen Lloyd/ Kailyn Stenhouse/ Jason Donev, Renewable and Sustainable Energy, Energy Education: http://energyeducation.ca/encyclopedia/Renewable_and_sustainable_energy (E.T: 11.03.18).
[25] Tessama, Zereay, et al. Mainstreaming Sustainable Energy Access into National Development Planning: The Case of Ethiopia. Stockholm Environment Institute, 2013, p.4.
[26] UN, The United Nations General Assembly declared 2012 as the International Year for Sustainable Energy for All, 2012: https://www.un.org/press/en/2012/ga11333.doc.htm (E.T: 11.03.18).

yoğunluğunun azaltılması - yani tüketilen enerji başına salınan karbon miktarının uzun vadeli iklim hedeflerine ulaşmanın temel hedefi olduğunu yinelemiştir. [27]

1.2. Nükleer Enerji

Bu başlık kapsamında, enerji kavramının teorik altyapısının sağlanması ile birlikte nükleer enerjinin kavramsal analizi ile birlikte gelişim süreçleri ele alınacaktır.

1.2.1. Nükleer Enerji Kavramı ve Tanımı

Nükleer kelimesi İngilizce kökenli, "nucleus" adının sıfatlanmış halidir. [28] TDK'nın Nükleer Enerji Terimleri Sözlüğünde Nükleer Enerji, "Bir nükleer yakıtın kütle birimi basma açığa çıkardığı toplam enerji" olarak tanımlamaktadır. [29] Amerikan Enerji Bilgi İdaresi (EIA) ise Nükleer Enerjiyi katı, sıvı ve gazları oluşturan moleküllerdeki küçük parçacıklar olarak zikretmektedir. [30] Nükleer Enerji kavramının teorik açıklaması ise Türkiye Atom Enerjisi Kurumu internet sitesinde "Nükleer Enerji Nedir?" başlığı altında detaylı bir şekilde açıklanmıştır. [31] Nükleer enerjinin temel bileşeni olan Uranyum;

---

[27] AGECC: Energy for a Sustainable Future: Report and Recommendations, 28 April 2010, New York, p.7.

[28] Denk, Erdem, Bir Kitle İmha Silâhı Olarak Nükleer Silâhların Yasaklanmasına Yönelik Çabalar, Ankara Üniversitesi SBF Dergisi, C. 66, S. 3, 2011. s. 93.

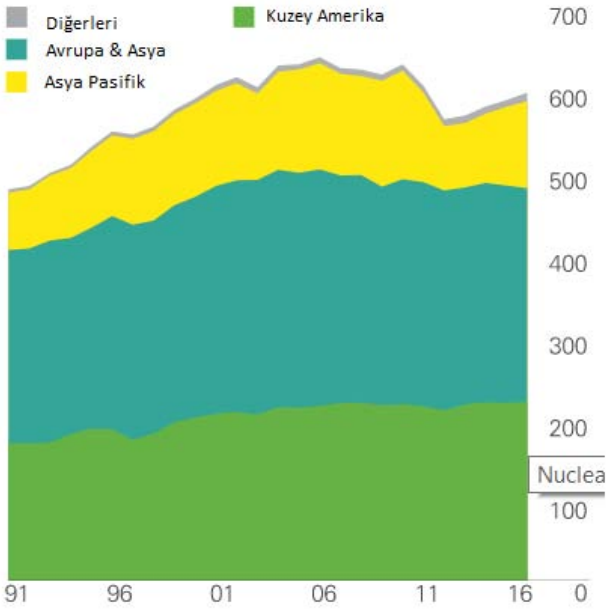
[29] Boyla, Mazhar/ Yılmaz Canküyer, Nükleer Enerji terimleri Sözlüğü, Ankara: Türk Dil Kurumu Yay., 1995, s. 118.

[30] EIA: https://www.eia.gov/energyexplained/index.cfm?page=nuclear_home#tab1 (E.T: 13.02.18).

[31] "Atom çekirdeklerinin parçalanması sonucunda büyük bir enerji açığa çıkmaktadır. Ağır atom çekirdeklerinin nötronlarla bombardımanı sonucunda bu çekirdeklerin parçalanması sağlanabilir; bu tepkimeye "fisyon" adı verilmektedir. Her bir parçalanma tepkimesi sonucunda açığa fisyon ürünleri, enerji ve 2-3 adet de nötron çıkmaktadır. Uygun şekilde tasarlanan bir sistemde tepkime sonucu açığa çıkan nötronlar da kullanılarak parçalanma tepkimesinin sürekliliği sağlanabilir (zincirleme tepkime). Bunun haricinde hafif atom çekirdeklerinin birleşme tepkimeleri de büyük bir enerjinin açığa çıkmasına sebep olmaktadır. Bu birleşme tepkimesine "füzyon" adı verilmektedir. Bu tepkimenin sağlanabilmesi için atom çekirdeğinde bulunan artı yüklerin birbirini itmesinden kaynaklanan kuvvetin yenilmesi gereklidir. Bu nedenle çok yüksek sıcaklığa çıkılan sistemler kullanılmaktadır. Çok yüksek sıcaklıkta yüksek enerjiye ulaşan atom çekirdeklerinin çarpışması ile füzyon tepkimesi sağlanabilmektedir. Fisyon ve füzyon tepkimeleri ile elde edilen

reaktör yakıtı, nükleer silahlar, uçak kuyrukları için dengeleyiciler ve zırh delici mühimmatlar gibi birçok sivil ve askeri alanda kullanılan ağır, hafif radyoaktif özellik gösteren ve metalik bir elementtir. [32]

Şekil 3: Bölgelere göre nükleer enerji tüketimi (milyon ton petrol eşdeğeri)



Kaynak: BP, 2017, s.43.[33]

Günümüzde çoğu enerji santrali, elektrik üretmek için bir türbini döndürmek üzere suyu buharlaştırmak için kömür, yağ veya doğalgaz yakmaktadır ve bu fosil yakıtları yakmanın bir alternatifi nükleer enerjidir çünkü nükleer enerji meydana getirmek için hiçbir malzeme yakılmamaktadır, bu

---

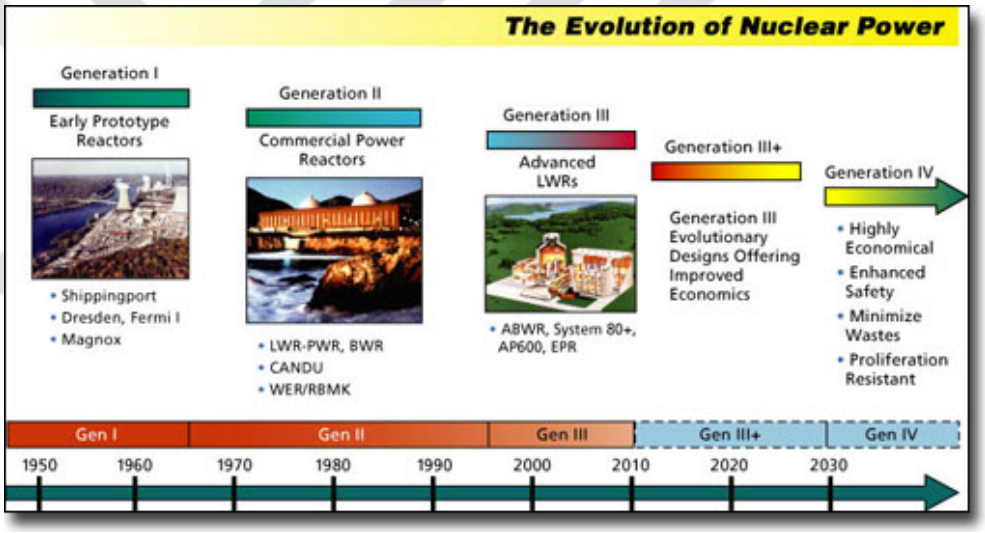
enerjiye "çekirdek enerjisi" veya "nükleer enerji" adı verilmektedir.", Türkiye Atom Enerjisi Kurumu: http://www.taek.gov.tr/nukleerguvenlik/nukleer-enerji-%20vereaktorler/169-%20nukleer-enerji/457nukleer-%20enerji-nedir (E.T: 13.03.18).

[32] Ferguson, Charles D., Nükleer Enerji: Herkesin Bilmesi Gerekenler, Ankara, Buzdağı Yayınevi, Birinci Baskı 2015, s.43.

[33] BP, BP Statistical Review of World Energy, 66th Ed. 2017, p.43.

nedenle atmosfere zararlı salınımlar yayılmamaktadır. [34] Nükleer enerji, ultra konsantre bir enerji kaynağıdır; bir ton doğal uranyum, kırk dört milyon kWh elektrik üretebilmektedir. Karşılaştırma yapmak gerekirse, aynı miktarda elektrik üretmek için yirmi bin ton kömür veya 8,5 milyon metreküp doğal gaz gerekmektedir. Bu bilgiler dâhilinde, nükleer enerji çevreye zararlı gaz salınımında bulunmaması ile birlikte nükleer enerji, kamusal alanda, esas olarak atom silahları, operasyonel güvenlik kayıtları ve ürettiği radyoaktif atık maddelerle ilgili ilişkisi nedeniyle tartışmalıdır. [35]

Şekil 4: Nükleer Enerji ve Santrallerin Evrimi



Kaynak: Mariotte, 2016.[36]

[34] Beckrich, Amanda, The Green Room: The Pros and Cons of Nuclear Energy, The Science Teacher, Vol. 80, No. 3, 2013, p.10.
[35] Tsoukalas, Lefteri H., and Rong Gao., A Future Role for Nuclear Energy? Understanding the Global Energy Crisis, edited by Eugene D. Coyle and Richard A. Simmons, Purdue University Press, West Lafayette, Indiana, 2014, p.167.
[36] Mariotte, Michael, Wishful Thinking: the Basis of New Nuclear Economics, March 28, 2016 : https://safeenergy.org/2016/03/28/wishful-thinking-the-basis-of-new-nuclear/#more-13790 (E.T: 15.03.18).

Nükleer enerjinin elektrik enerjisine dönüştürüldüğü tesis olan nükleer santraller de gelişen teknolojik altyapılarla birlikte evirilmiştir. Bu gelişim beşinci nesil nükleer güç santraline kadar uzanmıştır. Bu bağlamda beşinci nesil güç santralinin özellikleri ise oldukça ekonomik olması (highly economical), gelişmiş güvenlik (enhanced safety), atıkları minimize etmesi (minimized wastes) ve nükleer silahlara dayanıklı (proliferations resistant) olmasıdır. [37]

1.2.2. Nükleer Enerjinin Tarihçesi

Nükleer enerjisinin başlangıcı insan doğasında var olan test etme, gözlemleme ve hayal etme olgusundan türemiştir ve asırlar süren bir hayalin gerçeğe dönüşmesinin hikâyesi sonucunda ortaya çıkmıştır. [38] Nükleer enerjiyi anlamamızın hikâyesi 2400 yıl önce Antik Yunan'da, Sokrates öncesi Yunan filozofu Demokritus'un, dünyanın kendisinden daha küçük bir parçaya bölünemeyen "atom" adını verdiği bir yapı taşından meydana geldiğini ortaya koymasıyla başlamaktadır. [39] Geçmiş zamandan günümüze nükleer enerji evrimini sürdürerek daha modern ve karmaşık bir hal almıştır. Nükleer enerjinin gelişim endeksinde ise sanayileşmenin etkisi ve II. Dünya Savaşı kritik öneme haiz olmuştur. İlerleyen madde başlıklarında bu örnekler daha detaylı incelenecektir, lakin bahsi geçen iki gelişme aynı zamanda nükleer enerjinin kullanım alanlarını belirlemiştir ve nükleer enerjinin gelişimi insani ve askeri amaçlı olmak üzere ikiye ayrılmıştır.

---

[37] A.g.e.

[38] U.S. Department of Energy Office of Nuclear Energy, Science and Technology, The History of Nuclear Energy : https://www.energy.gov/sites/prod/files/The%20History%20of%20Nuclear%20Energy_0.pdf (E.T: 13.03.18).

[39] Ferguson, a.g.e., s.26.

Tablo 1: Nükleer Enerji Zaman Çizelgesi

1934	Fizikçi Enrico Fermi, Roma'da nötronların birçok çeşit atomu böldüğünü gösteren deneyler yapmıştır.
1938	Otto Hahn, Fritz Strassman ve Lise Meitner, Einstein'ın kütle ve enerji arasındaki ilişki teorisini kullanarak E = mc2'yi (enerji eşittir kütle çarpı ışık hızının karesi) kullanarak fizyon oluşumunu kanıtlamışlardır.
1942	Fermi liderliğindeki bir grup bilim insanı Chicago'da kendi kendini idame ettiren ilk kontrollü nükleer zincir reaksiyonunu üretmişlerdir.
1945	Hiroşima'ya atom bombası atıldı; üç gün sonra, Nagazaki'ye daha küçük bir bomba atıldı.
1946	Atom Enerjisi Komisyonu nükleer enerji gelişimini kontrol etmek ve nükleer enerjinin insani kullanımını araştırmak için oluşturulmuştur.
1951	Arco, Idaho'da, Deneysel Üretim Reaktörü I, nükleer enerjiden ilk elektrik gücünü üretmiştir.
1957	İlk büyük ölçekli nükleer santral, Shippingport, Pennsylvania'da faaliyete başlamıştır.
1971	Amerika Birleşik Devletleri'nde yirmi iki ticari nükleer santral faaliyet göstermektedir.
1979	28 Mart'ta Harrisburg, Pennsylvania yakınlarındaki Three Mile Island nükleer santralinde mekanik arıza ve insan hatası nedeniyle kaza meydana gelmiştir.
1979	Yetmiş iki lisanslı reaktör, ABD elektriğinin % 12'sini üretmiştir.
1986	26 Nisan'da, bir operatör hatası eski Sovyetler Birliği'ndeki Çernobil nükleer santralindeki 4 numaralı reaktörde iki patlamaya neden olmuştur.
1992	110 nükleer santral, ABD' de kullanılan tüm elektriğin yaklaşık % 22'sini sağlamıştır.
2011	Japonya'daki Fukushima enerji santrali, 9 aktif nükleer çekirdeğinin erimesiyle sonuçlanan 9.0 büyüklüğündeki depremde hasar görmüştür.

Kaynak: Palliser, 2012, s.15.[40]

[40] Palliser, Janna, Nuclear Energy, Science Scope, Vol. 35, No. 5, 2012, p. 15.

1.2.2.1.Sanayileşmenin Etkisi

Sanayi Devrimi 18. ve 19. yy' da Avrupa'da ve ilk olarak Birleşik Krallık 'ta gerçekleşmiştir ve sanayi devriminden önce dünyada kullanılan enerji kaynakları doğada bulunan su gücü ve yerel olanaklarla sınırlanmaktaydı. Ancak Sanayi Devrimi ile birlikte maden kömürü önem kazanmış ve maden kömürüne sahip olan ülkeler daha hızlı gelişmeye başlamışlardır. [41] Aynı şekilde, buharla çalışan motorlar üretkenlik, malların seri üretimi ve pazarın genişletilmesi alanında önemli rol oynamıştır. [42] 19.yy' la başlayan süreçle birlikte nükleer enerji, ülkelerin enerji ihtiyaçlarının karşılanmasında önemli faydalar sağlamıştır. Nükleer enerji, konumu ile kayda değer ölçüde değişmeyen maliyetlerle rekabetçi bir enerji kaynağı sağlamış, hava kirliliği problemini önemli ölçüde azaltmış ve diğer önemli çevresel avantajlara sahip olarak, dış ticarette olumlu bir unsur haline gelmiştir. [43] "Bu gelişmeler ışığında, nükleer santrallerin yaygınlaşması 1970'li yılların başındaki petrol krizi ile birlikte başlamıştır ve petrol ve diğer hidrokarbon kaynaklar bakımından fakir ülkeler, bu kaynaklara olan bağımlılıklarını azaltmak ve enerji arz güvenliklerini temin etmek için nükleer santrallere yönelmeleriyle birlikte nükleer santraller tüm dünyada hızlı bir şekilde işletmeye alınmıştır. 1979 yılında ABD'de yaşanan Three Mile Island (TMI) ve 1986 yılında Sovyet Rusya'da (bugün Ukrayna sınırları içinde) yaşanan Çernobil kazaları ile görece bir yavaşlama olsa da nükleer santraller tüm dünyada kurulmaya devam etmiştir." [44]

---

[41] Norouzi, Shiva, Uluslararası Hukukta Nükleer Programlar: İran Örneği, İstanbul Üniversitesi, Yayınlanmamış Yüksek Lisans Tezi, 2017, s. 6.

[42] Qasaymeh, K. A., South Africa's Peaceful Use of Nuclear Energy under the Nuclear Non-Proliferation Treaty and Related Treaties, University of South Africa, Yayınlanmamış Doktora Tezi, 2014, s.1.

[43] Ramey, James T., The Promise of Nuclear Energy, The Annals of the American Academy of Political and Social Science, Vol. 410, 1973, p.11.

[44] Enerji ve Tabi Kaynaklar Bakanlığı: http://www.enerji.gov.tr/tr-TR/Sayfalar/Nukleer-Enerji (E.T: 13.10.18).

Bir önceki başlıkta da zikredildiği üzere, özellikle beşinci nesil nükleer güç santralleri yine sanayileşmenin doğal bir neticesi olarak ülkeler artan enerji ihtiyaçlarını ekonomik ve çevre dostu santrallerle gidermeye çalışmışlardır.

1.2.2.2. II. Dünya Savaşının Etkisi

Nükleer enerjinin II. Dünya Savaşından etkilenmesi ve bu doğrultuda gelişim göstermesi, 1939'da II. Dünya Savaşı'nın başında Albert Einstein'ın ABD Başkanı FD Roosevelt'e atom bombasını geliştirmesini tavsiye etmesiyle başlamıştır. Bu kapsamda Einstein, Amerika Birleşik Devletleri'nde Enrico Fermi ve Leo Szilard; Fransa'da Frédéric Joliot ve eşi Irene Joliot-Curie'nin yaptığı araştırmalarla, büyük miktarda enerji açığa çıkaracak bir nükleer reaksiyon zincirinin tetiklenmesinin mümkün olacağını açıklamalarıyla birlikte bu prosedür aynı zamanda yeni bir tür bomba yapımını da mümkün kılmıştır. [45] Hiroşima ve Nagazaki'ye atılan atom bombaları, tüm nüfusu saniyeler içinde yok etme yeteneğine dayanan ve öngörülemez bir terörü ortaya çıkaran yeni bir siyasi düzeni başlatmıştır. [46] Evrenin gücünü kullanabilme ve güneşin enerji çıkışını ısı ve ışığın tahrip edici gücüyle rekabet edebilme yeteneği ile ölçülmüş olan Hiroshima' da ortaya çıkan nükleer enerjinin gücü, zaman içerisinde caydırıcılık unsuru olarak ortaya çıkmıştır. Bu gelişmelerin sonucunda 1960'ların ortalarında, ABD'de, Sovyet Rusya'da ve dünyanın başka bir yerinde hafif su reaktörü siparişlerinde [47] büyük artış olmuş ve nükleer enerjinin kullanımının yaygınlaşması da aynı şekilde artmıştır.

---

[45] Nuclear Energy, History of Nuclear Energy, 2017: https://nuclear-energy.net/what-is-nuclear-energy/history (E.T: 12.03.18).

[46] Gibson, A., The End, or Life in The Nuclear Age: Aesthetic Form and Modes of Subjectivity, University of Minnesota, Yayınlanmamış Doktora Tezi, 2012, s. 1.

[47] Särkikoski, T., Rauhan Atomi, Sodan Koodi : Suomalaisen Atomivoimaratkaisun Teknopolitiikka 1955-1970 [Peace Atom, War Code: Finnish Nuclear Atomic Solution Technology Policy 1955-1970], University of Helsinki, Yayınlanmamış Doktora Tezi, 2011, s. 4.

1.2.3. Günlük Hayatta Nükleer Enerji

Bir önceki başlıklarda nükleer enerjinin kavramsal olarak ortaya çıkış hikâyesi izah edilmeye çalışılmıştır. Bu bölümde ise, günlük hayatta nükleer enerjinin kullanım alanları incelenecektir.

1.2.3.1. Nükleer Enerjinin Kullanım Amaçları

Nükleer enerjinin etkisinin ortaya çıkışı her ne kadar Nagazaki ve Hiroşima'ya atılan atom bombalarıyla yıkıcı etkisini kanıtlamış olsa da, nükleer enerjinin kullanımı insani ve askeri olmak üzere farklı sahalarda etkin bir şekilde kullanılmaktadır. Nükleer enerjinin insani amaçla kullanımı tıp alanında röntgenin icadıyla başlamıştır ve askeri amaçla kullanımı ise nükleer silah olarak kullanılmasıyla başlamıştır.

1.2.3.1.1. İnsani Amaçla Kullanımı: Nükleer Endüstri

Nükleer enerji; sivil amaçlar çerçevesinde, ucuz ve temiz elektrik enerjisi üretmenin yanında, tarım ve tıp alanlarında iyileştirme ve geliştirme çalışmaları yapmak, yüksek düzeyde bilimsel araştırmalar yürütmek imkânı sağlayan, aynı zamanda siyasî otoritenin iradesi yönünde askeri amaçlı kullanıma da zemin veren "çift taraflı" bir teknolojidir. [48] İnsani amaçlı kullanım alanlarını şu şekilde özetleyebiliriz: [49]

- Tarım (Bitki mutasyonu ıslahında, Gübrelerde, Böcek kontrollerinde)

- Gıda (Gıda ışınlama)

- Sanayi (Endüstriyel yarışçılar, Muayene ve Enstrümantasyon,)

[48] Çetiner, Atıf/ Selim Sunal, Dünyada Nükleer Enerji Kullanımı ve Yeni Yaklaşımlar, 21yy Dergisi, 2008, s. 193.

[49] WNA, The Many Uses of Nuclear Technology, 2017: http://www.world-nuclear.org/information-library/non-power-nuclear-applications/overview/the-many-uses-of-nuclear-technology.aspx (E.T: 12.03.18).

- Tıp (Teşhis, Terapi, Sterilizasyon)

- Taşıma (Nükleer enerji ile çalışan gemiler, Uzay için nükleer reaktörler, Hidrojen, elektrik ve arabalar)

- Su kaynakları ve çevre (Çevresel tarayıcılar, Su kaynakları)

1.2.3.1.2. Askeri Amaçla Kullanımı: Nükleer Silahlar

Nükleer enerjinin askeri amaçla kullanımı genel hatlarıyla nükleer silah üretimi dâhilinde ele alınmaktadır. Nükleer silahlar dünyadaki en tehlikeli silah özelliğini taşımakta, tek bir tanesi bile bir şehri tamamen yok edip milyonlarca insanı öldürme potansiyeli bulunmaktadır ve uzun vadeli felaket etkileri ile doğal çevrenin ve gelecek nesillerin hayatlarını tehlikeye atabilmektedir. [50] Bununla birlikte, fisyon ve füzyonun gücü, yıkıcı tahribat meydana getirmek üzere çeşitli şekillerde açığa çıkarılabilmektedir. Bu duruma somut örnek olarak, Ağustos 1945'te Hiroşima ve Nagazaki'de ortaya çıkan 13 ve 21 kilotonluk patlama gösterilebilir. Her iki şehirde de onarılması uzun zaman alacak olan yıkıcı bir tahribat meydana gelmiştir: 200.000'i aşkın insanın hayatını kaybetmesine neden olarak aynı zamanda atom bombasının kullanımı dünya savaşını sona erdirmiştir ve Soğuk Savaş sahnesini kurmuştur. [51] Soğuk Savaş'ın zirvesinde yüksek teyakkuzda bulunan binlerce ABD ve Sovyet balistik füzeleri üretilmiştir ve o zamandan beridir nükleer silahlar genel olarak iki kategori altında anılmıştır: [52]

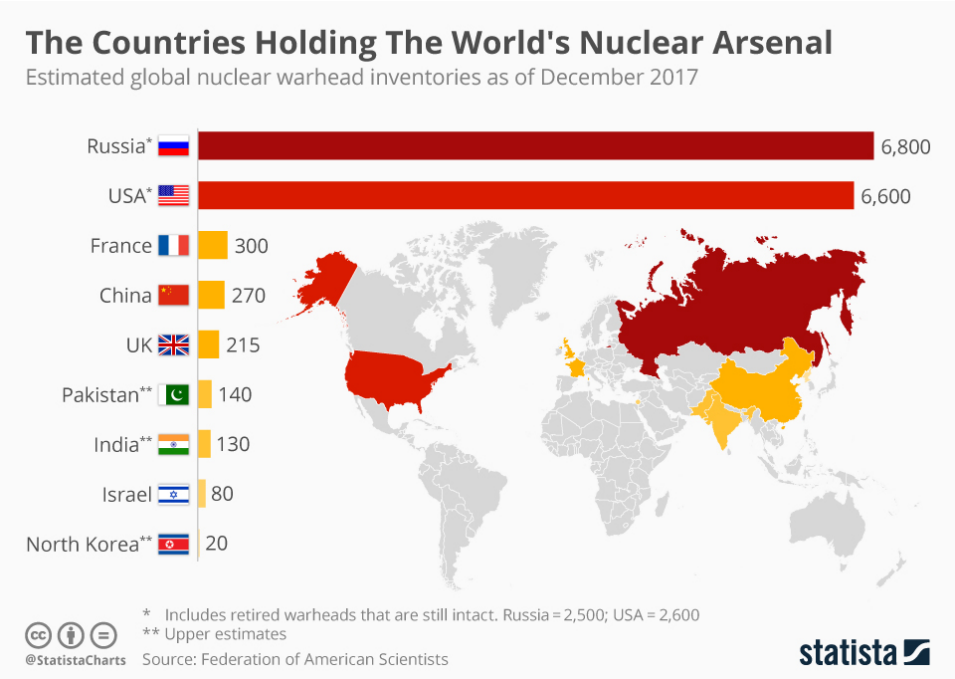
- Füzyon Silahları (atom bombası olarak da adlandırılır)

- Nükleer Silahlar ((HEU)-zenginleştirilmiş uranyum)

---

[50] UNODA, Nuclear Weapons: https://www.un.org/disarmament/wmd/nuclear/ (E.T: 12.03.18).
[51] Center for the Study of Technology and Society, Hiroshima and Nagasaki at Sixty, The New Atlantis, No. 9, 2005, p.139.
[52] CTBTO, General Overview of the effects of Nuclear Testing: https://www.ctbto.org/nuclear-testing/the-effects-of-nuclear-testing/general-overview-of-theeffects-of-nuclear-testing/ (E.T: 14.03.18).

Şekil 5: Küresel Nükleer Mühimmat İstatistiği



Kaynak: Armstrong, 2018.[53]

Dünyada toplam dokuz ülkede yaklaşık 15.000 nükleer silah bulunmaktadır. [54] ABD ve Rusya, herhangi bir uyarıdan sonra birkaç dakika içinde harekete geçmeye hazır nükleer silahlarının yaklaşık 1.800'ünü yüksek-uyarı statüsünde tutmaktadır ve çoğu 1945'te Japonya'ya atılan atom bombalarından çok daha güçlüdür. [55] Nükleer silahların askeri amaçla kullanımı sadece dünya üzerinde tahribata yol açmayıp, astronotların da maruz kalacağı doğal radyasyon tehlikelerine de sebep olmaktadır ve bu yüzden savaş zamanında var olabilecek insan kaynaklı tehlikelerin de göz önünde bulundurulması önem arz

[53] Armstrong, Martin, The Countries Holding The World's Nuclear Arsenal, Mar 2, 2018: https://www.statista.com/chart/8301/the-countries-holding-the-worlds-nuclear-arsenal/ (E.T: 14.03.18).

[54] Armstrong, a.e.
[55] ICAN, Nuclear Arsenals: http://www.icanw.org/the-facts/nuclear-arsenals/ (E.T: 14.03.18).

etmektedir. Özellikle, nükleer silahların kullanımı, askeri uzay operasyonlarında insanlar için ciddi bir sorun teşkil edebilme potansiyeline sahiptir. [56]

1.2.3.2. Nükleer Enerji Hakkında Güncel Tartışmalar

Nükleer enerji - 1950'ler ve 1960'larda ülkeler için bol miktarda enerji vaat etmekteydi. Ancak atık ve güvenlik konusundaki şüpheler 1970'lerde bu fikir akımını sona erdirmiştir. Three Mile Island ve Çernobil'deki kazalar hemen hemen tüm ülkelerde gelişmeyi durdurmuştur, ancak yeni reaktörler inşa etmek yerine, mevcut olanların güç kapasiteleri arttırılmış ve lisansları uzatılmıştır. Böylece yeni nesil reaktörler ortaya çıkmıştır. Son on yılda nükleer enerji, yeni nesil füzyon reaktörleri sayesinde (mevcut reaktör deneyimlerine dayanarak ve daha fazla otomatik güvenlik sistemi ekleyerek) yeniden ilgi odağı haline gelmiş[57] ve bu nedenle lehte ve aleyhte tartışmalar gündeme gelmiştir.

1.2.3.2.1. Lehte Tartışmalar

Nükleer enerjinin kullanımına dair lehte tartışmaların temel sebebi, önümüzdeki 50 yıl boyunca insanlık tarihin tamamının tükettiğinden daha fazla enerji tüketileceğinin öngörülmesidir. Bu nedenle, enerji tüketiminin artması ve yeni enerji teknolojilerinin gelişimi ile ilgili erken tahminler gerçekleşmiştir: [58] tüketim düzeyi çok daha hızlı büyürken, yeni enerji kaynakları 2030'dan daha geç olmamak üzere uygun fiyatlarla erişilebilir hale gelecektir. Böylelikle, Nükleer enerjinin daha cazip bir kaynak olacağı düşünülerek, lehteki temel görüşler arasında başlıca şu sebepler gelmektedir: [59]

---

[56] NASA: Nuclear Weapon Effects In Space: https://history.nasa.gov/conghand/nuclear.htm (E.T: 14.03.18).
[57] Grandin, Karl, et al., Nuclear Energy, Ambio, Vol. 39, Sup.1, 2010, p.26.
[58] Whitman, Christine Todd, The Case in Favor of Nuclear Power, Bloomberg Businessweek, 9.12.2007: http://www.nbcnews.com/id/20730356/ns/business-us_business/t/case-favor-nuclear-power/#.WwSRAEiFNPY (15.03.18).
[59] ROSATOM, Benefits of Nuclear Energy: http://www.rusatom-overseas.com/nuclear-energy/benefits-of-nuclear-energy/ (15.03.18).

- Büyük Enerji Kapasitesi

- Tekrar Kullanılabilirlik

- Sera Gazlarının Azaltılması

- Ekonomik gelişmeye katkısı

- Kuruluşta pahalı, işletmede ucuz

Nükleer uzmanlar, özellikle son yıllarda nükleer endüstrinin dünya çapındaki çöküşünün devam ettiğini ileri sürerek, bu olguyu anlamak ve algıları değiştirmek için çaba sarf etmişlerdir. Devam eden Post-Çernobil anti-nükleer iklimine rağmen, dünyada toplam çalışma reaktörü sayısı artmaya devam etmektedir. [60] Bu bilgiler dâhilinde, nükleer enerji hedeflerini etkileyen ilk faktör olarak elektrik talebinin büyüme oranı ile doğru orantılı olduğu gerçeğini unutmamak gerekmektedir. Özellikle Çin ekonomisi, başta ihracat sanayi üretimine odaklanmış bir ekonomi olmaktan çıkıp, hizmet sektörüne ve iç tüketime yönelmiş bir ekonomi olmak üzere, ülke ekonomisinde yapısal değişim gerçekleştirmeye başlatmıştır. Elektrik talebi de bu düzlemde şekillenerek 2002'den günümüze, Çin'in nükleer büyüme için kısa ve orta vadeli genişleme planı taslağı, 2020'de Çin'in 40 GW'lık nükleer kapasiteye erişmesini öngörmüştür. [61] Bu sebeplerden ötürü nükleer enerjiye karşı artan talepler, ülkelerin bu enerji kaynağını kullanmaları yönünde pozitif bir etki yaratmaktadır.

[60] Warwick, Joanna, Public Acceptance of Nuclear Energy in Canada, Energy Exploration & Exploitation, Vol. 8, No. 5, 1990, p. 339.

[61] Ramana, M. V., et al., A New Normal?: The Changing Future of Nuclear Energy in China, Learning from Fukushima: Nuclear Power in East Asia, edited by Peter Van Ness And Mel Gurtov, Anu Press, Australia, 2017, p. 104.

1.2.3.2.2. Aleyhte Tartışmalar

Nükleer enerjinin gerekliliğini savunan görüşler olsa da, bu enerjinin olumsuz sonuçlara yol açacağı endişesiyle nükleer enerjinin aleyhinde de görüşler mevcuttur. Nükleer enerji, küresel ısınmaya bir çözüm olarak alternatif gibi görünse de, birçok ülkede yıllar önce reddedilmesinin nedenleri arasında, nükleer atık imhası, reaktör kazaları, nükleer silahların yayılması, yüksek maliyet ve nükleer terörizm yer almaktadır. [62] Diğer enerji kaynakları ile kıyaslandığında, uzmanlar tarafından eleştiri odağı haline gelen nükleer enerjiyle ilgili diğer önemli unsur ise radyoaktivitedir. Radyasyonun insan sağlığı için yarattığı risk hakkında bir fikir edinmek için, niceliksel bir 'maruz kalma' ölçeğine ihtiyaç duyulmaktadır. Bunun sebebi ise, doğal radyasyon nedeniyle maruz kalınan dozun yılda 2,400 µSv olmasıdır. Öyle ki; tamamen göz ardı edilemeyen, doğal radyasyondan çok daha düşük olan insan kaynaklı tek kaynak, tıbbi tanıdır; yani, Xray ler (küresel ortalama yılda 400 µSv'dir, ancak zengin ülkelerde, gelişmiş tıbbi bakım ile kişi başına) ortalama yılda 1.200 µSv civarındadır). [63] Nükleer enerjiyle ilişkili tehlikeler, birçok yönden, diğer enerji elde etme yöntemlerinden karşı karşıya olduğumuz tehlikelerden farklıdır, çünkü enerji elde edilen enerji sürecinde ortaya çıkan radyoaktif atıklar ve salınımından doğan tehlike kansere yakalanma tehdidini de beraberinde getirmektedir. [64] Nükleer enerji üzerine çalışmaları olan bazı kurum/kuruluşlar ise nükleer enerjinin güvenli, temiz ve sürdürülebilir bir gelecekte yeri olmaması gerektiğini vurgulayarak, bu enerjinin hem pahalı hem de tehlikeli olduğunu ve nükleer kirliliğin görünmez olmasından dolayı temiz olduğu anlamına gelmeyeceğini yinelemektedirler[65].

---

[62] Martin, Brian, Opposing Nuclear Power: Past and Present, Social Alternatives, Vol. 26, No. 2, Second Quarter 2007, pp. 43-47.
[63] Cadenas, Juan José Gomez, The Nuclear Environmentalist: Is There a Green Road to Nuclear Energy?, Springer-Verlag Mailand, New York, 2012, p.106.
[64] Wilkerson, Jordan, Reconsidering the Risks of Nuclear Power, Harvard University Graduate School of Arts and Sciences, Blog, Specıal Edition: Dear Madam/Mister President, 2016: http://sitn.hms.harvard.edu/flash/2016/reconsidering-risks-nuclear-power/ (E.T: 15.03.18).
[65] GREENPEACE, Nuclear Energy: https://www.greenpeace.org/usa/global-warming/issues/nuclear/ (E.T: 15.03.18).

2. Nükleer Santraller

Enerji kaynağının yenilenebilir ve yenilenemez enerji olarak ikiye ayrılması ve nükleer enerjinin yenilenemez enerji kaynakları arasında olması bilgisi ışığında, bu bölüm başlığı altında ise nükleer santraller özelindeki başlıklar incelenecektir.

2.1. Nükleer Santrallerin Kurulma Amacı

Sistemli ve hızlı bir şekilde büyüyüp gelişen dünyada, enerji ihtiyaçları ülkelerin nüfusundan dahi daha hızlı büyüyerek, gelecek için öngörülen enerji gereksinimleri, elektrik enerjisi üretmek için atom enerjisi kullanmak zorunda olduğumuzu veya fosil yakıt kaynaklarımızın (kömür, petrol ve gaz) tükenmek üzere olduğunu açıkça göstermektedir. Bu durum ise, dünya medeniyetini ileriye taşıyan elektriği üretmek için nükleer enerjiyi kullanımını gerektirmektedir**.** [66] Nükleer santralleri vazgeçilmez yapan ve kurulma amaçlarının başında gelen 4 temel unsur yer almaktadır: [67]

- İlk olarak, nükleer santrallerin sicil kaydıdır. Dünya, şu anda 12.700 reaktör-yıllık tecrübeye sahiptir. Bugün işletilen tasarımların performans ve güvenlik kayıtları fonksiyonel olarak iyi durumdadır.

- İkincisi, enerji tahminleri kalıcı uzun vadeli büyüme göstermeye devam etmektedir.

- Üçüncü olarak enerji arz güvenliğidir. 1970'lerde petrol dalgalarının tetiklediği arz güvenliği endişeleri, hem Japonya'da hem de Fransa'da nükleer genişlemenin

[66] ERDA, Lyerly, Ray L./ Walter Mitchell, Nuclear Power Plants: https://www.osti.gov/includes/opennet/includes/Understanding%20the%20Atom/Nuclear%20Power%20Plants.pdf (E.T: 16.03.18).

[67] McDonald, Alan, Nuclear Power Global Status: A Look at Nuclear Power Generation Around The World and its Future Prospects, IAEA Bulletin Vol.49, Iss.2, March 2008, p.46.

başlıca nedenleri haline gelmiştir. Benzer kaygılar bugün de önemli bir faktör olabilmektedir.

- Dördüncü olarak, Çin ve Hindistan gibi kilit ülkelerdeki belirgin genişleme planlarının genel küresel beklentiler üzerinde büyük etkisi bulunmaktadır.

2.2. Türkiye'de ve Dünyada Nükleer Santraller

Enerji, gelişmiş ve gelişmekte olan bütün ülkelerde ekonomik faaliyetlerin önde gelen koşuludur. [68] Hâlihazırda Türkiye'de nükleer santral bulunmamaktadır ancak "3 Nisan 2018 tarihinde Mersin'in Gülnar ilçesinde bulunan Akkuyu Nükleer Güç Santrali'nin sahasında temel atma töreni düzenlendi. Bu tören, Rosatom Devlet Kuruluşu tarafından inşa edilecek ilk Türk nükleer güç santralinin yapımına yönelik kapsamlı çalışmaların başlanması anlamına gelmektedir.[69]" Bununla birlikte, Türkiye nükleer enerji programına başlamayı düşünerek nükleer reaktör dâhil olmak üzere Akkuyu dışında 2 nükleer santral daha kurmayı planlamaktadır. "Türkiye'nin yarım asırlık nükleer güç santrali kurma ideali, T.C. Hükümeti ile Rusya Federasyonu Arasında Akkuyu Sahasında Bir Nükleer Güç Santralinin Tesisine ve İşletimine Dair İşbirliğine İlişkin Anlaşma'nın 12 Mayıs 2010 tarihinde imzalanmasıyla gerçekleşmeye başlamıştır. Söz konusu Anlaşma, 15 Temmuz 2010 tarihinde TBMM Genel Kurulu tarafından kabul edilmiş, 6 Ekim 2010 tarihli ve 27721 sayılı Resmi Gazetede yayımlanmıştır. Adı geçen Anlaşmanın gerçekleştirilmesi kapsamında Proje Şirketi, 13 Aralık 2010 tarihinde Ankara'da Akkuyu NGS Elektrik Üretim A.Ş.

[68] Temurçin, Kadir/Alpaslan Aliağaoğlu, Nükleer Enerji ve Tartışmalar Işığında Türkiye'de Nükleer Enerji Gerçeği, Coğrafi Bilimler Dergisi, Cilt.1, Sayı.2, 2003, s.25.

[69] AKKUYU NÜKLEER, Akkuyu Nükleer Güç Santrali'nin Temeli Rusya Federasyonu Devlet Başkanı ve Türkiye Cumhuriyeti Cumhurbaşkanı'nın Katıldığı Törenle Atıldı, 03.04.2018 : http://www.akkunpp.com/akkuyu-nukleer-guc-santralinin-temeli-rusya-federasyonu-devlet-baskani-ve-turkiye-cumhuriyeti-cumhurbaskaninin-tatildigi-torenle-atildi/update (16.04.18).

adı ile kurulmuştur." [70] Türkiye enerji politikası, enerji arzının güvenirliliği konusunda güvenilir, yeterli ve zamanında bir şekilde yoğunlaşmıştır. Bu, ekonomik ve temiz şartlarda ve hedeflenen büyüme ve sosyal gelişmeyi destekleyecek ve yönlendirecek şekilde elde edilecektir. Bu nihai hedefe paralel olarak, Türkiye'nin enerji politikası aşağıdaki ana sütunlara sahiptir: [71]

- Artan talep ve ithalat bağımlılığı ile baş edebilmek için enerji güvenliği ile ilgili faaliyetlerin önceliklendirilmesi;

- Sürdürülebilir kalkınma çerçevesinde enerji zincirinin tüm aşamalarında çevresel kaygıları dikkate almak;

- Enerji sektöründeki reform ve serbestleştirme faaliyetlerini kolaylaştırmak, böylece genel üretkenliği ve verimliliği arttırmak ve rekabetçi bir çerçeve oluşturarak şeffaflığı arttırmak;

-Ar-Ge çalışmaları ve faaliyetleriyle ilgili enerji teknolojilerini yoğunlaştırmak;

-"Doğu-Batı" ve "Kuzey-Güney" Enerji Koridorları ve Terminallerinin tanınmasıyla hidrokarbonların taşınmasına ilişkin projelerin gerçekleştirilmesidir.

[70] T.C. Enerji ve Tabii Kaynaklar Bakanlığı, Türkiye'nin Nükleer Santral Projeleri: Soru-Cevap Nükleer Enerji Proje Uygulama Dairesi Yayın Serisi, 11 Ocak 2016, Yayın No. 1, s.24. : http://www.enerji.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FT%C3%BCrkiyenin_N%C3%BCkleer_Santral_Projeleri_Soru-Cevap.pdf (E.T: 10.03.18).

[71] IAEA, Country Nuclear Power Profiles: Turkey, 2017: https://cnpp.iaea.org/countryprofiles/Turkey/Turkey.htm (E.T: 16.03.18).

Tablo 2: Dünya Nükleer Enerji Üretimi ve Nükleer Santral Kapasitesi

ÜLKELER	NİSAN 2017 İTİBARİYLE			
	NUKLEER UNITE ADEDİ	NUKLEER KAPASİTE (MW)	NUKLEER ÜRETİMİ (GWH)	NUKLEER YAKIT PAYI (%)
Arjantin	3	1,632	7,677.4	5.6
Ermenistan	1	375	2,194.9	31.4
Belçika	7	5,913	41,430.5	51.7
Brezilya	2	1,884	14,970.5	2.9
Bulgaristan	2	1,926	15,083.5	35.0
Kanada	19	13,554	95,650.2	15.6
Çin	36	31,384	197,829.0	3.6
Çek Cumhuriyeti	6	3,930	22,729.9	29.4
Finlandiya	4	2,764	22,280.1	33.7
Fransa	58	63,130	386,452.9	72.3
Almanya	8	10,799	80,069.6	13.1
Macaristan	4	1,889	15,183.0	51.3
Hindistan	22	6,240	35,006.8	3.4
İran İslam Cumhuriyeti	1	915	5,924.0	2.1
Japonya	43	40,290	17,537.1	2.2
Kore Cumhuriyeti	25	23,077	154,306.7	30.3
Meksika	2	1,552	10,272.3	6.2
Hollanda	1	482	3,749.8	3.4
Pakistan	4	1,005	5,438.9	4.4
Romanya	2	1,300	10,388.2	17.1
Rusya	37	26,528	184,054.1	17.1
Slovakya	4	1,814	13,733.4	54.1
Slovenya	1	688	5,431.3	35.2
Kuzey Afrika	2	1,860	15,209.5	6.6
İspanya	7	7,121	56,102.4	21.4
İsveç	10	9,740	60,647.4	40.0
İsviçre	5	3,333	20,303.1	34.4
Tayvan, Çin	6	5,052	30,461.0	13.7
İngiltere	15	8,918	65,149.0	20.4
A.B.D*	99	99,319	805,327.2	19.7
Ukrayna	15	13,107	76,077.8	52.3
Toplam	451	391,521	2,476,671.2	

Kaynak: Uluslararası Atom Enerjisi Ajansı, 2017.[72]

Uluslararası Atom Enerjisi Ajansına göre, dünya nükleer güç kapasitesinde 2016 yılı seviyelerinden, 2030' da % 42, 2040' da % 83 ve 2050' de % 123 oranında artış meydana gelecektir. Düşük durumda, % 12'lik bir kapasite düşüşüne neden olmuştur. Nükleer enerjiye sahip olmak isteyen 28 ülke vardır. Hâlihazırda nükleer santrallerin işletildiği 31 ülkeden 13'ü ya yenilerini inşa etmekte ya da daha önce askıya alınmış inşaat projelerini hızlı bir şekilde

[72] IAEA: https://www.iaea.org/newscenter/news/iaea-releases-projections-on-global-nuclear-power-capacity-through-2050 (E.T: 16.03.18).

tamamlamakta ve 16 yeni reaktör inşa etmek için plan ya da önerileri mevcuttur. [73]

2.3. Önemli Nükleer Santral Kazaları

Nükleer santrallerin işletim esnasında büyük hasarlara neden olan kazalar meydana gelmiştir. Bunların bir kısmı güvenlik zafiyetinden kaynaklanırken bir kısmı da nükleer santrallerin hassas yapıda olmasından dolayı karşılaşılabilecek ufak bir doğal afetten etkilenerek gerçekleşmektedir. Yakın zamanda bahsi geçen sebeplere emsal teşkil edebilecek üç önemli kaza, kazaların bilançosunu özetlemektedir.

2.3.1. Three Mile Adası Kazası

Three Mile Island nükleer santrali, eyalet başkenti Harrisburg'a yaklaşık 15 km mesafede, Pennsylvania, ABD'deki Susquehanna Nehri'ndeki bir adada bulunmaktadır. Ünite 2 (TMI 2), 2700 MW'lık nominal termik çıkış gücüne sahip basınçlı bir su reaktörüdür. Reaktör, büyük bir kuru beton takviyeli muhafaza ile çevrilidir. TMI-2 oldukça yeni durumda idi ve kaza 28 Mart 1979'da gerçekleştiğinde henüz 1 yıldan beri faaliyet göstermekteydi. [74] Kazanın ortaya çıkış aşaması olarak, santralin nükleer olmayan ikinci bölümünde (sahadaki iki reaktörden biri) 28 Mart 1979 Çarşamba günü sabah saat 4'te meydana gelen bir arıza ile başlamıştır. Muhtemel mekanik ya da elektrik arızası, ana su besleme pompalarından çıkan suyun jeneratörlere aktarılmasını engellemiştir. Bu, santralin türbin-jeneratörüne ve daha sonra reaktörün kendiliğinden kapanmasına neden olmuştur. Birincil sistemdeki basınç (santralin nükleer kısmı) aniden artmaya başlayarak bu basıncı kontrol etmek üzere otomatik tahliye vanası

[73] IAEA, International Status and Prospects for Nuclear Power 2017, Official Report, 2017, p.1: https://www.iaea.org/About/Policy/GC/GC61/GC61InfDocuments/English/gc61inf-8_en.pdf (18.03.18).

[74] Högberg, Lars., Root Causes and Impacts of Severe Accidents at Large Nuclear Power Plants, Ambio, Springer on behalf of Royal Swedish Academy of Sciences, Vol. 42, No. 3, 2013, p. 269.

(basınçlandırıcının üstünde bulunan bir valf) açmıştır. Basınç uygun seviyelere düştüğünde vananın kapanmış olmaması gerekirken açık kalmıştır. Kontrol odasındaki aletler, fabrika personeline valfin kapalı olduğunu belirtmiştir. Sonuç olarak, tesis personeli, soğutma suyunun, takılıp-açılan vananın dışına dökülmesinden habersizdi ve bu yüzden ihmal kaynaklı facia meydana gelmiştir. [75] Bu gelişmeyle birlikte Federal hükümet 1979 'da Pennsylvania'da bulunan bu reaktörün kısmen erimesi ve küçük miktarlarda radyoaktif malzeme salınması sonucu Three Miles Adası kazasının yaşanmasını gerekçe göstererek mevzuat ve politika düzenlemelerinde daha katı bir tutum sergilemiştir ve bu gelişme de nükleer santraller üzerindeki çalışmaları yavaşlatmıştır. [76]

2.3.2. Çernobil Kazası

26 Nisan 1986'da, Rusya da Çernobil mevkiinde nükleer kaza meydana gelmiştir. [77] Çernobil, Nükleer Santral Ünitesi 4'ün patlaması sonrasında dönemin Sovyet hükümeti, hasarlı reaktörden kaynaklanan kirlilik derecesini belirleyen önemli pratik zorluklarla karşı karşıya kalmıştır. Bu zorluklar, yalnızca (ve kazadan sonraki haftalarda kayda değer kalan) salınımların karmaşık ve dinamik doğasından değil, aynı zamanda teknolojik ve kurumsal sınırlamalardan kaynaklanmıştır. [78] Olay zincirleme şeklinde gerçekleşmiştir. Çernobil'deki Nükleer santralde öncelikle 4. Ünite patlamıştır. Daha sonra enkaz havaya karışarak patlayan Ünite 4'ün hemen yanında yer alan Ünite 3'ün çatısı üzerine düşmüştür. Üniteler, ortak bir makine türbini salonunu, bitümlü bir çatı ile ve yanıcı bir malzeme ile paylaşılmaktaydı. Otuz bir zincirleme vaka meydana

[75] USNRC, Backgrounder on the Three Mile Island Accident, 2013: https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html (E.T: 16.03.18).
[76] Peterson, Per F., et al., Nuclear Freeze: Why Nuclear Power Stalled—and How to Restart It, Foreign Affairs, Vol. 93, No. 3, 2014, p.28.
[77] Baverstock, Keith. "Chernobyl 25 Years on: Lessons Have Not Been Learnt and the Full Public Health Implications Are Unknown." BMJ: British Medical Journal, vol. 342, no. 7804, 2011, p.936.
[78] Dion-Schwarz, Cynthia, et al., Earlier Lessons from the Chernobyl Experience, Technological Lessons from the Fukushima Dai-Ichi Accident, RAND Corporation, Santa Monica, Calif., 2016, p. 45.

gelmiştir. Kazanın gece meydana gelmesi büyük bir şans olmuştur, çünkü gündüz Çernobil 5. ve 6. Ünitesi yapımında 2000 kişi çalışmaktaydı. Bu yüzden zarar görmemişlerdir. [79] Çernobil kompleksi kazadan hemen sonra kapatılmış ve yeniden yerleşim süreci tamamlanmıştır. [80] Ordu, elektrik santrali personeli, yerel polis ve itfaiye hizmetlerinden yaklaşık 350 bin temizlik işçisi veya "tasfiye memuru", 1986-1987 yıllarında radyoaktif döküntülerin toplanması ve temizlenmesi ile ilgili olarak çalışmaya başlamıştır. Yaklaşık 240.000 tasfiyeci, reaktörün etrafındaki 30 km'lik alanda atık temizleme faaliyetleri yürütürken en yüksek radyasyon dozlarına maruz kalmıştır. [81] Bu faciadan sonra hem üst düzey hükümet yöneticileri hem de Sovyet halkı nükleer santraller aleyhinde bir görüş ortaya atarak nükleer santrallerin tamamen yok edilmesini talep etmişlerdir. [82]

2.3.3. Fukuşima Kazası

Fukuşima nükleer santral kazası meydana geliş açısından diğer kazalardan faklıdır ve etkileri de aynı sonuçları da endişe verici düzeyde olmuştur. [83] Pasifik Okyanusu depremi ve Tohoku Bölgesi ile Fukushima Daiichi ve Daini nükleer enerji santrallerini 11 Mart 2011'de 14.46'da (3/11) vuran tsunamilerden sonra, yüksek tahribatla bir nükleer kaza izlemiştir. O zamandan beri, tüm nükleer uzmanların sadece Japonya'da değil, dünyanın geri kalanında da hatırlanması için tarihi bir gün haline gelmiştir. Deprem 2011 yılında gerçekleşmesine rağmen, kazanın etkileri devam etmektedir. Fukushima'da yaklaşık 100,000 kişi tahliye

[79] WISE, Chernobyl: Chronology of a Disaster, No.724, March 11, 2011, p.4: https://www.wiseinternational.org/nuclear-monitor/chernobyl-chronology-disaster (19.03.18).
[80] UN, The Human Consequences of the Chernobyl Nuclear Accident: A Strategy for Recovery, A Report Commissioned by UNDP and UNICEF with the support of UN-OCHA and WHO, 2002, p.14.
[81] WHO, Health effects of the Chernobyl Accident: An Overview, 2006: http://www.who.int/ionizing_radiation/chernobyl/backgrounder/en/ (E.T: 16.03.18).
[82] CIA, The Chernobyl' Accident: Social and Political Implications, A Research Paper, Raport No: CIA-RDP08S01350R000300900002-4, 2012, p.5: https://www.cia.gov/library/readingroom/docs/CIA-RDP08S01350R000300900002-4.pdf (E.T: 16.03.18).
[83] Miwao Matsumoto., 'Structural Disaster' Long Before Fukushima: A Hidden Accident, Development and Society, Vol. 42, No. 2, 2013, p.166.

edilmiştir ve bu kişiler hala geçici konutta yaşamaktadır. Fukushima enerji santrallerindeki koşullar iyileşmiş olsa da, erimiş yakıt kalıntılarını alandan uzaklaştırmanın 40 yıldan uzun süreceği ön görülmektedir. [84] Bununla birlikte, doğal afetlerden gelen tahribat üst düzeye çıkmıştır. Ulusal polis teşkilatından elde edilen rakamlara göre19.000 insan hayatını kaybetmiştir. Dünya Bankası, deprem ve Tsunaminin ekonomik maliyetinin 235 milyar doların üzerinde olduğunu tahmin ederek, insanlık tarihinin en pahalı doğal felaketi olduğunu belirtmiştir. [85] Felaketin ardından, Japonya Başbakanı Naoto Kan, "II. Dünya Savaşı'nın bitiminden 65 yıl sonra, bu, Japonya için en zor ve en zor krizdir" şeklinde demeç vermiştir. [86] Bu olaydan sonra, dünyanın eksenin 25 cm kadar kaydığı tahmin edilmektedir ve kuzeydoğu Japonya'nın bazı kısımları Kuzey Amerika'ya 7 metreye kadar yükselmiştir. Ne yazık ki, yıkımın bedeli ve kapsamı, depremden kaynaklanan doğal tahribat ve sonuçta meydana gelen Tsunami ile sınırlı değildir. [87] Buna ek olarak, Mart 2011'de Fukushima olayından sonra, nükleer enerjiye yönelik ciddi bir yeniden gözden geçirme süreci başlamıştır ve nükleer enerjiye sahip olmayan yeni bir yol, hem Japonya'da hem de dünyanın birçok yerinde hayati bir olgu haline gelmiştir. [88] Alınan önlenlerin ise nükleer santrallerin güvenliğine dair hukuki çerçevelere sadık kalmak, kurucu işletmelere karşı sorumluluğa ilişkin Paris ve Viyana Sözleşmelerinde de belirtildiği üzere daha katı hükümler getirmek olmuştur. Yaşanan kazalardan sonra ise genel olarak nükleer enerji kullanımına yönelim olarak bu kazalardan sonra düşüş yaşanmıştır.

---

[84] Suzuki, Tatsujiro, et al., Nuclear Energy Policy Issues in Japan after the Fukushima Nuclear Accident, Learning from Fukushima: Nuclear Power in East Asia, edited by Peter Van Ness and Mel Gurtov, Anu Press, Australia, 2017, p.10.

[85] THE WORLD BANK: https://elibrary.worldbank.org/doi/10.1596/978-1-4648-0153-2_ch36 (E.T:17.03.18).

[86] Kan, Naoto, Statement by Prime Minister Naoto Kan upon the General Resignation of the Kan Cabinet: https://japan.kantei.go.jp/kan/statement/201108/30danwa_e.html (E.T: 17.03.18).

[87] Sanchez, Victoria Justine, Radioactive Reversal?: The Fukushima Accident As A Focusing Event For Comparative Policy Change on Nuclear Energy, University of Delaware, Yayınlanmamış Doktora Tezi, 2017, s.4.

[88] Kano, Chizu., Behavioral Change for Energy Conservation : Case Study of Post-Fukushima Experience İn Japan, Uppsala University, Yayınlanmamış Doktora Tezi , 2013, s.1.

3. Nükleer Terörizm

Nükleer santrallere yönelik olaylar sadece doğal afet ya da kaza nedeniyle meydana gelmemektedir. Nükleer santrallere yönelik terörizm faaliyetleri çerçevesinde de süreci değerlendirmek gerekmektedir. Bu bağlamda, bu başlık altında nükleer terörizm ve gelişim aşamaları incelenecektir.

3.1. Nükleer Terörizm Kavramı ve Tarihi

Nükleer terörizm kavramını Uluslararası Atom Enerjisi Ajansı "'Hırsızlık, sabotaj, yetkisiz erişim, yasadışı transfer veya nükleer malzeme, diğer radyoaktif maddeler veya bunların bağlantılı tesislerini içeren diğer kötü niyetli eylemler" olarak tanımlamaktadır. [89] 21.yy ile dünya yeni bir nükleer çağa girmiş bulunmaktadır. Dünya çapında büyük çaplı nükleer savaş riski azalıyor gibi gözükse de, bölgesel istikrarsızlık, silahların çoğalması ve bu silahları ortaya çıkaran tehditlerle birlikte, tek bir nükleer silah veya aygıtın patlaması riski endişelere yol açmaktadır. [90] Nükleer silahlara sahip teröristlerin beklentileri konusundaki tartışma, 1970'lere kadar uzanmaktadır ve o zamandan günümüze kadar aynı doğrultuda devam etmiştir. [91] Tartışmanın yeniden canlandırılması 1990'ların ortasından itibaren Dünya Ticaret Merkezi'nin 1993 yılında meydana gelen terörist bombalamaları, 1995'deki Oklahoma Şehri federal binası ve aynı yıl Tokyo'da yer alan sârin gazı saldırısının ardından gerçekleşmiştir. [92] ABD'nin 44. Başkanı Barack Obama da nükleer terörizm tehdidini şu şekilde açıklamıştır:

[89] IAEA, Concept and Terms: IAEA Safety Standards: http://www-ns.iaea.org/standards/concepts-terms.asp (E.T: 18.03.18).
[90] NTI, Global Nuclear Policy: http://www.nti.org/about/global-nuclear-policy/ (E.T: 18.03.18).
[91] Reed, Samuel Thomas, The Nuclear Terrorism Disconnect: Electoral Incentives And U.S. Policy Responses, University of British Columbia, Yayınlanmamış Yüksek Lisans Tezi, 2013, s.18.
[92] Richard A. Falkenrath, Robert D. Newman, and Bradley Thayer America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack, Cambridge Mass. , MIT Press, 1998, (Önsöz).

"ABD'nin güvenliği için en büyük tehdit, yakın, orta ve uzun vadede nükleer silah elde eden bir terör örgütü olasılığı olabilir … " [93] Bu gelişmelerle birlikte uluslararası nükleer terörizm endişesi 11 Eylül 2001'den bu yana istikrarlı bir şekilde artmış ve bu durumun engellenmesi için çok taraflı işbirliğini geliştirmek için özel ya da kısmen bir dizi resmi ve gayri resmi politika girişimi tasarlamıştır. Temel örnekler arasında Nükleer Terörle Mücadele Küresel Girişimi (GICNT), Silahların ve Kitle İmha Malzemelerinin yayılmasına karşı G8 Küresel Ortaklığı (GP), 1373 ve 1540 No'lu BM Güvenlik Konseyi Kararları (UNSCR) ve UAEA Nükleer Güvenlik'le alakalı resmi bir birimin kurulması yer almaktadır. Siyasi açıdan en dikkate değer girişimler, Nisan 2010'da Başkan Barack Obama'nın Nükleer Güvenlik Zirvesi'nin (NSS) nükleer terör tehdidiyle ilgili uluslararası farkındalığı artırdığı ve bu alandaki önleyici çabaları güçlendirmeyi amaçladığı çaba olmuştur. [94] Bu gelişmelere paralel olarak "nükleer enerjinin yayılması" ifadesi sıklıkla kullanılsa da, günümüzde nükleer enerjiye sahip olan devletlerde nükleer enerjinin yaygınlaşması ile nükleer enerjinin yeni ülkelere yayılma potansiyelini birbirinden ayırmak gerekmektedir. [95] Nükleer enerji barışçıl amaçlarla kullanıyor olsa da teröristlerin elinde yıkıcı etkisi olan bir silaha dönüşebilmektedir. Teknolojin ivme kat etmesiyle birlikte nükleer terörizmin uygulanması da çeşitlilik göstermektedir. Bu yüzden nükleer terörizmin kullanacağı birden çok metot vardır. [96] Bu endişeleri gidermek adına çeşitli düzenlemeler sistemli bir şekilde yapılmaktadır ve 2016 nükleer güvenlik zirvesi, dünyanın dört bir yanındaki nükleer malzemeyi güvence altına almak için uzun yıllar boyunca çaba göstermesi açısından önemli bir an olmuştur çünkü nükleer hırsızlık riskini azaltmak için önlemleri güçlendirmede önemli ilerlemelere yol

[93] BBC, US President Barack Obama Warns of Nuclear Terrorism, 12 April 2010: http://news.bbc.co.uk/2/hi/middle_east/8614695.stm (E.T: 18.03.18).
[94] Bowen, WYN Q., et al., Multilateral Cooperation and the Prevention of Nuclear Terrorism: Pragmatism over Idealism, International Affairs (Royal Institute of International Affairs 1944-), Vol. 88, No. 2, 2012, p.349.
[95] Sagan, Scott D., The Global Nuclear Future, Bulletin of the American Academy of Arts and Sciences, Vol. 63, No. 2, 2010, p. 38.
[96] Volders, Brecht, Nuclear Terrorism: What Can We Learn from Los Alamos?, Terrorism and Political Violence, 2017, p.3.

açan dört bienal toplantısının sonuncusu için 50' den fazla ulusal lider Washington'da bir araya gelmiştir. [97]

Uluslararası toplumların nükleer terörizm noktasında kaygılarını arttıran diğer husus ise diğer devletler tarafından nükleer silahların geliştirilmesini desteklemek için hassas nükleer metalarda (yani ekipman ve teknoloji) teröristlerin ve kaçakçılığın nükleer bir saldırıya yol açabileceği kullanılabilir silah materyallerin kaçakçılığıdır. [98] Bu yüzden son derece önemli olan bu konu hakkında, nükleer silahların yayılması ve tüm ulusların karşı karşıya kaldığı nükleer terörizm tehdidi göz önüne alındığında, hiçbir şey yapmamak sorumluluk sahibi olan milletler için bir seçenek değildir. [99]

3.2. Nükleer Terörizm Çeşitleri

Dünyanın herhangi bir yerinde nükleer terörizm eyleminin felaket getiren sonuçlara yol açacağı gerçeğini reddeden biriyle karşılaşmak mümkün gözükmemektedir. [100] 2005 tarihli Terörizmin Eylemlerin Önlenmesine Dair Uluslararası Sözleşme (ICSANT) Uluslararası Konvansiyonu'nun önsözünde de belirtildiği üzere, "nükleer terör eylemleri, ciddi sonuçların ortaya çıkmasına neden olabilir ve uluslararası barış ve güvenlik için bir tehdit oluşturabilir". [101] Nükleer terörizm çeşitleri, meydana geliş şekillerine göre değişebilmektedir. En yaygın şekilleri olarak nükleer terörizm çeşitli şekillerde kendini

[97] Malin, Martin B., and Nickolas Roth., A New Era for Nuclear Security, Arms Control Today, Vol. 46, No. 5, 2016, p. 8.
[98] Leonard S. Spector., Nuclear Material and Commodity Trafficking as International Crimes: Current Status, Gaps in Coverage, and Potential Steps Forward, Proceedings of the Annual Meeting (American Society of International Law), Vol. 105, 2011, p.133.
[99] Kimball, Daryl G., FOCUS: Eliminate NATO's Nuclear Relics, Arms Control Today, Vol. 40, No. 2, 2010, p.4.
[100] Salik, Naeem, Nuclear Terrorism: Assessing the Danger, Strategic Analysis, Vol.38, No.2, 2014, p.182.
[101] UN, International Convention on Suppression of Acts of Nuclear Terrorism, 2005: http://www.un-documents.net/icsant.htm (E.T: 18.03.18).

gösterebilmektedir: nükleer patlama, radyoaktif radyasyon yayma ve radyoaktif materyallerin yayılması. [102]

A. Nükleer Patlama: Nükleer terörizmin bu biçimi, can kayıplarının sayısı, devasa tahribat, insan sağlığına etkisi ve çevre üzerindeki ölümcül uzun vadeli etkileri bakımından en büyüğüdür. Belirlenen terörist gruplar, herhangi bir nükleer bombayı şu şekilde muhtemel yollardan alabilir ve patlatabilirler: [103]

1- Siyasi olarak istikrarsız olan eyalet/şehirlerde hırsızlık, yanıltma veya nükleer aygıtların ele geçirilmesi yoluyla bir bombanın ele geçirilmesi,

2- Destek veren bir devletten bomba alınması,

3- Destekleyici bir devletten ya da nükleer bir cihaza erişimi olan bireylerden bomba satın almak ve

4- Bölünebilir malzemeler elde etmek ve doğaçlama bir nükleer cihazı patlatmaktır.

B. Radyoaktif Radyasyon Yayma: Bu durum, nükleer güç santrallerine zarar vererek ve böylece Çernobil ve Fukuşima' da kazalarında yaşanan benzer etkilere sahip geniş bir radyoaktif madde yayılımı sağlayarak önemli ölçüde gerçekleştirilebilmektedir. Radyasyonun kasıtlı salınması birkaç yolla gerçekleşebilir: 1-Güç istasyonunun nükleer çekirdeğine uçakla saldırmak, 2-Stand-Off füze saldırısı, 3-Komando tipi teröristlerin güç istasyonuna nüfuz ederek nükleer çekirdeği imha etmesi, 4-Terör örgütü tarafından görevlendirilen kişilerin sabotajı ve 5-Kontrol sistemlerini devralarak ve nükleer yakıtın erimesi için gerekli koşulları yaratarak uzaktan siber terörizmden yararlanmaktır. Önemli miktarda radyasyon salabilecek diğer tesisler, harcanan yakıt depolama tesisleri,

[102] Dickstein, Phineas/ Sarah Vanunu, Nuclear Terror: The Essentials, Threats, Effects and Resilience, International Institute for Counter- Terrorism, 2016, p.4.
[103] Dickstein, a.g.e, s.9.

yeniden işleme tesisleri ve yüksek seviyeli radyoaktif atık depolama alanlarıdır. [104]

C. Radyoaktif materyallerin yayılması: Bu nükleer terörizm araçları çeşitli yollarla gerçekleştirilebilmektedir: 1- Kirli Bomba[105] 'Dirty-Bomb' - Geleneksel bir TNT bombasının radyoaktif materyalleri harekete geçirmesidir. Bomba patlatılırken, radyoaktif partiküllerin ve aerosollerin yayılması ile birlikte geleneksel patlayıcı etkisine sahiptir. "Kirli bomba" olarak adlandırılan bu aygıt, kitlesel bir yıkım silahı olarak değil de, duyarlı olmayan radyasyondan gelen insanlara uygulanan korku nedeniyle bir "kitle parçalama silahı" olarak görülmektedir. 2-Tıbbi teşhis, medikal tedaviler ve endüstriyel radyografi gibi radyoaktif materyallerin yayılması, insanları radyasyona maruz bırakacak ve radyasyon hastalığının oluşmasına neden olacaktır. Kirlenmiş olabilecek nispeten geniş bir alan boşaltılmalı ve temizlik prosedürlerine tabi tutulmalıdır. Bölgenin önemli bir süre kapanması ekonomik, ekolojik ve karmaşık sosyo-psikolojik etkileri beraberinde getirmektedir. 3-Radyoaktif kaynakların gıda ve su kaynaklarına sokulması veya insanların radyasyona maruz kaldığı bir alanda nükleer radyasyon kaynağının gizlenmesi yoluyla yerel radyoaktif zehirlenme şeklinde de olabilmektedir. [106] Bu düzlemde, nükleer terörün temelleri de çeşitlilik göstermektedir. Aşağıdaki bahsi geçen tabloda çeşitleri ve nedenleri de birlikte verilmiştir.

---

[104] Richelson, Jeffrey T., Nuclear Terrorism: How Big a Threat?, The National Security Archive, the George Washington University, National Security Archive Electronic Briefing Book No. 388, 2012.

[105] Radyoaktif maddelerin geniş bir alana yayılması için tasarlanmış olan, konvansiyonel patlayıcılarla harekete geçirilen silahlardır. Bkz: https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/dirty-bomb (E.T: 18.03.18).

[106] FAS, Nuclear & Radiological Terrorism: https://fas.org/issues/nuclear-and-radiological-terrorism/ (E.T: 18.03.18).

Tablo 3: Nükleer Terörün Temelleri

Tedarik	Talep
Kapasite • Nükleer ya da RDD (Radyolojik Yayılma Cihazı) • Uzmanlık	**Niyet** • Etki • Gerekçe
Bomba Üretme • Malzeme • Tasarım • İnşaat • Teslim	**Saldırı Planlama** • Hedef Seçimi • Gözetim • Lojistik • Uygulama
NÜKLEER SİLAH	**TERÖRİZM**

Kaynak: Uluslararası Atom Enerjisi Kurumu, 2009, s.5.[107]

Nükleer terörizm ile ilgili bilinmesi gereken bir diğer husus ise siber saldırılarıdır. Son 20 yılda bilişim teknolojisi büyük ölçüde gelişmiştir. Teknoloji ofis işlemlerini optimize etmeye yardımcı olmak için bir yönetim olgusundan çıkıp, endüstri, yönetim ve ordu için stratejik bir araç haline gelmiştir. 11 Eylül'den önce siber uzay riskleri ve güvenlik sorunları sadece küçük teknik uzman grupları içinde tartışılmaktaydı. Ancak, o günlerden itibaren, siber dünyanın giderek daha fazla birbirine bağımlı olan toplumlar için ciddi savunma zafiyeti yarattığı ortaya çıkmıştır. [108] Özellikle nükleer santrallere ait olan kritik altyapının bir kısmı, internet veya herhangi bir ağdan güvenlik önlemlerinin bir parçası olarak kesilebilir ve bu sistemler çok iyi bir siber saldırı ile imha edilerek

[107] Larssen, Rolf Mowatt, The Growing Threat of Nuclear Terrorism, IAEA Conference, 2009, p.5.
[108] NATO Review Magazine, New Threats: The Cyber-Dimension: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm (E.T: 18.03.18).

nükleer patlama meydana getirilebilmektedir. [109] Nükleer tesislerde sabotaj da dâhil olmak üzere, siber saldırı altındaki enerji sektörü gibi diğer yollarla da nükleer güvenlik tehlikeye girebilmektedir. Ayrıca, nükleer terörizmle ilgili tehditler aynı zamanda, nükleer tesisler hakkında içeriden bilgi sahibi teröristlere yıkıcı siber saldırıları başlatabilen sofistike ve iyi niyetli terör örgütleri, nükleer kaçakçılar veya hackerler gibi birçok kaynaktan gelmektedir. Tüm bu zorluklar, bu tehditlerin tesis operatörleri, nükleer düzenleyici kurumlar ve acil durum planlaması ve müdahaleden sorumlu kuruluşlar tarafından nasıl yönetildiğini etkilemektedir. [110]

3.3. Nükleer Terörizm Senaryoları

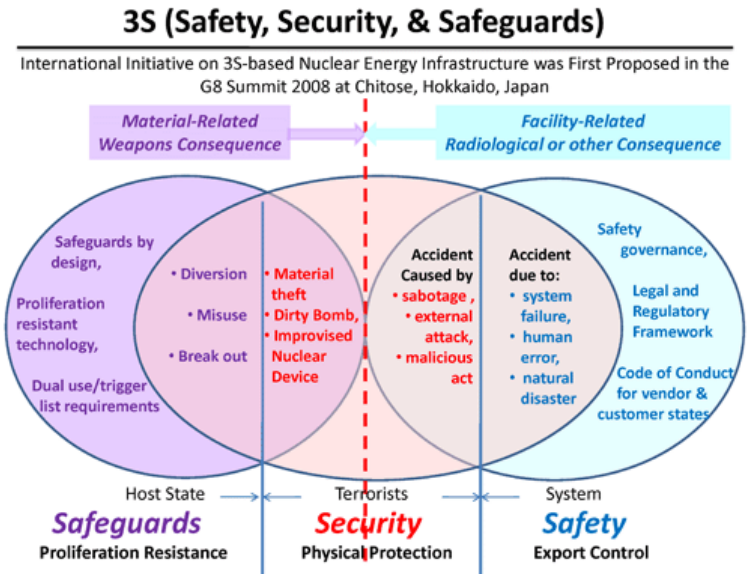
Son yıllarda, nükleer maddelerin, kimyasal ve biyolojik etmenlerin kaçakçılığı ve işlenmesi bağlamında bazı terör örgütlerinin bu konularda aktif olduğu gözlemlenmiştir. Nükleer terörizm tehdidi, karaborsadan nükleer silahlar tedarik eden veya savunmasız nükleer tesislerden uranyum çalan ve doğaçlama bir nükleer aygıtı kendi başlarına inşa eden terör örgütleri yoluyla olabilirken, terör örgütleri ve dolandırıcılar geçmişte kitle imha ve tahribatına neden olmak için biyolojik silahlar ya da toksin etmenleri edinmeye ve kullanmaya çalışarak saldırı planları kurmuşlardır. [111] Nükleer terörizmin saldırı senaryoları ise şu şekilde sıralanabilmektedir: [112] 1- Nükleer Güç Reaktörüne Saldırı, 2- Parçalanabilir Malzeme Çalma, 3- Kirli Bombalar (Dirty Bombs), 4- Hazır Nükleer Silah Edinme ve 5- Nükleer Silah Yapım'ıdır.

---

[109] Valo, Janne., Cyber Attacks and the Use of Force in International Law, University of Helsinki, Yayınlanmamış Yüksek Lisans tezi, 2014, p.5.
[110] Heinonen, Olli, Nuclear Terrorism: Renewed Thinking for a Changing Landscape, Briefing at the Open Debate of the United Nations Security Council, Foundation for Defense Democracies, New York, 2017, pp.1-2.
[111] Hashmi, Muhammad Jawad, Scenarios Of Nuclear Terrorism: An Analysis, Eurosia Review, 2012: https://www.eurasiareview.com/27012012-scenarios-of-nuclear-terrorism-an-analysis/ (E.T: 18.03.18).
[112] A.e.

Bu bilgiler ışığında nükleer terörizm saldırılarını günümüz dünyasına uyarlayarak daha somut örneklendirmek için, EK 1'deki[113] tabloya bakılabilir. Aşağıdaki şekil, nükleer santral güvenliğinin terörist saldırılarına karşı genel bilgi vermektedir.

Şekil 6: Nükleer Terörizmin "3S" Prensibi



***NOT: Safety**: Emniyet, **Security**: Güvenlik, **Safeguards**: Koruma, **Proliferation**: Silahlanma, **Diversion**: Saptırma, **Misuse**: Kötüye Kullanma, **Breakout**: Meydana Gelmek, **Malicious Act:** Kötü Niyetli Eylem, **Legal and Regulatory Framework**: Hukuki ve Düzenleyici Çerçeve, **Code of Conduct**: Uygulama Esası, **Trigger**: Tetiklemek (Çev. Cihad Furkan ELİAÇIK)*

Kaynak: JAEA.[114]

[113] Nunn, Sam., The Race between Cooperation and Catastrophe: Reducing the Global Nuclear Threat, The Annals of the American Academy of Political and Social Science, Vol. 607, 2006, pp. 44-48.

[114] JAEA, International Forum on Peaceful Use of Nuclear Energy and Nuclear Security : https://www.jaea.go.jp/04/np/activity/2011-12-08/report_en.html (E.T: 18.0.18).

3.4. Siber - Nükleer Güvenlik ve Tedbir

'Siber' kelimesi, bilgisayar ve elektromanyetik spektrumlu faaliyetler için bir ön ek olarak kullanılmaktadır ve siber alan sadece ağa bağlı bilgisayarların internetini değil, aynı zamanda intranetleri, hücresel teknolojileri, fiber optik kabloları ve uzay tabanlı iletişimleri de içermektedir. Bu alan, giriş engellerinin çok az olduğu, devlet dışı aktörlerin ve küçük devletlerin önemli roller oynayabileceği karmaşık insan yapımı bir ortamdır. [115] Siber tehdit nükleer riskleri en az iki şekilde etkilemektedir: Nükleer malzeme ve tesis operasyonlarının güvenliğini zayıflatmak için kullanılabilir ve nükleer komuta ve kontrol sistemlerini tehlikeye atabilir. Geleneksel nükleer güvenlik uygulamaları, fiziksel saldırıların önlenmesine odaklanmıştır ve bunlar: [116] 1) hırsızlık yapmak için materyallerin çalınmasını, 2) nükleer tesisin sabote edilmesini veya 3) nükleer yetkisiz erişimin engellenmesi için "silahlar, muhafızlar ve kapılar" komuta, kontrol ve iletişim sistemleridir. Bu "geleneksel" nükleer güvenlik alanında önemli ilerlemeler kaydedilmiştir, ancak siber saldırı tehdidi artmaktadır. [117] Nükleer operatörler ve bir dizi ulusal ve uluslararası kuruluş siber tehdit zorluğunu kabul ederek nükleer tesislerde siber güvenliğin güçlendirilmesi çabalarını hızlandırmaya başlamıştır. Ancak, hızla gelişen siber tehdit, dijital sistemlerin çoğalmasıyla birleşince, tehdidin önüne geçmeyi zorlaştırmaktadır. Vaka sonrası durum - İran'daki Natanz uranyum zenginleştirme tesisindeki Stuxnet saldırılarından, Güney Kore'deki Kore Hidro ve Nükleer Güçlerinin saldırılarına karşı, Alman nükleer santralindeki sistemlerde bulunan kötü amaçlı yazılımların açığa çıkarılması - mevcut yaklaşımın nükleer tesislerdeki siber güvenlik sorunu ile aynı değildir. Tesisleri dinamik, gelişen siber tehditlerden

[115] Nye, Joseph S. Jr, From Bombs To Bytes: Can Our Nuclear History Inform Our Cyber Future?, Bulletin of the Atomic Scientists, Vol. 69, No. 5, pp. 8-9.
[116] NTI, Addressing Cyber-Nuclear Security Threats: http://www.nti.org/about/projects/addressing-cyber-nuclear-security-threats/ (E.T: 19.03.18).
[117] A.g.e.

koruyan bir strateji hazırlamak, siber güvenliği yönlendiren kapsayıcı çerçevenin yeni ve kısıtsız bir incelemesini gerektirmektedir. [118]

Bununla birlikte siber saldırıların önlenmesi, yalnızca nükleer sektörden ziyade, tüm toplumsal sektörleri etkileyebilecek bir ulusal güvenlik sorunu olan devletler için önemli ve stratejik bir sorun haline gelmiştir. Devlet ya da devlet dışı aktörler tarafından yürütülen kasıtlı ya da kasıtsız siber saldırıların olasılığı, siber alandaki mevcut ve gelecekteki risklerle ilgili endişeleri ortaya çıkarmaktadır. Potansiyel riskler şunlardır: [119] 1- tesis faaliyetinin sekteye uğrama riski; 2- tesislere karşı fiziki hasar; 3- casusluk (ticari ve politik); 4- kritik altyapıya müdahale ("CI"); [120] 5- potansiyel radyolojik olay; 6- nükleer enerjide kamu güveninin sarsılması ve 7- nükleer veya diğer radyoaktif malzemelerin çalınmasıdır [121]. Nükleer terörizm tehditlerine karşı önleyici tedbir niteliğinde ülkeler, tehdit unsuru oluşturabilecek ülkelere karşı çeşitli operasyonlar düzenlemişlerdir. Buna örnek oluşturabilecek gelişme olarak, 2007'de İsrail Hava Kuvvetleri, Deyr ez-Zor bölgesindeki Suriye nükleer reaktörünü yok etmek için Orchard Operasyonu'nu başlatmıştır ve Esad rejiminin atom silahlarını kullanmasını engellemiştir. [122] Nükleer santrallere gerçekleştirilecek saldırılara karşı bir dizi önlemlerin alınması gerekmektedir. Nükleer tesisin yönetim sistemlerinin tedbir amaçlı almaları gereken bir takım önlemler vardır. Bu yönetim sistemi, politikaların ve hedeflerin oluşturulmasından ve hedeflerin verimli ve etkili bir şekilde gerçekleştirilmesini sağlamaktan sorumludur. Yönetim sistemleri, nükleer güvenlik kültürünün önemli bir destek unsurudur. Nükleer tesislerdeki birçok faaliyet yönetim sistemleri tarafından kontrol

[118] Dine, Alexandra Van/ Michael Assante / Page Stoutland, Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities, Nuclear Threat Initiative, 2016, p.1.
[119] Giaurov, Vesselin, The Cyber-Nuclear Security Threat: Managing the Risks, VCDNP, 2017, p.3.
[120] HS, Critical Infrastructure Sectors, 2017: https://www.dhs.gov/critical-infrastructure-sectors (E.T: 19.03.18).
[121] Vesselin, a.g.e., s.3.
[122] Kemp, Richard., Israel as a Strategic Asset of the West, Jewish Political Studies Review, Vol. 28, No. 1/2, 2017, p.23.

edilmektedir. Bunlar ideal olarak güvenlik, güvenlik, sağlık, çevre, kalite ve ekonomik unsurları tek bir yönetim aracıyla veya bir dizi entegre ve karşılıklı takviye sistemiyle bütünleştirmektedir. [123] Nükleer santrallerin siber tehdide karşı alması gereken tedbir amaçlı ilkeler şunlardır[124]:

- Bilgi varlıklarının tanımlanması ve sınıflandırılması;
- Resmi risk analizi;
- Mevzuat ve mevzuata uygunluk;
- İş operasyonel gereksinimleri;
- Kilit kişiler için yetkinlik gereksinimleri;
- İş devamlılığı;
- Mantıksal erişim yönetimi;
- Sistem yaşam döngüsü güvenliği;
- Konfigürasyon yönetimi;
- Bilgisayar güvenlik önlemlerinin değiştirilmesi ve onaylanması;
- Belirlenen bilgisayar güvenlik önlemlerinin uygulanması;
- Uygulanan bilgisayar güvenlik önlemlerinin kabulü;
- Onaylanmış bilgisayar güvenlik önlemlerine uygunluk;
- Bilgisayar güvenlik olaylarının anlık analizi ve uygun raporlama;
- Uyum konusunda düzenli raporlama;
- İç ve dış taraflar tarafından uygulanan güvenlik önlemlerinin (denetimler) düzenli gözden geçirilmesi;
- Farkındalık eğitimi;
- Yeni riskler ve belirlenen risklerdeki değişiklikler;
- Yasal ve düzenleyici gerekliliklerde değişiklikler;
- Bilgi güvenliği için orta vadeli planlardır.

Siber güvenlik uzun vadede evrimleşebilir ve daha güvenilir hale getirilebilmektedir, ancak devletlerin değişimlere ayak uydurmak için gerekli

[123] IAEA, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series, No. 17, 2011, p.14.
[124] IAEA, 2011, s.15-16.

ivmeyi toplamaya başlaması ve tehditlerle başa çıkmak için gerekli altyapıyı oluşturmaya yönelik pragmatik bir yaklaşım benimsemesi oldukça önem arz etmektedir. [125]

[125] Gluschke, Guido, Cyber Security at Nuclear Facilities: National Approaches, The Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences, First ed., June 2015, p.18.

4. Değerlendirme

Enerji olgusunu kavramsal olarak analiz etmek nükleer enerjinin ortaya çıkması ya da elektrik enerjisine dönüştürülmesinde izlenen yolları anlamada önem arz etmektedir. Bu sebeple, öncelikle enerji olgusu, tarihsel analizi ve hukuk bağıntısı noktasında açıklamaya gidilmiştir. Yenilenebilir, yenilenemez ve sürdürülebilir enerji kategorileri altında enerjinin çeşitlerine yer verilmiştir. Akabinde ise nükleer enerjinin kullanım sahaları ve ortaya çıkış hikâyesi analiz edilmiştir. Önceki başlıklarda da zikredildiği üzere, dünyanın nükleer enerji ile tanışmasına yol açan iki önemli gelişme vardır: Sanayileşme ve II. Dünya Savaşı. Buradan kasıt, nükleer enerjinin ilk ortaya çıkışı değildir, zira ilk insani kullanımı tıp alanında röntgenin uygulanması esnasında olmuştur. Daha sonra sanayileşmenin etkisi ve enerjiye duyulan taleple birlikte daha da önem kazanmıştır. II. Dünya Savaşı'nda ise nükleer enerjinin nükleer bir silah olarak kullanılabileceği gerçeği Hiroşima ve Nagazaki'ye atılan iki ayrı atom bombasıyla kanıtlanmıştır. Enerjiye duyulan ihtiyacın bir sonucu olarak kurulan sivil nükleer santraller de nükleer enerjiyi insani amaçla elektrik üretmek için arz etmektedir. Ancak oldukça kırılgan bir yapıya sahip olan nükleer santrallerin güvenliği de uluslararası kamuoyunda süregelen tartışma konusu olmuştur. Zira meydana gelebilecek en ufak bir hata, beraberinde büyük tahribat ve felaketleri getirmektedir. Olası bir nükleer santral kazası sonucunda, sadece anlık bir hasardan ziyade kalıcı radyoaktif atıklardan dolayı çevre muhitlerde yaşayan insanlarda da kalıcı hastalıklar meydana gelmektedir. Bu yüzden, nükleer santrallerin güvenliği büyük önem taşımaktadır. Three Mile, Çernobil ve Fukuşima kazaları, tarihsel süreçte bu facialarn somut örnekleri olarak karşımıza çıkmıştır. Doğal afet, iş kazası ya da teknik bir arızadan dolayı meydana gelebilecek nükleer santral kazalarına ilaveten 11 Eylül saldırılarıyla bu ihtimali güçlendiren 'nükleer terörizm' olgusu, nükleer santraller bağlamında uluslararası camiada yoğun çalışma gündemi oluşturmuştur. Nükleer terörizm senaryoları başlığında da belirtildiği üzere, teröristlerin nükleer santrallere karşı bu saldırıları gerçekleştirme olasılıkları gelişen teknolojiyle birlikte hem daha kolay hem de daha endişe verici boyutlara ulaşmıştır. 2007 te Estonya'da meydana gelen

Stuxnet siber saldırı vakası, nükleer santrallerin siber güvenliğinin ne derece önemli olabileceğini ortaya koymuştur.

Bu bilgiler ışığında, nükleer enerji kullanımına karşı talepler artarken aynı doğrultuda kurucu işletmeler ve devtletler nezdinde güvenlik endişleri de oluşmuştur. Nükleer santrallerin güvenliğine dair gerek UAEA gerek NTI, WNA ve diğer bağımsız kuruluşlar tarafından teknik düzenlemeler gerçekleştirilse de, oldukça karmaşık olan siber saldırı çeşitleri ve yöntemleri karşısında uluslararası kamuoyunda teknik ve hukuki uzlaşı tam anlamıyla sağlanabilmiş değildir.

İKİNCİ BÖLÜM

ULUSLARARASI NÜKLEER HUKUK ve GÜNCEL GELİŞMELER

1. Nükleer Hukuk Hakkında Temel Esaslar

Nükleer enerjiyi şekillendiren hukuki düzenlemeler Nagazaki ve Hiroşima'nın bombardımanından bu yana değişip gelişerek devem etmektedir. 6 Ağustos 1945'te Hiroşima kentine "Küçük Çocuk – Little Boy" bombasının ve aynı yılın 9 Ağustos'ta Nagazaki'deki "Şişman Adam- Fat Man" ın yıkıcı etkileri, nükleer enerjiye yönelik uluslararası toplum yaklaşımlarını derinden etkilemiştir[126]. Bu gelişmelere müteakiben, nükleer enerjinin ikili doğası, çevre ve gelecek nesiller için ciddi bir tehdit olarak algılanmıştır. Uluslararası Adalet Divanı (ICJ), Nükleer Silahların Tehlikesi veya Kullanımının Yasallığı Hakkında Tavsiye Niteliğindeki Görüş'ünde (AOLTUNW) [127] nükleer patlamanın etkisini şöyle tanımlamıştır: "Nükleer patlamanın yaydığı radyasyon, çok geniş bir alanda sağlık, tarım, doğal kaynaklar ve demografiyi etkileyecektir. Dahası, nükleer silahların kullanımı gelecek nesiller için ciddi bir tehlike olacaktır. İyonlaştırıcı radyasyon, gelecekteki çevre, gıda ve deniz ekosistemine zarar verme ve gelecek nesillerde genetik kusur ve hastalığa neden olma potansiyeline sahiptir. " [128] Hukuki çerçeve oluşturma çabaları devam ederken, 1950'lerin ikinci yarısı II. Dünya Savaşı'ndan sonra yeniden yapılanma çabalarına tanık olmuştur. Fakat Hiroşima ve

[126] Qasaymeh, Khaled Ahmed, South Africa's Peaceful Use of Nuclear Energy Under the Nuclear Non-Proliferation Treaty and Related Treaties, University of South Africa, Yayınlanmamış Doktora Tezi, 2014. s. 39.

[127] Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons 35 ILM 809 (1996). UAD, BM Tavsiyesi'nin 96. Maddesi uyarınca, 15 Aralık 1994 tarihinde kabul edilen 49/75 K sayılı BMGA kararı ile talep edildiği şekliyle bu Tavsiye Niteliğindeki Görüşünü sunmuştur., a.g.t. den aktarılmıştır.

[128] ICJ, Reports of Judgments, Advisory Opinions and Orders Legality of the Threat or Use of Nuclear Weapons, 1996: http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf (E.T: 18.04.18).

Nagazaki'nin etkisi hala taze idi. Bu yüzden, savaş sonrası yasal normlar nükleer savaş korkusunu yansıtmaktaydı ve sayısız barışçıl uygulamalarını korurken daha fazla askeri nükleer enerji kullanımını önleme amaçlı mekanizmalara odaklanmaktaydı. Bu durum, Birleşmiş Milletler Atom Enerjisi Komisyonu'nun (UNAEC) uluslararası nükleer yönetim organı ve BM Güvenlik Konseyi'ni (UNSC) nükleer meseleler konusunda yetkili bir otorite olarak tesis eden ilk BM Genel Kurulu (UNGA) Kararında da yansımıştır. [129] Bu olaylardan sonra bir dizi uluslararası düzenlemeler, aynı hadiselerin yaşanmaması adına uluslararası hukuki çerçeve oluşturma yöntemiyle soruna çözüm bulmaya çalışmıştır.

1.1. Nükleer Hukukun Kapsam ve Mahiyeti

En yaygın tanımıyla nükleer hukuk, bölünebilir maddeler, iyonlaştırıcı radyasyon ve doğal radyasyon kaynaklarına maruz kalma ile ilgili faaliyetlerde bulunan yasal veya gerçek kişilerin davranışlarını düzenlemek için oluşturulan özel yasal normlar bütünüdür. [130] Nükleer hukukun kapsam ve mahiyetinin doğrudan tanımı ise çevre yasası dışındaki tüm yasaların, yönetmeliklerin ve düzenlemelerin uygulanmasıdır. Bunlar: [131]

-Nükleer enerji santrallerinin, Kaynak Malzemenin, Yan Ürün Malzemesinin ve Özel Nükleer Malzemelerin düzenlenmesi;

-Düşük Düzeyli Atık ve Harcanan Nükleer Yakıtın düzenlenmesi;

-Nükleer Malzemeler, atıklar ve yakıtların yönetimi, taşınması ve depolanması;

-Korunma Bilgilerinin Düzenlenmesi;

-Nükleer Yakıtın Düzenlenmesi;

[129] Hafstad L.,Nuclear Reactor Developments, Stason E Lectures on Atomic Energy: Industrial and Legal Problems, 1952, pp. 3-16.
[130] Stoiber, Carlton et al., Hand Book on Nuclear Law, IAEA Press, Austria, 2003, p. 4.
[131] LAW INSIDER, Definition of Nuclear Laws: https://www.lawinsider.com/dictionary/nuclear-laws (E.T: 19.03.18).

-Uranyumun zenginleştirilmesi;

-Harcanmış Nükleer Malzemelerin, atıkların ve yakıtların imhası ve

-Nükleer Atık Fonu'na yapılan ödemeler için sözleşmelerdir.

1.2. Nükleer Hukukun Temel İlkeleri

Nükleer hukukun, bir dizi temel prensipler kapsamında işlemektedir ve bu prensipleri aşağıdaki gibi sıralanmaktadır: [132]

- **Emniyet Prensibi** (The Safety Principle) "önleme prensibi" ve "koruma prensibi" olarak ikiye ayrılmaktadır ve nükleer santrallerin emniyetli bir şekilde işletilmesi sürecini kapsamaktadır. Önleme ilkesinin temel amacı, santrallerde teknolojinin kullanımından kaynaklanabilecek zararları önlemek ve herhangi bir yanlış kullanım veya kazalardan kaynaklanan olumsuz etkileri bertaraf etmektir. Koruma ilkesi ise tamamlayıcı niteliktedir. Bir faaliyetle ilgili risklerin faydalardan ağır bastığı durumlarda, halk sağlığının, güvenliğin, çevrenin korunmasına öncelik verilmesi sürecini kapsamaktadır. [133]

- **Güvenlik Prensibi** (The Security Principle) bazı nükleer malzeme ve teknolojilerin, uygun ortamlarda muhafaza edilmedikleri durumlarda kişilerin ve sosyal kurumların güvenliği için risk oluşturmaktadır. Güvenlik prensibi ise bu sürecin güvenliğini kapsamaktadır. Radyasyon kaynaklarının terörist veya suç grupları tarafından alınması, kötü niyetli eylemlerde bulunmak üzere kullanılacak radyasyon dağıtma cihazlarının üretimine yol açabildiği için nükleer santral sahasının güvenliği de önem arz etmektedir. [134] Güvenlik prensibi ise bu koruma sürçlerini içermektedir.

---

[132] Stoiber, a.g.e. , s.5.
[133] A.g.e., s. 7.
[134] Thiele, Lisa, Introduction to Nuclear Law, Canadian Nuclear Safety Commission, July 13, 2017 : http://www.nuclearsafety.gc.ca/eng/pdfs/Presentations/VP/2017/20170713-lisa-thiele-WNU-Summer-Institute-eng.pdf (16.03.18).

- **Sorumluluk Prensibi** (The Responsibility Principle), nükleer enerjinin kullanımı genellikle araştırma ve geliştirme kurum ve kuruluşları, nükleer malzemenin işleyicileri, nükleer cihaz üreticileri veya iyonlaştırıcı radyasyon kaynakları, tıp pratisyenleri, mimar-mühendislik firmaları, inşaat şirketleri, nükleer tesisler işletmecileri, finansal kurumlar gibi çok sayıda düzenleyici kurumlar taraf içermektedir. Bu kapsamda, sorumluluk prensibi ise nükleer santrallerde meydana gelecek kaza olaylarında kimlerin sorumlu tutulacağını kapsamaktadır. [135]

- **İzin Alma Prensibi** (The Permission Principle) bir faaliyet kişi ya da çevreye karşı tanımlanabilir bir yaralanma riski taşıyorsa, kanunun bir kişinin bu faaliyeti gerçekleştirebilmesi için önceden izin almasını şart koşması gerekmektedir. [136] Nükleer santraller için gerçekleştirilecek bu faaliyetler için izin alma süreçlerine ise izin alma prensibi şeklinde tanımlanmaktadır.

- **Sürekli Kontrol Prensibi** (The Continuous Control Principle) ulusal nükleer mevzuatın, nükleer malzemenin kullanıldığı ve depolandığı tüm binalara düzenleyici denetçiler tarafından serbest erişim sağlaması gerektiği anlamına gelmektedir. [137]

- **Tazminat Prensibi** (The Compensation Principle) çeşitli teknik faktörlere bağlı olarak, nükleer enerjinin kullanımı kişi, mülk ve çevre için büyük hasar riskleri teşkil eden süreçleri ve zararın tazmin sürecini ele almaktadır. Önleyici tedbirler, söz konusu hasarın potansiyelini tamamen ortadan kaldıramayacağından, nükleer

---

[135] Nanda, Ved P. /Jon M. Van Dyke, International Nuclear Law: An Introduction, Nuclearintro_Macro, Vol. 35, No. 1, 2008, pp. 4-6.

[136] IET, Legal Framework for the Nuclear Industry in Great Britain: https://www.theiet.org/factfiles/ (E.T: 18.03.18).

[137] Furtado, Rebecca, A Brief Introduction to Nuclear Energy Laws, Pleaders, July 11, 2016 : https://blog.ipleaders.in/brief-introduction-nuclear-energy-laws/ (E.T: 19.03.18).

hukuk, devletlerin herhangi bir nükleer bir kaza durumunda yeterli tazminat sağlama tedbirlerini benimsemelerini gerektirmektedir. [138]

- **Sürdürülebilir Kalkınma Prensibi** (The Sustainable Development Principle), bazı bölünebilir materyaller ve iyonlaştırıcı radyasyon kaynaklarının uzun süreler boyunca sağlık, güvenlik ve çevresel riskler oluşturabilmesi nedeniyle bu sorunların optimize edilmesi süreçlerini kapsamaktadır. [139]

- **Uyum Prensibi** (The Compliance Principle) bölgesel ve küresel olarak, iki taraflı ve çok taraflı düzenlemeler uluslararası bir nükleer enerji yasası oluşturmaktadır. Bir devletin söz konusu uluslararası hukuki rejimlere bağlı kaldığı ölçüde, ulusal nükleer mevzuat da aynı ölçüde içerdikleri yükümlülükleri yansıtmalıdır. Bu süreç döngüsü ise uyum prensibi şeklinde tanımlanmaktadır. [140]

- **Bağımsızlık Prensibi** (The Independence Principle) nükleer hukukun, güvenlik konularıyla ilgili kararları nükleer enerjinin geliştirilmesine veya teşvik edilmesine dâhil olan kuruluşların müdahalelerine maruz kalmayan bir düzenleyici makamın (bağımsız makam/otorite) kurulması gerekmektedir. Bu bağlamda, nükleer teknoloji ile ilgili önemli riskler göz önüne alındığında, düzenleyici merciinin bağımsız ve uzman tarafından yürütülmesi gerekmektedir Bağımsızlık prensibi, bağımsız otoriteleri tanımlamaktadır. [141]

- **Şeffaflık Prensibi** (The Transparency Principle), nükleer enerjinin geliştirilmesi, kullanımı ve düzenlenmesine dâhil olan organların, özellikle halk sağlığı,

---

[138] Nuclear Power Plant and reactor Exporters, The Principles of Conduct: Compensation for Nuclear Damage : http://nuclearprinciples.org/principle/compensation-for-nuclear-damage/ (19.03.18).
[139] Staoiber et al, a.g.e. s. 9.
[140] Moxley, Charles J. Jr./ John Burroughs / Jonathan Granoff, Nuclear Weapons and Compliance with International Humanitarian Law and the Nuclear Non-Proliferation Treaty, Fordham International Law Journal, Vol. 34, No. 4, 2011, pp. 612-614.
[141] OECD- NEA/IAEA, International Nuclear Law in the Post-Chernobyl Period, No. 6146, 2006, pp. 74-75.

güvenliği ve çevre üzerinde etkisi olabilecek olay ve anormal olaylarla ilgili olarak, nükleer enerjinin nasıl kullanıldığıyla ilgili tüm bilgileri sunmasını gerektirmektedir. Bir santralde nükleer silah geliştirilmediği gerçeği yine şeffaflık prensibi kapsamında saptanmaktadır. [142]

- **Uluslararası İş birliği Prensibi** (The International Cooperation Principle) nükleer enerjinin uluslararası boyutu, güvenlik ve çevre alanında, sınır aşan etkilerin potansiyeli, hükümetlerin politikaları uyumlu hale getirmesini ve vatandaşlar ve bölgeler, küresel nüfus gibi hasar risklerini azaltmak için kooperatif programları geliştirmesini gerektirmektedir. Bir bütün olarak, bir devlette güvenliği arttırmaya yönelik uygulamalar, diğer devletlerdeki durumun iyileştirilmesi için önem arz etmektedir. [143] Nükleer terörizm olgusu, küresel bir boyutta faaliyet gösterdiği için uluslararası iş birliği prensibi nükleer santrallerin güvenliği esasında kritik öneme haizdir. [144]

UAEA bu konuda kapsamlı çalışma yürütmektedir ve BM Genel Kurulu'nda de nükleer hukuk ile ilgili temel prensipler belirlenmiştir. [145]

2. Nükleer Santrallerin Uluslararası Hukuk Açısından Temel Özellikleri

Nükleer santrallerin kapsam ve tanımı uluslararası kurum ve kuruluşlarca farklı şekilde zikredilmiştir. Bunlardan 28 Ocak 1964 Tarihli Ek Protokol ve 16 Kasım 1982 Tarihli Protokol ile Değiştirilen 29 Temmuz 1960 Tarihli Nükleer

[142] NSGEG, Promoting Greater Transparency for Effective Nuclear Security: Summary Report & Initial Policy Recommendations, the Stanley Foundation, February 2013, p.4. : https://www.stanleyfoundation.org/nsgeg/NSGEGLondonReport022013.pdf (E.T: 20.03.18).
[143] Emmerechts, Sam, General Principles of International Nuclear Law, OECD-NEA, 6 March 2008: http://qualidade.ipen.br/sq-cen/Atualizacao-CEN/4.14-Cursos/Curso-WNU/Main_Issues_of_Nuclear_Law-Sam_Emmerechts.pdf (E.T: 19.03.18).
[144] A.g.e.
[145] 67/97 sayılı BM Genel Kurul Kararı, Dış Mekânda Nükleer Güç Kaynaklarının Kullanımına İlişkin İlkeler, A/RES/47/68, 14 Aralık 1992, bkz: http://www.un.org/documents/ga/res/47/a47r068.htm (E.T: 19.03.18).

Enerji Alanında Üçüncü Şahıslara Karşı Hukuki Mesuliyete Dair Sözleşmeyi Değiştiren Protokol ün 1. Maddesinin (a) paragrafının (ii) bendinde şu şekilde tanımlanmıştır:

""Nükleer tesis": herhangi bir ulaştırma aracında yer alanlar haricindeki reaktörler; nükleer madde imalat ya da işleme tesisleri; nükleer yakıtın izotoplarını ayırma tesisleri; işlenmiş nükleer yakıtı yeniden işleme tesisleri; nükleer maddelerin taşınması sırasında gerçekleştirilen depolamalar dışında nükleer madde depolama tesisleri; nükleer maddelerin bertarafı için tesisler; işletimden çıkarma sürecinde olan herhangi bir tür reaktör, tesis, fabrika ya da işletmelerdir." [146] Nükleer tesis kavramının tanımlandığı bir diğer sözleşme ise 20 Eylül 1994 tarihinde ülkelerin imzasına açılan ve 24 Ekim 1996 tarihinde yürürlüğe giren Nükleer Güvenlik Sözleşmesidir. Nükleer tesis kavramı Nükleer Güvenlik Sözleşmesi'nin tanımlar kısmında Madde 4'te düzenlenmiştir. [147] Bu düzenlemeye göre: "Nükleer tesis" her Akit Taraf için, kendi etkisi altındaki aynı yerde bulunan ve nükleer güç santralinin işletimiyle doğrudan ilgili olan radyoaktif maddelerin idare edildiği ve işlendiği tesisler ile depolar dâhil herhangi bir sabit sivil nükleer güç santrali anlamına gelmektedir. Böyle bir tesis, reaktör korundan nükleer yakıtın kesin olarak çıkarılması, onaylanmış usullere göre güvenli olarak depolanması ve yetkili kurum tarafından sökülme programının kabul edilmesi halinde nükleer tesis olmaktan çıkmaktadır." [148] Uluslararası hukuki düzenlemelerde nükleer santraller kavramsal olarak bu şekilde zikredilmiştir.

[146] TAEK, Nükleer Enerji Alanında Üçüncü Şahıslara Karşı Hukuki Sorumluluğa ilişkin Paris Sözleşmesi'ni Yenileyen 2004 Protokolü, 2011: http://www.taek.gov.tr/attachments/article/761/908_paris_2004_tr.pdf (E.T: 19.03.18).
[147] Karauz, Ağâh Kürşat, Nükleer Santral İşletenin Hukukî Sorumluluğu, Nevşehir Barosu Dergisi, Yıl 1, Sayı 1, Mart 2014, s. 6.
[148] IAEA, Convention on Nuclear Safety: https://www.iaea.org/sites/default/files/infcirc449.pdf (E.T: 19.03.18).

2.1. Nükleer Santrallerin İnsani Amaçla Kullanımı

II. Dünya Savaşı sonrası ülkeler, dünya çapında nükleer enerjinin barışçıl kullanımlarının yanı sıra hem silahlara ilişkin hem de nükleer teknolojik seçeneklerini araştırarak bir dizi girişimlerde bulunmuşlardır. Devletlerin nükleer silah geliştirmeyi caydırmaya yönelik ilk girişimleri, barışçıl amaçlarla nükleer enerjiyi geliştirme yeteneklerine getirilen kısıtlamalar gereği kuşku ile yaklaşmışlardır. 1953'te ABD Başkanı Eisenhower'ın "Barış İçin Atom" konuşması, nükleer silahların yayılmasını önleme çabalarıyla ABD'nin uzlaşmacı bir girişimi olarak karşımıza çıkmıştır ve nükleer enerjinin insani olarak kullanımına dair önem arz eden bir konuşmadır. [149] Bu bilgiler ışığında, nükleer enerjinin barışçıl uygulamaları ve sunduğu avantajlar, nükleer silahların yayılması ve nükleer savaş beklentileriyle birlikte paradoksal olarak algılanır hale gelmiştir. [150] Bu nedenler, nükleer enerjinin barışçıl kullanımı iki zıt yasaya karşı bir meydan okuma anlamına gelebilmektedir. Bir yandan, bazı devletler nükleer enerjiyi kullanmak için daha uygun zeminler oluşturmaya çabalarken ve diğer devletler için nükleer enerjinin kullanılmasının teşvik edilmesi ve erişimi risk ve tehdit arz etmektedir. Bu kaygılar nükleer enerjinin kullanımını ve erişimini kısıtlayan ulusal ve uluslararası hukuki ve hukuki olmayan düzenlemeleri tetiklemektedir. [151] Ulusal mevzuat ve uluslararası hukuk, bu kaygılara ışık tutacak bazı düzenlemeler içermektedir.

[149] Eisenhower D., Atoms for peace, Amerika Birleşik Devletleri Başkanı Tarafından Birleşmiş Milletler Genel Kurulu'nun 470. Genel Kuruluna Hitaben Yapılan Konuşma, 1953, https://www.iaea.org/about/history/atoms-for-peace-speech (E.T: 19.03.18).

[150] ElBaradei, Mohamed / Edwin Nwogugu / John Rames, International Law And Nuclear Energy: Overview of The Legal Framework, IAEA Bulletın, Vol.3, 1995, p.16.

[151] Bothe, Michael, The Peaceful Use of Nuclear Energy and the Protection of the Environment, Jonathan L. Black/Branch Dieter Fleck (eds), Nuclear Non-Proliferation in International Law: Volume III Legal Aspects of the Use of Nuclear Energy for Peaceful Purposes, Canada, Asser Press-Springer, 2016, p. 295.

2.1.1. Ulusal Mevzuat

Ulusal mevzuatımızda nükleer enerji çalışmalarının çerçevesini belirlemek ve ilgili alanda çalışmalar yapmak üzere 9.7.1982 kabul tarihli 2690 sayılı Türkiye Atom Enerjisi Kanunu kabul edilerek 17753 sayılı 13.7.1982 tarihli Resmi Gazetede yayınlanarak yürürlüğe girmiştir. [152] Bu kanunun 1. maddesi uyarınca TAEK'in kuruluş esası: "Barışçıl amaçlarla Türkiye'de atom enerjisinin kalkınma planlarına uygun olarak ülke yararına kullanılmasını sağlamak, temel ilke ve politikaları belirleyip önermek, bilimsel, teknik ve idari çalışmaları yapmak, düzenlemek, desteklemek, koordine etmek ve denetlemek üzere Türkiye Atom Enerjisi Kurumunun kuruluşu, işleyişi, görev, yetki ve sorumluluklarını saptamaktır."[153] Daha sonra 5710 sayılı Nükleer Güç Santrallarının Kurulması ve İşletilmesi İle Enerji Satışına İlişkin Kanun Kapsamında Yapılacak Yarışma ve Sözleşmeye İlişkin Usul ve Esaslar İle Teşvikler Hakkında 10.3.2008 tarihli 2008/13347 sayılı Yönetmelikle [154] birlikte nükleer santrallerin hem kurulması hem de barışçıl yollarla kullanılmasının genel hatlarıyla hukuki çerçevesi oluşturulmuştur.

2.1.1.1. 5710 Sayılı Kanun'a Göre Nükleer Santral Kuracak Şirketin Belirlenmesi

Nükleer Güç Santrallerinin Kurulması ve İşletilmesi ile Enerji Satışına İlişkin 5710 Sayılı Kanun'un [155] 3. , 4. ve 6. maddelerinde nükleer santral kuracak şirketin belirlenmesine ilişkin kurallar yer almaktadır. Md. 6/3'te Enerji ve Tabii

[152] Türkiye Atom Enerjisi Kurumu Kanunu, 13.07.1982, Resmi Gazete, Sayı:17753: http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/arsiv/17753.pdf&main=http://www.resmigazete.gov.tr/arsiv/17753.pdf (19.03.18).

[153] a.g.k., madde 1/1.

[154] Nükleer Güç Santrallarının Kurulması ve İşletilmesi ile Enerji Satışına İlişkin Kanun Kapsamında Yapılacak Yarışma ve Sözleşmeye İlişkin Usul ve Esaslar ile Teşvikler Hakkında Yönetmelik, 19.03.2008, Resmi Gazete, Sayı:26821: http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2008/03/20080319.htm&main=http://www.resmigazete.gov.tr/eskiler/2008/03/20080319.htm (E.T: 19.03.18).

[155] 09.11.2007 tarihinde kabul edilmiş ve 21.11.2007 tarihli 26707 sayılı Resmi Gazete 'de yayımlanmıştır.

Kaynaklar Bakanlığı'nın görev vermesi halinde kamu şirketlerinin santral inşa edebileceği öngörülmüştür. Kanunun yorumu gereği santral kurabilecek şirketler: 1- Kamu Şirketleri ve 2- Kamuya Ait Olmayan Şirketler olarak ikiye ayrılmaktadır. Kamu şirketleri, kamuya ait olmayan şirketler ile iştirak kurabilmekte veya kamuya ait olmayan şirketler iktisadi devlet teşekkülleri ile iştirak ilişkisi kurabilmektedirler. Kamuya ait şirketler özel hukuk hükümlerine de tabi olabilmektedirler. Kamuya ait olmayan şirketler ise bu konuda iki gruba ayrılabilmektedirler: [156] 1- TETAŞ ile enerji satış sözleşmesi yapmayı talep eden şirketler, 2- TETAŞ ile enerji satış sözleşmesi yapmayı talep etmeyen şirketler. Bu kapsamda, sayılan tüm şirketler, mevzuatta öngörülen lisansları almak zorundadırlar.

5710 Sayılı Kanun md.6/2 uyarınca kamu şirketleri Kanun kapsamındaki santralleri yapabilir, yurt dışında yatırımlar yapabilir veya bunlara iştirak edebilirler. Santralleri inşa etmek için ya Bakanlık mevcut kamu şirketlerine görev vermekte, ya da Bakanlar Kurulu tarafından bu amaçla kurulan özel hukuk hükümlerine tabi bir kamu şirketini idari bir kararla görevlendirilmektedirler.

2.1.1.2. Milletlerarası Anlaşmalarla Nükleer Güç Santrali Kuracak Şirketin Belirlenmesi

12.05.2010 tarihinde "Türkiye Cumhuriyeti İle Rusya Federasyonu Hükümeti Arasında Türkiye Cumhuriyeti'nde Akkuyu Sahası'nda Bir Nükleer Güç Santralinin Tesisine ve İşletimine Dair İşbirliğine İlişkin Anlaşma" imzalanmıştır. [157] Anlaşmada nükleer güç santrali kurulması, işletilmesi ve sökülmesine ilişkin kapsamlı düzenlemelere gidilmiştir. Bu sayede nükleer santral kuracak şirketin uluslararası anlaşmayla belirlenmesi bir yöntem olarak benimsenmiş, adli ve idari yargıda iptal edilebilecek düzenlemelerin hayata

[156] 5710 Sayılı Kanun Md. 4/2.
[157] 21.07.2010 tarihli Resmi Gazete' de yayımlanan 15.07.2011 tarih ve 6007 sayılı Kanunla Anlaşmanın onaylanması TBMM' ce uygun bulunmuştur.

geçirilmesi için bir yol açılmıştır. Ayrıca Türkiye Cumhuriyeti Anayasasının 90. Maddesi uyarınca, "Usulüne göre yürürlüğe konulmuş milletlerarası antlaşmalar kanun hükmündedir. Bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz (Ek cümle: 7.5.2004-5170/7 md.). Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşma hükümleri esas alınır." [158] "Dolayısıyla Akkuyu anlaşması iç hukuk düzenimizde kanunlarla eşdeğerlidir. Bu nedenle milletlerarası anlaşmalarla da nükleer güç santrali kuracak şirket belirlenebilir. Bir milletlerarası anlaşma ile anlaşmanın tarafı ülke ya da kuruma, 5710 sayılı Kanunla getirilen rejimden daha avantajlı bir durum yaratılıyorsa Kanun'a dayanarak nükleer santral kurma hakkı elde eden şirketlerin, Kanun'da yer alan bu tür düzenlemelerin Anayasa'da yer alan eşitlik ilkesine aykırılık taşıdığını ileri sürmeleri mümkün olacaktır. Bu noktada Anayasa Mahkemesi, Kanun'da yer alan hükümleri denetleyebilecek, milletlerarası anlaşma hükümleri hakkında karar veremeyecektir." [159]

2.1.2. Uluslararası Düzenlemeler

Atom biliminin ortaya çıkışı ve gelişmesiyle birlikte, nükleer enerjinin barışçıl bir şekilde uygulanacağı ve elektrik sıkıntısı çeken bölgelere bol miktarda tedarik sağlayacağı kanısı mevcuttu. Bugüne kadar, bu amaç öngörülen ölçekte elde edilememiştir. Bu güçlü ve yeni enerji kaynağını barışçıl kullanımlarına uygulama sürecine başlamak üzere uluslararası kuruluşların çağrılarda bulunarak barışçıl kullanımın hukuki esaslarını oluşturmaya yönelik çalışmaları olmuştur. [160] Eisenhower'ın "Barış İçin Atom" konuşmasını takiben, 1954'ün başlarında ABD,

[158] TBMM, Türkiye Cumhuriyeti Anayasası: https://www.tbmm.gov.tr/anayasa/anayasa82.htm (E.T:20.03.18).
[159] Özdemir, Eyüp, Nükleer Güç Santrallarının Kurulmasına İlişkin Hukuki Esaslar, On İki Levha Yayıncılık, İstanbul, 2012, s.78.
[160] Nordyke, Mllo D., The Soviet Program For Peaceful Uses Of Nuclear Explosions, Science & Global Security, Vol.7, No.1, 2007, p.4.

BM nezdinde Atom Enerjisinin İnsani Amaçla Kullanımı Konferansı'nı önermiştir. Bu konferanslardan ilki, 1955 Ağustos'unda İsviçre'nin Cenevre kentinde gerçekleştirilmiştir. Kapsam ve nitelik itibariyle en büyük bilimsel toplantısı olarak anılmıştır ve 2500'den fazla katılımcı ile 1.000'den fazla teknik ve bilimsel makale sunulmuştur. [161] 1970'lerin başına gelindiğinde, nükleer enerji kapasitesi dünya çapında ortalama % 30 oranında büyümüştür ve zamanın ilerlemesiyle birlikte, dünya elektrik piyasası giderek daha büyük bir payı korumaya devam etmiştir; 1986'daki Çernobil kazası, küresel nükleer elektrik kullanımının %16'sını oluşturmaktaydı. O zamandan itibaren, bu oran aynı kalmıştır ve genel elektrik kullanımıyla aynı hızda büyümüştür. [162] 2000'li yıllara geldiğimizde Nükleer Enerjinin İnsani Amaçla kullanılmasına yönelik önemli girişimlerin olduğunu görmek mümkün hale gelmiştir. Özellikle UAEA'na bağlı Barışçıl Kullanım Girişimi (Peaceful Uses Initiative), kamuoyu gündeminde önemli çalışmalar yürütmektedir. [163] UAEA nezdinde çok taraflı anlaşmalarla birlikte ikili anlaşmalarla da uluslararası camiada nükleer enerjinin insani amaçla kullanımı teşvik edilerek hukuki zemini oluşturulmuştur. Temmuz 2016'da Varşova'da NATO İttifakları, nükleer caydırıcılık ve nükleer silahsızlanma ile nükleer enerjinin barışçıl amaçlar dâhilinde sürdürülmesi yönünde bir deklarasyon yayınlamışlardır ve bu içerik şu şekildedir: [164] "Müttefikler Nükleer Silahların Yayılmasını Önleme Antlaşması'nın (NPT) tam olarak uygulanmasına yönelik güçlü taahhütlerini vurgulanmıştır. İttifak, herkes için daha güvenli bir dünya arayışındaki kararlılığını ve nükleer silahsız bir dünyaya ilişkin şartların, Madde VI da dâhil olmak üzere, NPT'nin tüm hükümlerine tam olarak uygun bir şekilde uluslararası düzeyde istikrarlı ve teşvik edici biçimde herkes için sınırsız güvenlik ilkesine dayanarak doğrulanabilir maksatla oluşturulmasını sağladığını teyit etmektedir. Müttefikler, NPT'nin hedeflerini ve hedeflerini karşılıklı olarak

[161] Goldschmidt, Bertrand, The Atomic Complex, American Nuclear Society, 1982, pp. 257-62.
[162] El Baradei, Mohamed, Peaceful Uses of Nuclear Energy: Meeting Societal Needs, IAEA, Vienna- Austria, Nov. 15, 2014: https://www.iaea.org/newscenter/statements/peaceful-uses-nuclear-energy-meeting-societal-needs (20.03.18).
[163] PUI : https://www.iaea.org/newscenter/focus/peaceful-uses-initiative (E.T: 20.03.18).
[164] NATO, North Atlantic Council Statement on the Treaty on the Prohibition of Nuclear Weapons, 2017: https://www.nato.int/cps/ua/natohq/news_146954.htm (E.T: 20.03.18).

destekleyen üç temel dayanağı olan ilerlemeye olan bağlılıklarını yinelemişlerdir: nükleer silahsızlanma, nükleer silahların yayılmasını önleme ve nükleer enerjinin barışçıl kullanımı. " Nükleer enerjinin barışçıl amaçlarla kullanılması uluslararası kurum ve kuruluşlarca hukuki çerçevesi oluşturulmakla kalmayıp, aynı zamanda teşvik amaçlı girişimleri de görmek mümkündür. Bu kapsamda, 2017 Nobel Barış Ödülü, nükleer silahların herhangi bir şekilde kullanılmasının felaketle sonuçlanan insani sonuçlarına dikkat çekmek üzere yaptığı çalışmalardan ve anlaşmaya dayalı bir yasağa ulaşmak için gerçekleştirdikleri çabalarından ötürü Uluslararası Nükleer Silahların Kaldırılmasına Yönelik Uluslararası Kampanya (ICAN)'a verilmiştir. [165]

2.1.2.1. EURATOM ve ABD Arasında Nükleer Enerji'nin İnsani Amaçla Kullanılması Anlaşması

1958'de nükleer enerjinin barışçıl kullanımları ile ilgili ABD-Euratom İşbirliği Anlaşması, AAET (Euratom) ve Amerika Birleşik Devletleri'nin sanayi ve kurumları arasındaki nükleer alanda bilimsel, endüstriyel ve ticari ilişkilerin temelini oluşturmaktadır[166]. Avrupa Atom Enerjisi Topluluğu ve Amerika Birleşik Devletleri arasında imzalanan bu anlaşma, iki taraflı bir anlaşma gibi görülse de aldığı kararlar hasebiyle uluslararası camiada emsal teşkil edecek özellikler muhteva etmektedir. Öyle ki, Anlaşmanın 1. maddesi alt fıkraları uyarınca taraflar aşağıdaki alanlarda nükleer enerjinin barışçıl kullanımlarında işbirliği yapabilirler: [167]

- Taraflar arasında mutabakata varılabilecek şartlar üzerinde nükleer füzyon araştırması ve geliştirilmesi;

[165] NOBEL PRIZE, 2017 Nobel Barış Ödülü : https://www.nobelprize.org/nobel_prizes/peace/laureates/2017/ (E.T: 20.03.18).
[166] Duckwitz, C.A./ Taegder, K. Is The Euratom-US Cooperation Agreement Jeopardized?. Atw Atomwirtschaft, Atomtechnik, Vol.40, No.3., 1995, pp.159-163.
[167] EURATOM ve ABD Arasındaki Nükleer Enerji'nin İnsani Amaçla Kullanılması Anlaşması, 20 Mayıs 1996, Avrupa Birliği Resmi Gazetesi, Sayı: L 120 : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:21996A0520(01)&from=EN (E.T: 20.03.18).

- Madde 2'de belirtildiği gibi, karşılıklı çıkar ve yetkiye sahip nükleer güvenlik konuları;

- Kişiler ve teşebbüsler arasında endüstriyel veya ticari ölçekte değişim ve işbirliği faaliyetlerinin kolaylaştırılması;

- Bu Anlaşmanın hükümlerine tabi olarak, nükleer olmayan malzeme, nükleer malzeme ve teçhizatın tarafları arasında ve nükleer yakıt çevrimi hizmetlerinin tarafların veya üçüncü ülkelerin kullanımı ya da yararı için sağlanması;

- Uluslararası Atom Enerjisi Ajansı ile işbirliği konuları da dâhil olmak üzere uluslararası nükleer güvenlik önlemleri alanında ve nükleer enerji ile çevre arasındaki etkileşim üzerine kalkınmanın teşvik edilmesi ve karşılıklı ilgi ve yetkinlik alanlarında nükleer silahların yayılması gibi nükleer enerjiyle ilgili önemli uluslararası sorulara ilişkin bilgi değişimi;

- Çok taraflı projeler dâhil olmak üzere kontrollü termonükleer füzyon ve

- Diğer karşılıklı ilgi alanlarıdır.

Bu anlaşma, plütonyum ve diğer hassas nükleer malzemelerin zenginleştirilmesi, yeniden işlenmesi ya da içerik ve depolanması gibi belirli yakıt döngüsü faaliyetleri üzerinde çok sıkı kontroller sağlamaktadır. "ABD ve EURATOM, bu kontrolleri karşılıklı olarak, her iki tarafın kendi için belirleyeceği, birbirlerinin yakıt döngüsü tercihlerine müdahale etmemek koşuluyla söz konusu hükümlerin barışçıl nükleer ticaret için önemli bir normu temsil ettiğine dair ortak inançlarının bir yansıması olarak karşılıklı kabul etmiş olmuşlardır." [168]

[168] Clinton, Bill, EURATOM ve ABD Arasındaki Nükleer Enerji'nin İnsani Amaçla Kullanılması Anlaşması hakkında 104. Meclisinin 1. Oturumunda İlettiği Yazılı Mesaj, Meclis Evrak No: 104-108, ABD Hükümeti Basın Ofisi, Washington, 29 Kasım 1995, s.2, bkz: https://www.gpo.gov/fdsys/pkg/CDOC-104hdoc138/pdf/CDOC-104hdoc138.pdf (E.T: 20.03.18).

2.1.2.2. Nükleer Silahların Yayılmasının Önlenmesine İlişkin Antlaşma (NPT)

NPT, amacı nükleer silahların ve silah teknolojisinin yayılmasını önlemek, nükleer enerjinin barışçıl kullanımında işbirliğini ilerletmek ve nükleer silahsızlanma ile genel ve eksiksiz silahsızlanma hedefini daha da ileriye taşımak olan, uluslararası bir antlaşmadır. Antlaşma, nükleer silah devletleri tarafından silahsızlanma amacına yönelik çok taraflı bir anlaşmanın tek bağlayıcı taahhüdünü temsil etmektedir. 1968 yılında imza için açılan Antlaşma, 1970 yılında yürürlüğe girmiştir. 11 Mayıs 1995 tarihinde Antlaşma, süresiz olarak uzatılmıştır. Beş nükleer silah devleti de dâhil olmak üzere toplam 191 devlet anlaşmaya katılmıştır. [169] NPT üyeliği toplantılarında sıklıkla vurgulandığı üzere, anlaşma küresel nükleer silahsızlanma rejiminin temel taşı ve nükleer silahsızlanma arayışının temel dayanağı" olarak değerlendirilmektedir. Antlaşma, kapsamlı bir anlaşma ağının merkezinde yer almaktadır. NPT nükleer silahların yayılmasını sınırlandırarak ve nükleer santral faaliyetlerini düzenlemek için geniş çapta kabul edilen bir çerçeve sağlayarak, uluslararası barış ve güvenlik için önemli faydalar sağlamıştır. [170] NPT'nin hedefleri birbiriyle ilişkili ve karşılıklı olarak takviye edici üç temel direktifte özetlenmiştir: (1) nükleer silahların yayılmasını önleme (Madde I, II): nükleer silah ve teknolojilerin daha fazla yayılmasını veya transferini veya mevcut cephanelikleri genişletmeyi önleme ; (2) silahsızlanma (Madde VI): nükleer ve genel silahsızlanma hedefine ulaşmak; (3) ve nükleer enerjinin barışçıl kullanımı (Madde IV): devletlerin barışçıl amaçlarla nükleer enerjiye sahip olma hakkını tanımak ve uluslararası işbirliğini teşvik etmektir. [171] Önemli olan, Antlaşmanın UAEA sorumluluğu altında oluşturduğu ve sistemin uygunluğunu doğrulayan güvenceler sistemidir. NPT günümüzde de

[169] UNODA, Treaty on the Non-Proliferation of Nuclear Weapons (NPT) : https://www.un.org/disarmament/wmd/nuclear/npt/ (20.03.18).
[170] Meyer, Paul, Saving The Npt, Non-Proliferation Review, Vol.16, No.3, 2009, p.463.
[171] IAEA, Treaty on the Non-Proliferation of Nuclear Weapons (NPT): https://www.iaea.org/sites/default/files/publications/documents/infcircs/1970/infcirc140.pdf (E.T: 21.03.18).

büyük öneme sahiptir. Zira 5 nükleer silah devleti, 2015 NPT Gözden Geçirme Konferansı'nda ortaklaşa şu hususları vurgulamışlardır: "Kırk beş yıl boyunca NPT, nükleer silahların yayılmasını önleme rejiminin temel taşı ve nükleer silahsızlanmanın kolektif takipçisi olmuştur." [172] NPT olmadan, ülkelerin nükleer silah arayışını engellemek için meşru bir uluslararası gerekçe yoktur. Bu kapsamda NPT, devletlerin ve devlet dışı aktörlerin nükleer silahların yayılmasının sürmekte olan tehdidine hitap etmenin yanı sıra uluslararası güvenliğe yönelik devam eden tehditleri ele almayı hızlandırmak için güçlü bir yasal çerçeve sunmaktadır. [173]

2.1.2.3. Nükleer Denemelerin Kapsamlı Yasaklanması Antlaşması (Comprehensive Test Ban Treaty)

Nükleer Denemelerin Kapsamlı Yasaklanması Antlaşması (CTBT), tüm nükleer patlama denemeleri yasaklayan bir antlaşmadır. Anlaşma Cenevre'deki Silahsızlanma Konferansında müzakere edilmiştir ve Birleşmiş Milletler Genel Kurulu tarafından kabul edildi. 24 Eylül 1996'da imzaya açılmıştır. Antlaşmayı 182 ülke imzalamıştır ve 26 Mayıs 2010'da da Anlaşmayı onaylayan Trinidad ve Tobago olmuştur. 154 ülke 14 Haziran 2011'de Antlaşması'nı onaylamıştır. [174]

Nükleer Denemelerin Kapsamlı Yasaklanması Antlaşması (CTBT) üç bölümden oluşan bir Protokol içermektedir: I. Bölüm Uluslararası İzleme Sistemini (IMS); II. Bölüm Yerinde Denetimler, (OSI); ve III. Bölüm Güven Oluşturma Önlemlerine İlişkin kısımları detaylandırmaktadır (CBM'ler). Protokolün de iki eki vardır: Ek 2, IMS ile ilişkili çeşitli Antlaşma izleme varlıklarının yerini detaylandırmaktadır ve Ek 3 ise tarama etkinliklerinin

[172] DoS, 2015 NPT Gözden Geçirme Konferansı Ortak Bildirisi: https://2009-2017.state.gov/r/pa/prs/ps/2015/02/237273.htm (E.T: 21.03.18).
[173] NATO, NATO and the Non-Proliferation Treaty, Fact Sheet, 2017 : https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170323_170323-npt-factsheet.pdf (E.T: 21.03.18).
[174] CTBTO, : https://www.ctbto.org/the-treaty/article-xiv-conferences/2011/afc11-information-for-media-and-press/what-is-the-ctbt/ (E.T: 21.03.18).

parametrelerini detaylandırmaktadır. [175] Antlaşmanın başarıya ulaşması, özellikle de tahkikat meseleleriyle ilgili olarak, 1958'den beri göz önüne alındığında genellikle sorunla karşılaşmıştır. Daha az görünen bir başka engel ise uluslararası politik durum olmuştur. Örneğin, 1979'da Stratejik Silahların Sınırlandırılması Müzakereleri II'nin (SALT II) tamamlanmasıyla uzmanlar, Nükleer Denemelerin Kapsamlı Yasaklanması Antlaşmasının bir sonraki mantıksal adım olduğunu ve müzakere edileceği yönünde yüksek beklentilerin olduğunu vurgulamışlardır. [176] 1993 oturumunda, Silahsızlanma Konferansı, kapsamlı bir nükleer test yasağı anlaşmasını müzakere etme yetkisine sahip bir Nükleer Deneme Yasası Komitesini kurmuştur ve Başkan'dan yeni bir müzakere yetkisi hakkında görüşmelerde bulunmasını istemiştir (bkz. A / 48/27 Sayılı Konferans Raporu). Genel Kurulun kırk sekizinci oturumunda, Birinci Komitesinin (A / 48/671) önerisini takiben, Kurul 16 Aralık 1993 tarih ve 48/70 sayılı kararı kabul ederek Ad Hoc Komiteyi Nükleer Denemelerin Kapsamlı Yasaklanması Antlaşmasını müzakere etmek üzere 1994 teki oturumunda uygun bir müzakere yetkisi ile yeniden davet etmiştir. [177] Ağustos 1993'te Cenevre'deki Silahsızlanma Konferansı'nda (CD) bulunan ülkeler Antlaşmayı imzalamaya karar vermişlerdir. [178] Silahsızlanma Konferansında şunlar kaydedilmiştir: "Nükleer Denemelerin Kapsamlı Yasaklanması Antlaşması müzakeresine ilişkin girişimler dikkate alınarak, nükleer silahların tüm yönleriyle çoğalmasının önlenmesine etkin bir şekilde katkıda bulunmak ve nükleer silahsızlanma sürecine ve dolayısıyla da uluslararası barış ve güvenlik doğrultusunda, Antlaşma evrensel ve uluslararası ve etkili bir şekilde doğrulanabilir olmalıdır. Bu hedefe ulaşmak için,

[175] NTI, : http://www.nti.org/learn/treaties-and-regimes/comprehensive-nuclear-test-ban-treaty-ctbt/ (E.T: 21.03.18).
[176] Trofimenko, Henry, SALT II: A Fair Bargain, Bull. Atomic Scıentists, June 1979, p. 30.
[177] UN, Comprehensive Nuclear Test Ban Treaty, United Nations Audiovisual Library of International Law, p.3. : http://legal.un.org/avl/ha/ctbt/ctbt.html (21.03.18).
[178] Mackby, Jenifer, Nonproliferation Verification and the Nuclear Test Ban Treaty, Fordham International Law Journal, Vol.34, No.4, 2011, pp.699-700.

bu Antlaşmanın çok taraflı müzakere edilmesi önemlidir." [179] Bununla birlikte, Antlaşmanın önemli hüküm içeren maddeleri şunlardır: [180]

Madde 1: "Antlaşmaya taraf Devletler, herhangi bir nükleer silah denemesi veya herhangi bir nükleer patlamayı gerçekleştirmemeyi ve kendi yetki alanı veya kontrolü altındaki herhangi bir yerde bu tür nükleer patlamayı yasaklayıp engellemeyi taahhüt ederler. Taraflar ayrıca, herhangi bir nükleer silah testi veya herhangi başka bir nükleer patlamanın gerçekleşmesine katılmaya, cesaretlendirmeye veya herhangi bir şekilde katılmaktan kaçınmayı taahhüt ederler."

Madde 2: "Anlaşma, karar verme için bir İcra Kurulu ve anlaşmayı uygulamak için bir Teknik Sekretarya içeren bir Nükleer Denemelerin Kapsamlı Yasaklanması Antlaşması Örgütü (CTBTO) kurulmasını öngörmektedir. Antlaşmanın yürürlüğe girdiği zamana kadar, geçici bir yasal sekretarya tarafından desteklenen ve bağımsız, uluslararası, hükümetler arası bir örgütün varlığına sahip olan imza sahibi devletlerden oluşan bir Hazırlık Komisyonu, gerekli adımların atılmış olması için 44 gerekli devletin onayını ön şart koşmaktadır."

Madde 9: "Anlaşmanın sınırsız süreye sahip olduğu şartını koşmaktadır. Ancak, çoğu silah kontrol anlaşmasıyla tutarlı olarak, bir Taraf Devletin, "anlaşmanın konusuyla ilgili olağandışı olayların kendi yüksek çıkarlarını tehlikeye attığına" karar verirse, altı aylık ihbarda bulunma hakkını saklı tutmasını da sağlamaktadır."

---

[179] UN, Conference on Disarmament, Decision on Agenda Item 1 "Nuclear Test Ban" Adopted by the Conference on Disarmament, U.N. Doc. CD/1212 (Aug. 10, 1993): http://undocs.org/CD/1212 (E.T: 21.03.18).

[180] UNODA: https://www.un.org/disarmament/wmd/nuclear/ctbt/ (E.T: 21.03.18).

Ayrıca, hedeflerinin ve amaçlarının yerine getirilip getirilmediğini belirlemek ve yürürlüğe konan yeni bilimsel ve teknolojik gelişmeleri dikkate almak için yürürlüğe girdikten 10 yıl sonra anlaşmanın gözden geçirilmesi amacıyla bir hüküm (Madde 8) bulunmaktadır.

2.2. Nükleer Santrallerin Çalışma Esasları

Nükleer enerji, mevcut ve gelecek nesiller için tüm ilgili ülkelerde ekonomik enerji hizmetlerinin erişilebilirliğine katkıda bulunabilecek güvenilir, sürdürülebilir ve çevre dostu bir enerji kaynağı olma potansiyeline sahiptir. Nükleer enerjinin herhangi bir şekilde kullanılması, insanların ve çevrenin, nükleer silahların yayılmasını önleme ve güvenliğin korunmasıyla ilgili olarak yararlı, sorumlu ve sürdürülebilir olmalıdır. [181] Nükleer santraller, temel çalışma esası olarak üç bölümden oluşmaktadır. Bunlar: 1- Yararlı Kullanım (Faydaları, Şeffaflık), 2- Sorumlu Kullanım (İnsanların ve çevrenin korunması, Güvenlik, Silahsızlanma, Uzun vadeli taahhüt), ve 3- Sürdürülebilir Kullanım (Kaynak verimliliği, Sürekli gelişim) dır. [182]

2.2.1. Nükleer Santral Kuracak Şirketin Belirlenmesi

Bir nükleer santralin kuruluşu için atılması gereken ilk adım kurucu şirketin belirlenmesidir. Belirleme işlemini takiben kurucu şirketlerin, uygun yerlerde, kirlenmiş alanların rehabilitasyonu ve radyoaktif malzemelerin kullanımı, taşınması veya elleçlenmesi gibi faaliyetler için tesislerin tasarımı, inşası, işletmeye alınması, işletilmesi ve hizmetlerinden çıkarma veya kapama işlemlerinde güvenliği sağlama sorumluluğuna sahiptir. [183] Nükleer Malzemenin

[181] IAEA, Nuclear Energy Basic Principles, Nuclear Energy Series, No. EE-BP, Vienna, 2008, p.1.
[182] IAEA, a.g.e, s.1-2.
[183] IAEA, IAEA Requirement for the Governmental Level and for the Operator: https://www.iaea.org/ns/tutorials/regcontrol/legis/legis113.htm# (E.T: 23.03.18).

Fiziki Korunmasına İlişkin Sözleşme'nin (CPPNM) 2. Maddesinin A fıkrasında, her Taraf Devletin, fiziki korumayı yönetmek için yasal ve düzenleyici bir çerçeve oluşturmasını ve sürdürmesini gerektirmektedir. Temel İlke olan 10. Maddenin D fıkrasında Devletin, yasal ve düzenleyici çerçevenin uygulanmasından sorumlu yetkili bir makamı kurmasını veya tayin etmesini gerektirdiği ve atanan sorumluluklarını yerine getirmek için yeterli yetki, yetkinlik, mali ve insan kaynaklarına sahip olması gerektiği vurgulanmaktadır.[184]

Nükleer santral sahibi / işleticisi, bir nükleer enerji santrali işletmek için ulusal mevzuata ve nükleer yönetmeliklere uygun olarak lisanslanabilen tüzel kişilik haline gelmelidir. Ruhsatlı kuruluş, tesisin ömrü boyunca nükleer güvenlik konusunda nihai sorumluluğu taşır ve sorumluluklar devredilememektedir. [185] Hükümetler eğer mutabakata devam etmeye karar verirse, sorumlu taraflar arasında gerekli altyapıların geliştirilmesini koordine etmek için hükümet bakanlıkları, düzenleyiciler ve yüklenici firma ile nükleer santral projesi için gerekli girişimler başlatılmaktadır ancak 3 aşamadan oluşan lisans süreci kurucu şirketlerin belirlenmesinde ön şarttır. Bu 3 aşamadan oluşan tablo EK 2[186] ve EK 3[187] de detaylı bir şekilde belirtilmiştir. 17 Aralık 1971 Brüksel Sözleşmesinde de nükleer mevzuatın başlıca amaçlarından biri olan ve hem uluslararası hem de yerel olarak, nükleer tesislerin operatörü üzerindeki sorumlulukları üzerine durulmuştur. [188] UAEA'nın belirlediği kriterler göz önünde bulundurularak nükleer santralleri kuracak şirketler, uluslararası hukuk açısından önemlidir ve bu hukuki çerçeve nezdinde kurucu şirketler belirlenmelidir. [189]

---

[184] IAEA, Amendment to the Convention on the Physical Protection of Nuclear Material GOV/INF/2005/10-GC (49) INF/6, , Vienna, 2005, p.9.
[185] IAEA, Responsibilities and Capabilities of a Nuclear Energy Programme Implementing Organization, IAEA Nuclear Energy Series, No. NG-T-3.6, Vienna, 2009, p.3.
[186] IAEA, a.g.e, s.5-6.
[187] IAEA, a.g.e, s.7-8.
[188] Nuclear Energy, Brussels Convention 1971, The American Journal of Comparative Law, Vol. 20, No. 3, 1972, p. 533.
[189] Foreign Relations Law, Nuclear Nonproliferation, Congress Authorizes the President to Waive Restrictions on Nuclear Exports to India, Henry J. Hyde United States-India Peaceful Atomic Energy Cooperation Act of 2006, Pub. L. No. 109-401, Tit. I, 120 Stat. 2726 (to Be Codified at 22

2.2.2. Lisanslar

Lisans konusunda UAEA'nın yaklaşımı diğer ülkeler için de örnek teşkil etmektedir. Bu bağlamda Nükleer Güvenlik Konvansiyonu 7. Maddesinde, yasama ve düzenleyici çerçevenin, nükleer tesisler ve lisanssız nükleer tesislerin işletilmesi yasağı ile ilgili bir lisans sistemi sağladığını göstermektedir. Ruhsat, düzenleyici kurum tarafından başvuru sahibine, nükleer tesislerin kurulması, tasarımı, inşaatı, işletmeye alınması veya işletilmesi için genel sorumluluğa sahip olması için verilen herhangi bir yetki anlamına gelmektedir. Lisans, nükleer tesisler ile bağlantılı olarak belirli bir faaliyet veya faaliyetler setini yetkilendiren ve bu faaliyetlerin performansını düzenleyen şart ve koşulları belirleyen resmi bir belgedir. Bu tür faaliyetler genellikle şunlardır: yer bulma, inşaat, işletmeye alma, işletme ve hizmetten çıkarma. [190] Bu bağlamda, ruhsat ve onun bir dizi koşulları çeşitli işlevleri yerine getirmektedir: lisans, kuralcı olmayan yaklaşımı izlediğinde, mevzuatın / yönetmeliğin geliştirilmesi, yorumlanması ve tamamlanması için uygun (ve en iyi) araçlar olabilir ve zorunlu hale gelecektir. Rehber ve standartların uygun bölümleri ve ayrıca başvuru sahibi tarafından yapılan özel teklifler (bu genellikle kuralların ve çözümlerin seçiminin bu tekliflere dayandığı ve onay için düzenleyici kuruluşa sunulduğu, kuralcı olmayan bir yaklaşımda geçerlidir) önem arz etmektedir. Ruhsat, uygun düzenlemelerin mevcut olmadığı hallerde, yönetmeliklere eklenen işlevlerin bir kısmını yerine getirebilmektedir. [191] Ruhsat, başvurunun değerlendirmesinin (gözden geçirilmesi ve değerlendirilmesi) nihai sonucudur ve düzenleyici kurumun sonucunu ve kararlarını kendisine göre formüle etmekte ve bu nedenle başvuru sahibine belirlenen sınırlar içinde ilerlemek için resmi izin vermektedir. Bir yandan mevzuata göre ve diğer yandan ruhsatta yer alan şartlara göre. Lisans koşulları her zaman zorunludur ve hukukun yaptırım gücüne sahiptir. Lisansa açık olarak veya

---

U.S.C. §§ 2652c, 8001-8008, and 42 U.S.C. § 2153(d))., Harvard Law Review, Vol. 120, No. 7, 2007, p. 2021.

[190] IAEA, Organization and Staffing of the Regulatory Body for Nuclear Facilities, Safety Series No. GS-G-1.1, IAEA, Vienna, 2002, p.23.

[191] IAEA, a.g.e, s.24.

referans veya ek olarak dâhil edilmeleri gerekmektedir. Lisanslar, referans veya ek olarak alıntı yaparak, mevzuatın / yönetmeliğin ve diğer ilgili belgelerle ilgili kısımları içerebilmektedir. [192] Buna ilaveten yer bulma ve lisanslama süreci önemlidir çünkü politik, sosyal, ekonomik, enerji ve çevresel çıkarların bir araya gelmesini teşvik etmektedir. [193] Lisanslama sürecinde, lisans, "başvuru sahibi" nin yeni bir dizi faaliyetine başlamanın ve "başvuru sahibi" nin "ehliyete" sahip olmanın kilit noktasındadır. Koşulları ile lisans, yaşayan bir belgedir: değişen bir duruma (örneğin, adapte edilmesi bazen gerekebilir) adapte edilebilir (örneğin, tesisin modifikasyonu; geri bildirim deneyimi; araştırmanın getirdiği yeni bilgi); ayrıca askıya alınabilmekte veya iptal edilebilmektedir. Sadece düzenleyici kurum, bir lisansı değiştirmek, askıya almak veya iptal etmek için yasal güce sahiptir. Ruhsat sahibi, lisansının değiştirilmesini isteyebilir, ancak yeni bir uygulama yoluyla bunu yapmak zorundadır.[194]Bunun yanı sıra, düzenleyici, ilgili tarafın nükleer tesisini işletmek için uygun olduğunu ("operatör" ünün atanması) nükleer bir sitedeki sorumluluk rejiminde temel öneme sahip olduğundan emin olursa, belirlenen "operatör" ün lisansını almaktan sorumlu olmalıdır. [195] EK 4[196] te bir lisans sürecinin detaylı izahatı mevcuttur.

2.2.3. Yükümlülükler

OECD, Batı Avrupa'nın çoğu ülkeleri için nükleer sorumluluk rejimini kuran Nükleer Enerji Alanında Üçüncü Taraf Sorumluluğu Sözleşmesi'ni (Paris Sözleşmesi, 1960) hazırlamak için girişimde bulunmuştur. Bu, yükümlülük sorunları ile ilgilenen ilk nükleer sözleşmelerden birisidir. Paris Sözleşmesi'ne ek olarak, 29 Temmuz 1960 tarihli Paris Sözleşmesi Ek Sözleşmesi, 1963 Sözleşmesi

[192] IAEA, a.g.e, s.24-25.
[193] Sylves, Richard T. , Carter Nuclear Licensing Reform versus Three Mile Island, Publius, Vol. 10, No. 1, 1980, p.70.
[194] IAEA, a.g.e, s.26.
[195] Grimmitt, Melanie, The Mena Nuclear Renaissance, Energy & Environment, Vol. 22, No. 1/2, 2011, p.42.
[196] IAEA, Documents Produced by the Regulatory Body for a Specific Facility: Licence Document: https://www.iaea.org/ns/tutorials/regcontrol/docum/docum5124.htm# (24.03.18).

(Brüksel Ek Sözleşmesi), orijinal Paris Sözleşmesi kapsamında garanti edilenlerden daha fazla tazminat sağlamak amacıyla kurulmuştur. Daha sonra UAEA Paris Sözleşmesi'nin ilkelerini uluslararası bir çerçevede çoğaltmaya çalışmıştır ve Nükleer Hasar için Sivil Sorumluluk Üzerine Viyana Sözleşmesi (Viyana Sözleşmesi, 1963) doğmuştur. Bu sözleşmelerdeki geniş ilkeler şu şekilde özetlenebilir: [197]

Katı yükümlülük ilkesi (katı sorumluluk);

1- Sorumluluk sadece nükleer tesis işletmecisine (yasal mecraya yönlendirme) yönlendirilir; 2- Sadece nükleer kazanın meydana geldiği devlet mahkemeleri yetkisine (münhasır yargı yetkisi) sahip olacaktır; 3 -Sorunların miktarının sınırlandırılması ve tazminat talebinin zaman çerçevesi (sınırlı sorumluluk); ve 4- İşletmenin, borç tutarı kadar sigorta veya finansal garantileri olması gerekmektedir (yükümlülük mali olarak teminat altına alınmalıdır). [198]

Yükümlülükler üzerine dikkat edilmesi gereken diğer bir husus ise nükleer sorumluluk sözleşmelerinin ortak olarak iki amaca hizmet etmesidir: Birinci amaç, bir nükleer olayın mağdurlarının, kayıpları için yeterli tazminat talep edebilmelerini ve gerçekte tazminat alabilmelerini sağlamaktır. Ancak, nükleer tesislerin işletmecilerinin sorumluluğu için azami sınırlar getirerek nükleer enerjinin sivil kullanımını sağlamak da ek bir amaçtır. Bununla birlikte, sözleşme taraflarının ulusal düzeyde daha fazla sorumluluk veya sınırsız sorumluluk sağlama zorunluluğu bulunmadığına dikkat edilmelidir. Genel olarak, nükleer sorumluluk sözleşmeleri, yükümlülüğün yerine getirildiği koşulları tanımlamakta, çözümleri belirtmekte ve tazminat için yeterli araçların mevcut olmasını sağlamaya çalışmaktadır. [199] Nükleer sorumluluk sözleşmeleri, nükleer hasar için

[197] AMACAD, Nuclear Liability: A Key Component of the Public Policy Decision to Deploy Nuclear Energy in Southeast Asia: https://www.amacad.org/content/publications/pubContent.aspx?d=1507 (E.T: 24.03.18).
[198] AMACAD, a.g.e.
[199] INLEX, Civil Liability for Nuclear Damage: Advantages and Disadvantages of Joining the International Nuclear Liability Regime, IAEA, pp.10-11.

katı bir sorumluluk rejimi getirmektedir. Mağdurların, sorumlu kişinin hatasını kanıtlama zorunluluğu yoktur. Ayrıca şu maddeler de önemlidir:

-Nükleer sorumluluk sözleşmeleri, milliyet veya bölgelere dayalı ayrımcılık yapılmamasını ve ulusal yasalar uyarınca mevcut olmayabilecek bir avantajı gerektirmektedir. [200]

-Silahlı çatışma, iç savaş, istisnai doğal afetler, terör eylemleri gibi olağanüstü durumlar bu yükümlülüğün muafiyet gerekçelerinden birkaçı olarak kabul edilmektedir. [201]

-Sorumluluk, nükleer tesis işletmecisine yönlendirilir. [202] Mağdurlar sadece tazminat almak için yalnızca operatöre başvurabilirler. [203]

-"Nükleer hasar" kavramı tekdüze olarak tanımlanmıştır. Gözden geçirilmiş ve en yeni sözleşmelerde, sadece kişisel yaralanma ve mülk hasarını değil, aynı zamanda çevrenin eski haline getirilmesi ve önleyici tedbirlerin masrafları için alınacak önlemlerin maliyetleri de dâhil olmak üzere bir takım daha ileri hasarları da içeren geniş bir anlam verilmiştir. (tazminatın kapsamı kısmen geçerli ulusal mevzuata bırakılmıştır). [204]

- Hasar ve nükleer aktivite arasındaki gerekli illiyet bağı, sözleşmelerin kendileri tarafından detaylandırılmıştır. [205]

- Sözleşmeler ispat yükümlülüğü konusunda bazı kurallar koymaktadır. [206]

---

[200] Paris Sözleşmesinin 3. Maddesi; Viyana Sözleşmesinin 4. Maddesi.
[201] Paris Sözleşmesinin 9. Maddesi; Viyana Sözleşmesinin 4. Maddesinin 2. ve 3. fıkrası.
[202] Paris Sözleşmesinin 3. ve 6. Maddesi; Viyana Sözleşmesinin 2. Maddesi.
[203] Paris Sözleşmesinin 6. Maddesinin bir istisnası gibi gözükse de ibare sigortacıya veya finansal garantöre karşı da geçerlidir.
[204] Paris Sözleşmesinin 1. Maddesi.
[205] Paris Sözleşmesinin 3. Maddesi; Viyana Sözleşmesinin 2. Maddesi.
[206] Paris Sözleşmesinin 3. ve 4. Maddesi; Viyana Sözleşmesinin 2. Maddesi.

-Sözleşmeler, sözleşme tarafları arasında serbestçe devredilebilir meblağlar gerçekleştirir. [207]

2.3. Kurucu İşletmeler ve Sözleşme Esasları

Paris Sözleşmesi operatörlere, sorumluluk rejimi, tazminat ve bu kapsamda daha birçok muhteviyat içermektedir. Kurucu işletmeler ve sözleşme esasları özelinde ise "Sivil Amaçlı Nükleer Santrallerde 3. Kişilere Verilen Zararlarda İşletenin Sorumluluğu" bu konuda uluslararası hukuki çerçeve oluşturmaktadır.

2.3.1. Sivil Amaçlı Nükleer Santrallerde Üçüncü Kişilere Verilen Zararlarda İşletenin Sorumluluğu

Hükümetler, sınır ötesi hasara neden olan bir nükleer kaza riskini uzun zamandır kabul etmektedir. Bu durum, ülkelerin ilgili sözleşmelere taraf olduğu sürece, kazaların gerçekleştiği ülke dışındaki mağdurlar için adalete erişimin kolayca sağlanabilmesi için uluslararası çerçevelerin geliştirilmesine yol açmıştır. [208] 1997'den önce, uluslararası sorumluluk rejimi öncelikle iki unsur ile somutlaşmıştır: (1) UAEA'nın 1963 tarihli Nükleer Zarar için Sivil Sorumluluk Üzerine Viyana Sözleşmesi (1977'de yürürlüğe girmiştir) ve (2) 1968'de yürürlüğe giren ve 1963'te Brüksel Ek Sözleşmesi'nin desteklediği OECD'nin 1960'daki Nükleer Enerji Alanında Üçüncü Taraf Sorumluluğuna Dair Paris Sözleşmesi. Bu Sözleşmeler, iki ülkenin coğrafi kapsamını bir araya getirmek için 1988'de kabul edilen Ortak Protokol ile ilişkilendirilmiştir. Bu düzenlemeler ise medeni hukuk kavramına dayanmaktadır ve yukarıda ana hatları verilen ilkelere bağlı kalmaktadırlar. Özellikle aşağıdaki hükümleri içermektedir: [209]

[207] Paris Sözleşmesinin 12. Maddesi; Viyana Sözleşmesinin 15. Maddesi.
[208] WNA, Liability for Nuclear Damage: http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/liability-for-nuclear-damage.aspx (25.03.18).
[209] WNA, a.g.e.

-Sorumluluk yalnızca nükleer tesislerin işletmecilerine aktarılır (yasal kanallama, operatörün özel yükümlülüğü anlamına gelmektedir ve tedarikçileri korumaktadır);

-Operatörün yükümlülüğü mutlaktır, yani "silahlı çatışma, düşmanlık, iç savaş veya ayaklanma eylemleri" haricinde, operatör hatadan bağımsız olarak sorumlu tutulur;

-Operatörün sorumluluğu tutarı sınırlıdır. Viyana Sözleşmesi kapsamında işletme sorumluluğu üst tavanı sabit değildi; ancak her bir Devletteki mevzuatla sınırlanabilmekteydi. Alt limit 5 milyon ABD dolarından az olamaz. 1960 Paris sözleşmesi kapsamında, sorumluluk 15 Milyondan fazla Özel Çekme Hakları (SDR) ile sınırlı değildir.

-Sorumluluk zamanla sınırlıdır. Genel olarak, on yıl içinde bir eylem yapılmazsa, tazminat hakları her iki Sözleşmede de ortadan kaldırılır. Ek olarak, Devletler, 1960 Paris sözleşmesi kapsamında veya iki yıldan az bir süre sonra, 1960 Viyana sözleşmesinin altında, hasarın ortaya çıktığı andan itibaren, operatörün sorumluluğunu iki yıldan az bir süre ile sınırlayamaz.

-Operatör, yükümlülüğüne veya Kurulum Devleti tarafından belirlenen limite tekabül eden bir tutar için sigorta veya diğer mali güvenliği korumalıdır, bu da, Kurulum Devletinin kamu fonları sağlayabileceği seviyenin ötesinde, aynı zamanda işletmeciye başvurabilmektedir;

-Eylemler üzerindeki yargı yetkisi, yalnızca nükleer olayı meydana gelen bölgede bulunan Akit Tarafın mahkemelerine aittir;

-Nükleer hasarın tanımı mülk, sağlık ve yaşam kaybını kapsamakla birlikte çevresel zarar, önleyici tedbirler ve ekonomik kayıp için karşılık vermemektedir. Bu, olası hak talep edenlerin toplam sayısını büyük ölçüde azaltır, ancak kalan miktar için mevcut olan tazminat seviyesini arttırmaktadır.

3. Nükleer Santrallere İlişkin Uluslararası Hukuk

Uluslararası hukuk bağlamında operatörler, tazminat ve diğer alt başlıkların dışında doğrudan nükleer santralleri düzenleyen hukuki düzenlemeler vardır. Bu başlık altında bu düzenlemeler incelenecektir.

3.1. Nükleer Santrallere İlişkin Uluslararası Hukuki Rejim Teşekkülleri

Özellikle Hiroşima ve Nagazaki de meydana gelen hasarlar ve bundan çıkarılan dersle nükleer enerji kullanımı o zamanlarda azalsa da, ilerleyen zamanlarda barışçıl kullanımı ile ilgili bir dizi düzenlemeler olmuştur. Hukuki rejim oluşturma çabaları aşamalı olarak devam etmiştir. Hukuki çerçeve oluşturma aşamalarında kimi zaman hukuki teorisyenleri, (1969) Viyana Sözleşmesi'nde Antlaşmalar Yasası ile ilgili yer alan normatif ilkelerin, birbiriyle örtüşen yargı yetkisine sahip ve eşit olmayan taraflarla yapılan anlaşmaların çoğaldığı bir dünyada artık net bir rehberlik sağlamadığını kabul etmeye başlamışlardır. [210] Ancak bağlayıcı nitelikteki bir dizi girişimler de olumlu sonuçlar vermiştir.

3.1.1. Dünyanın Nükleer Enerjiyle Tanışması ve "Barış İçin Atom" Projesi

İkinci Dünya Savaşı'ndan sonra, 8 Aralık 1953'te, ABD Başkanı Eisenhower New York'ta Birleşmiş Milletler Genel Kurulu'na hitaben "Barış için Atom" konuşmasını yapmıştır. Soğuk Savaş ve nükleer silahlanma yarışı, Başkanın konuşmasının arka planını oluşturmakta idi. Tarihçilere göre, Eisenhower sadece atom savaşının tehlikelerine odaklanmamayı tercih etmemiştir, bunun yerine tarım, tıp ve güç üretiminde sivil nükleer uygulamaların gerekliliğini

[210] Mallard, Grégoire, Crafting the Nuclear Regime Complex (1950–1975): Dynamics of Harmonization of Opaque Treaty Rules, The European Journal of International Law, Oxford University Press, Vol. 25 No. 2, 2014, p.446.

vurgulamıştır. Nükleer enerjinin barışçıl kullanımını "tüm insanlığın yararına" teşvik edecek bir "Uluslararası Atom Enerjisi Ajansı" kurulmasını önermiştir. [211] Böylelikle bu alanda hukuki rejim oluşturma anlamında ilk adım atılmış olmuştur.

3.1.2. BM Genel Kurulu

BM ve nükleer enerji neredeyse eşzamanlı olarak ortaya çıkmıştır. Hiroşima ve Nagazaki'deki nükleer patlamalarla sonuçlanan İkinci Dünya Savaşı'nın ortaya çıkardığı bilanço, nükleer enerji ile ilgili meseleleri ele alma ihtiyacını ortaya çıkarmıştır. İlk kararla, Genel Kurul atom enerjisinin keşfiyle ortaya çıkan sorunları ele almak için BM Atom Enerjisi Komisyonunu kurmuştur. [212] 1953'te Amerika Birleşik Devletleri Başkanı Dwight D. Eisenhower'ın "Barış İçin Atom" adlı konuşması, UAEA'nın 1957 yılında kurulmasına sağlamıştır. Nükleer silâhların kullanımı BM'nin kuruluş ilkelerine ve amaçlarına aykırı olduğu gibi aynı zamanda BM'nin ihlâli olarak değerlendirildiği yine BM Genel Kurulu kararlarında yinelenmiştir. [213]

3.1.3. BM İnsan Hakları Komitesi

10 Aralık 1948'de Birleşmiş Milletler Genel Kurulu, İnsan Hakları Evrensel Beyannamesi'ni kabul ettikten hemen sonra ilan etmiştir. BM Evrensel İnsan Hakları Beyannamesinin 3. maddesi uyarınca "herkesin yaşam hakkı, özgürlüğü ve güvenliği vardır." [214] Daha sonra BM İnsan Hakları Komitesi bu konu hakkında kapsamlı çalışmalar yürütmüştür. Nükleer silahlarla ilgili yaşam hakkı

[211] IAEA, 60 Years of "Atoms for Peace", 2013: https://www.iaea.org/newscenter/news/60-years-atoms-peace (25.03.18).
[212] UN, Atomic Energy: http://www.un.org/en/sections/issues-depth/atomic-energy/ (25.03.18).
[213] BM Genel Kurulunun A/RES/1653 (XVI) sayılı Kararı, Nükleer ve Termo-nükleer Silahların Kullanımının Yasaklanması Bildirgesi, 24 Kasım 1961: https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/167/06/IMG/NR016706.pdf?OpenElement (25.03.18).
[214] BM, Evrensel İnsan Hakları Beyannamesi: http://www.un.org/en/universal-declaration-human-rights/index.html (25.03.18).

üzerine Uluslararası Medeni ve Siyasi Haklar Sözleşmesi'nin 6. Maddesinin 36 No'lu genel yorumunda şu şekilde bahsetmiştir:

"Özellikle hayati tehlike altında olan ve insan hayatını felaketle yok eden kitle imha silahlarının kullanımı özellikle de nükleer silahlar, yaşam hakkına saygı ile bağdaşmaz ve uluslararası hukuka göre suç teşkil etmektedir. Taraf Devletler, devlet dışı aktörler tarafından elde edilmelerini önleme tedbirleri de dâhil olmak üzere kitle imha silahlarının çoğalmasını durdurmak, bunları üretmekten, test etmekten, depolamaktan ve mevcut stokları imha etmekten kaçınmak için uluslararası yükümlülüklerine uygun olarak gerekli tüm tedbirleri almalıdır. Ayrıca, sıkı ve etkili uluslararası denetim altında nükleer silahsızlanma amacına ulaşmak için iyi niyetle müzakerelere devam etme konusundaki uluslararası yükümlülüklerine saygı göstermelidirler." [215] Bu bağlamda, BM İnsan Hakları Komitesi, nükleer enerjinin nasıl kullanılması gerektiği yönünde referans alınabilecek bir açıklamada bulunmuştur. Bu durum da, nükleer enerjinin insani amaçlarla kullanılması gerekliliği yönünde uluslararası hukuki bir çerçeve oluşturmaktadır.

3.1.4. Uluslararası Adalet Divanı

UAD'nın kararı, nükleer enerjinin hangi amaçlarla kullanılabileceği yönünde kritik öneme haizdir. Zira nükleer enerji kullanımındaki suç unsurları için de verdiği karar ya da görüşler emsal teşkil etmektedir ve birçok kurum ve kuruluşlar için bir yol haritası çizmektedir. 19 Aralık 1994 tarihli ve 6 Ocak 1995 tarihli Sicil Dairesi'nde, BM Genel Sekreteri, 15 Aralık 1994 tarihinde kabul edilen 49/75 K kararıyla Genel Kurul tarafından alınan kararı resmen Genel Sekreterliğe iletmiştir. Mahkeme'ye danışma başvurusunda bulunmak için aşağıdaki soruya

[215] Human Rights Committee, General comment No. 36 on article 6 of the International Covenant on Civil and Political Rights, on the right to life: Revised draft prepared by the Rapporteur: http://www.ohchr.org/Documents/HRBodies/CCPR/GCArticle6/GCArticle6_EN.pdf (25.03.18).

atıfta bulunulmuştur: "Uluslararası hukuk uyarınca her türlü koşulda nükleer silahların tehdidi veya kullanımı söz konusu mudur?" Karar, Mahkemeden "ivedi" tavsiye kararını vermesini istemiştir. Yazılı ifadeler 28 Devlet tarafından dosyalanmıştır ve daha sonra bu ifadelere ilişkin yazılı gözlemler iki Devlet tarafından sunulmuştur. Ekim ve Kasım 1995'te gerçekleşen sözlü yargılama sürecinde, 22 Devlet sözlü ifadeler sunmuştur. [216] UAD'nin yapmış olduğu çalışmalara göre nükleer silâhların kullanılması veya tehdit unsuru olarak kullanmanın uluslararası hukuk kuralları ile bağdaşmayacağı yönündedir. Ancak, mevzu bahis durumla uluslararası hukukta mutlak bir hüküm bulunmamaktadır. Bu uluslararası kuruma göre nükleer silâhların yasaklanması devletlerin hukuki yükümlülüklerinde olan bir olgudur [217]. Dünya Sağlık Örgütü 1993 yılında, Nükleer silâhlarla ilgili ilk danışma görüşü başvurusu yapan kuruluş olmuştur. [218] Çevre ve sağlık konusundaki etkilerinden dolayı herhangi bir devletin nükleer silâh kullanımının meşruiyeti ve uluslararası hukuka aykırı olup olmadığı konusunda hukuki yardım talebinde bulunmuştur. [219] Ancak bu başvuru nükleer silâhların "yasallığı" konusunda olmadığından dolayı bu örgütün danışma görüşü isteme yetkisinde olmadığı gerekçesiyle reddedilmiştir[220]. Bu konu daha sonra 1994 tarihinde BM Genel Kurulu tarafından UAD'nin önüne getirilmiştir. Nükleer silâhların kullanılması veya kullanma tehdidinde bulunması hukukiliği konusunda UAD danışma görüşünü 1996'da açıklamıştır. [221] Bu bağlamda mahkemenin

[216] ICJ, Legality of the Threat or Use of Nuclear Weapons : http://www.icj-cij.org/en/case/95 (25.03.18).
[217] ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, July 8, 1996, ICJ Rep. 1996, p. 226: http://www.icj-cij.org (25.03.18).
[218] Denk, Erdem, Bir Kitle İmha Silâhı Olarak Nükleer Silâhların Yasaklanmasına Yönelik Çabalar, Ankara Üniversitesi, SBF Dergisi, C. 66, S. 3, 2011. s. 115.
[219] Burroughs, John, Looking Back: The 1996 Advisory Opinion of the International Court of Justice, Arms Control Association, 2016: https://www.armscontrol.org/ACT/2016_07/Features/Looking-Back-The-1996-Advisory-Opinion-of-the-International-Court-of-Justice (25.03.18).
[220] Norouizi, a.g.t., s.43.
[221] Nicholas Rostow, The World Health Organization, the International Court of Justice, and Nuclear Weapons, Yale Yale Journal of International Law, Vol. 20, No.1, 1995, p.154-155.

verdiği karar önem arz etmektedir. Kararın 105. Paragrafta geçen maddeleri mahkemenin ilgili konuda yaklaşımını göstermektedir. Bunlar: [222]

A. Oybirliğiyle,

"Uluslararası Ceza Hukuku ve Uluslararası Teamül Hukukunda, nükleer silahların tehdidi veya kullanımıyla ilgili herhangi bir özel yetki yoktur";

B. 11/3 Oy

"Uluslararası Ceza Hukuku ve Uluslararası Teamül Hukukunda, nükleer silahların tehdidi veya kullanımı gibi kapsamlı ve evrensel herhangi bir yasak yoktur";

C. Oybirliğiyle,

"Birleşmiş Milletler Sözleşmesinin Md. 2/4 te aykırı olan ve Madde 51'in gereklerini yerine getiremeyen nükleer silahlar aracılığıyla bir tehdit veya güç kullanımı kanuna aykırıdır";

D. Oybirliğiyle,

"Herhangi bir tehdidin veya nükleer silahların kullanımının, özellikle uluslararası insan hakları prensipleri ve kurallarının yanı sıra, açıkça anlaşmaya varılan antlaşmalar ve diğer nükleer silah teşebbüslerinin altında özel yükümlülükler taşıyan silahlı çatışmalarda uygulanacak uluslararası hukukun gerekliliklerileyle de uyumlu olması gerekmektedir";

E. 7/7 Oyla ve Başkanın oyuyla,

[222] ICJ, Legality Of The Threat Or Use Of Nuclear Weapons, Reports Of Judgments, Advisory Opinions And Orders, 8 July 1996, pp.43-45.

"Yukarıda belirtilen gerekliliklerden, nükleer silahların tehdidi veya kullanımının, genellikle silahlı çatışmalarda uygulanan uluslararası hukuk kurallarına ve özellikle de insani hukukun ilke ve kurallarına aykırı olduğu";

"Bununla birlikte, uluslararası hukukun mevcut durumu ve gerçekte emrinde olan unsurları göz önünde bulundurulduğunda, Mahkeme, nükleer silahların tehdidi veya kullanımının, bir Devletin bekasının tehlikede olacağı meşru müdafaa ile ilgili olası bir durumda, durumum hukukiliği veya hukuka aykırı olup olmayacağına kesin olarak karar veremez";

F. Oybirliği ile,

"İyi niyetle ilerlemek ve sıkı ve etkili uluslararası denetim altında nükleer silahsızlanmaya yol açan bir sonuç müzakerelerine varmak için bir zorunluluk vardır."

UAD, nükleer silah kullanımının (ve bunun da nükleer kullanım tehdidi anlamına geldiğini), uluslararası hukuk ilkeleri, Birleşmiş Milletler (BM) Sözleşmesi, silahlı çatışma yasası çerçevesinde değerlendirilmesi gerektiğini belirtmiştir. Mahkemenin görüşüne göre, nükleer kullanım muhtemelen muhariplere ve sivillere yönelik saldırılara gereksiz acı çekmekle sonuçlanacak ve böylece insan hakları hukukunun iki temel ilkesini ihlal edecektir. [223] Ancak bir devletin nükleer silâhları kullanmasını ya da kullanım tehdidinde bulunmasıyla ilgili uluslararası sözleşmelerden ve teamüllerden kaynaklanan beynelmilel ve açık bir yasaklamanın olmadığı belirtilmiştir. Konunun hukukiliği konusunda UAD'nin kesin bir hüküm vermemesinden kaynaklanan muğlaklık sorunu doğmuştur.[224] Ancak, Divan bu kararında meşru müdafaa[225] gibi silahlı kuvvet

[223] Farrell, Theo, / Hélène Lambert, Courting Controversy: International Law, National Norms and American Nuclear Use, Review of International Studies, Vol. 27, No. 3, 2001, p. 309.
[224] Weiss, Peter, The American Journal of International Law, The American Journal of International Law, Vol. 94, No. 4, 2000, p. 816.

kullanmanın hukuki esaslara dayanmasını ve buna uygun olması için orantılı olan bir kuvvet kullanılmasını ve insani olmasını belirtmiştir.

3.1.5. Uluslararası Atom Enerjisi Ajansı

UAEA Statüsü, BM Genel Merkezinde düzenlenen Uluslararası Atom Enerjisi Ajansı Tüzüğü ile 23 Ekim 1956 tarihinde onaylandı. 29 Temmuz 1957'de yürürlüğe girmiştir. Tüzük, XVIII. Maddenin A ve C paragraflarında belirtilen prosedürün uygulanmasıyla üç kez değiştirilmiştir. [226] 31 Ocak 1963'te, Madde VI 'ün A.3 fıkrasının ilk cümlesindeki bazı değişiklikler yürürlüğe girmiştir; Değiştirilen tüzük, aynı maddenin (A paragrafının alt paragraflarının yeniden numaralandırılması dâhil) A ila D fıkralarında yapılan bazı değişikliklerin yürürlüğe girmesiyle 1 Haziran 1973'te değiştirilmiştir; 28 Aralık 1989'da A.l. paragrafın giriş bölümünde bir değişiklik yürürlüğe girmiştir. Tüm bu değişiklikler, daha önceki tüm sürümlerin yerine geçen Statü metninde yer almıştır. [227] Uluslararası Atom Enerjisi Ajansının amaçları ise şu şekilde zikredilmektedir: [228]

-Nükleer işbirliği için küresel odak noktası olarak hizmet veren Birleşmiş Milletler ailesinde bağımsız hükümetler arası, bilim ve teknoloji tabanlı bir organizasyondur;

-Üye Devletler, sosyal ve ekonomik hedefler bağlamında, nükleer bilim ve teknolojiyi, elektrik üretimi de dâhil olmak üzere çeşitli barışçıl amaçlarla

---

[225] UN, Chapter VII: Action With Respect To Threats To The Peace, Breaches Of The Peace, and Acts Of Aggression, Article 51: http://www.un.org/en/sections/un-charter/chapter-vii/ (25.03.18).
[226] David Fischer, History of The International Atomic Energy Agency, Vienna, A Fortieth Anniversary Publication, September1997, p.9.
[227] IAEA, History: https://www.iaea.org/about/overview/history (25.03.18).
[228] IAEA, The IAEA Mission Statement: https://www.iaea.org/about/mission (25.03.18).

planlamayı ve kullanmayı planlamakta ve bu teknoloji ve bilginin sürdürülebilir bir şekilde gelişmeye aktarılmasını kolaylaştırmaktadır. Üye devletler;

-Nükleer güvenlik standartları ve bu standartlara dayanarak, nükleer enerjinin uygulamalarında yüksek güvenlik seviyelerinin elde edilmesinin ve sürdürülmesinin yanı sıra insan sağlığının ve çevrenin iyonlaştırıcı radyasyona karşı korunmasını teşvik eder;

-Denetleme sistemi aracılığıyla Devletlerin, Nükleer Silahların Yayılmasını Önleme Antlaşması ve diğer nükleer silahların yayılmasını önleme anlaşmaları çerçevesinde, nükleer malzeme ve tesisleri yalnızca barışçıl amaçlarla kullanacaklarına dair taahhütlerini yerine getirdiğini göstermektedir.

Bu bilgiler ışığında, UAEA tarafından desteklenen küresel güvenlik rejimi, kısmen çeşitli hükümetler arası yasal araçlara dayanmaktadır. Dünya çapında yüksek güvenlik ve güvenliği sağlamak için tasarlanan bu yasal araçlar, doğada farklıdır. Bunlar arasında yasal olarak bağlayıcı olan Davranış Kurallarına, Antlaşmalar ve Sözleşmelerin de yanı sıra yasal olarak bağlayıcı olan Sözleşmeler bulunmaktadır. 1986'da Nükleer, Radyasyon, Ulaştırma ve Atık Güvenliği alanlarında beş sözleşme onaylanmıştır: [229]

-Nükleer Bir Kaza veya Radyolojik Acil Durumda Yardım Konvansiyonu[230] nükleer kazalar veya radyolojik acil durumlar için hızlı yardım ve destek sağlamak amacıyla Taraflar arasında ve UAEA ile işbirliği için uluslararası bir çerçeve hazırlamaktadır.

[229] IAEA, Nuclear Safety & Security: Conventions and Codes: http://www-ns.iaea.org/conventions/ (E.T: 25.03.18).
[230] IAEA: https://www.iaea.org/topics/conventions-on-emergency-preparedness-and-response#2 (E.T:25.03.18).

-Nükleer Güvenliğe ilişkin Sözleşme, [231] taraf devletlerin nükleer santralleri faaliyete geçirecek uluslararası ölçütler belirleyerek yüksek güvenlik düzeyini korumak için kara-bazlı nükleer santralleri işletmelerini yasal olarak taahhüt eder.

-Nükleer Malzemenin Fiziki Korunmasına İlişkin Sözleşme, [232] Akit Devletlerin uluslararası nükleer taşımacılık sırasında kendi toprakları dâhilinde nükleer malzemenin korunmasını veya gemilerinde veya uçaklarında bulunmasını temin etmesini zorunlu kılar.

-Nükleer Kaza veya Radyolojik Acil Durumun Erken Bildirimi Konvansiyonu[233] bir başka devlet için radyolojik güvenlik anlamında olabilecek uluslararası sınır aşan serbestleşme potansiyeline sahip nükleer kazalar için bir bildirim sistemi kurmaktadır.

-Tüketilen Yakıt Yönetiminin Güvenliği ve Radyoaktif Atık Yönetiminin Güvenliğine Dair Ortak Sözleşme, [234] bu alanlarda güvenliğe ilişkin ilk yasal bağlayıcı uluslararası sözleşmedir. İnsanların ve çevrenin korunması için küresel güvenlik rejiminin bir parçası olarak kullanılmış yakıtların ve radyoaktif atıkların yönetiminde sürekli yüksek bir güvenlik düzeyine ulaşma ve sürdürme konusunda katılımcı Devletlerin taahhüdünü temsil eder.

3.1.6. OECD – Nükleer Enerji Ajansı

İkinci Dünya Savaşı sonrası Avrupa ekonomik toparlanmasının ve özellikle nükleer enerjinin sunduğu olasılıkların hızla artan enerji ihtiyaçları[235] ile ilgili olarak, OECEC Konseyi (OECD'nin öncülü) 1958 Şubat ayında Avrupa Nükleer

[231] IAEA: http://www-ns.iaea.org/conventions/nuclear-safety.asp?s=6&l=41 (E.T:25.03.18).
[232] IAEA: https://www.iaea.org/topics/nuclear-security-conventions (E.T:25.03.18).
[233] IAEA: https://www.iaea.org/topics/conventions-on-emergency-preparedness-and-response (E.T:25.03.18).
[234] IAEA: http://www-ns.iaea.org/conventions/waste-jointconvention.asp?s=6&l=40 (E.T:25.03.18).
[235] NEWS: NEA/OECD Report on Radiological Impact Of Chernobyl Accident, Current Science, Vol. 57, No. 9, 1988, p. 471.

Enerji Ajansı'nı (ENEA) kurdu. Ajansın adı, 1972 yılında Avrupa'nın sınırlarının ötesinde büyüyen üyeliğini yansıtmak için Nükleer Enerji Ajansı (NEA) olarak değiştirilmiştir. [236] Nükleer Enerji Ajansı (NEA), nükleer güvenlik, teknoloji, bilim, çevre ve yasalarda mükemmelliği sağlamak için gelişmiş nükleer teknoloji altyapılarına sahip ülkeler arasında işbirliğini kolaylaştıran bir hükümetler arası kuruluştur. Ekonomik İşbirliği ve Kalkınma Örgütü çerçevesinde yer alan NEA, Fransa'nın Paris kentinde bulunuyor. Stratejik Planında da belirtildiği gibi NEA'nın amacı "Nükleer enerjinin barışçıl amaçlar için güvenli, çevreye duyarlı ve ekonomik kullanımı için gerekli olan bilimsel, teknolojik ve hukuki dayanaklarla, üye ülkelere uluslararası işbirliğini sürdürmek ve daha da gelişmesine yardımcı olmak için geniş kapsamlı OECD analizleri gibi temel konularda ortak anlayışlar oluşturmaktır." [237]

3.2. Sorumluluk Rejimi ve Uluslararası Anlaşmalar

Sivil nükleer sorumluluk rejimini tasvir eden iki uluslararası sözleşme, 29 Temmuz 1960 tarihli Nükleer Enerji Alanında Üçüncü Şahıslara Karşı Hukuki Sorumluluğu Dair Paris Sözleşmesi ve 21 Mayıs 1963'te Nükleer Zararlar Hakkında Hukuki Sorumluluğa Dair 1963 Tarihli Viyana Sözleşmesi vardır. Bu iki sözleşme, benzer nitelikte olup, her ikisi de nükleer bir kaza durumunda mağdurlar için bir tazminat planına sahiptir. Sözleşmelerin ana ilkeleri şunlardır: operatörün katı yükümlülüğü, işleticiye özel sorumluluk kanalı, zorunlu mali güvenlik, sorumluluk sınırları, bir hak talebi için zaman sınırı ve nükleer olayın meydana geldiği devlette özel mahkeme yargı yetkisidir. [238] Aşağıdaki alt başlıklarda daha ayrıntılı açıklamalar yapılacaktır.

---

[236] OECD-NEA, History of the OECD Nuclear Energy Agency: https://www.oecd-nea.org/general/history/ (25.03.18).
[237] OECD-NEA, The Nuclear Energy Agency: https://www.oecd-nea.org/general/about/ (E.T: 25.03.18).
[238] Goedde, Patricia, In Search of A Civil Nuclear Liability Regime For North Korea, Asian Perspective, Vol. 27, No. 1, 2003, p.227.

3.2.1. Üçüncü Şahıslara Karşı Hukuki Sorumluluğa İlişkin Paris Sözleşmesi

Paris Sözleşmesi, herhangi bir nükleer kazanın mağdurlarını tazmin etmek için bir nükleer sorumluluk ve tazminat rejimi kurmaktadır. Paris Sözleşmesi, Paris Sözleşmesine taraf olan tüm tarafların rızasıyla, üye olmayan ve doğru üye olmayan ülkelere OECD üye ülkelerine açıktır. [239] Normal bir hukukun bu alandaki belirli sorunlara çözüm getirmek için uygun olmadığı için, nükleer üçüncü şahıslara karşı sorumlu olan özel bir uluslararası rejim gerektirmiştir. Paris Sözleşmesini tasarlayanlar, nükleer bir kazadan kaynaklanan zararlar için kamuya yeterli tazminat sağlamaya ve nükleer endüstrinin büyümesinin sorumluluk yükü taşıyarak engellenmemesini sağlamaya karar vermiştir. [240] Sözleşme, bir dizi önemli ilke üzerine kurulmuş özel bir hukuk rejimini kurmaktadır ve bunlar: [241]

-Nükleer tesis operatörü, tesisindeki kazalardan veya nükleer maddelerin o tesise taşınması sırasında meydana gelen hasarlardan sorumludur. [242]

-Bu sorumluluk, ihmal veya ihmali temel alan genel haksız fiilin aksine "katı" dır. Paris Sözleşmesi kapsamında, bir arıza tesis edilip edilmeyeceğine bakılmaksızın, bu sorundan nükleer tesis operatörü sorumludur.

- Bir nükleer tesis işletmecisinin maksimum yükümlülüğü 15 milyon SDR [243] 'dir ve asgari yükümlülük 5 milyon SDR'dir. Ancak, NEA, Paris

[239] Radetzki, Marcus, Limitation of Third Party Nuclear Liability Causes, Implications and Future Possibilities. Nuclear Law Bulletin, Vol.63, 1993, pp.7-8.
[240] Cigoj, Stojan, International Regulation of Civil Liability for Nuclear Risk, The International and Comparative Law Quarterly, Vol. 14, No. 3, 1965, p. 809.
[241] OECD-NEA, Paris Convention on Nuclear Third Party Liability: https://www.oecd-nea.org/law/paris-convention.html (25.03.18).
[242] 1960 Tarihli Paris Sözleşmesi 1.Madde: https://www.oecd-nea.org/law/Unofficial%20consolidated%20Paris%20Convention.pdf (E.T: 25.03.18).
[243] Paris Sözleşmesi'nde kullanılan hesap birimi, Uluslararası Para Fonu (IMF) tarafından kilit uluslararası para birimlerine dayanan bir hesap birimi olan Özel Çekme Hakkıdır. SDR'nin para birimi değeri günlük olarak hesaplanır ve değerleme sepeti beş yılda bir gözden geçirilir ve ayarlanır.

Sözleşmesi devletlerinin azami yükümlülük tutarını 150 milyon SDR'den daha az olmamasını tavsiye etmiştir; çoğu devlet te o şekilde hareket etmiştir. [244]

-Nükleer tesis işletmecisi, yükümlülüğüne eşdeğer bir finansal güce sahip olmalıdır.

-Nükleer kazanın on yılı içerisinde yasal işlem yapılmazsa tazminat hakkı sona ermektedir.[245]

-Sözleşme, uyruk ya da muhit temelli herhangi bir ayrım yapılmaksızın uygulanmalıdır.

-Genel olarak, nükleer kazaların meydana geldiği devlet mahkemeleri tazminat talepleriyle ilgilenmektedir.

Bu sözleşmede vurgulanan unsurlar, kurucu işletmeler ve operatörlere katı yükümlülükler getirmektedir ve kaza tazminatlarıyla ilgili muhteviyatlar içermektedir.

3.2.2. Nükleer Zararlar Hakkında Hukuki Sorumluluğa İlişkin 1963 Tarihli Viyana Sözleşmesi

Nükleer Zararlar Hakkında Hukuki Sorumluluğa İlişkin 1963 Tarihli Viyana Sözleşmesi Uluslararası Atom Enerjisi Ajansı tarafından hazırlanarak onaylamaya tabi olan Sözleşme ve Protokol, tarafların katılımıyla düzenlenen bir konferansta kabul edilmiştir. [246] 21 Mayıs 1963'te kabul edilerek ve aynı gün imza için açılmıştır. 12 Kasım 1977'de yürürlüğe girmiştir, yani, beşinci onaylama aracının

[244] 1960 Tarihli Paris Sözleşmesi 7.Madde.
[245] 1960 Tarihli Paris Sözleşmesi 8.Madde.
[246] Cigoj, Stojan, International Regulation of Civil Liability for Nuclear Risk, The International and Comparative Law Quarterly, Vol. 14, No. 3, 1965, p.810.

Genel Direktörüne tevdi tarihinden üç ay sonra, XXIII. Madde uyarınca yürürlüğe girmiştir. [247] Nükleer Zararlar Hakkında Hukuki Sorumluluğa İlişkin 1963 Tarihli Viyana Sözleşmesi aynı zamanda nükleer hasara karşı sivil sorumluluk ile ilgili önemli uluslararası düzenlemelerden faydalanıp[248] bir sentez ortaya koyduğu için önemlidir. [249] Bu sözleşme Medeni hukuk mefhumuna dayanarak aşağıdaki ana ilkeleri paylaşır:

- Bir nükleer tesis işletmecisi, nükleer bir hasardan dolayı bu tür bir hasara neden olduğunun ispatıyla nükleer hasardan sorumludur; [250]

- Operatörün sorumluluğu mutlaktır, yani operatör arızadan bağımsız olarak sorumlu tutulur; [251]

-Sorumluluk tutarı sınırlıdır. Viyana Sözleşmesi kapsamında, 5 milyon ABD dolarından az olmamak üzere sınırlandırılabilir, ancak üst tavan sabit değildir. Paris Sözleşmesi, kurulum devletinin sigorta kapsamının mevcudiyetini göz önünde bulundurarak 5 milyon SDR'nin altında veya daha az bir miktar sağlaması koşuluyla, azami 15 milyon SDR yükümlülüğü getirmektedir. Brüksel Ek Sözleşmesi, Paris Sözleşmesi kapsamındaki mevcut miktarın ötesinde, kuruluşun ve sözleşmeci tarafların katkılarından oluşan toplam 300 milyon SDR'ye kadar ek fonlar kurmuştur;

[247] IAEA, Vienna Convention On Civil Liability for Nuclear Damage: https://www.iaea.org/sites/default/files/infcirc500.pdf (25.03.18).
[248] Handrlica Jakub, [Я., ХЭНДРЛИКА], Ядерные Технологии И Международная Ответственность В Рамках Венской Конвенции О Гражданской Ответственности За Ядерный Ущерб: Правовые Проблемы [Nuclear technologies and the international liability framework of the Vienna Convention on Civil liability for nuclear damage: legal problems revisited], Вестник Омского университета. Серия «Право», No. 1 (46), 2016, p.113.
[249] Gorove, Stephen, International Conventions on Civil Liability for Nuclear Damage, The American Journal of International Law, Vol. 62, No. 2, 1968, p.543.
[250] 1963 Tarihli Viyana Sözleşmesinin 2. Maddesi.
[251] 1963 Tarihli Viyana Sözleşmesinin 4. Maddesi.

-Sorumluluk zamanla sınırlıdır. Nükleer olay tarihinden itibaren on yıl içinde herhangi bir eylem yapılmazsa, tazminat hakları her iki Sözleşmede de ortadan kaldırılır. Kurulum Devletinin yasası uyarınca, işleticinin yükümlülüğü mali güvence kapsamındaysa, daha uzun süreler kabul edilebilir. Ulusal hukuk, daha az bir zaman sınırı oluşturabilir, ancak en az iki yıldan (Paris Sözleşmesi) veya üç yıldan (Viyana Sözleşmesi) talep sahibinin hasardan ve operatörden sorumlu olduğunu bilmesi gerekmektedir. [252]

Viyana Sözleşmesinde dikkat çeken değişiklikler, Paris Sözleşmesinde sorumluluk tutarının üst sınırı 150 Milyon SDR iken, Viyana Sözleşmesinde bu tutar 300 Milyon SDR ye kadar çıkartılmıştır. Bununla birlikte Viyana Sözleşmesi, sorumluluk kapsamını genişleterek Paris Sözleşmesini güncel bir hale getirmiştir.

3.2.3. 1964 Tarihli Paris Sözleşmesini Yenileyen Brüksel Ek Sözleşmesi

Bu Protokol, diğerlerinin yanı sıra nükleer hasarın daha iyi tanımlanmasını içermekte, çevresel hasar ve önleyici tedbirler kavramını ele almakta, 1963 Viyana Sözleşmesi'nin coğrafi kapsamını genişletmekte ve yaşam kaybı ve kişisel yaralanmalar için iddiaların getirilebileceği süreyi uzatmaktadır. [253] Paris Sözleşmesi fonlarının yetersiz kaldığı bir nükleer olay sonucu tazminatın telafi edilmesi için ek fon sağlamak amacıyla 29 Temmuz 1960 tarihli Paris Sözleşmesi Ek Sözleşmesi ("Brüksel Ek Sözleşmesi") 1963 yılında kabul edilmiştir. Brüksel Ek Sözleşmesi, kamu fonlarının sadece sorumlu işletmecinin nükleer tesisinin

[252] 1963 Tarihli Viyana Sözleşmesinin 6. Maddesi.
[253] Johnson, Larry D., International Atomic Energy Agency: Diplomatic Conference to Adopt A Protocol to Amend the Vienna Convention on Civil Liability for Nuclear Damage and to Adopt A Convention on Supplementary Funding, International Legal Materials, Vol. 36, No. 6, 1997, pp. 1454–1455.

bulunduğu devlet tarafından değil, bütün tarafların Brüksel Ek Sözleşmesi'ne yaptığı katkılarla da sağlanmasını öngörmektedir. Sözleşme böylece taraflar arasında güçlü bir mali dayanışma bağına dayanmaktadır. [254] Brüksel Ek Sözleşmesi, "nükleer kaza", "nükleer tesis", "nükleer maddeler" ve "nükleer hasar" kavramlarını tanımlayanlar başlık ve maddeler dâhil olmak üzere Paris Sözleşmesi'nde yer alan hükümlere tabidir. Coğrafi uygulama alanı, sözleşmeli bir devletin topraklarında meydana gelenler dışındaki nükleer olayların neden olduğu, ihale taraflarından birinin veya denizlerin üzerinde veya üzerinde meydana gelen hasarlarla sınırlıdır. [255] Paris / Brüksel rejimi, üç aşamada maksimum 300 milyon SDR'ye tazminat ödenmesini öngörmektedir:

- Paris Sözleşmesi uyarınca getirilen borç miktarına tekabül eden birinci seviye, yani Brüksel Tamamlayıcı Sözleşmesi'ne taraf olan her bir Tarafın, sigorta veya diğer finansal güvenlik tarafından sağlanacak olan en az 5 milyon SDR'lik bir işletme yükümlülüğü kanunu ile tesis edilmesi gerektiği anlamına gelmektedir. [256]

- 175 milyon SDR ile birinci kademe kapsamındaki tutar arasındaki farktan oluşan ikinci aşama, sorumlu bulunduğu ülkenin nükleer tesisinin bulunduğu bölgedeki kamu fonlarından sağlanacaktır; [257]

- Kamu fonlarından temin edilebilecek 125 milyon SDR'den oluşan üçüncü aşama, önceden belirlenmiş bir formüle göre bütün tarafların Brüksel Tamamlayıcı Sözleşmesi'ne ortak olarak katkıda bulunmaktadır.

---

[254] OECD-NEA, Brussels Supplementary Convention: https://www.oecd-nea.org/law/brussels-supplementary-convention.html (25.03.18).
[255] OECD-NEA, Convention of 31st January 1963 Supplementary to the Paris Convention of 29th July 1960, as Amended by the additional Protocol of 28th January 1964 and by the Protocol of 16th November 1982 ("Brussels Supplementary Convention"), : https://www.oecd-nea.org/law/nlbrussels.html (25.03.18).
[256] 1964 Tarihli Paris Sözleşmesini Yenileyen Brüksel Ek Sözleşmesi 3. Maddesi 2. Fıkrasının 1.Bendi.
[257] 1964 Tarihli Paris Sözleşmesini Yenileyen Brüksel Ek Sözleşmesi 3. Maddesi 2. Fıkrasının 2.Bendi.

Hâlihazırda Paris Sözleşmesi'ne taraf olmayan bir ülke olmadıkça, Brüksel Ek Sözleşmesi'ne herhangi bir devlet bir sözleşme tarafı olamaz. Brüksel Ek Sözleşmesi, Paris Sözleşmesi'nin de yürürlükte kaldığı sürece yürürlükte kalması yönünde nihai karara bağlanmıştır. [258]

3.2.4. Nükleer Enerji Alanında Üçüncü Şahıslara Karşı Hukuki Sorumluluğa ilişkin Paris Sözleşmesi'ni Yenileyen 1982 Ek Protokolü

Nükleer Enerji Alanında Üçüncü Şahıslara Karşı Hukuki Sorumluluğa ilişkin Paris Sözleşmesi'ni Yenileyen 1982 Ek Protokolü Federal Almanya Cumhuriyeti Hükümeti, Avusturya Cumhuriyeti, Belçika Krallığı, Danimarka Krallığı, İspanya Krallığı, Finlandiya Cumhuriyeti, Fransız Cumhuriyeti, Yunan Cumhuriyeti, İtalya Cumhuriyeti, Büyük Lüksemburg Dükalığı, Norveç Krallığı, Hollanda Krallığı, Portekiz Cumhuriyeti, İngiltere Büyük Britanya ve Kuzey İrlanda, İsveç Krallığı, İsviçre Konfederasyonu ve Türkiye Cumhuriyeti ülkelerinin bir araya gelerek oluşturdukları ek protokoldür. [259] İşbu Protokol, Sözleşmeci Devletlerin topraklarında meydana gelen nükleer kazalar veya bu tür bir bölgede maruz kaldığı Madde 6 (e) 'de belirtilen haklarla ilgili olarak zararlar için geçerli değildir. [260] Bu protokolün nükleer kaza ve sorumluluk rejimi ile alakalı önemli sayılabilecek maddeleri şunlardır:

---

[258] OECD: https://legalinstruments.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=197&Lang=en&Book=False (25.03.18).

[259] A.g.k

[260] OECD-NEA: Convention on Third Party Liability in the Field of Nuclear Energy of 29th July 1960, as amended by the Additional Protocol of 28th January 1964 and by the Protocol of 16th November 1982 : https://www.oecd-nea.org/law/nlparis_conv.html (25.03.18).

- Bir nükleer tesis işletmecisi için bu Sözleşmeye uygun olarak sorumluluk konuları: (1) herhangi bir kişinin yaşam veya hayat kaybı ve (2) dışındaki herhangi bir mülkün zarar görmesi veya kaybolması; [261]

- Nükleer yakıt ya da radyoaktif ürünler ya da nükleer bir olaya karışan atıklar birden fazla nükleer tesis içerisinde bulunuyorsa ve nükleer tesislerde hasar meydana geldiği zaman, daha önce sahip oldukları herhangi bir nükleer tesis işletmecisi hasar için sorumlu değildir. [262]

- Nükleer bir olayın neden olduğu hasar tazminatı hakkı, yalnızca bu Sözleşmeye uygun bir zarardan sorumlu bir işletmeci tarafından veya Sigortacıya ya da 10. Maddeye uygun olarak gerekli olan güvenliği sağlayan diğer mali garantöre karşı doğrudan bir eylem hakkı, sigortacı ya da diğer mali garantöre karşı ulusal hukuk tarafından verilir. [263]

3.2.5. Paris ve Viyana Sözleşmelerinin Ortak Uygulanmasına İlişkin 21.10.1988 Tarihli Ortak Protokol

Viyana Sözleşmesi ve Paris Sözleşmesi'nin Uygulanmasına İlişkin Ortak Protokol, Uluslararası Atom Enerjisi Ajansı ve Ekonomik İşbirliği ve Kalkınma Teşkilatı tarafından ortaklaşa düzenlenen Paris Sözleşmesi ile Viyana Sözleşmesi arasındaki İlişkiler Konferansı tarafından kabul edilmiştir. 21 Eylül 1988 tarihinde Viyana Uluslararası Atom Enerjisi Ajansı Genel Merkezi'nde imzalanmış ve bu tarihte imzaya açılmıştır. Anlaşma, Paris Sözleşmesi'ne en az beş Taraf Devlet tarafından Viyana Sözleşmesi'ne onay, kabul, tasdik veya katılma belgelerinin tevdi tarihinden üç ay sonra yürürlüğe girmesini öngören Madde VII uyarınca 27

[261] 1982 Ek Protokolün 3. Maddesinin 1. Fıkrası.
[262] 1982 Ek Protokolün 5. Maddesinin 1. Fıkrası.
[263] 1982 Ek Protokolün 6. Maddesinin 1. Fıkrası.

Nisan 1992 tarihinde yürürlüğe girmiştir. [264] Bu protokolü kritik kılan unsurlar ise şunlardır:

- Bir Tarafın topraklarında bulunan ve Viyana Sözleşmesine taraf bir nükleer tesis işletmecisi, o Tarafın topraklarında hem Paris Sözleşmesi hem de bu Protokolün nezdinde maruz kaldığı nükleer hasardan sorumlu olacaktır; [265]

- Bir Tarafın Paris Sözleşmesinde yer alan bir nükleer tesis işletmecisi, o Tarafın topraklarında hem Viyana Sözleşmesi hem de bu Protokolün nezdinde maruz kaldığı nükleer hasardan sorumlu olacaktır. [266]

- Viyana Sözleşmesi veya Paris Sözleşmesi, diğerinin hariç tutulması için nükleer bir kazaya uygulanacaktır. [267]

- Bu Protokol onaylama, kabul, tasdik veya katılmaya tabidir. Onay, kabul veya tasdik belgeleri sadece Taraf Devletlerden Viyana Sözleşmesi veya Paris Sözleşmesi'ne kabul edilir. Bu Protokolü imzalamayan herhangi bir Devlet buna katılabilir. [268]

- Viyana Sözleşmesi veya Paris Sözleşmesi taraf olmayı bırakan herhangi bir Akit Taraf, söz konusu Sözleşmenin uygulanmasının sona erdirilmesi ve bu fesih yürürlüğe girdiği tarihte tevdi edilir. [269]

[264] IAEA, Joint Protocol Relating to the Application of the Vienna Convention and the Paris Convention: https://www.iaea.org/sites/default/files/infcirc402.pdf (25.03.18).
[265] 21.10.1988 Tarihli Ortak Protokolün 2. Maddesinin 1. Fıkrası.
[266] 21.10.1988 Tarihli Ortak Protokolün 2. Maddesinin 2. Fıkrası.
[267] 21.10.1988 Tarihli Ortak Protokolün 3. Maddesinin 1. Fıkrası.
[268] 21.10.1988 Tarihli Ortak Protokolün 6. Maddesinin 1. Fıkrası.
[269] 21.10.1988 Tarihli Ortak Protokolün 9. Maddesinin 1. Fıkrası.

4. Değerlendirme

"Barış için Atom" konuşmasını takiben kurulan Uluslararası Atom Enerjisi Ajansı, nükleer enerji ve santraller üzerine kapsamlı çalışmalar yürütmüştür. Nükleer santraller temelinde kurucu işletmeler, operatörler, tazminat hakkı, sorumluluk rejimi ve tüm bu başlıkları düzenleyen uluslararası hukuk mercileri ve uluslararası hukuk metinleri (Sözleşmeler, Protokoller, EK Maddeler ve Uluslararası Adalet Divanı Mahkeme Kararları) incelenmiştir. Nükleer santrallerin çalışma prensipleri bu bağlamda ele alınmıştır. Bu kapsamda, nükleer hukuk başlığı altında kavramsal incelemeler analiz edilerek nükleer hukukun temel prensipleri irdelenmiştir. Bu düzlemde nükleer hukuk, nükleer santral kuracak şirket ya da diğer aktörlerin göz önünde bulundurması gereken bir dizi prensipler sıralamıştır. Herhangi bir nükleer santralde nükleer silah geliştirmenin önüne geçmek üzere "şeffaflık prensibi" bu bağlamda kurucu işletmeler nezdinde riayet etmeleri gereken bir ilke olmuştur.

Nükleer santrallerin güvenliğine dair çalışma ve düzenlemeleri temel olarak UAEA yürütmektedir. Radyoaktif atık yönetimi, çevreye verilen zararlar ve atıkların imhası konusunda UAEA, taraflara bilgilendirme sunmaktadır. Kurucu işletmeler dâhilinde uluslararası hukuk düzenlemeleri katı sorumluluklar getirmektedir. Bu kapsamda, ilk olarak Paris Sözleşmesi, akabinde Viyana Sözleşmesi; daha sonra Nükleer Zararlar Hakkında Hukuki Sorumluluğa İlişkin 1963 Tarihli Viyana Sözleşmesi, 1964 Tarihli Paris Sözleşmesini Yenileyen Brüksel Ek Sözleşmesi, Nükleer Enerji Alanında Üçüncü Şahıslara Karşı Hukuki Sorumluluğa ilişkin Paris Sözleşmesi'ni Yenileyen 1982 Ek Protokolü, Paris ve Viyana Sözleşmelerinin Ortak Uygulanmasına İlişkin 21.10.1988 Tarihli Ortak Protokol kurucu işletmeler, sorumluluk rejimi, tazminat ve bağlantılı diğer düzenlemeleri içermektedir.

Paris Sözleşmesi, bu bölümde daha detaylı açıklandığı üzere herhangi bir nükleer kazanın mağdurlarını tazmin etmek için nükleer sorumluluk ve tazminat rejimi kurmaktadır. Olası bir nükleer kaza durumunda ne kadar ücretin tazmin edileceğini de içermektedir ve operatörlere katı yükümlülükler getirmektedir. Viyana Sözleşmesi ise, Paris Sözleşmesindeki bazı maddeleri güncellemiştir. Bu kapsamda, Paris Sözleşmesinde sorumluluk tutarının üst sınırı 150 Milyon SDR

iken, Viyana Sözleşmesinde bu tutar 300 Milyon SDR ye kadar çıkartılmıştır. Paris Sözleşmesini Yenileyen Brüksel Ek Sözleşmesi, Paris Sözleşmesi'ni Yenileyen 1982 Ek Protokolü ve Paris ve Viyana Sözleşmelerinin Ortak Uygulanmasına İlişkin 21.10.1988 Tarihli Ortak Protokol ise, bir önceki sözleşmeleri güncelleyen ve ilave maddeler ekleyen düzenlemelerdir.

Bu bağlamda Paris Sözleşmesini Yenileyen Brüksel Ek Sözleşmesi yine bu bölümde daha geniş açıklandığı üzere, bir öncekilere kıyasla nükleer hasarın daha iyi tanımlanmasını içermekte, çevresel hasar ve önleyici tedbirler kavramını ele almakta, 1963 Viyana Sözleşmesi'nin coğrafi kapsamını genişletmekte ve yaşam kaybı ve kişisel yaralanmalar için iddiaların getirilebileceği süreyi uzatmaktadır. Aynı şekilde Paris Sözleşmesi'ni Yenileyen 1982 Ek Protokolü ise, sözleşmeye taraf olan devletlerin topraklarında meydana gelen nükleer kazalar ve çevre muhitlerde maruz kalınan zararları düzenlemektedir. Radyoaktif bir maddenin çevredeki zararı bu EK Protokolün içeriğine örnek teşkil etmektedir.

Paris ve Viyana Sözleşmelerinin Ortak Uygulanmasına İlişkin 21.10.1988 Tarihli Ortak Protokol, her iki sözleşmenin de müşterek ve eş zamanlı uygulanmasını ön gören hukuki düzenlemeler içermektedir. 21.10.1988 Tarihli Ortak Protokolün 2. Maddesinin 1. Fıkrasında da zikredildiği üzere "bir tarafın topraklarında bulunan ve Viyana Sözleşmesine taraf bir nükleer tesis işletmecisi, o tarafın topraklarında hem Paris Sözleşmesi hem de bu Protokolün nezdinde maruz kaldığı nükleer hasardan bu sözleşme kapsamında sorumlu olmaktadır."

Sonuç olarak bu bölüm, nükleer santrallerin kurulum sürecinden başlayıp nasıl işletileceğine; işlenen uranyumun nasıl imha edileceğinden çevredeki hasarlardan kimin sorumlu tutulacağına ve sorumluluk rejimi kapsamında ne gibi uluslararası hukuki düzenlemelerin olduğunu uluslararası hukuk dâhilinde ele almaktadır. Bu bölümde bahsi geçen hukuki düzenlemeler, teknolojinin de doğrudan/dolaylı eksiyle güncellenmek durumunda kalmıştır. Vurgulanması gereken diğer önemli husus ise nükleer santrallerin güvenliğine dair uluslararası hukuki düzenlemelerin de mevcut olmasıdır, ancak bu düzenlemeler temel olarak nükleer santrallerin fiziki güvenliği başlığı altında teknik olarak incelenmektedir.

Santrallerin siber güvenliğinin hukuki esasları noktasında uluslararası hukuki düzenlemeler yok denecek kadar azdır. Dolaylı olarak sorunsal, hukuki metinlerle ele alınmıştır ancak santrallere karşı herhangi bir siber saldırı durumunda hangi uluslararası hukuki usül ve esaslara göre saldırının değerlendirileceği ve yaptırımların uygulanacağı bilgisi uluslararası kamuoyunu meşgul eden bir problem olarak karşımıza çıkmatadır.

ÜÇÜNCÜ BÖLÜM

NÜKLEER SANTRALLERİN SİBER GÜVENLİĞİ ve ULUSLARARASI HUKUKİ TEMEL ESASLARI

1. Nükleer Güvenlik ve Hukuki Temel Esasları

Bir önceki bölümde nükleer santrallerin kuruluş öncesi/esnası/sonrası aşamalarının uluslararası hukuki boyutları ele alınmıştır. Bu bölünde ise, öncelikle nükleer santrallerin güvenliğinin neden kritik olduğunun izahatı, daha sonra ise uluslararası hukuki esasları analiz edilecektir.

1.1. Nükleer Terörizmin Tanımı ve Kapsamı

20. yüzyılda teknolojinin de ivme kat etmesiyle birlikte "nükleer" kelimesi ve 21. yüzyılda farklı saldırı şekillerini uygulayabilen bir kisveye bürünen "terörizm" olgusu bir araya geldiğinde devletler için tahrip edici sonuçlar doğuran bir felaket olgusu haline gelmiştir. [270] Hukuki tanım olarak nükleer terörizm, yasadışı ve kasıtlı olarak "Ölüm veya ciddi bedensel yaralanmaya neden olma amacıyla radyoaktif materyal kullanmak veya mülkiyete veya çevreye ciddi zarar verme niyetiyle; ya da gerçek veya tüzel bir kişiyi, uluslararası bir örgütü ya da bir eylemi yapmaktan kaçınan bir devleti zorunlu kılma niyetiyle işlenirse hukuki bir suç teşkil etmektedir." [271] Uluslararası kamuoyunun da bu konuda hem fikir olduğu nokta ise motive edilmiş terör saldırıları, dünya çapında devam edebilir ve

[270] Eaves, Elisabeth, What Does "nuclear terrorism" Really Mean?, 7 April 2016, Bulletin of the Atomic Scientists: https://thebulletin.org/what-does-nuclear-terrorism-really-mean9309 (E.T: 25.03.18).
[271] IAEA, Nuclear Terrorism: Threats and Risks, IAEA, 2017, p.4.

bir sorun olarak devam edebilmektedir. [272] 11 Eylül 2001 olayını takiben oluşan Teröristlerin Nükleer Silahla Saldırma (NWAT) ihtimali, 21. yüzyıldaki en tehlikeli radyasyon tehdidi olarak algılanmaktadır. [273] Soğuk Savaşın meydana getirdiği tehdit iklimi bitmiş gibi gözükse de, nükleer tehdit birçok analiste göre, her zamankinden daha yaygın bir hale gelmiştir. [274] UAEA Genel Direktörü Mohamed El Baradei, 2005 yılında "nükleer savaş tehdidi hiç bu kadar büyük ve tehdit edici seviyeye ulaşmamıştı" şeklinde durumu özetlemiştir. [275] 44. ABD Başkanı Barack Obama, 2009 Prag'da gerçekleşen Küresel Nükleer Güvenlik Zirvesinde yaptığı konuşmada, [276] "Teröristlerin hiçbir zaman nükleer silah elde etmemeleri sağlanmalıdır. Bu, küresel güvenlik için en amansız ve tehlikeli bir tehdittir." Bu tehdide karşı koyabilmek için dünyanın, soruna odaklanmış "uzun soluklu kurumlara" ihtiyaç duyduğunu ve ABD'nin nükleer güvenlik konusunda küresel bir zirveye ev sahipliği yapacağını belirtmiştir. [277] Herhangi bir terörist grubun nükleer patlama meydana getirmesi, görülmemiş sayıda yaralıya yol açacaktır ve radyolojik yayılma saldırısı ise daha az şiddetli gözükse de, kentleri önemli ölçüde kirletebilmekte ve ekonomik-sosyal bozulmaya neden olabilmektedir. Her iki tipte de saldırının tüm nüfus üzerinde önemli psikolojik etkileri olacaktır. [278] Nükleer terörizm, bir nükleer enerji santraline yapılan saldırıdan hırsızlığa ve nükleer silahın patlamasından farklı biçimlerde meydana gelebilmektedir. Bununla birlikte, her nükleer terörizm senaryosunun farklı bir olasılığa ve aynı zamanda çok farklı sonuçlara sahip olduğunu hatırlamak önem

[272] Badea, Constantina et al., In The Aftermath of Terrorism: Effects of Self Versus Group Affirmation on Support for Discriminatory Policies, Journal of Experimental Social Psychology, 2017, p.1.
[273] Takada, Jun, Radiation Hazard and Protection for the Nuclear Weapon Terrorism, International Congress Series, Vol. 1276, February 2005, p245.
[274] Ellingsen, Simen A., Safeguards Against Nuclear Terrorism: HEU vs Plutonium, Defence & Security Analysis, Vol.24, No.2, 2008, p.129.
[275] GUARDIAN: https://www.theguardian.com/environment/2006/may/26/energy.iran (E.T: 25.03.18).
[276] GUARDIAN: https://www.theguardian.com/world/2009/apr/05/nuclear-weapons-barack-obama (E.T:25.03.18).
[277] Brill, Kenneth C. / John H. Bernhard, A Convention on Nuclear Security: A Needed Step Against Nuclear Terrorism, Arms Control Today, Vol. 45, No. 5, 2015, p. 16.
[278] O'Neill, Kevin, The Nuclear Terrorist Threat, Institute for Science and International Security, August 1997, p.1.

arz etmektedir. [279] Her biri farklı riskler doğuran bu nükleer terörizm saldırılarında en yaygın üç tür nükleer ve radyolojik terörizm vardır ve bunlar: [280]

1- Gerçek bir nükleer bombanın, ya bir devletin cephaneliğinden elde edilen nükleer bir silah ya da çalınmış silahlarla kullanılabilen nükleer malzemeden üretilmiş doğaçlama bir nükleer cihazla patlatması;

2- Geniş bir radyoaktivite salınımına neden olan bir nükleer tesisin sabotajı ve

3- Radyoaktif materyal yaymak ve panik ve bozulma yaratmak için radyolojik bir dispersiyon cihazı veya "kirli bomba" kullanılmasıdır.

Buradan da anlaşılacağı üzere özellikle son on yıl içinde genel olarak terörizmle ilgili uluslararası gelişmeler göz önüne alındığında, tüm saldırıların küçük silahlar, araba bombaları ve doğaçlama patlayıcı aygıtlar gibi klişe algılar vardır, ancak gelişen teknoloji ve imkânla birlikte gizlenen bazı terörist grupların cephaneliklerine kitle imha silahlarının fazlaca bulunduğu bilinmektedir. [281] Bununla birlikte teröristlerin 11 Eylül'deki uçakları anlaşılmaz bir silah olarak kullandıkları gibi, teröristler büyük bir radyoaktivite salınımına neden olma ümidiyle bir nükleer tesise saldırabilme ihtimalleri vardır. [282]

1.1.1. Nükleer Güvenlik Hakkında Temel Esaslar

Bir önceki bölümde nükleer santrallerin güvenliğine dair genel bir bilgilendirmede bulunulmuştur. Nükleer santrallerin güvenliğinin neden kritik olduğu sorusu ise nükleer terörizmin varoluşu ile ilişkilendirilmiştir. Bu kısımdan

[279] CISAC, Understanding the Risks and Realities of Nuclear Terrorism, Institute for International Studies, Stanford University, October 2002, p.2.
[280] Bunn, Matthew /Martin B. Malin /Nickolas Roth William H. Tobey, Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?, Belfer Center for Science and International Affairs Harvard Kennedy School, Cambridge, MA, March 2016, p.4.
[281] Mattox, John Mark, Nuclear Terrorism: The 'Other' Extreme of Irregular Warfare, Journal of Military Ethics, Vol.9, No.2, 2010, p.160.
[282] Larssen, Rolf Mowatt, Nightmares of Nuclear Terrorism, Bulletin of the Atomic Scientists, Vol. 66, No. 2, 2010, p.43.

itibaren nükleer santrallerin güvenliğine dair uluslararası hukuki düzenlemeler incelenecektir.

1.1.1.1.Nükleer Güvenlik Rejimi

Bir devletin nükleer güvenlik rejiminin hedefi, kişileri, mülkiyeti, toplumu ve çevreyi nükleer güvenlik olayının zararlı sonuçlarından korumaktır. Bu Hedefe ulaşmak amacıyla, devletler bu tür nükleer güvenlik olaylarını önlemek, tespit etmek ve bunlara cevap vermek için etkili ve uygun bir nükleer güvenlik rejimini oluşturmalı, uygulamalı ve sürdürmelidir ve bilinmesi gereken önemi diğer bir husus ise güvenlik rejimi, devletlerin genel güvenlik rejiminin bir parçasıdır. [283] UAEA ya göre Nükleer Güvenlik Rejiminin oluşabilmesi için 12 temel ilke vardır ve bunlar: [284]

1- Devlet sorumluluğu,

2- Nükleer güvenlik sorumluluklarının teşhisi ve tanımlanması,

3- Mevzuat ve düzenleyici çerçeve,

4-Nükleer malzemenin ve diğer radyoaktif malzemelerin uluslararası nakliyesi,

5- Suçlama da dâhil olmak üzere suçlar ve cezalar,

6- Uluslararası işbirliği ve yardım

7- Nükleer güvenlik tehditlerinin tanımlanması ve değerlendirilmesi,

8- Hedeflerin belirlenmesi ve değerlendirilmesi ve olası sonuçlar,

9- Risk çerçeveli yaklaşımın kullanımı,

10- Nükleer güvenlik olaylarının tespiti,

11- Bir nükleer güvenlik olayı için planlama, hazırlık ve bunlara müdahale ve

14- Nükleer güvenlik rejiminin sürdürülmesidir.

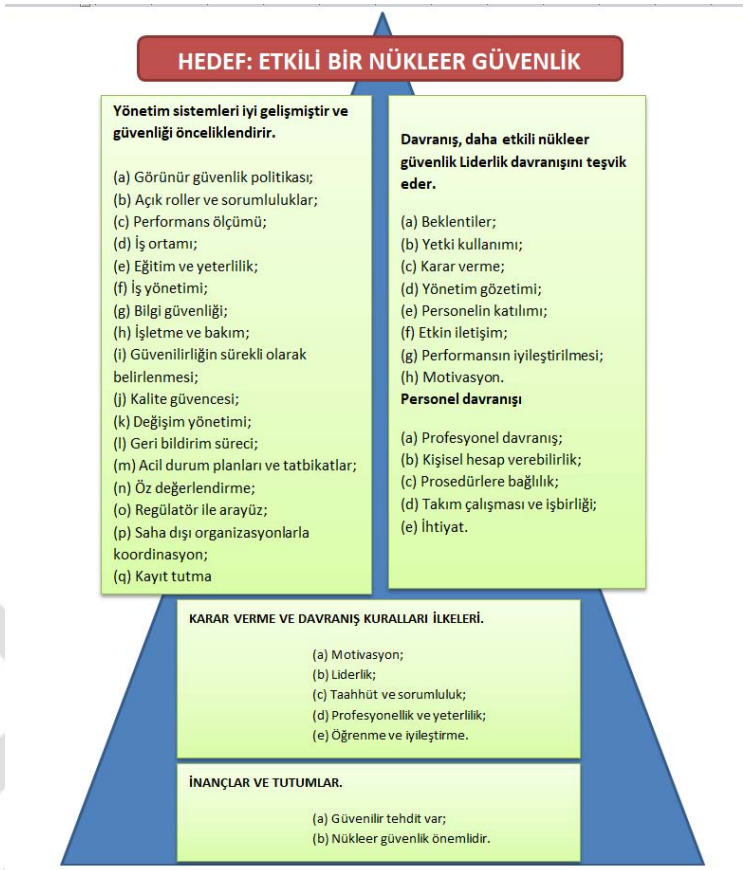
[283] IAEA, Nuclear Security Fundamentals: Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, Vienna, 2013, pp.3-10.
[284] IAEA, a.g.e, s.4-10.

1.1.1.2.Nükleer Güvenlik Kültürü

Nükleer güvenlik kültürü bireylerin, kurumların ve kurumların ihtiyatlı kalmasını sağlamada ve sabotaj tehdidini önlemek ve bunlarla mücadele etmek veya kötü niyetli eylemler için radyoaktif materyal kullanmak için sürekli önlemlerin alınmasında önemli bir rol oynamaktadır. [285] Artan katastrofik terörizm tehdidi ve yeni güvenlik sorunları, nükleer güvenliğin kapsamının ve ilgili kültürün, radyoaktif kaynaklar ve kullanılmış nükleer yakıtı da kapsayacak şekilde bu malzemeleri koruma görevinin ötesine geçmek için gerekli olduğunu açıkça ortaya koymuştur. [286] Nükleer güvenlik kültürü olgusunu örgütlerde ve bireylerde, öncelikli bir öncelik olarak koruma ve güvenlik konularının önemine dikkat çeken bir nitelik ve tutum olarak tanımlamak gerekmektedir. [287] Bununla ilgili izlence ve ilkeleri UAEA Şekil 7' de özetlemiştir.

Şekil 7: UAEA Nükleer Güvenlik Kültürü Modeli

[285] IAEA, Nuclear Security Culture: Implementing Guide, IAEA Nuclear Security Series No.7, Austria, 2008, pp. 3-4.
[286] Center for International Trade and Security, Nuclear Security Culture: The Case of Russia, The University of Georgia, Athens GA, December 2004, p.5.
[287] The UK Office for Nuclear Regulation, Maintenance of a Robust Security Culture, Document ID: CNS-TAST-GD-2.1 Revision 0, Record Reference: TRIM Folder 4.4.2.19072. (2017/100113), March 2017, p.4.



Kaynak: IAEA, 2017, s.6.[288]

1.1.2. Nükleer Terörizm Üzerine Güncel Çalışmalar

1990'ların başından bu yana, uluslararası nükleer terörizm eylemleri düzenli ve şiddetli bir şekilde artmıştır.[289] Bu yüzden nükleer terörizm üzerine uluslararası toplumlar, büyük ölçüde gönüllü eylemlere dayanan uluslararası antlaşmaların, örgütlerin ve inisiyatiflerin parçası olan bir nükleer güvenlik rejimi inşa

[288] IAEA, Self-Assessment of Nuclear Security Culture in Facilities and Activities: Technical Guidance, IAEA Nuclear Security Series No. 28-T, Vienna, 2017, p.6.
[289] Pluta, Anna M. / Peter D. Zimmerman, Nuclear Terrorism: A Disheartening Dissent, Survival, Vol. 48, No. 2, 2006, p. 55.

etmiştir.[290] 2005 tarihli değişiklikle henüz yürürlüğe girmemiş olan Uluslararası Nükleer Terörle Mücadele Sözleşmesi (ICSANT)[291] ve Nükleer Malzemelerin Fiziki Korunması Konvansiyonu (CPPNM)[292] hem muhteviyat olarak hem de devletlerden talep ettikleri konusunda çok genel bir çerçeve çizmiştir.

Son zamanlarda intihar saldırıları, silah ve bıçak saldırılarının gibi amansız meydana gelen geleneksel terörist eylemlerine karışı kırmızı alarm durumunda bulunulsa da daha fazla felakete yol açan nükleer terörizm tehdidine karşı yeterli hassasiyet gösterilmemektedir.[293] Ayrıca, Brüksel saldırılarının ardından ve 1 Nisan 2016 da Washington, DC de gerçekleşen Nükleer Güvenlik Zirvesi öncesinde, UAEA Genel Direktörü Yukiya Amano "terörizmin yayıldığını ve nükleer malzeme kullanma olasılığının göz ardı edilemeyeceği" konusunda bir uyarı metni yayınlamıştır.[294]

1.2. Nükleer Santrallere Karşı Güvenlik Tedbirleri ve Mukabil Tedbirlerin Hukuki Esasları

Nükleer Santrallere Karşı Tedbirler ve Mukabil Tedbirlerin Hukuki Esasları nükleer santrallerde meydana gelen kazalar sonrasında zamanla daha sıkı bir şekle bürünmüştür. İlk olarak 1979'da gerçekleşen Three Mile Island kazası, yedi yıl

[290] Brill, Kenneth C. / John H. Bernhard, A Convention on Nuclear Security: A Needed Step Against Nuclear Terrorism, Arms Control Today, June 2015: https://www.armscontrol.org/print/6990 (E.T: 26.03.18).
[291] BM Genel Kurul'unun 59/290 Sayılı Kararı, International Convention for the Suppression of Acts of Nuclear Terrorism, A/RES/59/290 : https://treaties.un.org/doc/source/docs/A_RES_59_290-E.pdf (E.T: 26.03.18).
[292] IAEA, The Convention on the Physical Protection of Nuclear Material, IAEA - INFCIRC/274/Rev. 1, May 1980: https://www.iaea.org/sites/default/files/infcirc274r1.pdf (E.T: 26.03.18).
[293] Kantor, Moshe, We Must Face Up to the Threat of Nuclear Terrorism, The Telegraph, 8 June 2016: https://www.telegraph.co.uk/news/2016/06/08/we-must-face-up-to-the-threat-of-nuclear-terrorism/ (E.T: 26.03.18).
[294] Landau, Emily B./ Shimon Stein, On the Brink of Nuclear Terror? A Threat and Response Balance Sheet, the Institute for National Security Studies, INSS Insight No. 814, April 13, 2016: http://www.inss.org.il/publication/on-the-brink-of-nuclear-terror-a-threat-and-response-balance-sheet/ (26.03.18).

sonra Çernobil felaketi ve özellikle 11 Eylül 2001 terörist saldırıları nükleer santrallerin güvenliği konusunda büyük bir kamuoyu yaratarak nükleer kazaların neden olabileceği hasarı göstermiştir. [295] Bu kazalara karşı alınan önlemlere rağmen, büyük nükleer kazaların hala mümkün olabileceği bilinmektedir. Caydırıcı unsur olarak uluslararası hukuk, tarihsel olarak devletler nezdinde uygulanarak devletlerarasındaki ilişkileri düzenlemiştir. Ancak, son elli yılda, uluslararası hukuk, başta insan hakları ve uluslararası ceza hukuku alanlarında olmak üzere, devlet dışı aktörlere karşı mukabil tedbirler alanında daha fazla çalışma yapmıştır. [296] Küreselleşme olgusunun doğal bir sonucu olarak sivil toplum örgütleri ve şirketler (özellikle çok uluslu şirketler) de dâhil olmak üzere diğer devlet dışı aktörler uluslararası hukukun oluşumunda rol oynamışlardır. [297] Özellikle UAEA ve BM Güvenlik Konseyi uluslararası güvenlik önlemleri dâhilinde hükümetleri nükleer kazaları ve kasıtlı nükleer kaza ile mücadele etme yolunda yardımcı ve tamamlayıcı nitelikte çalışmalar yürütmektedir. [298] Kurum ve kuruluşlar tarafından yapılan bu düzenlemelerin kimileri bağlayıcı nitelikler içerirken kimileri de tavsiye nitelinde hükümler içermektedirler.

1.2.1. Hukuki Bağlayıcı Nitelikte Uluslararası Düzenlemeler

Nükleer santrallere gerçekleşebilecek herhangi bir saldırı durumunda alınacak tedbirler ve mukabil tedbirlerin hukuki çerçevesi uluslararası düzenlemelerle belirlenmiştir. Uluslararası örgütler tarafından gerçekleştirilen bu düzenlemelerin

[295] Kim, Duyeon / Jungmin Kang, Where Nuclear Safety and Security Meet, Bulletin of the Atomic Scientists, Vol. 68, No. 1, 2012, pp. 86-87.
[296] Masters, Joshua, Nuclear Proliferation, Nonproliferation Review, Vol. 16, No. 3, 2009, p. 348.
[297] Ali, A. M., Legal Elements for Nuclear Security: Egyptian Nuclear Law as a Case Study, XI Radiation Physics & Protection Conference, Nasr City - Cairo, Egypt, 25-28 November 2012, p.323.
[298] Tashbook, Linda, Nuclear Law Research Guide, Hauser Global Law School Program, New York University School of Law , June 2017: http://www.nyulawglobal.org/globalex/Nuclear_Research1.html#io (E.T: 27.03.18).

bazıları bağlayıcı hükümler içerirken bazıları ise tavsiye niteliğinde hükümler içermektedir. [299]

1.2.1.1. UAEA Himayesinde Temel Hukuki Düzenlemeler

"Barış için Atom" la başlayan bir girişimin sonucu olarak kurulan UAEA, nükleer santrallerin güvenliğine dair kapsamlı çalışmalar yürütmüştür. Bu kapsamda bu başlık altında b düzenlemeler işlenecektir.

1.2.1.1.1. Nükleer Malzemelerin Fiziksel Korunması Sözleşmesi ve 2005 Tarihli Değişiklik

Nükleer Malzemelerin Fiziki Korunmasına İlişkin Sözleşme, 3 Mart 1980'de Viyana'da ve New York'ta imzalanmıştır. Sözleşme, nükleer malzemenin fiziksel korunumu alanında yasal olarak bağlayıcı tek uluslararası düzenleme olma özelliğini taşımaktadır. Nükleer malzeme ile ilgili suçların önlenmesi, tespiti ve cezalandırılması ile ilgili tedbirleri belirlemektedir. [300] Sözleşmeyi değiştirmek ve hükümlerini güçlendirmek için Temmuz 2005'te Diplomatik Konferans düzenlenmiştir. Değiştirilen Sözleşme, Taraf Devletlerin, nükleer tesislerin ve malzemenin barışçıl ev içi kullanım, depolama ve taşımacılıkta korunmalarını yasal olarak bağlayıcı kılmaktadır. Ayrıca, çalıntı veya kaçak nükleer malzemenin bulunması ve kurtarılması, sabotajın radyolojik sonuçlarını hafifletmek ve ilgili suçları önlemek ve bunlarla mücadele etmek için ivedi önlemler konusunda devletlerarasında ve aralarında genişletilmiş işbirliği yapılmasını öngörmektedir. [301] Değişiklik hükümlerinin Taraf Devletlerce uygulanması,

[299] Littlejohn, Allison, et al, Comparing Safety Culture and Learning Culture, Risk Management, Vol. 16, No. 4, 2014, p. 273.
[300] IAEA, Convention on the Physical Protection of Nuclear Material : https://www.iaea.org/publications/documents/conventions/convention-physical-protection-nuclear-material (29.03.18).
[301] IAEA, The International Legal Framework for Nuclear Security, IAEA International Law Series No. 4, Vienna, Austria, January 2011, p.3.

nükleer güvenlik açısından hayati derecede önemlidir ve Taraf Devletlerin nükleer terörizme karşı savunmasızlığının azaltılmasında önemli bir etkiye sahiptir. [302]

1.2.1.1.2. Nükleer Kazaların Erken Bildirimi Sözleşmesi

26 Nisan 1986'da, büyük hasarlı ekolojik felaketlerinden biri olan Çernobil nükleer santralinde kaza meydana gelmiştir. UAEA'na göre, reaktör tasarımının kusurlu olması, personel hataları ve güvenlik kültürünün düşük seviyede oluşu kazaya sebep veren mahaller arasındaydı. [303] Kaza sonrasında uluslararası kamuoyunda şu noktalara dikkat çekildi: dikkatsizlik, ihmal, iş güvenliği ihmali ve sağlık kurallarının ihmal edilmesi. Çernobil nükleer santral kazasından sonra 1986 yılında kabul edilen Nükleer Kazaların Erken Bildirim Sözleşmesi, başka bir devlet için radyolojik güvenlik açısından önemli olabilecek uluslararası sınır aşan serbestleşme potansiyeline sahip nükleer kazalar için bir bildirim sistemi kurmaktadır. [304] Bu sözleşme, devletlerin kaza zamanını, yerini, radyasyon salınımlarını ve durumu değerlendirmek için gerekli olan diğer verileri rapor etmelerini gerektirir. Bildirim, etkilenen devletlere doğrudan ya da IAEA aracılığıyla ve UAEA' nın kendisine yapılmalıdır. [305] Madde 1' de listelenen tesis ve faaliyetlerle ilgili herhangi bir nükleer kaza için raporlama zorunludur. Madde 3 uyarınca, devletler diğer kazaları da bildirebilirler. Nükleer silahlara sahip beş devlet (Çin, Fransa, Rusya, Birleşik Krallık ve Birleşik Devletler) nükleer silah ve nükleer silah testlerini içeren kazaları bildirmek için niyetlerini beyan etmişlerdir. [306]

---

[302] IAEA, Convention on Physical Protection of Nuclear Material (CPPNM) and Amendment thereto : http://www-ns.iaea.org/conventions/physical-protection.asp?s=6&l=42 (E.T: 30.03.18).
[303] Anisimov, Aleksey Pavlovich / Anatoliy Jakovlevich Ryzhenkov, Thirty Years After the Accident at the Chernobyl Nuclear Power Plant: Historical Causes, Lessons and Legal effects, Journal of Energy & Natural Resources Law, Vol. 34, No. 3, 2016, p. 265.
[304] IAEA, Convention on Early Notification of a Nuclear Accident : https://www.iaea.org/publications/documents/treaties/convention-early-notification-nuclear-accident (E.T: 30.03.18).
[305] McBrayer, Sharon, Chernobyl's Legal Fallout, GA. Journal of International Law & Comparative Law, Vol. 17, No. 303, pp. 304-305.
[306] Moore, George M., Out of control: Why Mandatory International Reporting is Needed for Radioactive Sources and Materials, Bulletin of the Atomic Scientists, Vol. 70, No. 6, 2014, p.63.

1.2.1.1.3. Acil Nükleer ve Radyolojik Kaza Durumunda Yardım Sözleşmesi

Çernobil nükleer santral kazasından sonra 1986 yılında kabul edilen Acil Nükleer ve Radyolojik Kaza Durumunda Yardım Sözleşmesi, taraf devletlerarasında işbirliği için uluslararası bir çerçeve hazırlamaktadır. Devletlerin mevcut uzmanlarını, donanımlarını ve yardım sağlamak için diğer materyallerini UAEA'ya bildirmelerini şart koşmaktadır. [307] Talep halinde, taraf devletlerden her biri, talep edilen yardımı ve kapsamı ile şartlarını yerine getirip getiremeyeceğine karar vermektedir. Diğerlerinin yanı sıra, gelişmekte olan ülkelerin ihtiyaçları ve nükleer tesisler olmayan ülkelerin özel ihtiyaçları da hesaba katılarak, yardım alınmadan yardım sunulabilmektedir. UAEA, bilgiyi kanalize ederek, çabaları destekleyerek ve mevcut hizmetlerini sunarak bu işbirliği için hizmet vermektedir. [308]

1.2.1.1.4. Nükleer Güvenlik Sözleşmesi

Nükleer Güvenlik Sözleşmesi, 17 Haziran 1994'te Viyana'da kabul edilmiştir. Sözleşme, 1992'den 1994'e kadar bir dizi uzman düzeyinde toplantılar esnasında oluşturulmuştur ve aynı zamanda hükümetler, ulusal nükleer güvenlik yetkilileri ve UAEA Sekretaryası tarafından kayda değer çalışmaların bir sonucu olarak ortaya çıkmıştır. Sözleşmenin amacı, devletlerin nezdinde üye olacağı uluslararası kıstasları belirleyerek yüksek güvenlik seviyesini korumak için nükleer santralleri işleten devletleri yasal olarak taahhüt etmektir. [309] Tarafların yükümlülükleri, büyük ölçüde UAEA Emniyet Esasları belgesinde yer alan "Temel Güvenlik İlkeleri" (SF-1) ne dayanmaktadır. Bu yükümlülükler; örneğin, konumlandırma, tasarım, inşaat, işletme, yeterli mali ve insan kaynaklarının mevcudiyeti, güvenlik,

---

[307] IAEA, Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency : https://www.iaea.org/publications/documents/treaties/convention-assistance-case-nuclear-accident-or-radiological-emergency (31.03.18).

[308] Simo, Augustin, What if There's a Next Time? Preparedness after Chernobyl and Fukushima, Bulletin of the Atomic Scientists, Vol. 72, No. 4, 2016, p. 265.

[309] IAEA, The Convention on Nuclear Safety : http://www-ns.iaea.org/conventions/nuclear-safety.asp?s=6&l=41 (31.03.18).

kalite güvencesi ve acil durum hazırlığının değerlendirilmesi ve doğrulanmasını kapsamaktadır. [310]Sözleşme, Tarafların, düzenli toplantılar yoluyla geliştirilecek ve desteklenecek olan daha yüksek güvenlik seviyelerine ulaşmak için ortak çıkarlarına dayanmaktadır. Sözleşme, Tarafları, UAEA' da yapılacak Tarafların toplantılarında "akran değerlendirmesi" yükümlülüklerinin yerine getirilmesi hakkında rapor sunma yükümlülüğünü getirmektedir. Bu mekanizma, Sözleşmenin ana yenilikçi ve dinamik unsurudur. [311]

1.2.1.1.5. Tüketilen Yakıt Yönetiminin Güvenliği ve Radyoaktif Atık Yönetiminin Güvenliğine Dair Ortak Sözleşme

Ortak Sözleşme, 5 Eylül 1997 tarihinde, UAEA tarafından 1-5 Eylül 1997 tarihlerinde genel kurul toplantısında düzenlenen Diplomatik Konferansta kabul edilmiştir. 29 Eylül 1997 tarihli IAEA Genel Konferansı'nda imzaya açılmıştır. Ortak Sözleşme'nin 40. Maddesi uyarınca operasyonel nükleer enerji santrallerine sahip 15 Devletin araçları da dâhil olmak üzere 25'inci onay, kabul veya onay belgesinin UAEA' ya tevdi edildiği tarihten 90 gün sonra yürürlüğe girmiştir. [312] Ortak Sözleşme, nükleer programlara sahip ve olmayan ülkelerdeki radyoaktif atıkların ve kullanılmış yakıtların yönetimi ve depolanması güvenliği ile ilgilenen ilk uluslararası araçtır. Aynı zamanda mevcut UAEA nükleer güvenlik rejimini önemli ölçüde detaylandırmakta ve genişletmekte ve bu alanda uluslararası standartları desteklemektedir. Sözleşme, kullanılmış yakıt ve radyoaktif atık yönetiminde yüksek düzeyde güvenliğin sağlanması ve sürdürülmesi, bu tür malzemelerin yönetiminin tüm aşamalarında olası tehlikelere karşı etkili savunmaların yapılmasını ve kazaların radyolojik sonuçlarla önlenmesini

[310] Jha, Anupam, Dynamics of Legal Regime on Safety of Nuclear Power Plants in India after Fukushima Disaster, Journal of Risk Research, Vol. 17, No. 1, 2014, p. 147.
[311] Kamminga, Menno T. , The IAEA Convention on Nuclear Safety, The International and Comparative Law Quarterly, Vol. 44, No. 4, 1995, pp. 872–882.
[312] IAEA, Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management : http://www-ns.iaea.org/conventions/waste-jointconvention.asp (31.03.18).

amaçlamaktadır. [313] Sözleşme, kullanılmış yakıtların ve radyoaktif atık yönetiminin sivil uygulamalardan korunmasını kapsamaktadır. Aynı zamanda askeri veya savunma kaynaklı harcanmış yakıt ve radyoaktif atığın yönetimi için de geçerlidir ve bu tür materyaller yalnızca sivil programlara kalıcı olarak aktarılır ve yönetilmektedir. Sözleşme, sözleşme taraflarını güvenlik gerekliliklerini gözden geçirme ve mevcut ve önerilen kullanılmış yakıt ve radyoaktif atık yönetim tesislerinde çevresel değerlendirmeler yapma çağrısında bulunmaktadır. Kullanılmış yakıt ve radyoaktif atık yönetiminin güvenliğini yönetmek için yasal ve düzenleyici bir çerçevenin kurulmasını ve bakımını sağlamaktadır. [314] Sözleşme, harcanan yakıt ve radyoaktif atığın sınır ötesi harekâtına ilişkin kurallar ve koşulların yanı sıra, Sözleşme ile tutarlı bir şekilde kullanılmış yakıt veya radyoaktif atıkları yönetmek için yeterli idari ve teknik kapasite ve düzenleyici yapıya sahip olması gereken bir varış yerinin gerekliliğini ortaya koymaktadır. Bir sınır ötesi harekâtın Sözleşmeye uygun olarak tamamlanamaması halinde, bir menşe Devleti, bu tür malzemenin topraklarına yeniden giriş yapmasına izin vermek için uygun adımlar atmasını zorunlu kılmaktadır. [315]

1.2.1.2. BM Himayesinde Temel Hukuki Düzenlemeler

BM nezdinde nükleer terörizm ve güvenlik konularında BM Güvenlik Konseyi "uluslararası barış ve güvenliğin korunmasında" birincil sorumluluğa

---

[313] NTI, Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management : http://www.nti.org/learn/treaties-and-regimes/joint-convention-on-the-safety-of-spent-fuel-management-and-on-safety-of-radioactive-waste-management/ (31.03.18).

[314] ASN, Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management : http://www.french-nuclear-safety.fr/International/International-reference-texts/International-conventions/Joint-Convention-on-the-Safety-of-Spent-Fuel-Management-and-Safety-of-Radioactive-Waste-Management (31.03.18).

[315] US DEPARTMENT OF ENERGY, Second National Report for the Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management : https://www.energy.gov/em/downloads/second-national-report-joint-convention-safety-spent-fuel-management-and-safety (31.03.18).

sahiptir. Konsey, 1990'dan beri faaliyetlerini çarpıcı bir şekilde arttırmakla birlikte askeri operasyonlar, yaptırımlar, silah denetimlerini, seçimleri izleme gibi bir dizi amaçları bünyesinde barındırmaktadır. [316] 11 Eylül terörist saldırılarının ardından, nükleer terörizmin baş göstermesi ABD başta olmak üzere diğer devletlerin de BM nezdinde bir araya gelmesiyle nükleer güvenliği geliştirmek için konu ile ilgili uluslararası yasal çerçeve oluşturma çabaları olmuştur. [317] Özellikle BM Güvenlik Konseyi'nin 1373 (2001) ve 1540 (2004) sayılı kararlarında, diğer düzenlemelerin yanı sıra, nükleer terörizm ve nükleer silahların yayılması tehdidine değinilmekte ve bu güçlüklere uluslararası müdahaleye karşı küresel tepkinin güçlendirilmesi için ulusal, bölgesel ve uluslararası işbirliği çağrısında bulunmaktadır. UAEA, 1373 ve 1540 sayılı Güvenlik Konseyi kararları ile ilgili olarak oluşturulan BM Komitelerine, talep üzerine, yardımda bulunmaktadır. Ayrıca, uygun durumlarda, bu kararlar kapsamındaki yükümlülüklerini yerine getirmede devletlere yardımcı olmaktadır. [318]

1.2.1.2.1. BM Güvenlik Konseyi 1373 (2001) ve 1540 (2004) Sayılı Kararları

BM Sözleşmesinin VII. Bölümünde 2001 yılında kabul edilen 1373 sayılı Güvenlik Konseyi kararı, uluslararası terörizm ve nükleer maddelerin yasadışı hareketi arasındaki yakın ilişkiyi kaygıyla not etmiştir. Karar, bu ciddi sorun ve uluslararası güvenlik tehdidine karşı küresel bir yanıtı güçlendirmek için ulusal, bölgesel ve uluslararası çabaların koordinasyonunu artırma gereğini vurgulamaktadır. Karar, bütün devletleri terörist faaliyetlere yönelik yardımları suçlu kılmaya, teröristlere mali destek ve güvenli sığınağı inkâr etmeyi ve suç eylemlerinin önlenmesi ve kovuşturulması için bilgi alışverişinde bulunmalarını

[316] UNSC, The Security Council : http://www.un.org/en/sc/ (31.03.18).
[317] Green, Michael Hamel, The implications of the 2017 UN Nuclear Prohibition Treaty for Existing and Proposed Nuclear-Weapon-Free Zones, Global Change, Peace & Security, 2018, p.3.
[318] IAEA, UN Security Council Resolutions : http://www-ns.iaea.org/security/sc_resolutions.asp (31.03.18).

zorunlu kılmaktadır. [319] Birleşmiş Milletler Güvenlik Konseyi'nin 1540 sayılı kararı, 2004'te Bölüm VII'de kabul edilmiştir ve tüm devletleri, özellikle devlet dışı aktörlerin nükleer silah üretmek, elde etmek, bulundurmak, geliştirmek, nakletmek, terörist amaçlar ve ilgili malzeme üzerinde uygun kontrollerin kurulması da dâhil olmak üzere nükleer silahların çoğalmasını önlemek için iç kontroller kurmak veya kullanmak için yasaklayan uygun yasaları kabul etmek ve uygulamakla yükümlüdür. Bu amaçla, Devletler çeşitli muhasebe ve kontrol tedbirlerini uygulamak zorundadır. Bunlar şunları içermektedir: fiziksel koruma önlemleri; sınır kontrolleri; yasa dışı ticaretin tespit edilmesi, caydırılması, önlenmesi ve bunlarla mücadele için alınması gereken önlemler ise ithalat ve ihracat kontrol önlemleri olarak belirlenmiştir. [320]

1.2.1.2.2. Terörist Bombalamalarının Engellenmesine Dair Uluslararası Sözleşme

Terörist Bombalamalarının Engellenmesine Dair Uluslararası Sözleşme'nin amacı, terörizm eylemlerinin önlenmesi ve faillerinin kovuşturulması ve cezalandırılması için etkili ve pratik tedbirlerin geliştirilmesi ve uygulanması konusunda devletlerarasında uluslararası işbirliğini geliştirmektir. [321] Herhangi bir kişi, kamuya açık bir yer, bir devlet ya da hükümet tesisi, bir toplu taşıma yerinin ölüm veya ciddi bedensel yaralanmaya neden olma niyetiyle veya sonuçta meydana gelebilecek veya büyük ekonomik kayıplarla sonuçlanabilecek büyük bir tahribatla sistem veya altyapı tesisi içinde ya da aleyhinde bir patlayıcı ya da başka bir ölümcül cihazı yasalara aykırı ve kasıtlı olarak gönderir, yerleştirir,

[319] BM Güvenlik Konseyi 1373 Sayılı Kararı : https://www.un.org/sc/ctc/resources/databases/recommended-international-practices-codes-and-standards/united-nations-security-council-resolution-1373-2001/ (01.04.18).
[320] BM Güvenlik Konseyi 1373 Sayılı Kararı : https://www.un.org/disarmament/wmd/sc1540/ (01.03.18).
[321] UNODC, International Convention for the Suppression of Terrorist Bombings (New York, 15 December 1997) : https://www.unodc.org/documents/treaties/Special/1997%20International%20Convention%20for%20the%20Suppression%20of%20Terrorist.pdf (02.04.18).

tahliye eder ya da patlatırsa, Sözleşme'nin kapsamı dâhilinde bir suç işlemiş olarak addedilmektedir. [322] Herhangi bir kişi, yukarıda belirtilen bir suç işlemeye teşebbüs ederse veya bir suçta suç ortağı olarak katılırsa, suç işlemeye veya başka bir şekilde suç işlemesine veya başka bir şekilde bu tür suçların işlenmesine katkıda bulunursa, aynı şekilde suça iştirak etmiş sayılmaktadır. [323] Sözleşme, bu nitelikteki bir eylemin Sözleşme tarafından tanımlanan herhangi bir uluslararası unsur içermediği durumlarda geçerli değildir. Tarafların, kendi iç hukuklarına göre, suçları işleyen, suç işlemekle suçlanan veya yargılamakla suçlanan ve suç işlemekle bağlantılı olarak yargılanma suçlarından yargılanmaları, cezalandırılması veya ibraz edilmeleri için cezalandırılması gerekmektedir. [324] Sözleşmede atıfta bulunulan suçlar, Taraflar arasında mevcut iade sözleşmeleri kapsamındaki ve Sözleşme'nin kendisi tarafından öngörülen suçlar olarak kabul edilmektedir. [325]

1.2.1.2.3. Nükleer Terör Faaliyetlerinin Önlenmesine Dair Uluslararası Sözleşme

1996 yılında, BM Genel Sekreteri BM Genel Kurul 50/53 Sayılı (A / RES / 50/53) [326] kararına uygun bir rapor hazırlayarak uluslararası terörizmle ilgili mevcut uluslararası yasal belgeleri incelemiştir ve mevcut antlaşmalar tarafından kapsanmayan alanlarda uluslararası antlaşmaların veya diğer mevzuatın detaylandırılması ihtiyacı doğmuştur. [327] BM Güvenlik Konseyi tarafından

---

[322] UNTC, 9. International Convention for the Suppression of Terrorist Bombings : https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-9&chapter=18&clang=_en (02.04.18).

[323] Johnson, Clifton M., Introductory Note to the International Convention for The Suppression of the Financing of Terrorism, International Legal Materials, Vol. 39, No. 2, 2000, p. 268.

[324] Witten, Samuel M., The International Convention for the Suppression of Terrorist Bombings, The American Journal of International Law, Vol. 92, No. 4, 1998, p. 774.

[325] UN, International Convention for the Suppression of Terrorist Bombings, International Legal Materials, Vol. 37, No. 2, 1998, p. 253.

[326] BM Genel Kurulunun A/RES/50/53 Sayılı Kararı: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/50/53 (02.04.18).

[327] International Convention for the Suppression of Acts of Nuclear Terrorism, International Legal Materials, Vol. 44, No. 4, 2005, p. 815.

önerilen tedbirler arasında teröristler tarafından kitle imha silahlarının kullanılmasının önlenmesi olmuştur. Taslak toplantı Rusya Federasyonu tarafından önerilmiş ve BM Genel Kurulu Hukuk Komitesi tarafından değerlendirilmiştir. 17 Aralık 1996 tarihli 51/210[328] sayılı UNGA Kararı, taslak sözleşmeyi detaylandırmak için bir Ad Hoc Komite kurulmuştur. Rusya Federasyonu, taslak sözleşmeye dair açıklayıcı notunda, 1980'de Nükleer Malzemelerin Fiziki Korunmasına İlişkin Sözleşme'nin (1980 -CPPNM), özellikle terör eylemini durdurma ve sonuçlarının ortadan kaldırılması aşamasında nükleer terör eylemlerine karşı bir takım önemli boşluklar olduğunu kaydetmiştir. [329] Genel Kurul, 11 Eylül 2001 saldırılarından bu yana kabul edilen ilk terörle mücadele anlaşması olan A / RES / 59/290 [330] sayılı kararı ile Genel Kurulun 91. Olağan Genel Kurul toplantısında 13 Nisan 2005 tarihinde Uluslararası Nükleer Terörle Mücadele Kanunu'nun kabul edilmesine oybirliğiyle onay vermiştir. Nükleer silahların devletler tarafından kullanılmasına yönelik yeni bir kısıtlama getirmeyen anlaşma, 14 Eylül 2005 tarihinde imzaya açılmış ve 22'nci tashihle (Bangladeş) 7 Temmuz 2007'de yürürlüğe girmiştir. Bu sözleşme, daha önce var olan 12 evrensel terörle mücadele sözleşmesine dâhil edilerek terör eylemleriyle bağlantılı olarak uluslararası yasal çerçeveyi ve hukukun üstünlüğünü daha da güçlendirmiştir. [331] Ayrıca işbu sözleşme, nükleer terörizm eylemini nükleer madde, nükleer yakıt, radyoaktif ürünler, atıklar ya da toksinler, patlayıcı ve diğer tehlikeli özelliklere sahip başka herhangi bir radyoaktif madde kullanmak üzere teşebbüste bulunmayı tehdit olarak tanımlamaktadır. [332]

---

[328] BM Genel Kurulunun A/RES/51/210 Sayılı Kararı: http://www.un.org/documents/ga/res/51/a51r210.htm (02.04.18).

[329] NTI, International Convention on the Suppression of Acts of Nuclear Terrorism: http://www.nti.org/learn/treaties-and-regimes/international-convention-suppression-acts-nuclear-terrorism/ (02.04.18).

[330] BM Genel Kurulunun A/RES/59/290 Sayılı Kararı: http://www.un-documents.net/a59r290.htm (02.04.18).

[331] Kibaroglu, Mustafa, The Threat of Nuclear Terrorism Requires Concerted Action, Strategic Analysis, Vol. 38, No. 2, 2014, p.211.

[332] MFA, Press Release Regarding The Deposition of the Instrument of Ratification of the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) to UN, No: 223, 24 September 2012,: http://www.mfa.gov.tr/no -223 -24-september-2012 -press-release-

Sözleşme, yalnızca bireyler tarafından gerçekleştirilen eylemlere uygulanır ve kapsamı, nükleer silahların nükleer silahların yayılmasını veya devletlerin ya da hükümetler arası örgütlerin oluşturduğu nükleer tehditleri içermemektedir. [333]

1.2.1.3. UDÖ Himayesinde Temel Hukuki Düzenlemeler

Gemilerin güvenliğini tehdit eden yasadışı eylemler ve yolcu ve mürettebatlarının güvenliği ile ilgili endişeler, mürettebatın kaçırıldığına dair raporlar ve kasti olarak gemilerin patlayıcılar tarafından imha edilmesi, uluslararası kamuoyunda bu tür olayların önüne geçmek üzere bir oluşum kurulmasını tetiklemiştir. [334] 1948'de Cenevre'de gerçekleşen uluslararası bir konferansta, UDÖ'nün (asıl adı IMCO - Hükümetler arası Denizcilik Danışma Örgütü idi, ancak adı 1982'de UDÖ olarak değiştirildi) kuruluş sözleşmesi kabul edilmiştir. [335] UDÖ Sözleşmesi 1958'de yürürlüğe girdi ve yeni Organizasyon ertesi yıl ilk kez bir araya gelmiştir. Sözleşmenin 1. Maddesinin A fıkrası uyarınca UDÖ, "hükümetler arasında işbirliği yapmak ve uluslararası ticarette yer alan nakliyeyi etkileyen her türlü teknik konularla ilgili uygulamaları sağlamak" ve "Deniz güvenliği, gemicilik ve gemilerden kaynaklanan deniz kirliliğinin önlenmesi ve kontrolüne ilişkin konularda en uygulanabilir standartların genel kabulünü teşvik etmek ve kolaylaştırmak" amacı ile hareket etmektedir. [336] Organizasyon ayrıca, bu amaçlarla ilgili idari ve hukuki meselelerle ilgilenmek için yetkilendirilmiştir. Bu bağlamda, UDÖ, güvenlik ve çevre sorunlarını, yasal

---

regarding-the-deposition-of-the-instrument-of-ratification-of-the-international-convention-for-the-suppression-of-acts-of-nuclear-terrorism- icsant -to-un.en.mfa (04.04.18).

[333] Fidler, David P., American Society of Internatonal Law, International Convention for the Suppression of Acts of Nuclear Terrorism Enters into Force, Vol. 11, No. 18, July 05, 2007: https://www.asil.org/insights/volume/11/issue/18/international-convention-suppression-acts-nuclear-terrorism-enters-force (E.T: 03.04.18).

[334] Hassan, Daud/ Sayed M. Hasan, Origion, Development and Evolution of Maritime Piracy: A historical Analysis, International Journal of Law, Crime and Justice, Vol. 49, 2017, pp. 1-2.

[335] IMO, Brief History of IMO, http://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx (E.T: 03.04.18).

[336] IMO, Adopting a Convention, Entry into force, Accession, Amendment, Enforcement, Tacit Acceptance Procedure : http://www.imo.org/en/About/Conventions/Pages/Home.aspx (04.04.18).

konuları, teknik işbirliğini, güvenliği ve verimliliği ele alan kapsamlı bir nakliyeye ilişkin hukuki çerçeve oluşturmuştur. [337] Bu yüzden gerçekleştirdiği bazı hukuki düzenlemeler bağlayıcı hükümler içermektedir.

1.2.1.3.1. Deniz Ulaştırması Güvenliğine Karşı Yasadışı Eylemlerin Önlenmesine İlişkin Sözleşme (1988 SUA Sözleşmesi)

Gemilerin güvenliğini tehdit eden yasadışı eylemler ve yolcularının, mürettebatının ve nakliyelerin güvenliği ile ilgili endişeler, 1980'lerde yolcu ve gemilere yönelik saldırı ve tehditler hakkında uluslararası camiada kamuoyu oluşturmuştur. [338] Achille Lauro olayının bir sonucu olarak, Kasım 1985'te UDÖ Meclisi, gemilerin güvenliğini ve yolcu ve mürettebatın güvenliğini tehdit eden yasadışı eylemleri önlemek için 1986 tarihli Deniz Güvenliğine ilişkin önlemler hakkında A.584 (14) [339] sayılı kararı kabul etti. Denizcilik Güvenlik Komitesi (MSC), gemilerdeki yolcu ve mürettebata karşı yasadışı eylemleri önlemek için MSC / Circ.443 [340] sayılı tedbir kararını yayınlamıştır. Sözleşmenin temel amacı, gemilere yasadışı eylem yapan kişilere karşı mukabil tedbirlerin uygulanmasını sağlamaktır. [341] Sözleşmenin kapsadığı diğer yasa dışı eylemler Madde 3' te belirtilmiştir: gemilerin zorla ele geçirilmesi; gemilerdeki insanlara karşı şiddet eylemleri ve aygıtları tahrip etme veya zarar vermedir. Ayrıca Sözleşme

[337] UN, Funds, Programmes, Specialized Agencies and Others : http://www.un.org/en/sections/about-un/funds-programmes-specialized-agencies-and-others/index.html (04.04.18).

[338] Obokata, Tom, Maritime Piracy as a Violation of Human Rights: A Way Forward for its Effective Prevention and Suppression?, The International Journal of Human Rights, Vol. 17, No. 1, 2013, p.21.

[339] UDÖ, A.584 (14) Sayılı Kararı: http://www.imo.org/blast/blastDataHelper.asp?data_id=22374&filename=A584%2814%29.pdf (E.T: 05.04.18).

[340] UDÖ, MSC/Circ.443 Sayılı Kararı: http://www.imo.org/en/OurWork/Security/SecDocs/Documents/Maritime%20Security/MSC.Circ.443.pdf (E.T: 05.04.18).

[341] IMO, Maritime Security, http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Default.aspx (E.T: 05.04.18).

Makamları, iddia edilen suçluları iade etmek ya da kovuşturmakla yükümlü kılmaktadır. [342]

1.2.1.3.2. SUA (Yasadışı Eylemlerin Önlenmesi) Sözleşmesinin 2005 Protokolleri

1988 Sözleşmesi ve ilgili Protokolü'ndeki önemli değişiklikler, 10 ila 14 Ekim 2005 tarihleri arasında düzenlenen SUA Sözleşmelerini Gözden Geçirilmesine Dair Diplomatik Konferans nezdinde kabul edilmiştir. Değişiklikler, SUA sözleşmeleri "2005 Protokolleri" biçiminde kabul edilmiştir. [343] 2005 Protokolü, Madde 3 e yeni kıstaslar eklemektedir ve bunlar: [344]

- Yasanın amacı, doğası veya bağlamı gereği, bir nüfusu sindirmek veya herhangi bir eylemde bulunmak veya bir eylemden kaçınmak için bir hükümeti/devleti veya uluslararası bir örgütü zorunlu kılmak,

- Herhangi bir patlayıcı, radyoaktif materyal veya BCN (biyolojik, kimyasal, nükleer) silahın gemilere yönelik veya gemide kullanılması veya ölüme veya ciddi yaralanma veya hasara neden olan veya sebep olabilecek bir şekilde sızdırılması,

-Ölüm veya ciddi yaralanmaya veya hasara neden olan veya muhtemel olan miktar veya yoğunluk bir gemiden, yağdan, sıvılaştırılmış doğal gazdan veya diğer tehlikeli veya zararlı maddelerden deşarj etmek,

---

[342] Hallwood, Paul / Thomas J. Miceli, The Economics of International Cooperation in the Apprehension and Prosecution of Maritime Pirates, Ocean Development & International Law, Vol. 43, No. 2, 2012, pp. 188-189.

[343] CIL, 2005 Protocol to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, National University of Singapore: https://cil.nus.edu.sg/2005-protocol-o-the-convention-for-the-suppression-of-unlawful-acts-against-the-safety-of-maritime-navigation/ (E.T: 05.04.18).

[344] IMO, Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/SUA-Treaties.aspx (E.T: 05.04.18).

-Ölüm veya ciddi yaralanmaya veya hasara neden olacak şekilde bir gemiyi kullanmak,

-Herhangi bir patlayıcı veya radyoaktif malzemenin gemiye taşınmasını, bir nüfusu korkutmak veya bir Hükümet veya bir uluslararası örgütlenme yapmak veya herhangi bir eylemden kaçınmak, [345]

-BCN silahı olduğunu bilerek, gemiye herhangi bir BCN silahını taşır,

-Nükleer bir patlayıcı faaliyette veya herhangi bir nükleer faaliyette kullanılmak üzere tasarlanmadığını bilerek, özel bölünebilir malzemenin işlenmesi, kullanılması veya üretimi için özel olarak tasarlanmış ya da hazırlanmış herhangi bir kaynak malzeme, özel bölünebilir malzeme veya UAEA kapsamlı koruma sözleşmesinde bahsi geçen donanım veya malzemeler ve

-Bir BCN silahının tasarımına, üretimine veya teslimatına önemli ölçüde katkıda bulunan herhangi bir donanım, malzeme ya da yazılım veya ilgili teknolojiyi, bu amaçla kullanılacağı şekilde nakleder.

1.2.2. Hukuki Bağlayıcı Nitelikte Olmayan Uluslararası Düzenlemeler

Bir önceki bölümde özelikle BM ve UAEA' nın bağlayıcı nitelikte hukuki düzenlemelerde bulunduğu bilgisi ışığında, bağlayıcı olmayıp tavsiye niteliğinde alınan kararlar da mevcuttur.

[345] US BUREAU OF INTERNATIONAL SECURITY AND NONPROLIFERATION, Protocol of 2005 to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation : https://www.state.gov/t/isn/trty/81728.htm (E.T: 06.04.18).

1.2.2.1. UAEA Himayesinde Bağlayıcı Olmayan Düzenlemeler

UAEA özellikle 11 Eylül saldırılandan sonra ciddi bağlayıcı düzenlemeler oluşturmuştur, ancak dinamik bir şekilde hukuki ve teknik kısımlarda taraf devletlere bilgi alışverişini sunarken, tavsiye niteliğinde de kararlar almıştır ve bu düzenlemeler mevcut nükleer santrali olan ve kuracak devletlere bilgilendirme niteliğinde olmuştur. [346]

1.2.2.1.1. Radyoaktif Kaynakların Emniyeti ve Güvenliğine İlişkin Uygulama Esasları ve Radyoaktif Kaynakların İthalatı ve İhracatı Hakkında Ek Düzenleme

Radyoaktif Kaynakların Emniyeti ve Güvenliğine İlişkin Uygulama Esasları 11 Eylül 2001 olaylarını takiben uluslararası uygulama esaslarını da göz önünde bulundurarak güçlendirilmiştir. Gözden geçirilen kural metni UAEA Yönetim Kurulu tarafından onaylanmıştır. Eylül 2003'teki GC(47)/RES/7 sayılı kararında, UAEA Genel Konferansı, Kurul'un onayını kabul ederken, kuralların yasal olarak bağlayıcı bir araç olmadığını kabul etmiştir. [347] Bahsi geçen kuralların amaçları, ulusal politikaların, yasaların ve yönetmeliklerin geliştirilmesi, uygulanması ve uluslararası işbirliğinin teşvik edilmesi yoluyla: [348]

(a) Radyoaktif kaynakların yüksek düzeyde güvenliğini sağlamak ve sürdürmek;

(b) Radyoaktif kaynakların yetkisiz erişimini, zarar görmesini, çalınmasını veya zarar görmesini engellemek, bu tür kaynaklara yanlışlıkla zararlı maruz

[346] Shea, Thomas E., The Verification Challenge: Iran and the IAEA, Arms Control Today, Vol. 45, No. 5, 2015, pp. 8-9.
[347] IAEA, Code of Conduct on the Safety and Security of Radioactive Sources, and Supplementary Guidance on the Import and Export of Radioactive Sources : http://www-ns.iaea.org/tech-areas/radiation-safety/code-of-conduct.asp (E.T: 06.04.18).
[348] IAEA, Code of Conduct on the Safety and Security of Radioactive Sources, Vieanna, Austria, 2004, pp. 4-5.

kalma olasılığını azaltmak veya bu kaynakların bireylere, topluma zarar vermek üzere kötü amaçlı kullanılması,

(c) Radyoaktif bir kaynağı içeren herhangi bir kaza veya kötü niyetli eylemin radyolojik sonuçlarını hafifletmek veya en aza indirmek,

(d) Bu hedeflere, ilk üretim aşamasından nihai bertaraf aşamasına kadar geçerli olan, radyoaktif kaynakların uygun bir düzenleyici kontrol sistemi kurulması ve bu tür kontrolün kaybedilmesi durumunda geri kazanılması için bir sistem kurulması yoluyla ulaşılması gerektirmektedir.

1.2.2.1.2. 2017 Tarihli Nükleer Malzemelerin ve Nükleer Tesislerin Fiziksel Korunmasına Dair Uluslararası Konferans

Konferansın amacı, yetkili makamlar, tesis işletmecileri, nakliyatçılar ve taşıyıcılar ile teknik destek örgütleri arasında, nükleer madde ve tesislerin ulaşımındaki nükleer malzeme dâhil olmak üzere, fiziki korunma ile ilgili bilgi, uygulama ve deneyimleri teşvik etmektir. [349] Konferans esnasında tartışılan ve emsal ve tavsiye niteliğinde şu noktalara değinilmiştir: [350]

1- Fiziksel koruma düzenleyici çerçevelerinin geliştirilmesi ve nükleer tesisler ile nükleer malzeme için taşımacılık sırasında da dâhil olmak üzere gereklilikleri paylaşmak; 2- Nükleer malzemenin kullanım, depolama ve nakliye ve nükleer tesislerin korunması için tehdit temelli, risk-bilinçli bir yaklaşımın kullanımı hakkında bilgi aktarımı; 4- Gelişen tehditlere nasıl cevap verileceğine dair bilgi değişimi; 5- Bilgisayar koruma dâhil olmak üzere, fiziksel koruma

[349] IAEA, General Conference: Resolution on Measures to Improve the Security of Nuclear Materials and Other Radioactive Materials, International Legal Materials, Vol. 41, No. 3, 2002, pp. 743–745.

[350] IAEA, International Conference on Physical Protection of Nuclear Material and Nuclear Facilities : https://www-pub.iaea.org/iaeameetings/50819/International-Conference-on-Physical-Protection-of-Nuclear-Material-and-Nuclear-Facilities (E.T: 06.04.18).

önlemlerinin ve sistemlerinin planlanması, kurulması, sürdürülmesi ve sürdürülmesi ile ilgili bilgi ve deneyim paylaşımı; 6- Fiziksel koruma önlemlerinin ve sistemlerin etkinliğini değerlendirmek için metodolojiler ve teknikler hakkında bilgi değişimi; 7- Nükleer malzeme ve tesislerin fiziki korunmasını iyileştirmek amacıyla ortak teknik önerilerin tartışılması; 9- Bir yandan nükleer malzeme muhasebesi ve kontrolü arasındaki ara yüzü ve nükleer malzemenin kullanımında, depolamada ve nakliyede fiziki olarak korunması; 10- Güvenlik ile güvenlik ara yüzleri ile ilgili deneyimleri paylaşma; 11- Nükleer güvenlik kültürünün değerlendirilmesi ve iyileştirilmesi ile ilgili deneyimlerin paylaşılması; 12- Nükleer tesislerdeki nükleer güvenlik olaylarına ve nükleer malzemenin taşınması sırasında (beklenmedik durum planları) planlama ve hazırlıklı olma ve bunlara müdahale etmektir.

1.2.2.2. BM Himayesinde Bağlayıcı Olmayan Düzenlemeler

BM nezdinde nükleer santrallerin güvenliğine dair çalışmalar 11 Eylül terör saldırılarıyla daha da artmıştır ve uluslararası kamuoyu oluşturulmaya çalışılmıştır. Alınan kararlar çoğunlukla bağlayıcı hükümler içerse de bazı düzenlemeler tavsiye niteliğinde olmuştur.

1.2.2.2.1. Birleşmiş Milletler Uluslararası Terörle Mücadele Stratejisi

Birleşmiş Milletler Uluslararası Terörle Mücadele Stratejisi, 8 Eylül 2006 tarihinde Üye Devletler tarafından benimsenmiştir. A RES/60/288 Sayılı Karar ve ekli Eylem Planı biçimindeki strateji, terörle mücadele için ulusal, bölgesel ve uluslararası çabaları geliştirmek üzere oluşturulmuş uluslararası tavsiye niteliğindeki bir çalışmadır. [351] Strateji, 19 Eylül 2006 tarihinde yapılan Genel Kurul toplantısında üst düzey bir toplantıda başlatılmış ve BM'ye üye 192 Devletinin terörle mücadelede ortak bir stratejik yaklaşım üzerinde anlaşmaya

[351] Dhanapala, Jayantha, The United Nations' Response to 9/11, Terrorism and Political Violence, Vol. 17, No. 1-2, 2005, pp.17-18.

vardığı ilk kez vurgulanmıştır. [352] Bu düzenleme 4 temel strateji belirler: 1- Terörizmin yayılmasına elverişli koşulları ele almak için bir eylem planı içerir; 2- Terörizmi önlemek ve mücadele etmek; 3- Terörle mücadele için devlet kapasitesinin inşa edilmesi için önlemler almak; Birleşmiş Milletlerin terörle mücadeledeki rolünü güçlendirmek; 4- Terörle mücadelede insan haklarına saygıyı sağlamaktır. [353]

1.2.2.3. EURATOM Himayesinde Bağlayıcı Olmayan Düzenlemeler

25 Mart 1957'de Roma'da imzalanan "Avrupa Atom Enerjisi Topluluğunu Kuran Antlaşma" (EURATOM), tarihsel ve kurumsal olarak uluslararası kamuoyunda aldığı kararlarla emsal teşkil edecek çalışmalarda bulunmuştur. Tarihsel olarak, 1951/52 yıllarında Belçika, Fransa, Almanya, İtalya, Lüksemburg ve Hollanda'nın kademeli olarak bütünleştirilmesi yönünde hareketin sonucu olarak Avrupa Kömür ve Çelik Topluluğu (CSC) kurulmuştur. EURATOM, o tarihten itibaren nükleer enerjinin kullanımı ve mukabil tedbirlere ilişkin bir dizi çalışmalar yürüterek bağlayıcı nitelikte olmayan düzenlemelerde bulunmuştur.

1.2.2.3.1. EURATOM Anlaşmasının 103. Maddesinin Uygulanmasına İlişkin Komisyon Tavsiyesi

EURATOM Antlaşması'nın 103. maddesi uyarınca, üye devletler, EURATOM Antlaşması'nın kapsamı içinde söz konusu antlaşmaların veya sözleşmelerin konularla ilgili olduğu ölçüde, üçüncü bir devlet, uluslararası bir örgüt veya üçüncü bir devletin vatandaşı ile Komisyon taslak anlaşmaları veya

[352] UN, United Nations General Assembly Adopts Global Counter-Terrorism Strategy: https://www.un.org/counterterrorism/ctitf/en/united-nations-general-assembly-adopts-global-counter-terrorism-strategy (06.04.18).
[353] Rosenow, Patrick, United We Fight? Terrorismusbekämpfung Im Rahmen Der Vereinten Nationen Seit Dem 11. September 2001, Die Friedens-Warte, Vol. 86, No. 3/4, 2011, pp. 15-17.

sözleşmelerle iletişim kurmak zorundadırlar. [354] Bir taslak anlaşma veya sözleşme antlaşmanın uygulanmasını engelleyen hükümler içeriyorsa, Komisyon bu tür bir bildirimin alınmasından itibaren bir ay içinde ilgili üye devlete yaptığı açıklamaları yapacaktır. Bir üye devlet, Komisyon'un itirazlarını yerine getirene veya Adalet Divanı'nın kararıyla, önerilen maddeleri antlaşma hükümleriyle uyumlu hale getirene kadar, önerilen anlaşmayı veya sözleşmeyi tamamlayamaz. [355] Bununla birlikte, son on yılda, EURATOM topluluk müktesebatı önemli ölçüde gelişmiştir. Yeni ikincil yasa nükleer tesislerin nükleer güvenliği, harcanan yakıt ve radyoaktif atıkların güvenli ve sorumlu yönetimi gibi alanları kapsamaktadır. [356] Ayrıca, radyasyon koruma gereksinimleri geliştirilmiştir. Bu nedenle, üye devletler, nükleer alanda üçüncü ülkelerle ikili anlaşmaların müzakere edilmesi sırasında, Euratom hukukunun artan miktarda şartı dikkate almak zorunda kalmışlardır. [357] İkincil hukuk eylemlerinin sayısı bu artış arz güvenliği açısından yenilenen faiz son yıllarda eşlik edilmiştir. Bu nedenlerle, Avrupa Komisyonu 103. maddenin tam kapsamı ile ilgili olarak daha özellikli rehberliğin garanti edildiği görüşündeydi. Bu nedenle, 4 Nisan 2016'da, Euratom Antlaşmasının 103. maddesinin uygulanmasına ilişkin bir tavsiye kabul edilmiştir. [358] Öneri, üye devletlere taslak anlaşmaların değerlendirilmesinde Komisyon tarafından özel olarak incelenecek hususlara ilişkin daha fazla yasal kesinlik sağlamayı amaçlamaktadır. Bu, komisyon tarafından itirazlara duyulan ihtiyacı azaltmalı ve böylece üye devletlerin ikili anlaşmalarının

[354] OECD-NEA, European Atomic Energy Community, Nuclear Law Bulletin, Vol. 2016/2, No. 98, 2016, p.85.
[355] EC, Commission Recommendation of 4.4.2016 on the Application of Article 103 of the Euratom Treaty : https://ec.europa.eu/energy/sites/ener/files/documents/1_EN_ACT_part1_v6_1.pdf (06.040.18).
[356] Ptasekaite, Rasa, The Euratom Treaty v. Treaties of The European Union: Limits of Competence and Interaction, The Swedish Radiation Safety Authority, Vol. 2011, No. 32, 2011, p.37.
[357] EC, Communication from the Commission Nuclear Illustrative Programme Presented Under Article 40 of the Euratom Treaty for the Opinion of the European Economic and Social Committee : http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52016DC0177 (06.040.18).
[358] Hartley, Trevor C., Federalism, Courts and Legal Systems: The Emerging Constitution of the European Community., The American Journal of Comparative Law, Vol. 34, No. 2, 1986, p. 232.

sonuçlandırılmasında gecikme riskini azaltmalıdır. [359] Bu tür anlaşmalar genellikle sivil nükleer programları, özel projeler personel değişimi işbirliği ve teknik bilgi veya uygulama başlatmak için üçüncü ülkelerle işbirliğinin temelini oluşturur ve böylece nükleer güvenlik, enerji politikası ve dış ticaret açısından büyük önem taşımaktadır. [360]

2. Nükleer Santrallerin Siber Güvenliği ve Uluslararası Hukuki Esasları

Nükleer enerji santralleri birçok ülke için önemli elektrik ve güç kaynağı olarak kabul edilmektedir. Ancak faydalarının yanı sıra, korumasız bırakılmaları durumunda potansiyel felaket riski de yüksektir. 1986 Çernobil kazası ve 2011 Fukushima Daichi nükleer felaketi, uygun güvenlik protokolleri takip edilmediği durumda ortaya çıkabilecek muhtemel hasarı göstermiştir. [361] UAEA başta olmak üzere nükleer santrallerin güvenliği ve korunmasına dair uluslararası düzenlemelerde bulunmuşlardır. Bu bağlamda nükleer santraller, diğer kritik altyapı gibi, siber saldırılara karşı daha hassas ve kırılgan olmasından dolayı tehdit riski yüksektir. Nükleer tesislerin dijitalleşme nedeniyle çok daha fazla siber tehdit riskine maruz kalması muhtemeldir ve bu alanda ilgili çalışmalar uluslararası kamuoyu nezdinde gerçekleşmeye devam etmektedir. [362]

---

[359] Smedt, Anne Boerger-De., Negotiating the Foundations of European Law, 1950—57: The Legal History of the Treaties of Paris and Rome, Contemporary European History, Vol. 21, No. 3, 2012, p. 339.

[360] Rasmussen, Morten., Establishing a Constitutional Practice of European Law: The History of the Legal Service of the European Executive, 1952—65, Contemporary European History, Vol. 21, No. 3, 2012, p. 382.

[361] Cimbala, Stephen J., Nuclear Deterrence and Cyber Warfare: Coexistence or Competition?, Defense & Security Analysis, Vol. 33, No.3, 2017, p.193.

[362] PWC, Why Nuclear Power Plants Are More Vulnerable to Cyber Attacks Today : https://www.pwc.com/us/en/industries/capital-projects-infrastructure/asset-classes-sectors/nuclear-power-industry/nuclear-cyber-security.html (E.T: 06.04.18).

2.1. Siber Güvenliğin Tanımı ve Kapsamı

Siber güvenlik, bilgisayar ve sunucuları, mobil cihazlar, elektronik sistemler, ağlar ve kötü niyetli saldırılardan verileri savunma uygulamalarıdır. Bilgi Teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinmektedir. [363] Siber güvenlik ayrıca bilgilerin çalınmasını, ele geçirilmesini veya saldırılmasını önlemek için önleyici yöntemleri de bünyesinde barındırmaktadır ve siber güvenlik stratejileri, kimlik yönetimi, risk yönetimi ve olay yönetimi içermektedir. Virüsler ve diğer kötü amaçlı kodlar gibi potansiyel bilgi tehditlerinin tanımlanarak savunma sisteminin geliştirilmesi gerekmektedir. [364] Konunun önemine binaen, ABD hükümeti siber güvenlik konusunda 2017 de 19 Milyar Dolar harcamıştır, [365] ancak siber saldırıların hızlı bir şekilde evrimleşmeye devam ettiği konusuna dikkat çekmektedir. UAEA'nın yapmış olduğu çalışmalara göre, nükleer santrallerin siber güvenliği açısından ise nükleer güvenlik, nükleer malzeme, diğer radyoaktif maddeler, ilgili tesisler veya ilişkili faaliyetler ve doğrudan veya dolaylı olarak kişilere, mülklere, topluma veya çevreye zararlı sonuçlara yol açabilecek diğer kasıtlı eylemlerin önlenmesi, tespit edilmesi ve bunlara yanıt verilmesini içermektedir. [366] Siber güvenlik kapsamında bilgisayar güvenliği bu hedeflere ulaşılmasını sağlamak için giderek daha önemli bir rol oynamaktadır. Siber güvenlik olgusunun nükleer santraller nezdinde öneme sahip olmasının sebebi ise tesisin emniyetli ve güvenli çalışması için ve hırsızlık, sabotaj ve diğer kötü niyetli eylemleri önlemek üzere kritik olan bilgisayar sistemleri, ağ ve dijital sistemleri korumak üzere dijital sistemler tarafından

[363] KASPERSKY, What is Cyber-Security? https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (06.04.18).
[364] McCoy, Frank, Job Horizon: So You Want To Be A Cyber Security Professional, US Black Engineer and Information Technology, Vol. 36, No. 4, 2012, p. 6.
[365] STATISTA, Proposed Budget of The U.S. Government for Cyber Security in FY 2016-2017 (in billion U.S. dollars) : https://www.statista.com/statistics/675399/us-government-spending-cyber-security/ (06.04.18).
[366] IAEA, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, Vienna, 2011, p.2.

santrallerin korunmasıdır. [367] Herhangi bir nükleer güvenlik olayı potansiyel veya nükleer güvenlik için fiili etkileri olan bir olay olarak karşımıza çıkmaktadır ve günümüz dijital çağında, siber saldırının nükleer güvenliği etkileyebileceği gerçeği göz önünde bulundurulmalıdır. [368] Siber güvenlik, siber terörizm kapsamında ele alındığında ise nükleer santrallerde bilgisayar tabanlı internet terörizmin yanı sıra potansiyel zararları öngörülebilen nükleer terörizm olarak da kabul edilmektedir. [369] Ayrıca, nükleer santrallere gerçekleştirilen siber saldırılar tek boyutlu olmayıp farklı tekniklerle bilgisayar sistemlerine hasar verilebilmektedir. Bunun sebepleri incelenecek olursa, Dijital Aygıt ve Kontrol (I&C) sistemleri, nükleer santralleri (npps) izleyen ve kontrol eden bilgisayar tabanlı cihazlardır ve Analog I&C sistemleri geleneksel olarak nükleer santrallerde izleme ve kontrol fonksiyonlarını gerçekleştirmek için kullanılmaktadır. [370] Ancak, III.+ ve IV. nesil reaktörleri dijital I&C sistemleri ile donatılmasından dolayı genel olarak, Npp kontrol ağları iletim ve dağıtım talepleri ile güç üretimini koordine etmek için SCADA sistemleri ile iletişim kurmaktadır. Dijital I&C sistemlerinin kurulması ve nükleer santrallerin kontrol ağları ile harici ağlar arasındaki bağlantı, nükleer reaktörlere karşı fiziksel zarar verebilen siber saldırılara açık alan bırakmaktadır. [371] Nükleer tesislerdeki siber saldırı açıklarından dolayı saldırılar çeşitlilik göstermektedir. Örneğin, nükleer santraller kurumsal ağ üzerinden Slammer Worm (Slammer Solucanı) saldırısı, santralin ağındaki veri trafiğini artırarak, tesisin Güvenlik Parametresi Görüntüleme Sistemi (SPDS) ve santral işlem bilgisayarlarının birkaç saatliğine erişilebilmesini engellemektedir ve nükleer santrallerin ağına sızarak sistemleri etkisiz hale

[367] A.e, s.3.
[368] IAEA, Computer Security Incident Response Planning at Nuclear Facilities, Vienna, 2016, p.4.
[369] Cho, Hyo Sung/Tae Ho Woo, Cyber Security in Nuclear Industry – Analytic Study from the Terror Incident In Nuclear Power Plants (NPPs), Annals of Nuclear Energy, Vol. 99, January 2017, p.47.
[370] Rrushi, J. and Campbell, R., 2008, in IFIP International Federation for Information Processing, Vol. 290; Critical Infrastructure Protection II, eds. Papa, M., Shenoi, S., (Boston: Springer), p.41.
[371] R. Krutz, Securing SCADA Systems, Wiley, Indianapolis, Indiana, 2006, p.10.

getirebilmektedir. [372] Nükleer santrallere gerçekleştirilen yaygın diğer saldırılardan bir tanesi de Stuxnet siber saldırısıdır. Diğer adı gelişmiş kalıcı tehdit (APT) olarak bilinen Stuxnet, bilgisayarlara bulaşmak üzere önceden bilinmeyen çok sayıda Windows güvenlik açığından yararlanan son derece karmaşık bir bilgisayar solucanıdır. [373] Amacı sadece bilgisayar sistemlerine zarar vermekle kalmayıp, özellikle nükleer silahlara ve reaktörlere güç veren zenginleştirilmiş uranyumu üretmek için kullanılan santrifüjleri hedeflemektedir. [374] Stuxnet ile ilgili diğer önemli bilgi ise her ne kadar uranyum zenginleştirme tesisinin kontrol sistemi dış ağdan yalıtılmış olmasa da, Stuxnet bir çalışan tarafından hedeflenebilir ve sistemin belirli bir bileşenini hedef alınabilmektedir. Böylelikle Stuxnet, yalıtılmış ağın bilgisayar korsanları tarafından da saldırıya açık hale getirilmektedir. [375] Sonuç olarak geçmişteki siber saldırılar, genellikle Hizmet Engelleme (DoS) saldırıları, bilgisayar virüsleri veya solucanları veya yetkisiz girişimler (hack) şeklinde genellikle tek boyutluyken saldırılar çoğunlukla web sitelerine, posta sunucularına veya istemci makinelere karşı başlatılmaktaydı. Bu siber tehditler, son zamanlarda teknolojiyle doğru orantılı bir şekilde temel olarak değişerek çeşitli saldırı araçları ve teknolojilerini kullanan ve / veya hedefleyen çok aşamalı ve çok boyutlu saldırılarla sonuçlanan bir çeşitliliğe bürünmüştür. [376]

---

[372] Kim, Do-Yeon, Cyber Security Issues Imposed on Nuclear Power Plants, Annals of Nuclear Energy, Vol. 65, March 2014, p.142.

[373] Kushner, David, The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware That Stymied Iran's Nuclear-Fuel Enrichment Program, IEEE, 26 Feb 2013 : https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (E.T: 07.04.18).

[374] Fruhlinger, Josh, What is Stuxnet, Who Created it and How Does it Work?, CSO, Aug 22, 2017: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html (E.T: 06.04.18).

[375] Kim, Heeeun et al., Identification of The Risk Induced by Malicious Attack on the NPP HMI system, Nuclear Safety and Simulation, Vol. 7, No. 2, December 2016, pp.153-154.

[376] Shen, Dan/ Genshe Chen/ Jose B. Cruz, Jr/ Erik Blasch/ Martin Kruger, Game Theoretic Solutions to Cyber Attack and Network Defense Problems, Twelfth International Command and Control Research and Technology Symposium (12th ICCRTS), 19-21 June 2007, Newport, RI, p.7.

2.2.Siber Saldırı, Siber Suç ve Siber Savaş Karşılaştırması

Siber saldırı, siber suç ve siber savaş olguları kavramsal olarak benzer anlamları çağrıştırsa da esasında farklı muhteviyatları içermektedirler. Siber saldırıların boyutunu anlamak için siber suçları da bilip ikisi arasındaki farkları anlamak gerekmektedir. Siber saldırı hakkında çeşitli tanımlar kullanılsa da bu tanımlar arasında ABD Savunma Bakanlığı'nın (DoD) uzun süren çalışmaları neticesinde getirdiği tanım önem arz etmektedir. Bu tanıma göre siber saldırı, bilgisayar veya ilgili ağları veya sistemleri kullanarak rakibin kritik siber sistemlerini, varlıklarını veya işlevlerini bozmaya ve / veya yok etmeye yönelik düşmanca bir eylemdir. [377] Bu tanım, altyapının bozulmasını veya yok edilmesini amaçlayan girişimleri içerir, böylelikle bu tür bir saldırının, tek başına fiziksel bilgisayar sistemlerine veya verisine yönelik hedeflenen sonuçları sınırlandırmamaktadır. [378] NATO'nun Tallinn El Kitabının 30. Maddesi ise siber saldırıyı, ister saldırgan ister savunmacı olsun, insanlara zarar vermesi veya ölümüne veya nesnelere zarar vermesine ya da tahrip olmasına neden olan bir siber operasyon olarak tanımlamaktadır. [379] Bu saldırılar, bilgisayar teknolojileri ortamındaki güvenliğin standart hedefleri olarak kabul edilen bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini bozmayı amaçlamaktadır. [380] Esas itibariyle gizlilik, "verileri gizli ve özel tutma" anlamına gelirken bütünlüğü ise verilerin güvenilmez hale gelmesi için "izinsiz olarak değiştirilmediğinden veya işlevsiz hale getirilmediğinde" emin olmayı ifade etmektedir ve kullanılabilirlik, "sistemi öngörüldüğü gibi kullanabilmek" anlamına gelmektedir. [381] Tanımından dolayı, bu

[377] The US Department of Defense, the DoD Cyber Strategy, April 2015: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (E.T: 07.04.18).
[378] Çelikpala, Mitat, Cyber Security and Nuclear Power Plants: International Frameworks, EDAM, 05.04.2016: http://edam.org.tr/en/cyber-security-and-nuclear-power-plantsinternational-frameworks/#_ftn4 (08.04.18).
[379] CCDCOE, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: https://ccdcoe.org/tallinn-manual.html (E.T: 08.04.18).
[380] Singer, P.W. / Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs To Know, Oxford, OUP, 2014, p.36
[381] A.e., s.34-35.

saldırılar neredeyse tüm devlet faaliyetlerine ve kritik altyapıya işaret etmektedir. Siber saldırının farklı tanımlarının karşılıklı kaygısı, bunu stratejik amaçlara yönelik olarak bilgisayar sistemlerinin ve / veya kritik altyapının unsurlarına doğrudan girme girişimi olarak görmektedir. [382] Saldırganlar siber saldırıları yürütürken, karmaşık yöntemler kullanarak bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini bozmaya çalışmaktadırlar. [383]

Siber suç, analitik düzlemde siber saldırılardan kavramsal olarak farklı olsa da henüz uluslararası kamuoyunda tam anlamıyla tanımlanmamıştır. [384] Siber suç, hızla büyüyen bir suç alanı olmakla birlikte giderek daha fazla suçlu, fiziksel veya sanal hiçbir sınır tanımayan, ciddi zararlara neden olan ve dünya çapındaki kurbanlar için çok ciddi tehditler oluşturan çeşitli suç faaliyetlerini yürütmek üzere internetin hızını ve kapasitesini düşüren bir teşebbüstür. [385] Bir bilgisayar, donanımı veya yazılımı çalındığında bir suçun 'nesnesi' haline gelebilirken [386] sahtekârlık, hırsızlık, gasp gibi geleneksel suçları işlemek için ya da DDoS saldırıları, kötü amaçlı yazılımlar (Malware), kimlik hırsızlığı, çocuk pornografisi veya telif hakkı ihlalleri gibi 'yeni' suç faaliyeti türleri bir 'araç' olarak kullanıldığında siber suçun 'konusu' haline gelebilmektedir. [387] Siber suçun kavram ve mahiyeti, yeni internet ortamlarının, siber suç gruplarının ve yeni 'akıllı' virüslerin bir sonucu olarak son zamanlarda önemli ölçüde değişmiştir. [388] Yeni erişilebilir teknolojilerin geliştirilmesi ve internetin genişlemesi ile birlikte

[382] Pool, Phillip, War of the Cyber World: The Law of Cyber Warfare, The International Lawyer, Vol. 47, No. 2, 2013, p.303.
[383] Satapathy, C. , Impact of Cyber Vandalism on the Internet, Economic and Political Weekly, Vol. 35, No. 13, 2000, p.1060.
[384] Hathaway, Oona A. / Rebecca Crootof, The Law of Cyber-Attack, Faculty Scholarship Series, Paper 3852, Vol. 100, No. 817, 2012, p.833.
[385] INTERPOL, Cybercrime : https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (E.T: 08.04.18).
[386] Brenner, S./ LL Clarke, Distributing Security: Preventing Cyber Crime, John Marshall Journal of Computer and Information Law, Vol.23, No.4, Summer 2005, p. 6.
[387] Brenner, S. / Bert-Jaap Koops, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, p.7.
[388] Brenner, S., Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law, Murdoch University Electronic Journal of Law, Vol.8, No. 2, June 2001, p. 2.

yeni suçlu davranış biçimleriyle sonuçlanmıştır. [389] Böylelikle siber suç, sınırları ve çerçevesi tam olarak tanımayan bir hal almıştır. [390] Bu sınır, bir ülkede işlenen yasadışı eylemlerin başka bir ülkede doğrudan ve ivedi etkisi olabileceği için, fail ve suçun mağduru için gereksiz bir durumdur ve bu 'yeni' suç eylemleriyle mücadele etmek için uluslararası kamuoyunda özel bir mevzuat oluşturma ihtiyacına yol açmıştır. [391] Teknolojik ivme ile birlikte kavramsal olarak siber suçlar bir dizi aktivite arasında değişmektedir. Bir noktada, dijital depolarda tutulan bilgilerin bütünlüğü ve bir kuruma ya da bir kişiye şantaj yapmak için yasadışı yollarla elde edilen dijital bilginin kullanımına yönelik saldırılar gibi kişisel ya da kurumsal mahremiyetin temel ihlallerini içeren suçlardır. [392] Bilgisayarın siber suçtaki rolü, bilgisayarın bir nesne, bir araç veya bilgisayar olarak çevre veya bağlam olarak kullanılabileceği dar veya geniş anlamda sınıflandırılabilir. Siber suçlar aşağıdaki gibi geniş bir şekilde sınıflandırılabilir: [393] 1- Bireylere karşı siber suçlar, 2- Mülkiyete karşı siber suçlar ve 3- Hükümetlere/Kurum ve Kuruşlara/Topluma karşı siber suçlardır. Böylesi siber suçlarda, bireysel kişiler etkilenir. Bireylere karşı siber suçların amacı hırslı ve naif tip insanların zayıflığından istifade etmektir. Bu örnek dâhilinde özel olarak çocuk pornografisi, gizlilik ihlali, e-posta sahtekârlığı yoluyla bir kişinin tacizi, hackleme, siber saptırma, iftira, hile, dolandırıcılık, e-posta sahtekârlığı, şifre çalma, kredi kartı sahtekârlığı, kumar vb. örneklerdir. [394] Mülkiyete karşı siber suçlar olarak Fikri Mülkiyet Suçları, siber işgal, siber vandalizm, sistemin işlevlerini bozan / veriyi silecek veya ekli cihazların arızalanmasına yol açan kötü

[389] Cassim, Fawzia, Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players, The Comparative and International Law Journal of Southern Africa, Vol. 44, No. 1, 2011, p. 124.

[390] BBC, Cybercrime and Fraud Scale Revealed in Annual Figures, 19 January 2017 : http://www.bbc.com/news/uk-38675683 (E.T: 08.04.18).

[391] Granville, Johanna, The British Journal of Criminology, The British Journal of Criminology, Vol. 43, No. 2, 2003, p. 452.

[392] Dennis, Michael Aaron, Cybercrime, 3-9-2018: Encyclopedia Britannica: https://www.britannica.com/topic/cybercrime (E.T: 09.04.18).

[393] Arora, Bhavna, Exploring and Analyzing Internet Crimes and their Behaviours, Perspectives in Science, Vol. 8, September 2016, p. 541.

[394] Furnell, Steven/ David Emm/ Maria Papadaki, The Challenge of Measuring Cyber-Dependent Crimes, Computer Fraud & Security, Vol. 2015, No. 10, October 2015, pp.6-7.

amaçlı yazılımların iletilmesi, siber izinsiz giriş, internete dayalı hırsızlıklar mülkiyetlere karşı en popüler siber suçlardan birkaçıdır. [395] Son olarak Hükümetlere/Kurum ve Kuruşlara/Topluma karşı siber suçlar, bireylerin ve grupların, uluslararası hükümetleri ve bir ülkenin vatandaşlarını tehdit etmek için elektronik medyayı ve siber uzayı kullanarak, bir hükümet veya askeri web siteleri saldırıya uğradığında ve hayati bilgiler alındığında karşı tarafı teröre maruz bıraktığından dolayı diğer iki siber suçtan daha tehlikeli ve kapsamlıdır. [396]Organizasyona ve topluma karşı siber suçlar, bilgisayar, yetkisiz giriş, DDoS saldırıları, kötü amaçlı yazılım saldırıları, Usenet grubundan çıkan suçlar, endüstriyel ajanlık / casusluk, ağ saldırıları, kalpazanlık, web sayfası çökertme vb. saldırı türleri olarak karşımıza çıkmaktadır. [397] Bu bağlamda, siber suç, gelişmekte olan bir uluslar üstü suç türüdür ve en hızlı büyüyen bir suç türü olarak internetin hayatımızın neredeyse zorunlu bir parçası haline gelmesiyle, tüm dünyada bilgi ve iletişim sağlayan suçlular da bu konuda avantaj sağlamaktadır. [398] Dünya çapında iki milyardan fazla kullanıcısı olan siber uzay, suçlular için ideal bir yer haline gelmiştir çünkü onlar, bilerek veya bilmeden, çevrimiçi olarak sakladığımız her türlü kişisel bilgiye anonim olarak erişebilir ve erişim sağlayabilmektedirler. [399] İnternet güvenliğine yönelik tehditler son yıllarda

[395] Willis, Terry D., Criminal Liability in Cyberspace, GPSolo, Vol. 23, No. 1, 2006, pp. 37-38.
[396] Moslemzadeh, Pardis Tehrani/ Nazura Abdul Manap/ Hossein Taji, Cyber Terrorism Challenges: The Need for A Global Response to A Multi-Jurisdictional Crime, Computer Law & Security Review, Vol. 29, No. 3, June 2013, p. 208.
[397] Zulkefli, Zakiah/ Manmeet Mahinderjit Singh/ Azizul Rahman Mohd Shariff/ Azman Samsudin, Typosquat Cyber Crime Attack Detection via Smartphone, Procedia Computer Science, Vol. 124, 2017, p.666.
[398] Eliasson, Jan, Cyber Crimes, UNIS: http://www.unis.unvienna.org/unis/en/events/2015/crime_congress_cybercrime.html (09.04.18).
[399] Grimes, Roger A., Why it's So Hard to Prosecute Cyber Criminals: The Bad Guys Are Wreaking Havoc. Why Can't They Be Brought to Justice?, December 6, 2016: https://www.csoonline.com/article/3147398/data-protection/why-its-so-hard-to-prosecute-cyber-criminals.html (E.T: 09.04.18).

büyük ölçüde artmıştır ve siber suçlar artık dünya çapında 431 milyondan fazla yetişkin kurbanı etkilemektedir. [400]

Şekil 8: Siber Saldırı Çeşitleri

By Victim Count			
Crime Type	**Victims**	**Crime Type**	**Victims**
Non-Payment/Non-Delivery	81,029	Lottery/Sweepstakes	4,231
Personal Data Breach	27,573	Corporate Data Breach	3,403
419/Overpayment	25,716	Malware/Scareware	2,783
Phishing/Vishing/Smishing/Pharming	19,465	Ransomware	2,673
Employment	17,387	IPR/Copyright and Counterfeit	2,572
Extortion	17,146	Investment	2,197
Identity Theft	16,878	Virus	1,498
Harassment/Threats of Violence	16,385	Crimes Against Children	1,230
Credit Card Fraud	15,895	Civil Matter	1,070
Advanced Fee	15,075	Denial of Service	979
Confidence Fraud/Romance	14,546	Re-shipping	893
No Lead Value	13,794	Charity	437
Other	12,619	Health Care Related	369
Real Estate/Rental	12,574	Terrorism	295
Government Impersonation	12,344	Gambling	137
BEC/EAC	12,005	Hacktivist	113
Tech Support	10,850		
Misrepresentation	5,436		
Descriptors*			
Social Media	18,712	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.	
Virtual Currency	1,904		

Kaynak: FBI, 2016, s.17. [401]

Siber suç ve çeşitlerine dair detaylı açıklamalar EK 5'te[402] izah edilmekle birlikte, FBI'ın 2016 da yayınladığı çalışmada da görüldüğü üzere DDoS ve kötü amaçlı yazılım (Malware) saldırıları başta olmak üzere diğer saldırı türleri de eklendiğinde, bu siber saldırılardan zarar gören kurban sayısı yüzbinleri

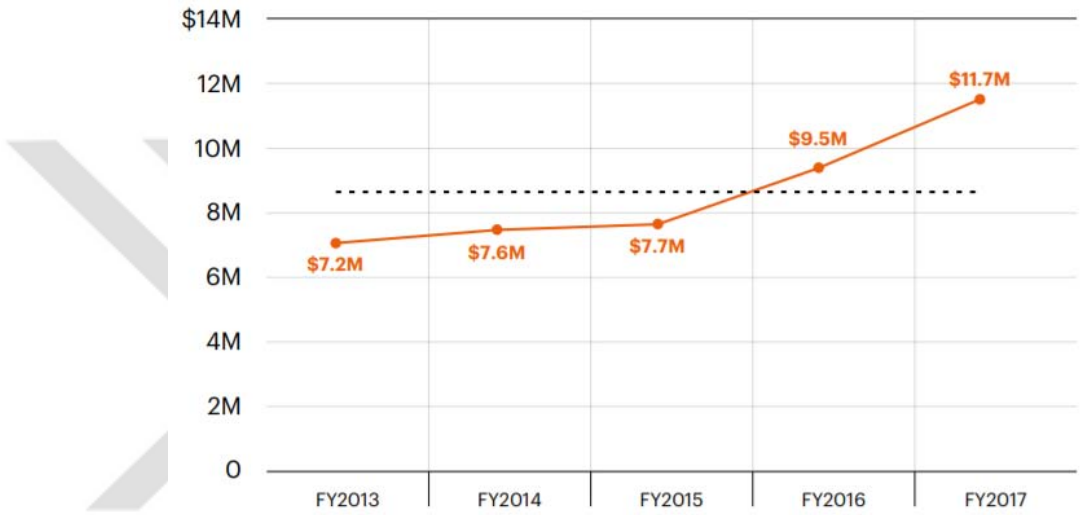
[400] Driscoll Aimee O', 100+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2018 EDITION], February 15, 2018: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/ (E.T: 09.04.18).

[401] FBI, 2016 Internet Crime Report, Internet Crime Complaint Center, 2016, p.17.

[402] Alpna et al., Cyber Crime-Its Types, Analysis and Prevention Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 6, No. 5, May 2016, pp. 145-146.

bulabilmektedir. Şekil 9 [403] da görüldüğü üzere, siber saldırılardan dolayı son beş yılda küresel ortalama maliyeti küçümsenmeyecek ölçüde fazladır. İlk üç yıl boyunca istikrarlı bir artış sonrasında, 2017 deki önemli artış, %27,4'lük bir artışla devam etmiştir. 2013-2017 arasındaki toplam maliyet ise $43,7 Milyon Dolar olarak belirtilmiştir.

Şekil 9: 2013-2017 arası Küresel Siber Suç Ortalama Maliyeti



Kaynak: Ponemon, 2017, s.12.

Siber savaş, siber uzayda bilgi ve bilgisayar ağlarına saldırmak ve savunmak, aynı zamanda bir rakibin de aynısını yapma yeteneğini engelleyerek [404] siber savaş, casusluk veya sabotaj amacıyla bir hedefin stratejik veya taktiksel kaynaklarına saldırmak için 'hack'lemenin kullanılması anlamına gelmektedir. [405] BM, 'siber' kelimesini "İnternete dâhil bilgisayarların, iletişim altyapısının,

[403] Ponemon, Cost of Cyber Crime Study: Insights on the Security Investments That Make a Difference, 2017, s.12: https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50 (10.04.18).
[404] Kenneth V. Peifer, B.S, An Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy, December 1997 : http://iwar.org.uk/iwar/resources/usaf/maxwell/students/1997/peifer_kv.pdf (E.T: 11.04.18).
[405] FORBES, How Does Cyber Warfare Work?, Jul 18, 2013: https://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/#2bda262044ce (E.T: 11.04.18).

çevrimiçi kaynakların, veri tabanlarının ve genel olarak Net olarak bilinen bilgi sistemlerinin küresel sistemi"[406] olarak tanımlasa da siber savaş ile ilgili henüz tanım getirememiştir. [407] Siber savaş kavramının genel kabul görmüş bir tanımı olmamakla birlikte, Bilgisayar Ağ Saldırısı (CNA), (saldırgan) bilgi operasyonu (IO) ve bilgi savaşı (IW) terimleri sıklıkla birbirinin yerine kullanılmaktadır. [408] ABD Savunma Bakanlığı (DOD), CNA'yı "bilgisayar ağlarında veya bilgisayarlarda bulunan bilgilere hasar vermek, engellemek veya yok etmek üzere bilgisayar ağının kullanımı yoluyla gerçekleştirilen eylemler" [409] olarak tanımlamaktadır. Siber savaş aynı zamanda askeri bir çatışma sırasında, yabancı ülkelerin siber saldırıları sadece bilgi çalmakla kalmayıp sivil ekonominin altında yatan kritik altyapı sistemlerini, devlet kurumlarının işleyişini ve askeri operasyonlarını zedelemelerini veya engellemelerini kapsayabilmektedir. [410] Modern siber savaş, telgraf, telefon ve telsizle birlikte, hem sivil hem de askeri liderler, asker hareketleri ve konuşlandırmalar gibi uzun mesafeli telekomünikasyonlarla bağlantılıdır. [411] Mevcut tahminler ışında, küresel siber kayıpları 2021 yılına kadar $6 Trilyon Dolar 'a ulaşıp, bunun gelecekte daha da artacağını düşünülmektedir ve bu yüzden "toplumun bütünü" ilgilendiren siber savaşla mücadele etmek için 180° yaklaşımını gerektiren mücadele ve strateji geliştirmek gerekmektedir. [412]

---

[406] UN, Cybersecurity: A Global Issue Demanding a Global Approach, 12 December 2011, New York : http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html (E.T: 11.04.18).

[407] Andress, Jason/Steve Winterfield, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Elsevier-Syngress, Waltham, MA, 2011, p.3.

[408] Döge, Jenny, Cyber Warfare: Challenges for the Applicability of the Traditional Laws of War Regime, Archiv Des Völkerrechts, Vol. 48, No. 4, 2010, p.488.

[409] DOD, s.7.

[410] Vatis, Michael, The Next Battlefield: The Reality of Virtual Threats, Harvard International Review, Vol. 28, No. 3, 2006, pp. 59–60.

[411] Limnéll, Jarno, The Command Imperative: Crafting Protocols for Cyber Conflict, Georgetown Journal of International Affairs, 2014, p.526.

[412] Fleming, T. Casey, et al., The Secret War Against the United States: The Top Threat to National Security and the American Dream Cyber and Asymmetrical Hybrid Warfare An Urgent Call to Action, The Cyber Defense Review, Vol. 2, No. 3, 2017, p.29.

Şekil 10: 'Yeni' Küresel Rekabetçi Model: Asimetrik Hibrid Savaşlar

Kaynak: Fleming et al, 2017, s.31.

Birçok saldırı yöntemi unsurlarını bünyesinde barındıran siber savaş, Şekil 10 da da belirtildiği üzere askeri olmayan siber saldırıların yaygın bir türü olan teknolojij savaş (technological warfare), medya savaşı (media warfare); askeri ordular arasındaki istihbarat savaşı (intelligence warfare) ve askeri savaşlarda terörist ve gerilla (terrorist and guerrilla) saldırıları siber savaş türlerinin başını çekmektedir. Genel çerçevede ise siber savaş, Şekil 10 da bahsi geçen Asimetrik Hibrid Savaşların (AHW) tamamını kapsamaktadır. Bu bilgiler bağlamında, siber-uzmanlar ve askeri strateji uzmanları, henüz bir siber savaşın gerçekleşmemesine rağmen, önümüzdeki birkaç yıl içinde büyük bir devletlerarası siber savaşın gerçekleştirilebileceğini öngörmektedirler. [413] Uluslararası hukuk perspektifinden bu duruma dair endişe verici durum ise, şu anda ortaya çıkan bu tehdide ilişkin

[413] Hodge,Nathan, General: We Just Might Nuke Those Cyber-Attackers, WIRED, 13 May 2009, https://www.wired.com/2009/05/general-we-just-might-nuke-those-cyber-attackers/ (E.T: 11.04.18).

yetersiz hukuki düzenleme ve yönetişim sistemlerinin var oluşudur çünkü küresel toplumlar, hem en temel hem de en kritik işlevleri için siberuzaya daha fazla bağımlı hale geldikçe, tam ölçekli bir siber saldırıdan kaynaklanan ekonomik ve sosyal etki, modern bir devleti yıkabilme potansiyeline sahiptir. [414] Bununla birlikte, geleneksel savaş gibi siber savaş da araçsaldır: Savaşan taraflar, bazı siyasi amaç veya hedefler doğrultusunda onlara saldırarak düşmanlarına iradesini dayatmaya çalışmaktadırlar. [415] Ancak, geleneksel savaşın aksine, siber savaşın yalnızca siberuzayda meydana geldiği bilgisi ışığında, bilgisayar sunucularını veya telekomünikasyon kablolarını bombalayarak sanal ağları fiziksel olarak yok eden "kinetik" eylemlerin bir siber savaş değil, geleneksel bir savaş biçimi olduğunu unutmamak gerekmektedir. [416]

Tablo 4: Farklı Siber Eylemlerin Temel Özellikleri

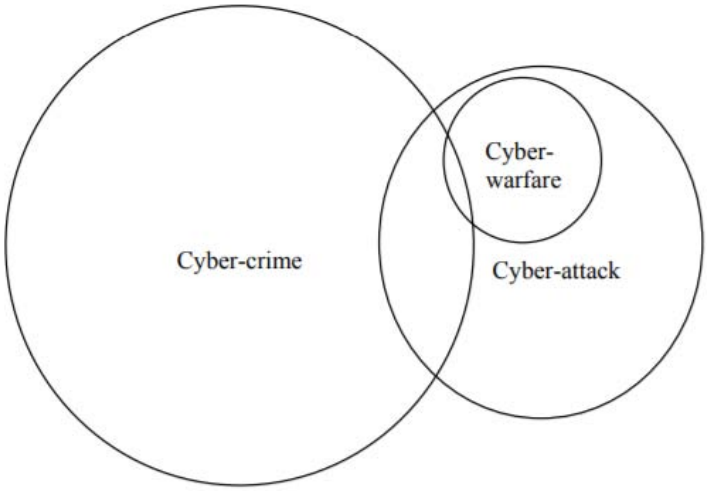
	Siber Saldırı Çeşitleri		
	Siber Saldırı	**Siber Suç**	**Siber Savaş**
Yalnızca devlet dışı aktörleri içermektedir		√	
Bir bilgisayar sistemi ile işlenen ceza hukuku ihlali olmalıdır		√	
Amaç, bilgisayar ağının işlevini zayıflatmaktır	√		√
Politik veya ulusal bir güvenlik amacına sahip olmalıdır	√		√
Etkiler bir "silahlı saldırı" ya eşdeğer olmalı ya da silahlı çatışmalar bağlamında bir etkinlik olmalıdır			√

[414] Hughes, Rex, A Treaty for Cyberspace, International Affairs (Royal Institute of International Affairs 1944-), Vol. 86, No. 2, 2010, pp. 524.
[415] Carl von Clausewitz, on War, Edited and Translated by Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976); Thomas Rid, Cyberwar and Peace: Hacking Can Reduce Real-World Violence, Foreign Affairs, Nov./Dec. 2013, pp. 77-87.
[416] Kenney, Michael, Cyber-Terrorism in a Post-Stuxnet World, Orbis, Vol. 59, No. 1, 2015, p. 114.

Kaynak: Hathaway/Crootof, 2012, s.833.

Siber savaş eylemi diğer saldırı türleri ile kıyaslandığında mahiyet ve kapsam olarak en nitelikle siber eylem olarak karşımıza çıkmaktadır.

Şekil 11: Siber Eylemler Arasındaki İlişki



Kaynak: A.e, s.833.

NOT: **Cyber-Crime**: Siber Suç, **Cyber-Warfare**: Siber-Savaş, **Cyber-Attack**: Siber Saldırı (*Çev. Cihad Furkan ELİAÇIK*)

Siber savaş da siber saldırı ve siber suçu teşkil edebilmektedir. Şekil 11'deki üç çember arasındaki kesişim alanı, devlet dışı bir aktör tarafından gerçekleştirilen iki tür saldırıyı içermektedir. Öncelikle siber savaş, bir bilgisayar ağının politik veya ulusal güvenlik amacıyla işlevini baltalayan, ceza hukukunu (örneğin savaş suçları) ihlal eden ve bir bilgisayar veya ağ sistemi aracılığıyla işlenen silahlı çatışma bağlamında yapılan saldırıları içermektedir. [417] Ayrıca siber savaş, geleneksel bir silahlı saldırıya eşdeğer etki yaratan saldırıları, bir bilgisayar ağının politik veya ulusal güvenlik amacıyla işlevini zayıflattığını ve bir bilgisayar

[417] Lotrionte, Catherine, A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence, Georgetown Journal of International Affairs, 2013, p. 84.

sistemi ya da ağı aracılığıyla işlenen ceza hukukunun ihlal edildiğini göstermektedir. [418]

2.3.Güncel Siber Saldırılar

Siber saldırı türleri başlığında da detaylıca izah edildiği üzere, siber saldırılar daha büyük maddi ve fiziki hasarlara yol açmak için teknolojik aygıtlara gerçekleştirilmektedir. Nükleer santrallere gerçekleştirilen siber saldırılar ise başlıca Stuxnet, DDoS ve Malware türü siber saldırılardır.

Tablo 5: Nükleer Tesislere Gerçekleştirilen Siber Saldırı Örnekleri

Tarih	Santral	Açıklama
Ocak 2003	Davis- Besse (ABD)	Harici bir ağdan kaynaklanan Slammer solucanı, lisans alanın kurumsal ağını (gizli bağlantıyla) etkiledi ve ardından kontrol sistemi ağına yayıldı. Güvenlik Parametre Görüntüleme Sistemi (SPDS) ve Santral İşlem Bilgisayarı (PPC) birkaç saatliğine erişilemedi. Santral olay anında çevrim dışı kalmıştır.
Ağustos 2006	Browns Ferry (ABD)	Ağ donanımının arızalanması, tesisin su devridaim pompaları için değişken frekanslı sürücü kontrol ünitelerini kilitleyen çok sayıda ağ trafiği yarattı.
Mart 2008	Hatch (ABD)	Bir mühendis, kurumsal ağda bir bilgisayar üzerinde bir yazılım güncellemesi gerçekleştirmiştir. Ancak, bu bilgisayar kontrol ağında başka bir sistemle iki yönlü iletişim kurdu. Güncellenen bilgisayar yeniden başlatıldığında, kontrol ağı sistemi üzerindeki veriler sıfırlanmıştır.
2010 da	Natanz	Zenginleştirme için kullanılan santrifüjleri devre dışı

[418] Geist, Edward, Deterrence Stability in the Cyber Age, Strategic Studies Quarterly, Vol. 9, No. 4, 2015, p. 49.

farkedilmiştir	(İran)	bırakmak için santral bilgisayarlarına saldırılmıştır.
Ocak 2014	Monju (Japonya)	Bir bilgisayardaki bir yazılım güncellemesi kötü amaçlı yazılım tarafından kontrol odası bilgisayarına erişmeye çalışmıştır.
Nisan 2016	Gundremmingen (Almanya)	Conficker ve W.32 Ramnit dahil olmak üzere kötü amaçlı yazılımlar, birkaç bilgisayar ve tesisteki medya (örneğin, USB flash sürücüler) üzerinde keşfedildi.

Kaynak: Varuttamaseni/Bari/ Youngblood, 2017, s.107. [419]

Nükleer santrallere gerçekleşen siber saldırılar Tablo 5 ten ibaret olmamakla birlikte siber saldırı teşebbüsleri günden güne hızlanmaktadır. Dünya genelinde ise gerek nükleer santrallere gerekse kişi ve kurumlara karşı gerçekleşen siber saldırıların yüzdesi neredeyse ikiye katlanarak, 2016 yılına göre aynı döneme kıyasla ortalama % 26'dan % 48'e yükselmiştir. [420] WannaCry ve NotPetya gibi son zamanlarda gerçekleşen siber saldırı türleri de yaygınlaşmaktadır. Teknolojiye endeksli bir şekilde siber saldırı türleri de değişip gelişmektedir. Daha ayrıntılı siber saldırı örnekleri EK 6[421] da izah edilmiştir.

2.4.Nükleer Santrallere Karşı Siber Saldırı Senaryoları

Nükleer santraller (NPP'ler) başta olmak üzere altyapılara yönelik siber saldırılar son zamanlarda, nükleer santrallerin eski analog sistemlere göre önemli avantajlar elde etmek üzere dijitalleştirilmesiyle birlikte siber saldırılara karşı savunmasızlıklarını aynı doğrultuda arttırmıştır. [422] Harici veya dâhili kötü niyetli

[419] Varuttamaseni, Athi /Robert A. Bari/ Robert Youngblood, Construction of a Cyber Attack Model for Nuclear Power Plant, NPIC&HMIT 2017, San Francisco, CA, June 11-15, 2017, p.107.
[420] CHECKPOINT, What is a Cyber Attack? : https://www.checkpoint.com/definition/cyber-attack/ (E.T:11.04.18).
[421] A.g.e.
[422] Kim, Hee Eun et al, Systematic Development of Scenarios Caused By Cyber-Attack-Induced Human Errors in Nuclear Power Plants, Reliability Engineering and System Safety, Vol. 167, 2017, p. 290.

bir saldırgan tarafından yapılan saldırı, verilerin gizliliğini, bütünlüğünü veya kullanılabilirliğini ihlal edebilmektedir. Bu nedenle, bir I&C nükleer santral sistemine karşı gerçekleştirilebilecek siber saldırı, sistematik olarak kazanın başlamasıyla radyoaktif malzemenin çevreye salınmasına neden olabileceğinden, siber saldırılara karşı siber saldırı senaryolarının kuvvetli olması gerekmektedir. [423] Bu bağlamda, nükleer santralleri işleten kuruluşlar acil durum planları ile ilgili etkili testler ve eğitim için gerçekçi siber saldırı senaryolarına sahip olmaları gerekmektedir. [424] Bu tür uygun siber saldırı senaryoları, nükleer santrallerin siber güvenliği için gereklidir ve aşağıdaki faaliyetler için de kullanılabilir: [425]

- saldırıların doğasını anlamak;
- bir saldırı veya saldırganın kullanabileceği potansiyel mekânları anlamak;
- tasarım temelli tehditler geliştirmek (DBT'ler);
- karşı önlem tanımı;
- risk yönetimi;
- etki (penetration) testi;
- siber güvenlik planlarını ve programlarını uygulamaktır.

NSS-17 Ek I'de, saldırı senaryoları geliştirme sürecinin bir örneğini vermektedir. Verilen örnekte, saldırı senaryoları aşağıdaki adımları içeren ayrıntılı bir açıklama olarak tanımlanmıştır: [426]

- hedef tanımlama;
- keşif;

[423] Fovino IN, Guidi L, Masera M, Stefanini A. Cyber Security Assessment of A Power Plant, Electr Power Syst Res, Vol.81, 2011, p.26.
[424] USNRC, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71, January 2010, p.6.
[425] Ten, Chee-Wooi/ Manimaran Govindarasu / Chen-Ching Liu, Cybersecurity for Critical Infrastructures: Attack and Defense Modeling, IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, Vol. 40, No. 4, 2010, p.855.
[426] USNRC, s.9.

- sistem erişimi / uzlaşma;
- saldırı uygulaması;
- saldırıyı engellemek için aşamaların öngörülmesidir.

Nükleer santrallere karşı saldırgan, ilk siber saldırıyı kasıtlı olarak başlatan potansiyel bir tehdit aracı veya bir grup tehlike aracıdır. Bir saldırgan, nükleer santrallerin iç sistemine doğrudan erişimi olup olmamasına bağlı olarak, dâhili veya harici saldırgan olarak sınıflandırılmaktadır. [427] Tablo 6, tahmin edilebilir, tipik nükleer santral saldırganlarını listelemektedir.

Tablo 6: Nükleer Santrallere Karşı Saldırganlar

Saldırganlar	Örnekler
Dâhili / İçerideki Saldırganlar	- Davetsiz misafir - Gizli ajan - Hoşnutsuz çalışan / kullanıcı - Üçüncü taraf / refakatçi personel
Harici / Yabancı Saldırganlar	- Kötü Amaçlı Yazılım - Hacker - Hoşnutsuz çalışan / kullanıcı (tesiste artık çalışmamaktadır) - Nükleer enerjiye karşı rakip Militanlar - Organize suçlar - Teröristler - Ulus devletler

Kaynak: Ahn et al, 2015, s.5.

[427] Ahn, Woogeun et al, Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs, International Journal of Distributed Sensor Networks, Vol. 2015, Article ID 836258, 2015, p.5.

Siber saldırılarına karşı önleyici tedbirlerin geliştirilmesinde, saldırıların ve saldırı veya saldırganların ilgili bilgileri elde etmek ve hedef bilgisayar sistemlerine erişmek için kullanabilecekleri potansiyel mekânları anlamak önem arz etmektedir. UAEA NSS 17 No'lu çalışmasında tasvir edilen saldırılar kurgusal olsa da, diğer endüstrilerde görülen benzer saldırılar üzerine inşa edilen makul senaryolarla ilgilidir ve nükleer santrallere gerçekleştirilebilecek siber saldırı senaryoları UAEA'nın EK 7[428] deki çalışmasında ayrıntılandırılmıştır.

2.5.Siber Güvenliğin Hukuki Esasları

Nükleer santrallerin güvenliği ve emniyeti başlığı altında 'siber güvenliği'ne dair ulusal ve uluslararası çalışmalar mevcuttur. Bu konu dâhilinde ulusal ve uluslararası hukuki rejim oluşturma çabaları sürmektedir.

2.5.1. Ulusal Mevzuat

Siber suçlarla ilgili ulusal mevzuatımızda çeşitli tanımlamalar yapılsa da,[429] siber güvenliğe dair hukuki düzenlemeler dolaylı bir şekilde ele alınmıştır, doğrudan düzenlemeler ise son zamanlarda ilgili makamlar tarafından yapılmaktadır. Bu doğrultuda siber suçlarla ilgili kavram sorunu doğmuştur ve bu nedenle mutlak hükümlerin tekâmül evresine ulaşabilmesi için multi-disipliner bir yaklaşımla ele alınması gerekmektedir. [430] Bilişim suçu tanımı kapsamında doktrinde ve uygulamada kimi zaman bilgisayar suçu ve bilişim suçu birbirinin yerine kullanılmıştır." [431] Bu bilgiler ışığında, "Siber suçların Türk Ceza Kanunu'nda ilk yer alışı, 6 Haziran 1991 tarihli 3756 Sayılı Türk Ceza

[428] IAEA, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, Vienna, 2011, pp. 55-57.
[429] Çakır, Hüseyin, Güncel tehdit: Siber Suçlar, Seçkin Yay., Ankara, 2014, s. 21.
[430] Erdoğan, Yavuz, Türk Ceza Kanununda Bilişim Suçları: Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle, Legal Yay. , İstanbul, 2013, s. 47.
[431] Karagülmez, Ali, Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri, Seçkin Yay. Ankara, 2014, s. 54.

Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun ile olmuştur. Bu değişikliğin 20. maddesi ile "Bilişim Alanında Suçlar" başlığı altında bir bap eklenmiş ve bir bilgisayardan programların, verilerin veya diğer unsurların hukuka aykırı olarak ele geçirilmesi veya bunların başkasına zarar vermek üzere kullanılması, nakledilmesi veya çoğaltılması yasayla ceza unsuru olarak kabul edilmiştir."[432] Bu gelişmeler ışığında daha sonra "Eylül 2004'te yürürlüğe giren 5237 sayılı Türk Ceza Kanunu ile tanım genişletilerek siber suç kavramı da ceza kanununa eklenmiştir. Burada "Bilişim Alanında Suçlar" başlığını taşıyan 10. Bölümde üç grup faaliyet bilişim suçu olarak tanımlanmaktadır: 243. maddede 'Bilişim sistemine girme'; 244. maddede sistemi engelleme, bozma, verileri yok etme veya değiştirme ile 245. maddede banka veya kredi kartlarının kötüye kullanılması." [433] Ayrıca 5809 sayılı Elektronik Haberleşme Kanunu'na 2014 yılında eklenen EK MADDE 1 – (Ek: 6/2/2014-6518/106 md.) doğrultusunda, UDHB Bakanının başkanlığında, kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur. [434]

Siber güvenlik ile ilgili alınması gereken tedbirler, görev ve yetkiler Kanun seviyesinde UDHB görev ve yetkileri arasında tanımlanmıştır: [435]

"**Madde 5** – (1) h) (Ek: 6/2/2014-6518/102 md.) Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, Siber Güvenlik Kurulunun sekretaryasını yapmak, ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber

[432] Bıçakcı, Salih, /F.Doruk Ergün/Mitat Çelikpala, Türkiyede Siber Güvenlik, EDAM, 1. Baskı, İstanbul, Mart 2016, s.30.
[433] A.e.
[434] Göçoğlu, Volkan, Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi, Hacettepe Üniversitesi, Yayınlanmamış Doktora Tezi, 2018, s.153.
[435] DİJİTAL DÖNÜŞÜM: Siber Güvenlik Mevzuatı: https://www.dijitaldonusum.gov.tr/siber-guvenlik-mevzuati/ (11.04.18).

müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak."

2013-2014 Eylem Planı 4. Maddesi uyarınca Telekomünikasyon İletişim Başkanlığı tarafından siber güvenlik ile ilgili tehdit ve alınacak önlemlere ilişkin ulusal ve uluslararası çalışmalar yapmak için Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) kurulmuştur. [436] Bu merkez; "ülkemizin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerini azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla kurulmuştur. Aynı şekilde, ulusal ve uluslararası seviyede siber ortamda ortaya çıkan tehditler ile ilgili kendisine ulaştırılan ihbarları da değerlendirerek, söz konusu tehditlerin tespit ve bertaraf edilmesi için Kamu Kurumları ve özel kişiler ile koordinasyonunu sağlamaktadır. Bu itibarla gelen ihbar ilk aşamadan başlanarak, çözüm sürecine kadar takip edilerek değerlendirilmektedir. Diğer taraftan ulusal ve uluslararası siber güvenlik tatbikatları düzenlenerek kamu kurum ve kuruluşlarının siber saldırılara karşı farkındalığının ve hazırlığının arttırılması faaliyetleri ile bilinçlendirme ve yönlendirme faaliyetlerini sürdürmektir." [437] Bu gelişmeler doğrultusunda 11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ kapsamında Kurumsal SOME'ler (Siber Olaylara Müdahale Ekipleri) kurulması kararlaştırılarak ilgili birimlerin çalışma usul ve esasları belirtilmiştir. [438] Devam eden çalışmalar bağlamında, UDHB nin 2016-2019 Ulusal Siber Güvenlik

[436] A.e.
[437] USOM, USOM Hakkında : https://www.usom.gov.tr/hakkimizda.html (11.04.18).
[438] Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, Resmi Gazete, 11.03.13, Sayı: 28818 : http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm (E.T: 12.04.18).

Stratejisi ve Eylem Planı ise siber güvenliğe dair mevzuatın kapsam ve muhteviyat eksenli genişleten bir çalışmadır. Bu kapsamda, "bu planın ana amacı; siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılmasıdır. Bu ana amacı gerçekleştirmek üzere, hedeflerin ve alt eylem maddelerinin belirlenmesi, bunların gerçekleştirilmesinin sağlanması ve denetlenmesi de bu dokümanın amaçlarındandır. [439]

Bu amaçlar doğrultusunda: [440]

-Ulusal siber uzayın tamamını kapsamak şartıyla, bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve bilgi/veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin, gizliliğinin ve mahremiyetinin sağlanmasına,

- Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kolluk kuvvetlerince daha etkin araştırılmasının ve soruşturulmasının sağlanmasına,

-Siber güvenliğin, gizliliğin ve mahremiyetin sağlanmasında kritik teknolojilerin ve ürünlerin ülkemizde üretilmesine, üretilemiyorsa, dışarıdan alınan teknoloji ve ürünlerin salt bu maksatla ve güvenle kullanılabilmesini sağlayacak önlemlerin alınmasına yönelik bileşenler bu planda yer almaktadır.

---

[439] UDHB, 2016-2019 Ulusal Siber Güvenlik Stratejisi, s.9 : http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (12.04.18).
[440] A.g.e., s. 9-10.

3 Nisan 2018 tarihinde Akkuyu Nükleer Güç Santralleri (NGS)'nin inşaatının başlanmasına ilişkin resmi tören, Cumhurbaşkanı Recep Tayyip Erdoğan ve Rusya Federasyonu Devlet Başkanı Vladimir Putin'in katılımıyla gerçekleşmiştir. [441] Bununla birlikte nükleer santrallerin siber güvenliğini doğrudan mercek altına alan hukuki düzenleme henüz tam olarak mevzuata girmemiş olsa da konu ile ilgili farkındalık ve ihtiyaçlara ilişkin açıklamalar bürokrasinin en üst mercilerinden gelmeye başlamıştır. Zira Başbakan Binali Yıldırım 29 Kasım 2017 de Ankara'da düzenlenen Netaş 50. Yıl Etkinliğinde, "siber tehditlere yönelik önlemlerin 'gecikmesiz' alınması gerektiğini söyleyerek, bu alandaki açıklara dikkat çekmiştir. Yıldırım, 'Gelecek 5 yılda on binlerce siber güvenlik uzmanına ihtiyacımız olacak' şeklinde ifadede bulunmuştur. [442]

Ulusal mevzuatta genellikle bilişim hukuku bağlamında değerlendirilen siber saldırılar, "sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK 244. md.) başlıklı maddenin 1. fıkrasında 'bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır' şeklinde karşılık bulmaktadır."[443] Ayrıca, "bilgisayar sistemlerinin güvenilirliğine, dokunulmazlığına ve tasarruf edilebilirliğine yönelik saldırılar, hem bu saldırıların sıklığı ve zarar verme potansiyelleri hem de hukuksal sorunlar açısından bilgisayar suçlarının çekirdek alanını oluşturmaktadır." [444] Bilişim yoluylaişlenen hakaret suçlarında soruşturma ve kovuşturma usulü başlığı aldında suç vasfının tayini amacıyla araştırılacak hususlar bağlamında ise "suç bir bütün olarak değerlendirilip yazı sahibinin asıl kastı araştırılmalıdır."[445]

---

[441] AKKUYU NÜKLEER, Projenin Tarihçesi: http://www.akkunpp.com/projenin-tarihcesi (E.T: 12.04.18).
[442] MİLLİYET, Başbakan Yıldırım: Onbinlerce Siber Güvenlik Uzmanına İhtiyaç Olacak, 29.11.2017: http://www.milliyet.com.tr/basbakan-yildirim-teknolojiler-siyaset-2563498/ (E.T: 12.04.18).
[443] Parlar, Ali, Türk Ceza Hukukunda Bilişim Suçları, Bilge Yay. Ankara, 2011, s.24.
[444] Sieber, Ulrich, Bilgisayar Suçluluğu, Ünver Yener (ed.), İnternet Hukuku, (İstanbul: Seçkin Yay., Birinci Baskı, Nisan 2013,), s. 26.
[445] Demir, Ömer/ Mehmet Arıç/Halil Polat, Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar: Soruşturma ve Kovuşturma Yöntemleri, Adalet Yay. İstanbul, 2015, s. 195.

Bilişim suçları bağlamında değerlendirilen siber suçlar, kapsam ve mahiyet itibariyle sınır aşan suçlar teşkil etmektedir. "Bilişim suçları genellikle bir ağ ile birbirine bağlı olan sistemler üzerinde ve/veya aracılığıyla işlenmektedir. Bugün için en yaygın ağ sistemi "internettir".[446] Sınıraşan nitelikte olmasından dolayı kapsama alanı da aynı orantıda artmaktadır.

2.5.2. Uluslararası Düzenlemeler

Nükleer santrallerin siber güvenliğine dair ulusal mevzuatta olduğu gibi uluslararası hukuk rejim ve düzenlemelerinde de alandaki boşluğu tamamıyla giderecek düzenlemeler bulunmamaktadır. UAEA nükleer altyapı güvenliği ve küresel ölçekte standartlaştırılması konusunda çalışan en önemli uluslararası kuruluş olmakla birlikte bilgisayar güvenliği ortamını hızla değişen ve gelişen bir senaryo olarak tanımlamaktadır. [447] Nükleer santrallerin bilgisayar güvenliği noktasında UAEA nın çalışmaları bulunurken, BM'nin "Barış için Atom" açılımıyla başlayan süreden bu yana Genel Kurulda uluslararası gelişmeler neticesinde aldığı kararlar santrallerin fiziki güvenliği noktasında ülkeleri bilgilendirmektedir. NATO, bu hususta nükleer santrallere karşı tedbirleri siber savaş bağlamında ele alırken, Estonya'da kurulan NATO Müşterek Siber Savunma Merkezinde (NMSSM) siber saldırılara karşı çalışmalar yürüterek 'siber tatbikatlar yürütmektedir.

Aynı şekilde kapsamlı bir uluslararası yasal çerçeve şu anda tüm siber saldırıları ihtiva etmese de, ABD ve diğer ülkelerin konu ile ilgili gerçekleştirdikleri çalışmalar bu büyüyen tehdidi kontrol etmek üzere kullanabilecekleri bazı düzenlemeler sunmaktadır. Siber saldırıları doğrudan

[446] Dülger, Volkan, Bilişim Suçları ve İnternet İletişim Hukuku: 6518, 6526, 6527 ve 6552 Sayılı Yasa Değişiklikleri İle, Seçkin Yay., Ankara, 2014, s. 185.
[447] IAEA, Resolutions and Other Decisions of the General Conference: GC55/Res/10 Nuclear Security, Adopted by the General Conference on Fifty-fifth Regular Session 19-23 September 2011, p.3.

düzenlemek için Birleşmiş Milletler, NATO, Avrupa Konseyi, Amerikan Devletleri Örgütü ve Şangay İşbirliği Örgütü tarafından oluşturulan yasal mekanizmaları incelemek, alanda yapılan çalışmaların mahiyetini anlamak için önem ar etmektedir. Hem Avrupa Konseyi hem de Amerikan Eyaletleri Örgütü siber suçla ilgili çalışma ve eylemlerde bulunurken, yukarıda da belirtildiği gibi kısmen siber saldırılarla örtüşen bir faaliyet kategorisi, artan bilgisayar ağı koruması ve siber saldırılarla savaşmak üzere düzenlemeleri de yine bu sahada gösterilen çabalarla ilgilidir. Genel olarak bu organize önlemler, ortak hukuki çerçeveler aracılığıyla bu konuyu ele almaktadır. Yine de bu çabalar, tüm siber saldırıları etkili bir şekilde yönetebilecek sıkı bir yasal çerçevenin oluşturulma noktasında yetersiz kalmıştır.

2.5.2.1. 'Karşı Tedbirler' Bağlamında Siber Saldırı Değerlendirmesi

Karşı Önlemlere Dair Uluslararası Teamül Hukuku, devletlerin kendini savunma mekanizmaları dâhilinde (yani, dolaylı olarak siber saldırıları da dâhil olmak üzere) kendini savunma amaçlı bir silahlı saldırı seviyesine yükselmeden uluslararası hukuk ihlallerine karşı nasıl tepki vereceğini ele almaktadır. [448] Devlet Sorumluluğu ile ilgili Taslak Sözleşmeler, karşı önlemleri, "Sorumlu Devlete karşı zarar görmüş bir Devletin uluslararası yükümlülüklerine aykırı olan önlemler ve tazminat temin etmek için ikincisinin uluslararası haksız fiiline tepki olarak önceden elde edilmemesi..." olarak tanımlamaktadır. [449] Uluslararası karşı tedbirler kanunu Karşı Önlemlere Dair Uluslararası Teamül Hukuku, bir siber saldırının ne zaman yasa dışı olduğu tanımlanmamaktadır. Buna ilaveten, Taslak Sözleşmeler doğrudan siber saldırıları ele almamaktadır. Uygulama esasında hukuk, bir devletin uluslararası bir hukuk ihlaline maruz kaldığında, sebep olan

[448] McLaughlin, Kevin L.,Cyber Attack! Is a Counter Attack Warranted?, Information Security Journal: A Global Perspective, Vol.20, No. 1, 2011, p.61.

[449] Ruiz, Gaetano Arangio, Fifth report on State Responsibility, A/CN.4/453 and Add.1-3, United Nations, Extract from the Yearbook of the International Law Commission: 1993 Document, Vol. II (1), p.109.

devlete karşı tedbirle karşılık verebileceğini belirtmektedir. [450] Bu bağlamda, herhangi bir silahlı saldırı seviyesine çıkmayan bazı siber saldırılar, yine de, müdahale etmeme kuralı ekseninde uluslararası teamül hukuku kurallarını ihlal etmektedir. Uluslararası hukukun bu ihlalleri, sorumlu devleti yasaya uygun hale getirmek için zarar verici devlete karşı önlemler almaya hak kazandırabilmektedir. [451] Bununla birlikte, BM Sözleşmesi, "saldırganlık eylemlerini" yasaklamaktadır ve barış zamanında "tehdit veya güç kullanma" yı kısıtlamaktadır. [452] Sözleşmenin 41. Maddesi, Güvenlik Konseyi'nin, "ekonomik ilişkilerin, demiryolu, deniz, hava, posta, telgraf, radyo ve diğer iletişim araçlarının tamamen veya kısmen kesintiye uğraması ve diplomatik ilişkilerin sona erdirilmesi" yoluyla bu kısıtlamaların uygulanmasına katkıda bulunmaktadır. Bu tedbirlerin yetersiz kalması halinde, Madde 42 de bahsi geçen, "uluslararası barış ve güvenliği sağlamak veya yeniden düzenlemek için gerekli olabilecek hava, deniz veya kara kuvvetleri" gibi eylemler noktasında destek sağlamaktadır. Bu tür eylemler, gösteriler, abluka ve hava, deniz veya kara kuvvetleri tarafından yapılan diğer işlemleri içerebilmektedir. [453] Bir BM üyesi, herhangi bir "silahlı saldırı" ya maruz kalırsa, sözleşme, kendisine bireysel ve kolektif savunma hakkını saklı tutmaktadır. Ancak, kuvvet uygulanmayan bir eyleme karşı tepki vermek yasaktır. BM Genel Kurulu'nun 3314 Sayılı Kararı, [454] saldırganlığı "silahlı kuvvetin kullanımı… bir başka devletin egemenliğine, toprak bütünlüğüne veya siyasi bağımsızlığına, ya da [BM] Sözleşmesine herhangi bir şekilde aykırı ya da karşı olmak" olarak tanımlamaktadır. Saldırganlık örnekleri olarak, karar işgalci güçlerin işgali, saldırı, işgal, bombardıman ve ablukayı belirtmektedir. [455]

---

[450] A.g.e., s.120.
[451] Grove, G./ S. Goodman / S. Lukasik, Cyber-Attacks and International Law, Survival, Vol. 42, No. 3, 2000, p.91.
[452] BM Genel Kurulununun A/RES/29/3314 Sayılı Kararı.
[453] Grove, s.93.
[454] UN, Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX), 14 December 1974 : http://hrlibrary.umn.edu/instree/GAres3314.html (E.T: 12.04.18).
[455] Hua, Jian / Sanjay Bapna, How Can We Deter Cyber Terrorism?, Information Security Journal: A Global Perspective, Vol. 21, No. 2, 2012, p.110.

Bir olgunun ya da saldırının bir güç eylemi olup olmadığını etkileyebilecek faktörler, beklenen ölümcül, yıkıcı ve saldırganlığa bağlı olarak belirlenmektedir. Ölümcüllük, hem birincil hem de makul bazı ikincil etkilerden kaybedilen yaşamlarla ölçülürken; yıkıcılık maddi mallara verilen zararı yansıtmaktadır ve saldırganlık ise, egemen bir düşmanın coğrafi topraklarına saldırı anlamına gelmektedir[456]. Mevcut görüş, ekonomik yaptırımların ve diplomatik tepkilerin BM Şartı altında güç oluşturmadığı yönündedir. Dahası, Madde 41, haberleşmeyi (communication) kesintiye uğratmanın kendiliğinden bir güç kullanımı olmadığını öne sürmektedir. 2. madde, "herhangi bir devletin toprak bütünlüğü veya siyasi bağımsızlığına" karşı güç kullanımını yasaklamaktadır. Madde 2'nin yasaklamalarının Madde 41'in ışığında yorumlanması da, bir bilgi işleminin haberleşmeyi, öldürücü olmayan, tahribatsız ve saldırgan olmayan bir şekilde kesintiye uğratmak için kullanılmasının, Sözleşme dâhilinde izin verilebileceği sonucuna varılmaktadır. [457]

Bu bilgiye ilave olarak, öldürücü, yıkıcı veya istilacı bilgi operasyonları (siber saldırılar) açıkça bir güç kullanımı anlamına gelebilmektedir. Bazı bilgi teknolojisi operasyonları, silahlı kuvvet kullanımına eşdeğer bir tahribata neden olabilir ve bu nedenle kendileri de kuvvet kullanımı olarak kabul edilebilmektedir. [458] Örneğin, baraj kontrol sistemine kötü amaçlı (malware) saldırısı yaparak arızaya sebebiyet vermek, bir şehri yok edebilecek bir sele neden olmak, açıkça bir güç kullanımı teşkil edecektir. Borsaların çökmesine neden olarak büyük ekonomik krizlere neden olan daha da azaltılmış yıkım biçimlerinin güç kullanımının olduğu da benzer örneklerdendir. [459] Açıkça bir güç kullanımı oluşturan eylemler ile açıkça oluşturmayanlar arasında büyük bir gri alan bulunmaktadır. Genellikle 41. Madde tarafından yetkilendirilen kuvvet

[456] Ellis, LTC Bryan W., The International Legal Implications and Limitations of Information Warfare: What are Our Options?, U.S. Army War College, 10 April 2001, pp. 4-6.
[457] Greenberg, Lawrence T. /Seymour E. Goodman/Kevin J. Soo Hoo, Information Warfare and International Law, National Defense University Press, Washington, DC, 1998, pp- 7-11.
[458] Grove, s.94.
[459] Sharp, Walter Gary, CyberSpace and the Use of Force, Aegis Research Cooperation, The USA, p. 102.

uygulanmamış bir misilleme olarak haberleşme kesintisi veya ekonomik ilişkiler, yetkilendirilmemiş olan ve aslında Madde 42 tedbirlerinin etkisiz kalması durumunda, Madde 42'de izin verilen abluka ile gerçekleştirilebilmektedir. Bu nedenle, haberleşmeyi kesmek için yapılan 41. Maddeyi harekete geçiren bir Güvenlik Konseyi kararı, söz konusu abluka haberleşmeyi kesmeye çalışsa bile, herhangi bir ablukaya izin vermemektedir. Bunun yerine, 42. Maddeye göre bir karar gerekli olacaktır. [460] Bu bilgiler ışığında, bazı bilgi operasyonları güç kullanımı ve diğerlerinin olmadığı ve durumun her zaman net olmayacağını unutmamak gerekmektedir. Gerçek dünyada, özellikle bilgi işlemlerinin etkileri iyi anlaşılmadan önce, bir kararlılığa ancak gözlemlenen ölümcül, tahrip edici ve saldırganlık temelinde ulaşıldıktan sonra ulaşılabilir. [461] Ayrıca, bilgi işlemlerinin, bunları başlatan devlet tarafından öngörülemeyen ya da tasarlanamayan etkileri olabilmektedir. Örneğin, güç kesintisi yoluyla istihbarat toplama operasyonunu devre dışı bırakmak için tasarlanan bir saldırı, elektrik kesintisinin yayılması ve kritik sistemlerin hastanelerde ve havaalanlarında başarısız olmasına neden olursa, ölümlere yol açabilmektedir. [462]

BM Sözleşmesine ek olarak, Uluslararası Adalet Divanı (UAD) altı davada, uluslararası teamül hukuku kurallarına ve yasal kullanım için geçerli olan genel prensiplerin kuvvet kullanımına işaret etmiştir. Bunlar: Silahlı saldırı veya askeri müdahaleyi meşru müdafaa konusunda haklı kılmak için değil, saldırının da meşru müdafaaya sebebiyet verecek nitelikte olmalıdır; öz-güvenliğin gerçekleştirildiği devlete atfedilebilir olmalıdır; kuvvet kullanımı son çare olmalıdır ve savunmayı sağlama konusunda başarılı olmalı ve maruz kaldığı zarar ile orantılı olmalıdır. [463] Bu koşulları siber güç eylemlerine uygulamayı denemek,

[460] Haataja, Samuli, The 2007 Cyber Attacks Against Estonia and International Law on the Use Of Force: an Informational Approach, Law, Innovation And Technology, Vol. 9, No. 2, 2017, p. 163.
[461] Kulesza, Joanna, International Internet law, Global Change, Peace & Security, Vol. 24, No. 3, 2012, p.360.
[462] Meulenbelt, Stephanie, The 'Worm' as a Weapon of Mass Destruction, The RUSI Journal, Vol. 157, No. 2, 2012, p. 64.
[463] O'Connell, Mary Ellen/ Louise Arimatsu, Cyber Security and International Law Meeting Summary, Chatnam House, London, the UK, 29 May 2012, p. 10.

imkânsız değilse de zordur. Somut nesnelerin zarar görmesi, sadece İran'daki Stuxnet saldırısı durumunda meydana gelmiştir. Bu tür bir hasar, silahlı saldırıların BM Sözleşmesi Madde 51'i tetiklemek için yeterli ya da önemli olduğu anlamına gelmemektedir. [464] UAD, Nikaragua davasında şöyle demektedir: [465] "Silahlı saldırıların yasaklanması, bölgeye herhangi bir devlet tarafından silahlı grupların gönderilmesi için geçerli olabilir. Başka bir devlet, eğer böyle bir operasyon varsa, ölçeği ve etkileri nedeniyle, düzenli bir silahlı kuvvetler tarafından gerçekleştirilmiş bir sınır olayından ziyade silahlı saldırı olarak sınıflandırılmış olacaklardır." UAD, Petrol Platformları, Wall Advisory Opinion ve Kongo Demokratik Cumhuriyeti (DRC) vs. Uganda davasında şiddet eyleminin "ölçek ve etkileri" dâhilinde benzer değerlendirmelerde bulunmuştur. Stuxnet saldırısı yasadışıyken silahlı saldırıya eşdeğer olmadığını belirtmek gerekmektedir. [466]

2.5.2.2.Siber Saldırıları Doğrudan Düzenleyen Uluslararası Hukuk Rejimleri

Yukarıdaki başlıkta da belirtildiği üzere, nükleer santrallerin siber güvenliğine geçmeden önce siber saldırıları doğrudan düzenleyen bir hukuk metni yoktur ancak uluslararası hukuki düzenlemeleri ilgili bazı uluslararası kurum/kuruluşlar nezdinde hukuki rejim oluşturma çabaları mevcuttur.

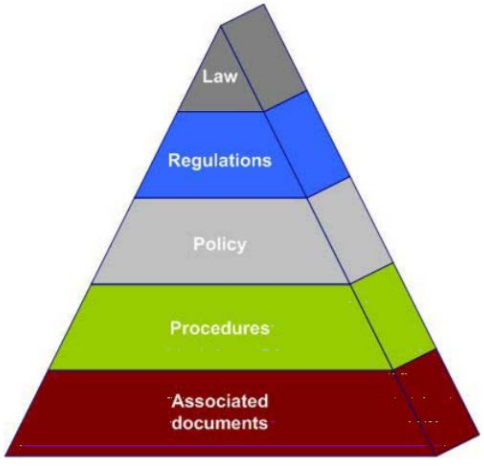
2.5.2.2.1. UAEA

Nükleer ve radyolojik tesislerde bilgisayar tabanlı sistemlerin kullanımı, standart olmayan pek çok bilgi teknolojisi sisteminin kullanımı dâhil olmak üzere, artmaya devam etmektedir. Tüm bu sistemlerin kötü niyetli bilgisayar tabanlı eylemlere karşı güvenli bir şekilde korunması önemliyken aynı zamanda,

[464] A.g.e, s.12.
[465] ICJ, Case Concerning Military and Paramilitary Activities in and Against Nicaragua, Judgement of 27 June 1986, p. 93. : http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (E.T: 12.04.18).
[466] O'Connell, s.13.

bilgisayar ağları ve bilgisayar tabanlı sistemler, kötü niyetli eylemler için daha büyük bir hedef haline gelmiştir. Bilgisayar güvenliği, dijital verilerin korunması ve sistemlerin ve ağların zararlı eylemlere karşı korunması ile ilgilidir. [467] Bilgisayar tabanlı sistemler aynı zamanda tesislerin yönetmelik ve gözetiminde yetkilileri desteklemektedir. UAEA, Devletlere kapsamlı bilgisayar ve bilgi güvenliği faaliyetleri geliştirmede yardımcı olmak için rehberlik ve eğitim sağlamaktadır. UAEA için bir devletin temel rolü nükleer güvenlik ve genel olarak bilgisayar güvenliği için yasal çerçevenin oluşturulmasıdır. Bunlar, uygulanacak olan nükleer tesislerin güvenliği üzerinde büyük bir etkiye sahip olmalıdır. Devletin hukuk sistemi, en azından hassas bilgilerin korunmasını kapsayan ve nükleer güvenlik ihlallerini azaltacak/yok edecek herhangi bir faaliyeti ele alan yasama ve düzenleyici çerçeveyi sağlamalıdır. [468] Bu bağlamda, UAEA nükleer santrallerin güvenliğine dair devletler için hukuki norm oluşturmuştur ve nükleer santral kuracak devletlerin de nükleer güvenlik için bu hukuki sıralamaya dikkat etmelerini talep etmiştir.

Şekil 12: UAEA Nezdinde Nükleer Santrallerin Güvenliğinin Hukuki Normları



Kaynak: IAEA, a.g.e, s.9.

[467] IAEA, Computer and Information Security : https://www.iaea.org/topics/computer-and-information-security (E.T: 12.04.18).
[468] IAEA, NSS No.17, s.9.

NOT: Law: Kanun, **Regulations**: Yönetmelikler, **Policy**: Politikalar, **Procedures**: Usuller, **Associated Documents**: İlişkili Belgeler (*Çev. Cihad Furkan ELİAÇIK*)

Şekil 12, bir nükleer tesiste bilgisayar güvenlik programının kurulması ve uygulanması ile ilgili normatif araçların hiyerarşisinin basitleştirilmiş bir görselleştirmesini göstermektedir. Sorunlarının özgünlüğü nedeniyle, bilgisayar güvenliği, bilgisayar sistemleriyle ilişkili benzersiz suçları ve çalışma modlarını dikkate almak için özel yasal hükümlere ihtiyaç duyabilmektedir. Devletler, mevcut mevzuatlarının, bilgisayar yardımı ile gerçekleştirilebilecek kötü niyetli eylemleri yeterince kapsayıp kapsamadığını dikkatlice değerlendirmelidirler. [469] Diğerleri arasında, bilgisayar güvenliğini ve uygulanmasını etkileyebilecek önemli yasalar şunlardır: [470]

- Bilgisayar suçlarıyla ilgili yasalar;
- Terörle ilgili yasalar;
- Kritik ulusal altyapının korunması ile ilgili yasalar;
- Bilgilerin ifşa edilmesini öngören yasalar;
- Kişisel bilgilerin gizliliği ve kullanımı ile ilgili yasalardır.

UAEA, nükleer santrallerin siber güvenliğine dair hukuki rejim oluşma çabaları başka kanyaklarda da mevcuttur. NSS No.13, NSS No.10, NSS No.8, NSS No.7 ve International Law Series No. 4, bu konu ile ilgili sürdürülen diğer çalışmalar arasındadır.

2.5.2.2.2. BM

[469] IAEA, Conducting Computer Security Assessments at Nuclear Facilities, Vienna, 2016, pp. 4-6.
[470] IAEA, Computer Security Incident Response Planning at Nuclear Facilities, Vienna, 2016, pp. 11-16.

Siber güvenlik konusunda sınırlı sayıda BM düzenlemeleri olmuştur. BM Genel Kurulu, ilgili konu hakkında çeşitli ilgili kararlar almıştır. [471] Bununla birlikte, bu kararlar belirsizdir ve BM üyeleri tarafından herhangi bir özel işlem gerektirmemiştir. [472][473] Ağustos 1999'da, Birleşmiş Milletler, gelişmekte olan bilgi teknolojilerinin güvenlik etkilerini daha iyi kavramak için Cenevre'deki uzmanlardan oluşan uluslararası bir toplantıya sponsor olmuştur. [474] 2002 yılında yapılan bir Genel Kurul kararı, "bilgi güvenliği" hakkında daha fazla araştırma yapmak ve tartışmak için çağrıda bulunmuştur. Karar, uluslararası bilgi güvenliği konularıyla ilgili yeni bir çalışma çağrısında da bulundu, ancak küçük eylemler sonuçlanmıştır. [475] Birleşmiş Milletler, 2003 ve 2005 yıllarında Bilgi Toplumu Dünya Zirvesi olarak adlandırılan, ancak yine de çok az somut sonuçlarla, iki aşamalı bir zirveye sponsor olmuştur. [476] Temmuz 2010'da Birleşmiş Milletler, ABD, Çin ve Rusya gibi büyük siber güçler de dâhil olmak üzere on beş ülkeden siber güvenlik uzmanlarının BM Genel Sekreteri'ne bir dizi öneri sunduğunda, konu ile ilgili önemli bir adım atılmıştır. Bu girişim aynı zamanda yeni teknolojilerin gerektirdiği güvenlik ve istikrar için uluslararası çerçeveyi oluşturmaya yönelik ilk adımdır." [477] Bu öneriler şu talepleri içermekteydi: [478]

---

[471] Bkz: BM Genel Kurulunun Res. 58/32 Sayılı Kararı, BM'nin A/RES/58/32 Sayılı 8 Aralık 2003 Tarihli Kararı, BM'nin A/RES/59/61 Sayılı 3 Aralık, 2004Tarihli Kararı, BM'nin A/RES/60/45 Sayılı 6 Ocak 2006 Tarihli Kararı, BM'nin A/RES/61/54 Sayılı 19 Aralık 2006 Tarihli Kararı, BM'nin A/RES/62/17 Sayılı 8 Ocak 2008 Tarihli Kararı, BM'nin A/RES/63/37 Sayılı 9 Ocak 2009 Tarihli Kararı, , BM'nin A/RES/64/25 Sayılı 14 Ocak 2010 Tarihli Kararı.

[472] UN, Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, A/RES/58/199, 30 January 2004: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (E.T: 12.04.18).

[473] UN, Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures, G.A. Res. 64/211, U.N. Doc. No. A/RES/64/211 (Mar. 17, 2010).

[474] UN, Developments in the Field of Information and Telecommunications in the Context of International Security, G.A. Res. 54/49, 4 December 1998 : https://gafc-vote.un.org/UNODA/vote.nsf/958591109a21b54c05256705006e0a5c/0e4088ff35d5505d0525681200673c74?OpenDocument&ExpandSection=5 (E.T: 12.04.18).

[475] Bkz: BM Genel Kurulunun G.A. Res. 61/54, G.A. Res. 62/17, G.A. Res. 63/37 ve G.A. Res. 64/25 Sayılı Kararları.

[476] WSIS, 2003 Tunis 2005 : http://www.itu.int/net/wsis/index.html (E.T: 12.04.18).

[477] U.N. Secretary-General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 4, UN, Doc.

- Devletlerarasında daha fazla diyaloğun esas alınması;

- Güven oluşturma, istikrar ve risk azaltma önlemleri. . . Çatışmada [bilgi ve iletişim teknolojileri] kullanımına ilişkin ulusal görüş alışverişi dâhil olmak üzere;

- Ulusal mevzuat ve ulusal bilgi ve iletişim teknolojileri güvenlik stratejileri ve teknolojileri, politikaları ve en iyi uygulamaları hakkında bilgi alışverişi;

- Az gelişmiş ülkelerde kapasite geliştirmeyi destekleyecek tedbirlerin belirlenmesi;

- Ortak terimleri ve tanımları detaylandırmak için çalışamlar yürütmektir.

Soruna ilişkin tam çözümler belirsiz kalsa da, bu öneriler, ABD ve Rusya arasında siber güvenlik sorunlarının nasıl ele alınacağı konusundaki uzun bir çıkmazın üstesinden gelmede gerçek bir ilerlemeyi temsil etmektedir. [479] İşbirliği, Rusya'nın da olduğu Birleşmiş Milletler himayesinde gelecekteki çok taraflı bir antlaşma için olasılıklar önerebilmektedir ve konu ile ilgili bir süredir savunuculuk yapmaktadır. 2007'de Estonya, 2008'de Gürcistan ve 2010'da İran'a yapılan siber saldırılar, devletlerin birbirlerini casusluklarına ilişkin açıklamalarla birlikte bu ivmeyi daha da arttırmıştır. Bu nedenle, BM Genel Kurulu'nun çeşitli komitelerinde, çeşitli konularda Hükümet Uzmanlarının çeşitli Topluluklarında mutabakata varılması da dâhil olmak üzere, bu tarz etkinlik ve düzenlemeler

---

A/65/201, 30 July 2010, p.7. : http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf (E.T: 13.04.18).

[478] A.g.e, s. 6-8.

[479] Maurer, Tim, Cyber Norm Emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-Security, Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project, Harvard Kennedy School Belfer Center for Science andd International Affairs, September 2011, pp. 10-11.

görülebilmektedir. [480] Bununla birlikte, siber güvenlik meseleleri de BM Güvenlik Konseyi'nde, Ekonomik ve Sosyal Konsey ve çeşitli iştirak organları ve uzmanlaşmış ajanslar tarafından 'terörist faaliyetleri' bağlamında görülmüştür. Şu anda, Birleşmiş Milletlerin siber güvenlik konusundaki rolü tartışmalar ve bilgi paylaşımı ile sınırlı kalırken, siber güvenlik konusunda çalışmalarını sürdürmektedir. [481] Zira Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü (UNIDIR), Birinci Genel Kurul Komitesinin 71. Oturumu sırasında 5 Ekim 2016'da siber uzay ve uluslararası barış ve güvenlik konularında bir yan etkinlik düzenlemiştir. [482] Aynı düzlemde BM'ye bağlı Uluslararası Telekomünikasyon Birliği (ITU), ikinci Küresel Siber Güvenlik Endeksi'ni (GCI) yayınlayarak, ülkelerin yaklaşık yüzde 38'inin siber güvenlik stratejisi yayınladığını ve hükümetlerin yüzde 12'sinin de kalkınma sürecinde olduğunu belirtmiştir. [483] Ajans bu kritik alanda daha fazla çaba gerektiğini vurgulayarak, özellikle de hükümetlerin dijital riskleri yüksek öncelikli olarak gördüklerini ifade ettikleri için. "Siber güvenlik, yasaların, organizasyonların, becerilerin, işbirliğinin ve teknik uygulamanın en etkili olması için uyum içinde olması gereken bir ekosistemdir" şeklinde zikredilen raporda, siber güvenliğin "ülkelerin karar vericilerinin zihninde giderek daha fazla yer alması" olduğunu belirmiştir." [484]

2.5.2.2.3. NATO

[480] Henderson, Christian, The United Nations and the regulation of cyber-security, Chapters, in: Research Handbook on International Law and Cyberspace, Chapter 22, Edward Elgar Publishing, 2015, p. 480. Edward Elgar Publishing.
[481] Markoff, John, Step Taken to End Impasse Over Cybersecurity Talks, New York Times, July 2010 : https://www.nytimes.com/2010/07/17/world/17cyber.html (E.T: 13.04.18).
[482] UN, The UN, Cyberspace and International Peace & Security-Side Event-October 5th, October 7th, 2016 : https://www.un.org/disarmament/update/the-un-cyberspace-and-international-peace-security-side-event-october-5th/ (E.T: 13.04.18).
[483] ITU, Global Cybersecurity Index 2017, p.13. : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (E.T: 13.04.18).
[484] UN, Half of all Countries Aware but Lacking National Plan on Cybersecurity, UN Agency Reports, 5 July 2017 : https://news.un.org/en/story/2017/07/560922-half-all-countries-aware-lacking-national-plan-cybersecurity-un-agency-reports (E.T: 13.04.18).

NATO, 2007'deki Estonya siber saldırısına tepki olarak, "hem tutarlı bir siber doktrinin hem de kapsamlı siber stratejinin eksik olduğunu" öne sürerek bu olay kapsamlı bir karşılık vermemiştir. Bu saldırının ilerleyen safhalarında, NATO ilk toplantısını - 2008 Bükreş Zirvesi – düzenleyerek siber saldırıları ele almıştır. Bu zirve siber saldırılara odaklanan iki yeni NATO bölümünün kurulmasını sağladı: [485] Siber Savunma Yönetimi Kurumu ve Müşterek Siber Savunma Merkezi. Siber Savunma Yönetimi Kurumu, NATO üyeleri arasında siber güç yeteneklerini merkezileştirmeyi amaçlamaktadır. Müşterek Siber Savunma Merkezi, "uzun vadeli NATO siber savunma doktrini ve stratejisinin geliştirilmesini ilerletmeyi" amaçlamaktadır. Kuzey Atlantik Konseyi, NATO siber politikasının ve savunmasının kontrolünü elinde tutmaktadır. Doğu Avrupa ülkelerinden gelen güçlü baskılara rağmen, siber saldırıların, yalnızca NATO antlaşmasının 4. maddesini aktif hale getirdiği düşünülmekte, bu da siber saldırıların olduğu durumlarda üyelere "birlikte hareket etmek" için çağrıda bulunmakta, ancak onları her birine "yardımcı olmaya" zorlamamaktadır çünkü bu durum 5. Madde uyarınca gerekli olacaktır. [486]

NATO'nun bu iki kurumu oluşturması konu ile ilgili somut ilerlemeyi ve daha tutarlı bir siber stratejinin gerekliliğini kabul etmesini sağlasa da, "e-düşmanları bertaraf etmek için yeterli olmamıştır ve Avrupa-Atlantik topluluğuna konuşlandırılan NATO dijital merkez üsleri bu saldırıları yok engelleyememiştir." [487] NATO'nun siber stratejik planları ve kapasitesi gelişmeye devam emektedir. Siber savunmanın güçlendirilmesinin bir parçası olarak, 2017 yılında NATO Müttefikleri yeni bir Siber Operasyon Merkezi oluşturmayı kabul etmiştirler. Kurulumu üzerinde çalışma devam ederken, NATO Bilgisayar Olayları Müdahale Merkezi (NCIRC), NATO'nun kendi ağlarını tüm gün boyunca

[485] Kettemann, Matthias C., Ensuring Cybersecurity Through International Law, Revista Española De Derecho Internacional, Vol. 69, No. 2, 2017, p. 289.
[486] Shackelford, Scott, Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks, Journal of Internet Law, Forthcoming, November 4, 2009, pp. 5-6.
[487] Van Epps, Geoff, Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain, Connections, Vol. 12, No. 4, 2013, p. 15.

siber savunma desteği ile korumaktadır. 200 uzmandan oluşan ekibi, olayları inceleyerek karşılaşılan siber güçlüklerin güncel analizini NATO ve Müttefiklere sağlamaktadır. [488]

NATO, Müttefiklerin siber savunmalarını şu şekilde desteklemelerine yardımcı olmaktadır[489]: (1)Tehditlerle ilgili özel bir kötü amaçlı yazılım bilgi paylaşım platformu aracılığıyla gerçek zamanlı bilgi paylaşımı ve siber tehditler hakkında en iyi uygulamaları paylaşma; (2) Siber güçlüklerle mücadelede Müttefiklere yardım etmek üzere gönderilebilecek hızlı tepki siber savunma ekiplerinin sürdürülmesi; (3) Müttefiklerin siber savunma yeteneklerine ortak bir yaklaşımı kolaylaştırmak için hedefler geliştirmek ve (4) Dünyanın en büyük siber savunma egzersizlerinden biri olan Siber Koalisyon gibi eğitim, öğretim ve egzersizlere yatırım yapmaktır.

2.5.2.2.4. Avrupa Konseyi

Avrupa Konseyi, uluslararası kuruluşlar arasında özellikle de siber suçlarla alakalı bugüne kadar siber güvenlik sorununun bir alt kümesini düzenlemek üzere en doğrudan ve somut yaklaşımı benimsemiştir. İnternet ve diğer bilgisayar ağlarını kullanarak işlenen suçlarla ilgili ilk uluslararası anlaşma olarak, 2001 tarihli Avrupa Siber Suçlarla Mücadele Sözleşmesi ("Siber Suçlar Sözleşmesi" - SSS), "siber suçlara karşı uluslararası işbirliğini teşvik ederek toplumu korumaya yönelik ortak bir ceza politikası" düzenlemiştir. [490] Siber saldırılar, "yasadışı erişim, veri müdahalesi ve sistem müdahalesi" gibi "gizlilik, bütünlük ve

[488] NATO, NATO Cyber Defence, February 2018 : https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf (E.T: 13.04.18).
[489] NATO, A.g.e.
[490] EC, Reform of Cyber Security in Europe : http://www.consilium.europa.eu/en/policies/cyber-security/ (E.T: 13.04.18).

bilgisayar verilerinin ve sistemlerin kullanılabilirliği" ile ilgili suçları Siber Suç Sözleşmesi içerisinde kapsamaktadır. [491]

Bununla birlikte, bu kurallar, kolluk kuvvetleri ya da ulusal güvenlik hedefleri nezdinde alınsa dahi, hükümet eylemlerine uygulanamaz niteliktedir. Örneğin, Sözleşme'nin 2. maddesi, devletlerin kasten işlendiğinde, kendi iç hukukuna göre suç teşkil eden suçlar olarak algılayıp, haklı bir bilgisayar sisteminin tamamına veya bir kısmına erişim dâhilinde "yasama ve diğer önlemleri benimsemelerini" gerektirmektedir. [492] Sözleşmenin beraberindeki "açıklayıcı rapor", "haksız" uyarının, meşru müdafaa veya zorunluluk gibi klasik yasal savunmalara izin verdiğini, aynı zamanda "kamu düzenini korumaya, ulusal güvenliği korumak veya cezai suçları araştırmaya" yönelik eylemleri içeren "yasal hükümet otoritesine uygun olarak etkilenmemiş davranışlar bıraktığını" açıklığa kavuşturmuştur. " [493] Bununla birlikte, Siber Suçlar Sözleşmesi, ülkeleri onaylama yoluyla siber saldırı operasyonlarının yürütülmesine kısıtlamalar getirebilmektedir. Sözleşmenin tarafları "birbirleriyle bilgisayar sistemleri ve verilere ilişkin cezai suçlarla ilgili soruşturma veya yargılama işlemleri için mümkün olan en geniş ölçüde işbirliği yapmaya karar verebilmektedirler." [494] Açık olmamakla birlikte, bu işbirliği anlaşması, Sözleşmenin taraflarının, diğer devlet taraflarına karşı siber saldırı gerçekleştirebilme derecesini sınırlayabilmektedir, çünkü bu, anlaşmanın genel amacını zayıflatabilmektedir. Bununla birlikte, Sözleşme'nin bir devlet tarafı tarafından niyetinin ve amacının ihlali sonucu ortaya çıkacak sonuçların veya yansımaların ne olduğu

[491] Schaap, Arie J., Cyber Warfare Operations: Development and Use Under International Law, Vol. 64, The Air Force Law Review, 2009, p.121.
[492] Weber, Amalie M., The Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. ,2003, p. 427.
[493] CE, Convention on Cybercrime: Explanatory Report, 109th Session 38, November 8, 2001, : http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (E.T: 13.04.18).
[494] Aslan, Yasin, Global Nature of Computer Crimes and the Convention on Cybercrime, Ankara Law Review, Vol.3 No.2, Winter 2006, p.139.

belirsizdir. [495] Bu nedenlerden ötürü Sözleşme, siber saldırıları doğrudan düzenleyen en gelişmiş uluslararası yasal çerçeve oluştursa da siber saldırılara karşı genel mücadelenin sadece bir kısmını ele almaktadır. Özellikle, gerek devlet taraflarının saldırılarını, gerekse büyük ölçüde bölgesel üyeliğini düzenleyememesiyle sınırlıdır. Yine de, yasadışı siber saldırıların düzenlenmesi için kapsamlı bir uluslararası çerçevenin tasarlanması adına bir başlangıç noktası sunmaktadır. [496]

2.5.2.2.5. Şangay İşbirliği Örgütü

Çin, Kazakistan, Kırgızistan, Rusya, Tacikistan ve Özbekistan tarafından 2001 yılında kurulan hükümetler arası ortak bir güvenlik örgütü olan Şangay İşbirliği Örgütü (ŞİÖ), siber güvenlik alanında işbirliğine yönelik önemli adımlar atmıştır. [497] 16 Haziran 2009 tarihli Yekaterinburg Deklarasyonu'nda, SCO üyesi ülkeler, uluslararası bilgi güvenliğinin uluslararası güvenlik sisteminin ortak unsurlarından biri olarak ele alınmasının önemini vurgulamışlardır [498]. Örgüt, siyasal istikrarı zayıflatmak üzere siber teknolojinin kullanımını içeren siber saldırıların kapsamlı bir uzlaşma sağlamıştır. Burada da belirtildiği üzere, siber saldırıları düzenlemeye yönelik uluslararası çabalar hala devam etmektedir. Avrupa Konseyi'nin Siber Suçlar Sözleşmesi bu çabaların en başarılı örneği olsa da, çoğu uluslararası anlaşma gelecekteki stratejileri tartışma aşamasının ötesine

[495] Baron, Ryan M.F., A Critique of the International Cybercrime Treaty, Commlaw Conspectus, Vol. 10, 2002, p.273.
[496] Miriam F. Miquelon-Weismann, The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?, 23 The John Marshall Journal of Information Technology & Privacy Law, Vol. 23, No. 2, 2005, p. 337.
[497] SCO, SCO Responds to Cyber Challenges, 09.06.2011: http://infoshos.ru/en/?idn=8349 (E.T: 13.04.18).
[498] MFAPRC, Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation, 2009/06/17 : http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t569701.shtml (E.T: 13.04.18).

geçememiştir. [499] Bununla birlikte, siber saldırıları düzenlemek üzere bir dizi ulus ötesi çalışmaların oluşmasında artan ilgiyi göstermektedir. Bu örgütler tarafından benimsenen yaklaşımların çeşitliliği, aynı zamanda, merkezi mücadelenin, uluslararası bir anlaşmada ele alınması gereken faaliyetin kapsamını tanımlayacağını göstermektedir. [500] Bununla birlikte, siber saldırıları ele alan yerel yasaları dolaylı olarak düzenleyen uluslararası rejimleri özetleyerek mevcut yasal resmi tamamlamak gerekmektedir.

2.5.2.3.Siber Saldırıları Dolaylı Düzenleyen Uluslararası Hukuk Rejimleri

Siber saldırıları doğrudan düzenlemeyen araçlar da mevcuttur. Ancak muhteviyat dâhilinde siber saldırıları dolaylı bir şekilde ele alıp, uygulama esasları bağlamında siber saldırılar konusu hakkında emsal teşkil edecek uygulamalar mevcuttur.

2.5.2.3.1. Telekomünikasyon Hukuku

Uluslararası telgraf veya radyo frekansı iletişimini içeren siber saldırılar telekomünikasyon yasasına tabi olabilmektedir. Modern uluslararası telekomünikasyon kanunu, bilgi ve iletişim teknolojisi için çok uluslu standartlar oluşturan Uluslararası Telekomünikasyon Birliği (UTB) tarafından düzenlenmektedir. Birliğin belirttiği amaç, "bütün devletlerin barışın ve ekonomik/sosyal kalkınmanın verimli telekomünikasyon hizmetleri aracılığıyla korunmasıdır. " [501] Uluslararası Telekomünikasyon Birliği, tüm üye ülkeleri bağlayan anlaşmalar olan İdari Düzenlemeler ve aynı zamanda bağlayıcı olmayan

[499] Kizekova, Alica, The Shanghai Cooperation Organisation: Challenges in Cyberspace, The S. Rajaratnam School of International Studies, 22 February 2012 : https://www.rsis.edu.sg/rsis-publication/cms/1695-the-shanghai-cooperation-organ/#.WvNGVIiFNPZ (E.T: 13.04.18).
[500] Wei, Yuxi, China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty, The Henry M. Jackson School of International Studies, University of Washington, June 21, 2016 : https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/ (E.T: 13.04.18).
[501] ITU, About International Telecommunication Union (ITU) : https://www.itu.int/en/about/Pages/default.aspx (E.T: 13.04.18).

Telekomünikasyon Standartları olarak da bilinen kuralları yürürlüğe koyarak, tüm taraflara Radyo Düzenlemeleri kapsamında bilgi akışı sağlamaktadır. Birlik, radyo ve telekomünikasyon teknolojilerinin kullanımını, üye devletlere verimli ve adil bir şekilde dağıtmak üzere (örneğin radyo spektrumlarına haklar atama yöntemleri geliştirerek) düzenlemektedir. [502] Uluslararası Telekomünikasyon yönetmelikleri, elektromanyetik spektrum veya uluslararası telekomünikasyon ağlarından yararlanan siber saldırıları ele almak için kullanılabilir. Örneğin, bir ülkeden yayın yapan istasyonlar, diğer devletlerin hizmetlerinin yetkili frekanslarındaki yayınlarına müdahale etmeyebilmektedirler. [503] Üye devletler, "Devletin güvenliği için tehlikeli veya yasalarına aykırı görünebilecek, kamu düzenine ya da genel olarak sadece belirli ilişkiler için ve / ya da "uluslararası telekomünikasyon hizmetlerini askıya alabilecek" Genel Sekreter aracılığıyla diğer üye devletlerin her birine bu tür eylemleri derhal bildirmesi koşuluyla, belirli türden yazışmalar, giden, gelen veya transit herhangi bir devlet dışı özel telekomünikasyon sistemini kesebilmektedirler. [504]

Üye devletler aynı zamanda “radyatör servisinin veya diğer güvenlik hizmetlerinin işleyişini tehlikeye sokan veya bir radyo-iletişim hizmetini ciddi bir şekilde bozan, engelleyen ya da tekrar tekrar kesen” ve “uluslararası yazışmaların gizliliğini sağlamak üzere mümkün olan tüm önlemleri takip eden” zararlı müdahaleye karşı da düzenlemelidirler. Böyle bir gizlilik kendi iç yasalarına veya uluslararası sözleşmelere aykırı bir durum oluşturmaktadır. [505] Bu istisnalara rağmen, uluslararası telekomünikasyon kanunu, siber saldırılar gibi askeri amaçlar için telekomünikasyon kullanımını özel olarak yasaklamamaktadır. 48. Madde, "Üye Devletlerin askeri telsiz tesislerine ilişkin tüm özgürlüklerini koruduklarını"

[502] Sounnalat, Khamla, Cyber Crimes Legislation and Implementation, Cyber Crimes Conference 17-20 June, 2015, Strasbourg, France.
[503] Dunlap, Charles J., Perspectives for Cyber Strategists on Law for Cyberwar, Strategic Studies Quarterly, vol. 5, no. 1, 2011, p. 93.
[504] Gjelten, Tom, Shadow Wars: Debating Cyber 'Disarmament', World Affairs, Vol. 173, No. 4, 2010, p. 33.
[505] Tikk-Ringas, Eneken, The Implications of Mandates in International Cyber Affairs, Georgetown Journal of International Affairs, 2012, p. 42.

belirtmektedir. [506] Madde, devletlerin bu kullanımı sınırlandırmasını talep etmektedir: "Bununla birlikte, bu tesisler, mümkün olduğunca, zararlı parazitleri önlemek için alınacak önlemleri göz önünde bulundurmalıdır." Uluslararası Telekomünikasyon Birliği, "zararlı müdahale" ye karşı uyarıda bulunur, ancak bu mekanizmaların bir raporlama mekanizması gerektirmeksizin veya kullanımını sınırlamaksızın askeri bir şekilde iletilmesine izin vermektedir.

2.5.2.3.2. Havacılık Hukuku

Askeri olmayan havacılığı hedef alan veya bu havzaya müdahale eden siber saldırı operasyonları üç kritik havacılık yönetmeliği dâhilinde ele alınmaktadır: 1944 Uluslararası Sivil Havacılık Şikago Sözleşmesi (Şikago Sözleşmesi), [507] 1971 Montreal'in Sivil Yasalara Karşı Hukuka aykırı eylemlerin bastırılması için Montreal Sözleşmesi (Montreal Konvansiyonu) [508] ve Uluslararası Sivil Havacılığa Hizmet Veren Havaalanlarında Yasadışı Şiddet Eylemlerinin Bastırılmasına İlişkin 1988 Protokolü (Montreal Protokolü) dür. [509] Örneğin, hava trafik kontrolünün kesintiye uğraması, uçuş yolcu listelerinin değiştirilmesi veya bir ülkenin uçuşa yasak listeye eklenmesi, havacılık yasasını etkileyen siber saldırıları örneklemektedir.

1944 Chicago Konvansiyonu, uluslararası hava yolculuğunu koordine edip düzenleyen özel bir BM birimi kurmuştur. Ayrıca hava sahası, uçak, navigasyon, kayıt ve güvenlik konusunda bir dizi kural oluşturmuştur. [510] Sözleşme, bütün devletlerin "sivil uçakların seyrüsefer güvenliğini " kriterini sağlaması gerektiğini

---

[506] ITU, Constıtutıon of The International Telecommunication Union : https://www.itu.int/council/pd/constitution.html (E.T: 13.04.18).
[507] ICAO, Convention on International Civil Aviation Done at Chicago, 7th Day of December 1944: https://www.icao.int/publications/Documents/7300_orig.pdf (E.T: 13.04.18).
[508] IATA, Montreal Convention 1999, 28 May 1999 : https://www.iata.org/policy/Documents/MC99_en.pdf (E.T: 13.04.18).
[509] ICAO, Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation : https://www.icao.int/secretariat/legal/List%20of%20Parties/VIA_EN.pdf (E.T: 13.04.18).
[510] Andrews, J. A, The Modern Law Review, The Modern Law Review, Vol. 30, No. 1, 1967, p. 111.

şart koşmaktadır. Sivil saldırı uçuşlarını hedefleyen siber saldırı operasyonları, bir hükümet tarafından başka bir aktöre karşı başlatıldıysa, bu duru Sözleşmenin sivil uçuşlara müdahale edilmesine karşı korunması ile ters düşmektedir. [511] Böyle bir operasyon, uçuşta bir sivil uçağı hedef alan silahların kullanılmasına karşı 1984'te yapılan değişikliğin bir sonucudur. Ancak, Sözleşme, bir üye devletin, devletin Konsey'e bildirdiği süre boyunca, savaşın veya devletin acil durumlarındaki yükümlülüklerini yerine getirmesine izin vermemektedir. [512]

Montreal Konvansiyonu, sivil havacılığın güvenliğini tehlikeye atabilecek yasa dışı özel bir davranışın genel olarak ana hatlarını oluşturmaktadır. Madde 1, bir kimsenin kasten ve yasadışı bir şekilde hava seyrüsefer tesislerine ya da operasyonlarına müdahale ederek, bir uçağı harekete geçirecek ya da uçuş sırasında uçağın güvenliğini tehlikeye atacak bir dizi eylemde bulunmayı denediği veya yapmaya çalıştığı durumlarda bir suç işlediğini belirtir, uçağın uçuş emniyetini tehlikeye atmaktadır. [513] Bu anlaşma herhangi bir siber-saldırı operasyonunu, uçamayan bir uçağı (örneğin, uçağın işletim sistemine müdahale ederek) veya uçuşta iletişim veya uçak navigasyonunun diğer kısımlarıyla birlikte bir uçağın emniyetini tehlikeye atmadıkça (örneğin, hava trafik kontrolüne müdahale ederek) kısıtlamamaktadır. [514]

Montreal Protokolü, "havalimanlarındaki kişilerin güvenliğini tehlikeye sokan ya da bu tür havaalanlarının güvenli çalışmasını tehlikeye atan şiddet eylemleri" ile alakalı sivil hava araçlarından gelen yasal çerçeveyi genişletmiştir. Madde 2, bir kişinin bir cihazı, bir maddeyi veya silahı kullanırken kasıtlı olarak

[511] Larsen, Paul B, Recent Changes in Space Law's Concept of Sovereignty, Proceedings of the Annual Meeting (American Society of International Law), Vol. 88, 1994, p. 266.
[512] Cheng, Bin, A New Era in the Law of International Carriage by Air: From Warsaw (1929) to Montreal (1999), The International and Comparative Law Quarterly, Vol. 53, No. 4, 2004, p. 855.
[513] George Leloudas, The Cambridge Law Journal, The Cambridge Law Journal, Vol. 65, No. 2, 2006, p. 466.
[514] Cheng, Bin, The International and Comparative Law Quarterly, The International and Comparative Law Quarterly, Vol. 56, No. 2, 2007, p. 465.

ve yasa dışı bir şekilde aşağıdakileri yapmaya veya teşebbüs etmesi halinde bir suç işlediğini belirtmektedir: [515]

- Uluslararası sivil havacılığa hizmet eden bir havaalanında ciddi yaralanma veya ölüme neden olan veya bu duruma neden olabilecek bir kişiye karşı bir şiddet eylemi gerçekleştirmek; ya da

- Uluslararası sivil havacılık hizmeti veren bir havalimanının tesislerini ya da üzerinde bulunmayan uçakları tahrip eder ya da ciddi şekilde havalimanının hizmetlerini sekteye uğratırsa veya bu havaalanında güvenliği tehlikeye sokması muhtemelse, havaalanının hizmetlerini aksatmaktadır.

Böylelikle, bu Protokol, bir uluslararası havaalanına karşı yolcu bildirimleri veya bir havalimanının bilgisayar ağ sistemine karşı güvenliği engelleyen siber saldırı müdahalelerini yasaklamaktadır.

2.5.2.3.3. Uzay Hukuku

Bilgisayar tarafından işletilen uyduların uluslararası telekomünikasyon ve askeri operasyonların ayrılmaz bir parçası olduğu bilgisi ışığında, siber saldırılar uzay hukuku dâhilinde de incelenmesi gerekmektedir çünkü saldırılar, uzay hukuku bağlamında da değerlendirilmektedir. Araştırmacılar, uzay nesneleri, uydu, ay ve uzay nesnelerinden kaynaklı hasarın yanı sıra ele bu kaynakların ele geçirilmesine dair düzenlemelerin, siber saldırıları düzenlemek için kullanılabileceğini öne sürmüşlerdir. [516] Uydu Düzenlemelerine ve Uzayın Sömürü ve Kullanımındaki Faaliyetleri Kapsayan İlkelere İlişkin Antlaşma, [517]

[515] UNODC, Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation 1988 ('Montreal Protocol')
https://www.unodc.org/pdf/crime/terrorism/Commonwealth_Chapter_5.pdf (E.T: 13.04.18).
[516] Greenberg, Lawrence T. / Seymour E. Goodman / Kevin J. Soo Hoo, Information Warfare and International Law, National Defense University Press, 1998, p.8.
[517] UN, United Nations Treaties and Principles on Outer Space, United Nations, New York, 2002, p.3.

siber saldırılara ilişkin bir takım bilgiler sunmaktadır. Bununla birlikte, bu antlaşmaların siber saldırıların düzenlenmesi hususunda yeteri kadar mahiyetli değillerdir. 1967 Dış Uzay Antlaşması, uzayın özgürce keşfedilmesini sağlayarak belirli yıkıcı amaçlar için alan kullanımını yasaklamaktadır. [518] Aynı şekilde bu Anlaşma, taraf devletlerin nükleer silah taşıyan ya da başka bir tür kitle imha silahı taşıyan nesneleri dünya etrafında yörüngeye yerleştirmemeyi ya da bu silahları uzayda başka bir şekilde konumlandırmamayı taahhüt etmektedir. Ay ve diğer gök cisimleri, bütün taraf devletler tarafından Antlaşma' ya münhasıran barışçıl amaçlarla kullanılacaktır. [519] Dış Uzay Antlaşması, yer yörüngesindeki askeri keşif uyduları, uzaktan algılama uyduları, askeri küresel konumlandırma sistemleri ve herhangi bir anti balistik füze sisteminin uzay temelli yönleri gibi belirli askeri kullanım alanlarına açıkça izin vermektedir. Siber saldırıların, anlaşmada öngörüldüğü türden kitle imhaya yol açmasının muhtemel olmaması nedeniyle, siber saldırıların antlaşma tarafından yasaklandığına dair doğrudan bir anlam çıkartmak uygun değildir. [520] Uydu düzenlemeleri, siber saldırı düzenlemeleri için başka bir potansiyel yol sunmaktadır. 1971 Uluslararası Telekomünikasyon Uydu Teşkilatı (Telekomünikasyon Uydu Organizasyonu) ve 1979 Uluslararası Denizcilik Uydu Organizasyonu (Deniz Uydu Organizasyonu) ile ilgili Anlaşma, "barışçıl amaç" nezdindeki uydular için geçerli olan Dış Uzay Antlaşmasına benzer hükümleri içermektedir. [521] Bununla birlikte, uyduların siber saldırılarda bir rolü olması muhtemel olmasına rağmen, bu anlaşmaların saldırıları düzenleme noktasında yeterli açılımlar getirememiştir. 2000 yılında, "küresel ticari telekomünikasyon uydu sisteminin uzay segmentinin tasarımı, geliştirilmesi, inşası, kurulması, işletilmesi ve bakımı" nı ileri sürmekle görevlendirilmiş

[518] A.g.e., s. 13.

[519] UNOOSA, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies : http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html (E.T: 14.03.18).

[520] Fidler, David P., Cybersecurity and the New Era of Space Activities, CFR, April 03, 2018 : https://www.cfr.org/report/cybersecurity-and-new-era-space-activities (E.T: 14.03.18).

[521] Couriel, Deborah Housen, Cybersecurity and Outer Space: Connected Challenges, Israel Defense, February 2, 2017 : http://www.israeldefense.co.il/en/node/28413 (E.T: 14.03.18).

hükümetler arası bir organ olarak kurulan Telekomünikasyon Uydu Organizasyonu, 2000 yılında özelleştirilmiştir. [522]

Bu hukuki gelişmelerle birlikte, 2011 yılında ABD-Çin Ekonomik ve Güvenlik İnceleme Komisyonu tarafından hazırlanan bir raporda da belirtildiği üzere, 2007 ve 2008 yıllarında Norveç'teki bir yer istasyonu aracılığıyla iki ABD uydusunun ele geçirildiğini bildirilerek saldırının internet üzerinden gerçekleştirildiği saptanmıştır. Saldırının şiddeti endişe verici düzede olmuştur, çünkü 2008 saldırısında, bilgisayar korsanları herhangi bir zarara yol açmamakla birlikte uyduya komuta etmek için gereken tüm adımları başarıyla gerçekleştirmişlerdir. Potansiyel olarak, bilgisayar korsanları çalıntı veriye sahip olup, güneş paneli dizisini onları yok etmek üzere yönlendirmekle kalmayıp bir çarpışmaya ya da patlamaya neden olmak için uyduyu da değiştirebilmektedirler. [523] 2014 yılında ABD Ulusal Okyanus ve Atmosfer İdaresi tarafından işletilen bir uydunun, herhangi bir veriyi tehlikeye atmamış olsa da, uydularından birindeki hacklemenin tespit edildiğini doğruladığı üçüncü bir olay gerçekleşmiştir. [524]

Ayrıca, son zamanlarda özellikle BM ve Çin'in uzay hukuku bağlamında siber güveliğe dair çalışmalarının kapsam ve mahiyetini arttırma çalışmaları içerisinde olduğu gözlemlenmektedir. Özellikle yeni Çin kanunu hakkında ilk dikkat çeken kısım, siber güvenlik hususlarına vurgu yapmasıdır. Söz konusu mevzuatın göze çarpan özelliklerinin bir incelemesi, Çin'in, daha geniş bir ulusal

[522] Petras, Christopher M., The Use of Force in Response to Cyber-Attack on Commercial Space Systems - Reexamining Self-Defense in Outer Space in Light of the Convergence of U.S. Military and Commercial Space Activities, Journal of Air Law and Commerce, Vol. 67, p. 1251.
[523] USCC, 2015 Report to Congress of the U.S.-China Economic and Security Review Commission: Executive Summary and Recommendations, One Hundred Fourteenth Congress First Session November 2015, p. 8. : https://www.uscc.gov/sites/default/files/annual_reports/2015%20Executive%20Summary%20and%20Recommendations.pdf (E.T: 14.04.18).
[524] Duggal, Pavan, Cyber Security Law, its Regulation and Relevance for Outer Space, UNOOSA : http://www.unoosa.org/documents/pdf/hlf/HLF2017/presentations/Day2/Session_7b/Presentation5.pdf (14.04.18).

güvenlik alanı içinde siber güvenliğin karıştığı konusunda kendine özgü bir yaklaşım benimsemiş olduğunu göstermektedir. Kanun, kültürden eğitime, siber uzaya kadar tüm alanlarda "güvenliğin" sürdürülmesi gerektiğini vurgulamaktadır. Kanun kapsamı genişlemiştir, örneğin, güvenliğin uluslararası deniz yatakları, kutup bölgeleri ve hatta uzayı bile kapsamaktadır. [525] Bununla birlikte BM Dış İlişkiler Ofisi'nin (UNOOSA) 2017 de yaptığı çalışmada, uzayda içerisinde 'nükleer enerji' nin de bulunduğu çalışmalarda, güvenlikle ilgili asıl sorumluluğun, uzay Nükleer Güç Kaynağı (NPS) misyonunu yürüten kuruluş ile birlikte olması gerektiğini vurgulamıştır. Bu bağlamda, uzay NPS misyonunu yürüten organizasyon, güvenlik için birincil sorumluluğa sahiptir. Bu organizasyon, uzay NPS uygulaması için belirlenen güvenlik gereksinimlerini karşılamak üzere misyondaki ilgili tüm katılımcıları (uzay aracı sağlayıcısı, fırlatma aracı sağlayıcısı, NPS sağlayıcısı, fırlatma sitesi sağlayıcısı vb.) içermeli veya bunlarla ilgili resmi düzenlemeler içermelidir. [526] Yönetim için özel güvenlik sorumlulukları şunları içermelidir: [527]

- Gerekli teknik yeterliliklerin oluşturulması ve sürdürülmesi;
- İlgili tüm katılımcılara yeterli eğitim ve bilgi sağlanması;
- Tüm makul öngörülebilir koşullar altında güvenliği teşvik etmek için prosedürlerin oluşturulması;
- Alan NPS kullanan görevler için uygun olduğu şekilde özel güvenlik gereksinimleri geliştirmek;
- Güvenlik testleri yapmak ve belgelemek ve hükümet misyonunun lansman yetki sürecine girdi olarak analiz etmek;
- Güvenlik hususlarında güvenilir karşıt görüşleri göz önünde bulundurarak;
- Halka doğru, zamanında ve amaca uygun bilgi sağlanmasıdır.

[525] Ramsey, Carly / Ben Wootliff, China's Cyber Security Law: The Impossibility of Compliance?, Forbes, May 29, 2017 : https://www.forbes.com/sites/riskmap/2017/05/29/chinas-cyber-security-law-the-impossibility-of-compliance/#4ff0f4a7471c (E.T: 14.04.18).
[526] UNOOSA, International Space Law: United Nations Instruments, United Nations, New York, May 2017, p.100.
[527] UNOOSA, a.g.e, s.101.

2.5.2.3.4. Deniz Hukuku

1982 Birleşmiş Milletler Deniz Hukuku Konvansiyonu (UNCLOS) [528] - özellikle 19, 109 ve 113 maddeleri - denizde siber saldırı operasyonlarını teğetsel olarak etkilemektedir. Bir geminin, başka bir ülkenin karasularında masum geçişine izin veren 19. madde, faaliyetleri "barış, iyi düzen veya kıyı devletinin güvenliği için zararlı" olmadığı sürece, geleneksel uluslararası hukuk olarak kabul edilmektedir. 19. maddede yasaklanan faaliyetler şunlardır: [529]

(a) Kıyı Devletinin egemenliğine, toprak bütünlüğüne veya siyasi bağımsızlığına karşı ya da Birleşmiş Milletler Tüzüğünde yer alan uluslararası hukuk ilkelerini ihlal eden herhangi bir şekilde herhangi bir tehdit veya güç kullanımı;

(c) Kıyı Devletinin savunması veya güvenliğine zarar verecek bilgi toplama amaçlı herhangi bir eylem;

(d) Kıyı Devletinin savunmasını veya güvenliğini etkilemeyi amaçlayan herhangi bir propaganda eylemi;

(k) herhangi bir iletişim sistemine veya kıyı devletinin diğer tesislerine veya tesislerine müdahale etmeyi amaçlayan herhangi bir eylem…

Bu düzenlemeler, özellikle bölüm (k), denizde bulunan gemiler üzerinde bilgisayar sistemleri kullanan siber saldırıları yasaklamak için yorumlanabilmektedir. Bununla birlikte, serbest geçiş ilkesi "freedom of passage"

[528] UN, United Nations Convention on the Law of the Sea : http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf (E.T: 14.04.18).
[529] UN, a.g.e, Madde 109 (1), 109 (2), 109 (3).

kapsamında geçen gemiler kıyı güvenliğini terör eylemleri dâhilinde tehdit edebilme potansiyeline sahiptirler. [530]

3. Savaş Hukuku Bağlamında Siber Saldırı/Savaş Tartışmaları

"Siber savaş" terimi, nükleer santrallere karşı gerçekleştirilebilecek olası bir nükleer terörizm durumunda olay örgüsünü açıklamada kullanılabilmektedir. Savaş hukuku tarafından ele alınabilecek siber faaliyetlerin kapsamını yakından incelemek, siber saldırıları analiz ederken göz ardı edilmemesi gereken bir unsur olarak karşımıza çıkmaktadır. Bu bölümde, bir siber saldırının *jus ad bellum* altında silahlı bir saldırı oluşturduğunu ve böylelikle "siber savaş" olarak kabul edilip edilemeyeceğini incelenerek bu boşluğun doldurulması hedeflenmektedir. Bu bilgilere paralel olarak, savaş sırasında yönetilen yasaların nasıl yürüdüğünü de incelenmesi gerekmektedir. Siber saldırılara karşı *jus ad bellum* ve *jus in bello*' yu genel hatlarıyla incelemek gerekecektir, çünkü bu alandaki derinlemesine soruşturmalar somut olaylara dayalı olgulardır. Bilinmesi gereken diğer bir husus ise savaş hukuku tarafından ele alınacak olan genel siber saldırı türlerini ortaya koymak ve saldırının siber temelli doğası ile geleneksel savaş hukuku analizinde, sonucun önemli ölçüde karmaşık olduğu unutulmamalıdır. [531] Savaş hukuku, en tehlikeli siber saldırıların bazılarına ele almak için faydalı düzenlemeler sunarken, savaş çerçevesi kanununun nihayetinde tüm siber saldırıların sadece küçük bir bölümünü ele almaktadır. Siber savaş, çok daha büyük bir sorunun sadece küçük bir tetikleyicisidir. [532] Öncelikle, mevcut savaş hukuku çerçevesini siber saldırılara uygulanmasının oldukça zor olduğunu belirtmek gerekmektedir. Savaş esnasındaki kuralları ele alan kilit anlaşması olan Cenevre Sözleşmeleri, son olarak II. Dünya Savaşı'nın ardından revize edilmiştir. Cenevre Sözleşmelerinin

[530] Caşın, Mesut Hakkı, Modern Uluslararası Hukukun Temel Esasları, Legal Yayıncılık, Cilt I, İstanbul, 2013, s. 603 – 605.
[531] DOD, Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, p.2.
[532] Lucas, George R. Jr. Ethics and Cyber Conflict: A Response to JME 12:1 (2013), Journal of Military Ethics, Vol. 13, No. 1, 2014, p.21.

taslaklarında, dünya çapında bir bilgisayar ağı üzerinden yapılan saldırılardan daha fazla bilgi içerek bir açıklama yoktu. [533]

Herhangi bir siber saldırının, BM Sözleşmesinin 51. Maddesi uyarınca bir meşru müdafaa hakkı doğuran bir "silahlı saldırı" oluşturduğu başka bir devlet tarafından iddia etmemiş olsa da, aynı şekilde herhangi bir devlet, siber saldırıların genellikle yasaklanmış bir güç kullanımı oluşturduğunu iddia etmemiştir. [534] Ancak bu tür saldırıların sayı ve kapsamda artmakta olduğu gerçeği, bir siber saldırının silahlı bir saldırı veya güç kullanımı oluşturduğu zaman devletlerin uzlaşmaya varma ihtiyacının arttığını göstermektedir. Durumla ilgili anlaşmaların olmayışı ve uluslararası hukuki boşluğu ve bu durumların doğal bir sonucu olarak saldırılardaki artış, devletlerin geleneksel askeri araçlarla bir siber saldırıya tepki verebilme olasılığını arttırmaktadır. [535] Saldırılardaki artış, aynı zamanda, savaş yasalarına tabi olmayacak olan, geniş çaplı ekonomik hasara yol açanlar gibi faaliyetleri düzenlemek üzere daha kapsamlı bir yasal çerçeve için daha acil bir ihtiyaç doğurmaktadır. *Jus ad bellum* altında ele alınması gereken önemli bir soru ise herhangi bir siber saldırının, BM Sözleşmesinin 51. Maddesi uyarınca meşru müdafaayı haklı kılan silahlı saldırı seviyesine çıkıp çıkmadığıdır. [536] Bir siber saldırının nitelendirilmesi, saldırının fiziksel tahribatla sonuçlanıp sonuçlanmadığı ya da "kinetik etki" olarak adlandırılan bir konvansiyonel saldırı ile karşılaştırılabilir olup olmadığına bağlıdır. Bu sonuca varmak yalnızca Sözleşme metnini (ki bu oldukça genel ve belirsiz) değil, aynı zamanda zaman içinde devlet pratiği ve yorumlama yoluyla o metne verilen anlamı incelemeyi gerektirmektedir. [537] Çünkü bir silahlı çatışma hiçbir zaman

[533] Döge, 2010, s. 487.
[534] Schmitt, Michael N, International Law and the Use of Force: The Jus Ad Bellum, Connections, Vol. 2, No. 3, 2003, p. 91.
[535] Brown, Gary, and Keira Poellet, The Customary International Law of Cyberspace, Strategic Studies Quarterly, Vol. 6, No. 3, 2012, p. 129.
[536] Tom Ruys, The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are 'Minimal' Uses of Force Excluded from UN Charter Article 2(4)? The American Journal of International Law, Vol. 108, Vo. 2, 2014, p. 161.
[537] Makowski, Andrzej, More on War, Israel Journal of Foreign Affairs, Vol. 11, No. 2, 2017, p. 308.

sadece bir siber saldırı sonucu başlamamıştır, siber saldırıların silahlı bir karşılığı haklı çıkardığı konusunda bir devlet uygulaması bulunmamaktadır. [538]

3.1. Jus ad Bellum

Jus ad bellum, devletlerin savaşa veya genel olarak silahlı kuvvet kullanımına başvurabilecekleri koşulları ifade etmektedir. Birleşmiş Milletler 1945 tarihli Sözleşmesinde yer alan devletlerarasında güç kullanımı ve onun istisnaları (meşru müdafaa ve BM'nin yetki kullanımı için yetkilendirme) yasağı, *jus ad bellum*'un temel bileşenleridir. [539] *Jus ad bellum*, güç kullanma kararlarının yasallığını belirler ve ilkeleri BM Şartı'nın temeli olarak hizmet etmektedir. Sözleşme, devletlerin "uluslararası ilişkilerini tehdit veya güç kullanmalarından uzak tutmasını" talep ederek güç kullanma kararlarının yasallığına karşı bir varsayım yaratmaktadır. Bununla birlikte sözleşme, aynı zamanda, herhangi bir karar kullanmaya açıkça izin veren, bu kuralın istisnalarını yaratmaktadır. [540] BM Güvenlik Konseyi tarafından yetkilendirilmiş kuvvet ve sözleşmenin, bir devlete karşı "silahlı saldırı meydana geldiğinde, bireysel veya toplu savunma hakkına zarar vermediğini" belirtmektedir. Bu nedenle, Güvenlik Konseyi yetkisi veya silahlı saldırıya karşı savunmak için herhangi bir güç kullanma kararı, yasal olarak kabul edilirken, diğer herhangi bir güç kullanımı kanuna aykırı olarak tanımlanmıştır. [541] Bu bilgiler ışığında, hangi yasal düzenlemenin siber saldırılara karşı meşru müdafaada silahlı güce başvurma hakkını hukuki dayanak gösterdiği sorusunun cevabını bulabilmek için üç unsura ihtiyaç vardır. İlk olarak, BM Sözleşmesinin 2 (4) Maddesinde yer alan uluslararası ilişkilerde kullanım ya da güç tehdidi hakkındaki genel yasağı özetlemek gerekmektedir. İkinci olarak,

[538] Lilienthal, Gary/ Nehaluddin Ahmad, Cyber-Attack as Inevitable Kinetic War, Computer Law & Security Review, Volume 31, Issue 3, June 2015, pp. 391-392.
[539] ICRC, What Are Jus Ad Bellum and Jus In Bello?, 22 January, 2015 : https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0 (E.T: 14.04.18).
[540] ILPI, ICJ's Advisory Opinion on Nuclear Weapons: A Brief Overview of the Conclusions of International Court of Justice in 1996, Nutshell Paper No 3/2011, pp.1-2.
[541] Barnett, Sophie, Applying Jus Ad Bellum in Cyberspace, September 1, 2016 : http://www.e-ir.info/2016/09/01/applying-jus-ad-bellum-in-cyberspace/ (15.04.18).

kolektif güvenlik operasyonları ve meşru müdafaa için bu yasakların istisnaları iyi irdelenmelidir ve ayrıca bir siber saldırının meşru müdafaaya başvuruyu haklı kılacağına özellikle dikkat etmek gerekmektedir. [542] Son olarak, *jus ad bellum* zorunluluğunun ve orantılılığın geleneksel uluslararası hukuk gerekliliklerini ve *jus ad bellum* gereksinimlerinin siber saldırılara uygulanmasının sınırlamalarını ve sorunlarını detaylandırarak açıklığa kavuşturulması gerekmektedir. Devletlerin, siber saldırıların etkileri geleneksel bir silahlı saldırıya eşdeğer ise, sadece siber saldırıya karşı savunma silahlı kuvvetleri kullanabileceği sonucuna varılabilmektedir. [543]

3.1.1. Yasal Mevzuatı Yönetme: İç İşlerde Güç ve Müdahale Kullanımına İlişkin Yasak

BM Sözleşmesinin 2. Maddesinin 4. fıkrası, üye devletlerin uluslararası ilişkilerini, herhangi bir devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı tehdit veya güç kullanımından veya BM Amaçları ile tutarlı olmayan durumlardan uzak durmaları noktasında onlara şart koşmaktadır. ”Bu yasak, devletlerin diğer devletlerin içişlerine müdahale etmelerini yasaklayan geleneksel bir uluslararası norm olmayan hukuk normu ile tamamlanmaktadır. [544] Uluslararası Adalet Divanı (“UAD”), müdahalenin bir güç kullanımı veya tehdidi biçiminde olduğu durumlarda, geleneksel uluslararası hukuk normunun, Madde 2 (4) ile tutarlı olduğu sonucuna varmıştır. [545] Uluslararası tehdidin yasağı ya da kullanımı konusundaki kesin kapsamı, yoğun uluslararası ve bilimsel tartışmalara konu olmuştur. Daha zayıf devletler ve bazı akademisyenler, Madde 2 (4) ün

[542] Roscini, Marco, World Wide Warfare Jus Ad Bellum and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, Vol. 14, 2010, p.90.
[543] Nguyen, Reese, Navigating Jus Ad Bellum in the Age of Cyber Warfare, California Law Review, Vol. 101, No. 4, 8-1-2013, p. 1112.
[544] Henderson, Christian, The Use of Cyber Force: Is The Jus Ad Bellum Ready?, April 30, 2016 : http://www.qil-qdi.org/use-cyber-force-jus-ad-bellum-ready/ (15.04.18).
[545] Kretzmer, David, The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum, The European Journal of International Law, Oxford University Press, Vol. 24, No. 1, 2013, p.239.

sadece silahlı kuvvetin kullanılmasını değil, aynı zamanda politik ve ekonomik baskıyı da yasakladığını iddia etmişlerdir. [546]

Bununla birlikte, fikir birliği, Madde 2 (4) 'ün sadece silahlı kuvvetleri yasaklamasıdır. Siber saldırılarla ilgili tartışmaların, Madde 2 (4) kapsamında tartışmaları yeniden alevlendirme potansiyeli vardır. Siber saldırıları geleneksel saldırıları başlatmaktan çok daha az maliyetli olduğu ve son derece sanayileşmiş devletlerin genellikle bilgisayar ağlarına daha fazla bağımlı oldukları ve siber saldırılara karşı daha savunmasız oldukları için, siber saldırıların zayıfların güçlü bir silahı olduğu anlamına gelebilmektedir. [547] Saldırı kabiliyetlerinin maliyet yapısındaki bu değişiklik, siber saldırıların olasılığını artırabilir ve Madde 2 (4) kapsamının farklı yorumlarının siyasi değerini değiştirebilir, daha güçlü devletler, siber saldırılar gibi zorlayıcı faaliyetleri yasaklayan Madde 2 (4) 'ün daha geniş kapsamlı yorumlamaya ve dolayısıyla bunu desteklemeye başlayabilirler. [548] Siber saldırılar, giderek yaygınlaşan devlet pratiği ve fikir yargısının kaydettiği gibi, geleneksel uluslararası hukuk normlarını da ihlal edebilmektedir. Birincisi, devletler genellikle siber saldırılara açıkça katılmazlar, aksine saldırıları teknik yollarla kamufle ederek ve devlet kurumları ile muğlak ilişkilerde olan devlet dışı aktörler aracılığıyla saldırıları gerçekleştirerek sorumluluklarını gizlemeye çalışırlar. [549] Başka bir deyişle, devletlerin siber saldırılarını gizlemeye çalıştıkları gerçeği, bu tür saldırıların hukuka aykırı güç kullanımı teşkil edebileceğine dair bir endişeye ihanet edebilmektedir. İkincisi, devletlerin siber saldırı kurbanı olduklarını kabul ettikleri zaman, onlar ve onların müttefikleri saldırıları kınama

[546] Silver, Daniel B., Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, International Law Studies, Vol. 76, Computer Networ Attack and International Law, Mitchal N. Schmitt & Brian T. O'Donnell (Editors), p. 74.
[547] Nguyen, a.e, s.1114.
[548] Taşdemir, Fatma / Gökhan Albayrak, The Law of Cyber Warfare in Terms of Jus Ad Bellum and Jus in Bello: Application of International Law to the Unknown?, December 23, 2017, E-Journal of Law, Forthcoming, pp. 4-6.
[549] Sklerov, Lieutenant Matthew J., Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty To Prevent, The Judge Advocate General's School, United States Army, Yayınlanmamış Yüksek Lisans Tezi, 2009, s.86.

eğilimindedirler. [550] Üçüncüsü, siber-savunmaya ortak yaklaşımda, NATO, siber saldırıların tarafların NATO anlaşmasının 4. maddesi kapsamındaki yükümlülüklerini ortaya koyduğunu, bunun yalnızca "Tarafların herhangi birinin toprak bütünlüğü, siyasi bağımsızlığı veya güvenliği tehdit edildiğinde" geçerli olduğunu belirtmiştir. Bu hükmün başlatılması, NATO üyesi ülkelerin siber saldırıların, olağan dışı davranış normu veya ilgili uluslararası hukuk normu kurallarını ihlal ettiğine inandığını kuvvetle göstermektedir. Yine de, bir siber saldırının hukuka aykırı olması, silahlı kuvvetin karşılık olarak kullanılabileceği anlamına gelmemektedir. [551]

3.1.2. Kolektif Güvenlik ve Meşru Müdafaa İstisnaları

Madde 2 (4) te bahsi geçen güç tehdidinin kapsamlı kullanım yasağı, iki istisnaya tabidir: toplu güvenlik operasyonlarının bir parçası olarak sürdürülen eylemler ve kendini savunma eylemleri. İlk istisna BM Sözleşmesinin 39. Maddesi kapsamındadır. 39. Madde, Güvenlik Konseyine "barışı tehdit etme, barışın ihlali veya saldırganlık tehdidinin varlığını belirleme ve uluslararası barış ve güvenliği yeniden tesis etme" yetkisi vermektedir. [552] Güvenlik Konseyi, "silahlı kuvvet kullanımını içermeyen önlemler" uygulayabilir ve "hava, deniz veya kara kuvvetleri ile eylemi" yetkilendirebilir. 39. Madde kapsamında toplu güvenlik operasyonları politik olarak zor olabilir, bunun sebebi genellikle kilitlenmiş veya yavaş hareket eden Güvenlik Konseyi tarafından yetkilendirilmeleri gerektiğindendir. [553] Madde 2 (4) 'ün ikinci istisnası, 51.

[550] Damrosch, Lori Fisler/ Bernard H. Oxman, Editors' Introduction, The American Journal of International Law, Vol. 97, No. 3, 2003, p. 555.
[551] Bills, Amanda, Cyber Warfare and Jus in Bello – The Regulation of Cyber 'Attacks' under International Humanitarian Law, Lund University, Yayınlanmamış Yüksek Lisans Tezi, s. 15-17.

[552] Hofmeister, Hannes, Watch What You Are Saying: The UN Charter's Prohibition on Threats to Use Force, Georgetown Journal of International Affairs, Vol. 11, No. 1, 2010, p. 107.
[553] BM Sözleşmesi, Madde 39 : https://treaties.un.org/doc/publication/ctc/uncharter.pdf (E.T: 15.04.18).

Maddede, bahsi geçen "silahlı saldırı meydana gelmesi durumunda, bireysel veya toplu savunma hakkını geçersiz kılar" ı öngören kuraldır. Yasal kolektif güvenlik eylemlerini, tanımlamak daha zordur. Bunun sebebi ise, birçok silahlı çatışmada, her iki taraf da kendini savunma konusunda harekete geçtiğini iddia etmektedir ve uluslararası tartışmalar, hukuki doktrinden ziyade, gerçek ve politik anlaşmazlıklara odaklanma eğilimindedirler. [554]

Bununla birlikte, meşru müdafaanın hukukiliğini belirleyen kritik sorunun, silahlı bir saldırının gerçekleşip gerçekleşmediği durumudur. Bir siber saldırı, bir devletin 51. Madde uyarınca hukuki olarak karşılık vermesi için silahlı saldırı seviyesine çıkması gerekmektedir. "Silahlı saldırı" terimi, BM Sözleşmesindeki diğer ilgili terimlerden dilbilimsel olarak farklıdır ve onlardan muhteviyat olarak önemli ölçüde daha dar olduğu bilinmesi gereken bir gerçektir. [555] Örneğin, Madde 2 (4) 'ün, silahlı saldırı seviyesine çıkmayan güç kullanımı ya da yasağı üzerindeki yasağı ihlal eden ve Madde 51 uyarınca öz-savunma hakkını tetiklemeyen eylemler meydana gelebilmektedir. [556] UAD, "ölçek ve etkileri" bakımından önemsiz olan sınır ötesi saldırıların "silahlı saldırılardan" ziyade "sınır eylemler" olarak sınıflandırılabileceğini belirtmiştir. Bunun yerine, Madde 51 uyarınca herhangi bir karşılığı haklı çıkarmak üzere yeterli silahlı saldırı olarak nitelendirmek için, saldırılar "güç kullanımının en ağır biçimlerini" oluşturmalıdır. [557] Bununla birlikte, 51. Madde uyarınca savunma kuvvetine başvuramayacakları durumlarda (bir saldırı "silahlı saldırı" seviyesine yükselmediği için), devletlerin dikkatle yasaklanan yasal sınırlar dâhilinde retoriklerle veya zorlayıcı karşı tedbirlerle karşılık vermelerine izin verilebilmektedir. Siber saldırılara *jus ad bellum* uygulaması üzerine yapılan

[554] Berman, Franklin, The UN Charter and the Use of Force, Singapore Year Book of International Law and Contributors, 10 SYBIL, 2006, p. 12.
[555] Paust, Jordan J., Self-Defense, Laws of War, and Human Rights, Die Friedens-Warte, Vol. 81, No. 2, 2006, pp. 81-82.
[556] Wolter, Detlev, The UN Takes a Big Step Forward on Cybersecurity, Arms Control Today, Vol. 43, No. 7, 2013, p. 27.
[557] Arend, Anthony Clark, International Law and the Preemptive Use of Military Force, The Washington Quarterly Vol. 26, No. 2, p. 92.

bilimsel tartışmalarda, siber saldırının silahlı saldırıyı tetikleyen silahlı saldırıyı ne zaman tetiklediğini belirlemek için üç öncü görüş ortaya çıkmıştır: araç temelli yaklaşım, hedefe dayalı yaklaşım ve tercih edilen yaklaşımdır (etkileri temel alan yaklaşım). [558] Bu bağlamda, araç temelli yaklaşım dâhilinde tek başına bir siber saldırı, neredeyse hiçbir zaman, geleneksel askeri silah kullanmadığı için, diğer bir deyişle, "askeri zorlama ile geleneksel olarak ilişkilendirilen fiziksel özelliklerden yoksun olduğu için" Madde 51'in amaçlarına yönelik bir silahlı saldırı oluşturmayacaktır.

Bu yaklaşım, siber saldırıyı silahlı saldırı olarak sadece askeri silah kullanıyorsa ele almaktadır. [559] Bombalama, bilgisayar sunucuları veya internet kablolarına karşı önemli hasarlara yol açacak şekilde gerçekleşmesi durumunda, silahlı saldırının gerekliliklerini karşılayabilecektir. [560] BM Sözleşme metni, araç temelli yaklaşım için kısmi bilgi sağlamaktadır, zira 41. Maddede "silahlı kuvvet kullanımını içermeyen bir önlem" olarak "telgraf, telsiz ve diğer iletişim araçlarının tam veya kısmi kesintisi…" olarak nitelendirilmektedir. BM Genel Kurulu'nun Saldırganlık Tanımı, dolaylı olarak da araca dayalı görüşü desteklemektedir: Madde 51 uyarınca silahlı saldırıdan daha geniş bir kategori olan ve 39. maddeye göre "saldırganlık" teşkil edecek bir dizi eylemi listelemektedir ve bunların hepsi askeri silah veya güç içermektedir. [561] NATO da bu görüş ile aynı çizgide olduğunu şu şekilde bildirmiştir: siber-savunmaya yönelik yeni ortak yaklaşımı, siber saldırının üye devletlerin NATO antlaşmasının 4. maddesi kapsamında birbirleriyle "istişare" etmesini zorunlu kıldığını, ancak siber saldırıların üye devletlere yardımcı olmaları için Antlaşma'nın 5. maddesi

[558] Paust, Jordan J., Self-Defense Targetings of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan, Journal of Transnational Law & Policy, Vol. 19, No. 2, Spring 2010, p. 241.
[559] Schmitt, Michael N., Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 Colum, Journal of Transnational Law & Policy, Vol. 885, No. 909, 1991, p.1041.
[560] A.g.e, s. 1042.
[561] Drumbl, Mark, et al., Self-Defense in an Age of Terrorism, Proceedings of the Annual Meeting American Society of International Law, Vol. 97, 2003, p. 141.

kapsamında silahlı bir saldırı oluşturmayacağını belirlemektedir. [562] Araç temelli yaklaşımın, geleneksel araçlardan kaynaklanmayan zararları hesaba katmak için temel yetersizliğini kabul ederek, hedefe dayalı yaklaşım, bir bilgisayar sistemini hedef alan herhangi bir siber saldırıyı silahlı bir saldırı olarak sınıflandırmaktadır. [563] Bu yaklaşımın temel amacı, bir siber saldırının ne zaman karşılık vermek gerektiğini öngören meşru müdafaa hakkının hukukiliğini doğrulamaktır. Hedefe dayalı yaklaşım, kritik ulusal sistemlerin saldırgan korumasına izin vermenin avantajını sağlarken, geniş çaplı meşru müdafaa, siber-çatışmaların daha yıkıcı geleneksel silahlı çatışmalara dönüşme olasılığını arttırmaktadır. [564] Bir siber saldırı, fiziksel, kinetik bir savaş başlatabilen geleneksel bir askeri karşılığı haklı çıkarmak için sadece kritik bir sisteme girmeye ihtiyaç duymaktadır. Bu yaklaşım, savaşı çok daha muhtemel hale getirerek uluslararası toplumun güvenliğini zayıflatabilme potansiyeline sahiptir. Son olarak, etki temelli yaklaşım, siber saldırıyı, etkilerinin mahiyetine göre silahlı saldırı olarak sınıflandırmaktadır. [565] Araç ve hedefe dayalı görüşler arasında, etki temelli yaklaşım en yaygın kabul gören yaklaşımdır. [566] Etkilere dayalı yaklaşımın farklı versiyonları, etki faktöründen zararın ciddiyetine, siber saldırının kendisi ile nihai zarar arasındaki illiyet bağının mahiyetine kadar çeşitli faktörlerden herhangi birine atıf yaparak ölçebilmektedir. Bununla birlikte, etkilere dayalı yaklaşımla ilgili problem, ne tür etkilerin kendini savunmayı haklı kıldığını öne sürmektedir. [567]

---

[562] Mertus, Julie, Assessing the NATO Intervention Under the UN Charter, Proceedings of the Annual Meeting, American Society of International Law, Vol. 94, 2000, pp. 310–311.
[563] Hathaway, s. 846.
[564] Jensen, Eric Talbot, Cyber Deterrence, 26 Emory International Law Review, Vol. 773, No. 773, 2012, p. 795.

[565] Hmoud, Mahmoud, Are New Principles Really Needed? The Potential of the Established Distinction Between Responsibility for Attacks by Nonstate Actors and the Law of Self-Defense, The American Journal of International Law, Vol. 107, No. 3, 2013, pp. 57–578.
[566] Hmoud, a.g.e, s.579.
[567] Sofaer, Abraham D., The Best Defense? Preventive Force and International Security, Foreign Affairs, Vol. 89, No. 1, 2010, pp. 111-113.

3.1.3. Ad Bellum Gerekliliği ve Orantılılığı

Bir devletin siber saldırıya karşılık olarak silahlı kuvvet kullanması, sadece BM Sözleşmesi ve silahlı kuvvet kullanımına ilişkin uluslararası hukuk sınırlarına riayet etmekle kalmamalı, aynı zamanda geleneksel uluslararası kurallar gereğince gerekliliğin ve orantılılığın *jus ad bellum* ilkelerine uygun olması gerekmektedir. [568] Gereklilik ilkesi, bir diplomatik çözüm gibi barışçıl yolların devletin genel amacına ulaşamadığı durumlarda, gücün sadece son çare olarak kullanılmasını gerektirmektedir. Orantılılık, bu mantığı genişletmektedir ve eğer gücün genel kapsamı ve yoğunluğu, devletin gerçek veya yakın tehlikesi ile ilgili olarak aşırı ise, gücü yasaklamaktadır. [569] İhtiyaç ve orantılılık ilkeleri net olsa da, bu ilkeleri siber saldırılara karşı devletin uygulayacağı karşılığa göre uygulamak zordur. Meşru müdafaa girişiminin gereklilik ve orantılılık ilkelerine uygun olup olmadığını değerlendirmek, geleneksel saldırılar için dahi zor ve olgusal bir gerçektir ve siber saldırılar yeni ve karmaşık sorunsallar meydana getirmektedir. Örneğin, silahlı saldırının yarattığı etki seviyesine kadar yükselen siber saldırılar, karar merciindeki kişilerin/kurumların, bilgisayar ağlarına zararı ölçmenin yollarını ve bunun yasal bir karşılık teşkil edeceğini belirlemek üzere daha geleneksel zarar türlerine kıyasla dolaylı etkilerini tasarlamalarını gerektirebilmektedir. [570] Mevcut *jus ad bellum* çerçevesini siber saldırılar bağlamında uygulamak oldukça zor bir süreçtir. Bu çerçeve sadece Güvenlik Konseyi kararları tarafından ele alınan ya da silahlı saldırı teşkil eden siber saldırıların küçük alt kümeleri için geçerli olup, Madde 51 uyarınca bir meşru müdafaa hakkı doğurmaktadır. [571] Sonuç olarak, sadece az sayıda siber saldırılar, savaş yasalarının geçerli olduğu "siber savaş" olarak kabul edilmektedir.

---

[568] Haque, Adil Ahmad, Necessity and Proportionality in the Law of War (August 22, 2016). Cambridge Handbook on Just War (Larry May ed, CUP 2016). August 22, 2016, p.18.
[569] Gardam, Judith, The Place of Necessity and Proportionality in Restraints on the Forceful Actions of States, Cambridge University Press, 0521837529, December 2004, pp.1-4.
[570] Hathaway, s.849.
[571] O'Connell, Mary Ellen, The Limited Necessity of Resort to Force, Imagining Law: Essays in Conversation with Judith Gardam, edited by Dale Stephens and Paul Babie, University of Adelaide Press, South Australia, 2016, pp. 48-49.

3.2. Jus in Bello

"*Jus in Bello*, "savaşı sürdürme hukuku" anlamına gelen Latince bir terimdir. Bu, savaş sırasında savaşanlara yasak olan uygulamaları ele alan uluslararası savaş hukukunun bir yönüdür. *Jus in Bello*, bir ülkenin savaşı yürütebileceği standartları tanımlar ve savaş sırasındaki eylemler adil olmalıdır. *Jus in bello*, iki ayrımcılık ve orantı ilkesini içerir. Ayrımcılık meşru hedefleri tanımlar ve orantılılık ne kadar kuvvetin kullanılabileceğini tanımlamaktadır". [572] Tek başına bir siber saldırı bir silahlı çatışmayı teşvik etme noktasında zayıf kalsa da, geleneksel provokasyonlara karşı savaşlarda ya da yakın bir konvansiyonel saldırıya yol açmak için siber saldırılar kullanılmıştır. Bu kapsamda, geleneksel silahlı çatışmalar sırasında kullanılan *jus in bello* gereklilikleri ve siber saldırılar arasındaki ilişkiyi incelemek önem arz etmektedir. [573] Siber uzayın yeni koşulları, gereklilik, orantı, ayrım ve tarafsızlık ilkelerine göre *jus in bello* uygulamak konusunda zorluklar doğurabilmektedir. Siber saldırıların çoğu zaman ölümcül veya yıkıcı olmadığından ve sadece geçici olarak ağ sistemlerinde yetersizliğe neden olabileceğinden, siber saldırıların orantılı olup olmadığını değerlendirmek zor olabilmektedir. [574]

3.2.1. In Bello Gerekliliği

Siber saldırının gerekliliğinin değerlendirilmesi zor olsa da, bu zorluk siber saldırılardan kaynaklanmayan ve *in bello* siber saldırılarına özgü olmayan

---

[572] USLEGAL, Jus in Bello Law and Legal Definition: https://definitions.uslegal.com/j/jus-in-bello/ (E.T: 15.04.18).

[573] Moussa, Jasmine, Can Jus Ad Bellum Override Jus In Bello? Reaffirming the Separation of the Two Bodies of Law, International Review of the Red Cross, Vol. 90, No. 872, December 2008, pp. 965 – 966.

[574] Sharma, Bhaskar, Cyber War and Jus in Bello, Foreign Policy Journal, Dec 3, 2012: https://www.foreignpolicyjournal.com/2012/12/03/cyber-war-and-jus-in-bello/ (E.T: 15.04.18).

konuyla ilgili çerçeve oluşturma tartışmalarından kaynaklanmaktadır. [575] *In Bello*'nun gerekliliği, belirli bir düşmanlık eyleminden elde edilecek somut askeri avantaj ile ilgilidir. Askeri hedefini ilerletmezse, bireysel bir siber saldırı gereksiz kalmaktadır. Siber saldırıların yasal olması gerekmekle birlikte, *bello* gerekliliğini değerlendirmek yeni zorluklar ortaya çıkarmamaktadır. [576]

3.2.2. In Bello Orantılılığı

In Bello orantılılık ilkesi, "sivillerin ölümüne, sivillerin zarar vermesine, sivillerin eşyalarının zarar görmesine veya bunların oluşumuna yol açabilecek somut ve doğrudan askeri avantaj sağlamaya yönelik aşırı olan saldırıları" yasaklamaktadır. [577] *In Bello* orantılılık analizini yürütmek üzere, askeri karar vericiler, potansiyel sivil kayıplar, sivil mülklerin tahrip edilmesi ve askeri bir hedefe ulaşmak üzere sivil eşyaların kaybını da göz önünde bulundurmaları gerekmektedir. [578] Sebebiyet verdikleri zararın doğası gereği siber saldırıların orantısı kendine özgü zorluklar doğurmaktadır. Siber saldırıların doğrudan etkileri olabileceğinden, bir saldırının "sivil yaşam kaybı, sivillere zarar verme, sivil eşyalarındaki hasar veya bunların bir kombinasyonu" gibi ilgili kategorilere göre orantılı olup olmayacağını değerlendirmek zor olabilmektedir. [579] İnternetten bilgi aktarımını engelleyen bir siber saldırı sadece kamuoyu nezdinde sorun çıkartabilirken, hastanelerin hayati bilgileri iletememesine ve yaşam kaybına yol

[575] Mégret, Frédéric, Jus in Bello and Jus Ad Bellum, Proceedings of the Annual Meeting (American Society of International Law), Vol. 100, 2006, pp. 121–123.
[576] CYBER WAR LAW, The Principles of Humanity and Military Necessity in Cyber War : http://cyberwarlaw.eu/the-principles-of-humanity-and-military-necessity-in-cyber-war/ (E.T: 15.04.18).
[577] Haque, Adil Ahmad, A Theory of Jus in Bello Proportionality (May 4, 2015). Forthcoming in Weighing Lives: Combatants & Civilians in War (Jens David Ohlin, Larry May, Claire Finkelstein eds., 2015), pp.1-3.
[578] Martinez, Jenny/Antoine Bouvier, Assessing the Relationship Between Jus in Bello and Jus Ad Bellum: An 'Orthodox' View, Proceedings of the Annual Meeting (American Society of International Law), Vol. 100, 2006, pp. 111-112.
[579] Mertus, Julie, The Danger of Conflating Jus Ad Bellum and Jus in Bello, Proceedings of the Annual Meeting (American Society of International Law), Vol. 100, 2006, pp. 116–117.

açmasına neden olabilen örnekler daha ciddi sonuçlara da yol açabilmektedir. [580] Bir DDOS atağı için *ex ante* (tahmini) *in bello* orantı analizinde de daha önce izah edildiği üzere, geleneksel bir saldırıdan çok daha büyük bir belirsizlik derecesine sahip olabilmektedir. Bu nedenle, *in bello* orantılılık analizi, bir eylemin olası sonuçlarını öngörmeyi gerektirmektedir, ancak bu duruma başka bir belirsizlik eklendiğinde, bu analizi siber bağlamda daha da zorlaştırmaktadır. [581] Sonuç olarak, siber saldırılar devletleri planlı saldırıların hukukiliğine dair karar verirken tipik olarak karşılaştıklarından daha fazla belirsizlikle yüzleşmeye zorlayabilecek kapasiteye sahiptir. [582]

3.2.3. Farklar/Ayrımlar

Devletlerin sivil ve askeri personeli ayırt etmelerini ve saldırıları askeri hedeflere göre kısıtlamalarını gerektiren ayrım ilkesi, başka bir yasal sorun meydana getirmektedir. Bu prensibe göre, komutanlar doğru bir şekilde hedef alabilecek silahlar kullanmalı ve sivil ve askeri hedefleri birbirinden ayırmak için bunu kullanmalıdır. [583] Ek olarak, savaş hukuku, kontrol edilemeyen, öngörülemeyen veya sivil ve askeri hedefler arasında ayrım yapmayan *in bello* siber saldırılarını yasaklamaktadır. Bu bilgiler dâhilinde, ayrım ilkesinin siber saldırılara kolaylıkla uygulanabileceği durumlar mevcuttur. [584] Örneğin, bir askeri hava trafik kontrol sistemini hedefleyen ya da asker nakliyesi esnasında

[580] Pavlischek, Keith, Proportionality in Warfare, The New Atlantis- Journal of Technology & Society : https://www.thenewatlantis.com/publications/proportionality-in-warfare (E.T: 15.04.18).
[581] Petkis, Stephen, Rethinking Proportionality in the Cyber Context, Georgetown Law, pp. 1446-1447. : https://www.law.georgetown.edu/academics/law-journals/gjil/recent/upload/Petkis.PDF (E.T: 15.04.18).

[582] Petkis, a.g.e., s.1448.
[583] Beck, Louise Doswald, Some Thoughts on Computer Network Attack and the International Law of Armed Conflict, International Law Studies, Vol. 76, Computer Network Attack and International Law, Michael N. Schmitt & Brian T.. O'Donnell (Editors), 2002, p.65.
[584] Giladi, Rotem, The Jus Ad Bellum/Jus in Bello Distinction and the Law of Occupation, Israel Law Review, Hebrew University International Law Research Paper No. 18-08, Vol. 41, November 1, 2008, pp. 247-249.

gerçekleşen bir siber saldırı, ayrımcılık ilkesine uygun bir durum ortaya çıkartmaktadır. Sivil bankacılık sektörüne ya da hastanelere, müzelere ya da ibadet yerleri gibi diğer siber saldırılar, ayrımcılık ilkesini açıkça ihlal etmektedir.[585] Bu hedefleri yöneten ağlara karşı siber saldırılar, bu nesneler üzerindeki diğer herhangi bir saldırı gibi, yasa dışı kabul edilmektedir. Sonuç olarak, ayrım analizi genellikle siber saldırı bağlamında karmaşık hale gelmektedir çünkü muhtemel hedefler aynı anda çok sayıda aktör tarafından kullanılmaktadır.[586]

3.2.3.1. Bir Siber Saldırıda Hukuki Olarak Hedeflenen Kim Olabilir?

Savaş hukukuna göre, yalnızca üç kategoride bireyler hedef alınabilir: savaşçılar, düşmanlara doğrudan katılan siviller ve sürekli savaş işlevi gören siviller. Sivillerin "düşmanlıklarda doğrudan rol aldıkları" ölçüde hedef alınmama haklarını yitirmektedirler.[587] Ayrıca, Uluslararası Kızılhaç Örgütü tarafından onaylanan uluslararası teamül hukuku kapsamında, sürekli savaş işlevi gören siviller de hedef alınabilmektedirler[588]. Bu kurallar 11 Eylül sonrası bağlamında sıklıkla görüşmüştür. Ancak göz önünde bulundurulması gereken diğer bir husus ise, sivil katılımların siber saldırılara katılımı ve katkısı, doğrudan katılım, sürekli muharebe işlevi ve düşmanlıkların uygulanması noktasında diğer katılım türleri arasındaki çizgiyi bulanıklaştırmasıdır.[589] Herhangi bir silah sisteminin sivil tasarımcısı, düşmanlıklarda doğrudan sorumlu kişi olarak atfedilmemiştir. Ancak, askeri istihbarat ile çalışan yazılımcı, saldırı anına kadar saldırıyı gerçekleştirmek

---

[585] Maiese, Michelle, Jus in Bello, Beyond Intractability, June 2003 : https://www.beyondintractability.org/essay/jus_in_bello (E.T: 15.14.18).
[586] Sassòli, Marco; The Distinction and Relationship between Jus ad Bellum and Jus in Bello, Chinese Journal of International Law, Vol. 11, No. 3, 1 September, 2012, pp. 610-611.
[587] CPS, Cybercrime - Prosecution Guidance: Legal Guidance, Cyber / Online Crime : https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (E.T: 15.04.18).
[588] Melzer, Nils, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, ICRC, May 2009, pp. 43-45.
[589] Avcı, Maya Ezgi, A Lawful Response to Cyber Attacks, Law & Justice Review, Year.7, Issue.12, June 2016, pp. 409-411.

için kodu değiştirebilmektedir. [590] Özellikle de bu tür faaliyetlerde düzenli olarak yer alan bir sivilin gerçekleştirecek olduğu eylemler, "sürekli bir işlev olarak düşünülmektedir. Sonuç olarak, siber saldırılara karışan siviller, karşı saldırıların yasal hedeflerini ortaya koyarak, savaş hukuku kapsamında statülerini değiştiren görevleri yerine getirmiş olmaktadırlar. [591]

3.2.3.2. Kim bir Siber Saldırı Gerçekleştirebilir?

Bir siber saldırı durumunda kimlerin hedef alınabileceği sorusuna ek olarak, ayrım ilkesi devletlerin siber savaşçı güçlerini nasıl oluşturduğunu kısıtlamaktadır. Sivillerin güç kullanmasını destekleyen bir devlet, bu sivilleri silahlı çatışma yasası altında sahip oldukları korumaların dışında bırakarak savaşçılarla siviller arasındaki ayrım ilkesini baltalayabilmektedir. [592] Hukuki sonuçlara rağmen, devletlerin siber bağlamda sivilleri kullanmak üzere birçok nedenleri vardır. İlk olarak, siviller hükümetlerin sahip olmadığı teknik uzmanlığa sahip olabilmektedirler. İkincisi, siber saldırıları gerçekleştirmek için siviller kullanmak suretiyle, devletler bu tür operasyonlarda kendi katılımlarını maskeleyebilmektedirler. [593] Örnek verilecek olursa, Vladimir Putin tarafından başlatılan Kremlin yanlısı bir gençlik grubu olan Nashi, Estonya'ya yönelik 2007 siber saldırılarının sorumluluğunu üstlenmiştir. [594] Rus işadamlarının Nashi'nin Rus hükümeti tarafından tercih edilen siber saldırıları gerçekleştirmesi noktasında destek sağladıkları iddia edilmiştir. Rus hükümeti ise saldırıya karıştığını makul

[590] Kodar, Erki, Applying the Law of Armed Conflict to Cyber Attacks, ENDC Proceedings, Volume 15, 2012, pp. 108–109.
[591] Williams, Ja Rai A., The Legal Limits of Targeting the Cyber Capabilities of a Neutral State, Air Command and Staff College Air University, Yayınlanmamış Yüksek Lisans Tezi, 2015, s. 15.
[592] USAF, Cyberspace Operations: Air Force Doctrine Document 3-12 15 July 2010, Incorporating Change 1, 30 November 2011, pp. 9-14.
[593] Hern, Alex, Cyber-Attacks and Hacking: What You Need to Know, The Guardian, 1 Nov. 2016 : https://www.theguardian.com/technology/2016/nov/01/cyber-attacks-hacking-philip-hammond-state-cybercrime (E.T: 15.04.18).
[594] Lowe, Christian, Kremlin Loyalist Says Launched Estonia Cyber-Attack, Reuters, March 13, 2009: https://www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313 (E.T: 15.04.18).

gerekçelerle inkâr etmiştir. [595] Bu gerekçeyle, devletler sivil siber saldırganları silahlı çatışma hukukunu ima eden takdir yetkisini kullanacakları faaliyetlerde bulunmak için kullanamazlar.

3.2.4. Tarafsızlık

In bello siber saldırısının yasallığını değerlendirmede son zorluk ise, bir siber saldırının 'tarafsızlık' durumundan ortaya çıkabileceği gerçeğidir. Bir devlet, İsviçre gibi kalıcı olarak ya da belirli bir çatışmanın süresi boyunca tarafsızdır. Tarafsızlık ilkesi hem hakları hem de sorumlulukları içermektedir: [596] "Tarafsız ulusun temel hakkı dokunulmazlıktır; Başlıca görevleri, çekimser ve tarafsız olmaktır. Aynı şekilde, savaşan bir devletin birinci görevi karşı devletin 'çekimserlik' ilkesine saygı göstermek ve ikinci görevi ise 'tarafsız' olmasında ısrarcı olmasına da aynı düzeyde saygı göstermelidir. Siber saldırıların bu çok yönlü özellikleri, karmaşık olan tarafsızlık ilkesinin değerlendirmesini daha da zorlaştırmaktadır. [597] Siber saldırganlar, herhangi bir birey bu durumun farkına varmadan, devlet/hükümetin ise çok az bir kısmının haberdar olabileceği ve kim oldukları gerçeğini bir dizi sunucu ve bilgisayar aracılığıyla maskeleyerek, zombi bilgisayarlarını başka bir ülkedeki ağlara zarar vermek için kullanabilmektedirler. [598] Bu türden siber saldırılar, iki nedenden dolayı tarafsızlık ilkesi kapsamında analiz edilememesine sebep olmaktadır. Birincisi, bir ülke bilgisayarlarının siber saldırı için kullanıldığının farkında olmamış olabilir ve bu nedenle tarafsızlığının tehdit edildiğinin bilincinde olmayabilir. İkincisi, tarafsızlık ilkesi, menşe ülkesinin kimliğine dayanan saldırılara karşı yasal

[595] Markov, Sergei, Behind The Estonia Cyberattacks, March 06, 2009 : https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html (E.T: 15.04.18).
[596] Ingber, Rebecca, Untangling Belligerency from Neutrality in the Conflict with Al-Qaeda, Texas International Law Journal, Vol. 47, No. 1, pp. 80-89.
[597] Heinegg, Wolff Heintschel von, Neutrality in Cyberspace, 2012 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012, NATO CCD COE Publications, Tallinn, pp. 35-37.
[598] McMahon, Jeff, Morality, Law, and the Relation Between Jus ad Bellum and Jus in Bello, ASIL Proceedings, 2006, pp. 46-48.

karşılıkları belirlemektedir. [599] Sonuç olarak, saldırıların belirli bir duruma atfedilememesi tarafsızlık analizine engel olmaktadır. Bununla birlikte, siber saldırıya karşı hukuki karşılıkların siyasi belirsizliği, saldırılara atfedilememesi olarak göz ardı edilmesi de mümkündür; Siber saldırıları düzenleyen yasal çerçeve daha net bir hale gelmesi durumunda, atfedilmenin önündeki engelleri de azaltmış olacaktır. [600] İlişkilendirmenin siyasi sorunları, atfedilmenin bariz zorluklarına katkıda bulunsa da, bir ülkenin saldırılarını bilmediği ihtimalleri sınırlarından kaynaklanıyor olabilir. BM Şartının 51. Maddesinde bahsi geçen meşru müdafaa ve savaş hukuku çerçevesi, hem *jus ad bellum* hem de *jus bello* dâhilinde izin verilen saldırı ve savunmasız siber saldırıların kapsamını belirlemeye çalışan devletler için eksik ve muğlak olsa da, meşru müdafaanın hukukiliğini (jus ad bellum) ve karşılık verirken riayet edilmesi gereken kuralların (jus ad bellum) genel çerçevesini oluşturmaktadır. Ancak siber saldırıların büyük çoğunluğunu düzenlemediği gerçeği unutulmamalıdır. [601] Aynı şekilde, çoğu siber saldırı bir silahlı saldırı seviyesine erişmememektedir yahut herhangi bir silahlı çatışma bağlamında gerçekleşmemektedir.

[599] Jastram, Kate/ Anne Quintin, The Internet in Bello: Cyber War Law, Ethics & Policy, Seminar held 18 November 2011, Berkeley Law, pp. 20-26.
[600] Robin Geiss, The Conduct of Hostilities in and via Cyberspace, Proceedings of the Annual Meeting (American Society of International Law), vol. 104, 2010, pp. 372-373.
[601] INFOSEC INSTITUTE, Jus in Cyber Bello: How the Law of Armed Conflict Regulates Cyber Attacks Part I, APRIL 10, 2014 : http://resources.infosecinstitute.com/jus-cyber-bello-law-armed-conflict-regulates-cyber-attacks-part/#gref (E.T: 15.04.18).

4. Değerlendirme

Bu bölümde, ikinci bölümden farklı olarak nükleer santrallerin güvenliğinin uluslararası hukuki boyutları incelenmiştir. Nükleer güvenliğin önem arz etmesinin sebebi ise nükleer terörizmin 11 Eylül olayından sonra daha muhtemel olması ihtimali ve teröristlerin bu saldırıları oldukça kırılgan yapılarda olan nükleer santrallere karşı gerçekleştirebilme ihtimallerinden ileri gelmektedir. Nükleer güvenliğe dair uluslararası hukuki düzenlemeler bu kapsamda nükleer santral kurulmadan önce, kurulma esnasında ve sonrasındaki süreçleri kapsamaktadır. Uluslararası hukuk özelinde, nükleer santrallerin güvenliği ilk olarak güvenlik kültürü ve rejimi kapsamında ele alınması gerekmektedir. UAEA, BM, UDÖ kurumları nükleer santrallerin güvenliği genelinde düzenlemelerde bulunmuşlardır ve taraflar nezdinde bağlayıcı hükümler içermektedir. Yine UAEA, BM ve EURATOM ise bağlayıcı hükümlerden ziyade teknik bilgilendirme mahiyetinde düzenlemeler yapmıştır. Bu kapsamda, UAEA'nın Nükleer Malzemelerin Fiziksel Korunması Sözleşmesi ve 2005 tarihli Değişiklik, Nükleer Kazaların Erken Bildirimi Sözleşmesi, Acil Nükleer ve Radyolojik Kaza Durumunda Yardım Sözleşmesi, Nükleer Güvenlik Sözleşmesi, Tüketilen Yakıt Yönetiminin Güvenliği ve Radyoaktif Atık Yönetiminin Güvenliğine Dair Ortak Sözleşme düzenlemeleri bağlayıcı hükümle içermektedir. Nükleer Malzemelerin Fiziksel Korunması Sözleşmesi ve 2005 tarihli Değişiklik, muhteviyat olarak nükleer santrallerde uranyum gibi kullanılacak maddelerin güvenliğine dair düzenlemeler içermektedir. Nükleer Kazaların Erken Bildirimi Sözleşmesi ise herhangi olası bir kaza durumunda durumun acilen bildirilmesi gerektiği ve bununla ilgili etap ve süreçleri kapsamaktadır. Acil Nükleer ve Radyolojik Kaza Durumunda Yardım Sözleşmesi, muhtemel radyolojik kazalarda gerçekleşecek yardım süreçleri ile ilgili kısımları kapsamaktadır. Radyoaktif Atık Yönetiminin Güvenliğine Dair Ortak Sözleşme ise radyoaktif atıkların yönetim sürecini ele almaktadır. BM nezdindeki bağlayıcı düzenlemeler olarak BM Güvenlik Konseyi 1373 (2001) ve 1540 (2004) Sayılı Kararları, Terörist Bombalamalarının Engellenmesine Dair Uluslararası Sözleşme ve Nükleer Terör Faaliyetlerinin

Önlenmesine Dair Uluslararası Sözleşme düzenlemeleri mevcuttur. Bu kapsamda, BM Güvenlik Konseyi 1373 (2001) ve 1540 (2004) Sayılı Kararları, uluslararası terörizm ve nükleer maddelerin yasadışı hareketi arasındaki yakın ilişkiyi ve bu ciddi sorunu ve uluslararası güvenlik tehdidine karşı küresel bir karşılıkla güçlendirmek için ulusal, bölgesel ve uluslararası çabaların koordinasyonunu artırma gereğini vurgulamaktadır. Terörist Bombalamalarının Engellenmesine Dair Uluslararası Sözleşme ve Nükleer Terör Faaliyetlerinin Önlenmesine Dair Uluslararası Sözleşme ise olası bir terörist saldırısı durumundaki usul ve esasları temel almaktadır. UDÖ Himayesinde Temel Hukuki Düzenlemeler ise Deniz Ulaştırması Güvenliğine Karşı Yasadışı Eylemlerin Önlenmesine İlişkin Sözleşme (1988 SUA Sözleşmesi) ve SUA (Yasadışı Eylemlerin Önlenmesi) Sözleşmesinin 2005 Protokolleridir. Bu sözleşmeler ise deniz taşımacılığı esnasında herhangi bir terör eylemleri durumunda hangi süreçlerin izlenmesi gerektiğini açıklığa kavuşturmaktadır. Radyoaktif maddelerin seyrüsefer esnasında teröristler tarafından salınımı da yine bu sözleşmelerin maddelerine dâhil edilmiştir. UAEA Himayesinde Bağlayıcı Olmayan Düzenlemeler ise Radyoaktif Kaynakların Emniyeti ve Güvenliğine İlişkin Uygulama Esasları ve Radyoaktif Kaynakların İthalatı ve İhracatı Hakkında Ek Düzenleme ve Tarihli Nükleer Malzemelerin ve 2017 Tarihli Nükleer Tesislerin Fiziksel Korunmasına Dair Uluslararası Konferans tır. Bu çalışmalar ise nükleer terörizmde güncel gelişmeler ışığında mevcut mevzuatı düzenlemeye yönelik düzenlemeler niteliğindedir ve tavsiye niteliği taşımaktadır. BM Himayesinde Bağlayıcı Olmayan Düzenlemeler olarak da Birleşmiş Milletler Uluslararası Terörle Mücadele Stratejisi, EURATOM Himayesinde Bağlayıcı Olmayan Düzenlemeler ve Euratom Anlaşmasının 103. Maddesinin Uygulanmasına İlişkin Komisyon Tavsiyesidir. Aynı şekilde, muhteviyat ekseninde bu düzenlemeler doğrudan bağlayıcı hükümlerden ziyade tavsiye ve görüş niteliğindedir.

Bu kısma kadarki olan uluslararası hukuk düzenlemeleri nükleer santrallerin güvenliğini ‘genel’ olarak ele almaktadır. Nükleer güvenlik genelindeki bu düzenlemeler, nükleer santrallerin fiziki güvenliği ve nükleer terörizm olgusuna değinmektedir. Nükleer santrallerin siber güvenliği özelinde ise karşı tedbirler ve

bu tedbirlerin hukuki esasları bağlamındaki çalışmalar uluslararası hukuki nitelik taşımaktadır. Bu bağlamda, UAEA, NATO, Avrupa Konseyi ve Şangay İşbirliği Örgütü siber saldırıları doğruda düzenleyen uluslararası hukuk rejimleridir. Telekomünikasyon Hukuku, Havacılık Hukuku, Uzay Hukuku ve Deniz Hukuku dolaylı olarak siber saldırıları düzenleyen uluslararası hukuk rejimleridir. UAEA, siber saldırıları nükleer santrallerin fiziki güvenliği genelinde 'bilgisayar güvenliği' başlığı altında ele almıştır. NATO ise Estonya'nın Başkenti Tallinn de bir siber mücadele merkezi kurmuştur ancak gerçekleştirdiği çalışmalar daha çok 'siber savaş' özelinde olmaktadır. Avrupa Konseyi ise Siber Suçlar Sözleşmesi kapsamında bu alanda doğrudan düzenlemeye gitmiştir ve İnternet ve diğer bilgisayar ağlarını kullanarak işlenen suçlarla ilgili ilk uluslararası anlaşma niteliğini taşıyan bu sözleşme, 'siber suç' alanına yoğunlaşmaktadır. Şangay İşbirliği Örgütü, uluslararası bilgi güvenliğinin uluslararası güvenlik sisteminin ortak unsurlarından biri olarak ele alınmasının önemini vurgulamışlardır ve bu kapsamda uzlaşma sağlamışlardır. Siber saldırılar bağlamında dolaylı uluslararası düzenlemeler özelinde ise Telekomünikasyon Hukuku, haberleşme ağı üzerinden gerçekleşebilecek siber suçlara odaklanırken Havacılık Hukuku ise uçakların bilişim sistemlerine ve diğer havacılık sektöründeki ekipmanlara gerçekleşebilecek siber saldırıları dolaylı olarak düzenlemektedir. Oldukça yeni bir disiplin olan uzay hukuku ise uzaydaki uyduların hacklenmesi ve bu aygıtlara yönelik siber saldırıları ele alarak emsal teşkil edebilecek düzenlemeler içermektedir. Deniz Hukuku ise daha önce de vurgulandığı üzere seyrüsefer dâhilinde gerçekleşebilecek siber suçlara dikkat çekmektedir.

Siber suç, siber saldırı ve siber savaş üçgeninde değerlendirilebilecek herhangi bir saldıya karşı *jus ad bellum* ve *jus in bello* ile karşılık verebilmek mümkündür. *Jus ad bellum*, bi saldırıya karşı meşru müdafaanın hukukiliğini ele alırken *jus in bello* ise karşılık verme sürecinde dikkat edilmesi gereken hususları kapsamaktadır. Uluslararası hukuk yönüyle nükleer santrallere gerçekleşecek herhangi bir siber saldırı durumunda ise *jus ad bellum* ile karşılık vermem hukuki olarak mümkün gözükse de saldırının aslında kimin gerçekleştirdiğinin tespitinin zorluğu nedeniyle ihtilaf içermektedir.

Sonuç olarak, nükleer santrallerin kurulumuna başlamadan önce ve kurulduktan sonra bir kurucu işletmenin/devletin riayet etmesi gereken nükleer güvenlik kültürü ve rejimi vardır. Nükleer güvenlik, genel olarak santrallerin fiziki güvenliğini kapsarken siber güvenliği ise bilişim teknolojileri aracılığıyla gerçekleştirilecek saldırılara karşı korunmayı kapsamaktadır. Bu bağlamda siber saldırı senaryoları ve güncel siber saldırıları başlıklarında da zikredildiği üzere, saldırganlar tarafından bu tarz girişimler daha önce olmuştur. Nükleer santrallere karşı gerçekleştirilecek herhangi bir siber saldırıya karşı 'koru(n)ma' ve 'karşılık' ın uluslararası hukuki düzenlemeleri yetersiz düzeydedir. Kazuistik bir Sözleşme gerektiren bu durum, UAEA, BM gibi bazı kurum ve kuruluşların konu ile ilgili bazı özel başlıklar altında gerçekleştirdikleri düzenlemelerden ibarettir.

SONUÇ VE ÖNERİLER

Sonuç olarak, farklı amaçlar dâhilinde ihtiyaç duyduğumuz ‘enerji’ olgusunun keşfedilip kaynaklarının işlenmesi ile birlikte, kullanım sahaları da farklılık göstermiştir. Enerjiye karşı artan ihtiyaç, Sanayi devrimi ile hızlanmış ve enerji olgusu da bu kapsamda daha kritik bir ihtiyaç haline gelmiştir. Yenilenemez enerji kaynakları, enerji tedarik zincirinde üst sıralarda yer alırken enerjiye karşı ihtiyacın teknolojik gelişmeler ve artan nüfusla birlikte daha da artması yenilenemez enerji kaynaklarına yönelimi hızlandırmıştır. Yenilenemez enerji kaynaklarından olan nükleer enerji ise gerek sanayileşme gerekse II. Dünya Savaşı sonrasında hem kuruluşta pahalı ancak işletmede ucuz olması hem de olası bir patlamada yıkıcı etki meydana getirmesi hasebiyle ikiyüzlü bir enerji kaynağı olarak tezahür etmiştir. Özellikle Hiroşima ve Nagazaki’ye atılan atom bombalarından sonra nükleer enerjinin yıkıcı etkisi, uluslararası camiada endişe oluşturmuştur ve bu durum da nükleer enerjinin askeri amaçlı kullanımından ziyade insani amaçlı kullanılması gerekliliğini ortaya çıkartmıştır. Bu durumun en somut örneği BM nezdinde gerçekleşen “Barış için Atom” oturumudur. Bu gelişmeyle birlikte nükleer enerjinin insani amaçla kullanılması yönündeki ilk somut adım da atılmış ve beraberinde UAEA kurulmuştur. Bununla birlikte nükleer santrallerin kırılgan yapıda olması ve olası bir kaza durumunda ortaya çıkabilecek bilançonun tahmin edilemeyecek boyutlara ulaşması, nükleer santralleri kuracak şirketlerin son derece hassas olmasını gerektirmektedir. Bu durum ise UAEA’nın uluslararası hukuki çerçevesini oluşturduğu temel olarak Paris ve Viyana Sözleşmelerinde ele alınmıştır. Kurucu işletmeler ve Sözleşme esasları, kurucu operatörlere katı yükümlülükler getirmektedir ve olası bir durumda nükleer santrallerde meydana gelecek kazalardaki tazminat bedeli ve süreci ise yine uluslararası hukuk boyutuyla çerçevelenmiştir. Nükleer santrallerin

fiziki güvenliği noktasında UAEA ve BM başta olmak üzere diğer kurum ve kuruluşların düzenlemeleri mevcut olmakla birlikte nükleer santrallerin siber güvenliği konusunda ise uluslararası hukuki düzenlemeler oldukça yetersiz düzeydedir. Teknolojik gelişme endeksine paralel olarak nükleer terörizmin vukuu buluşu da değişmektedir. Bilişim sistemlerinin siber saldırı yoluyla hacklenmesi ise nükleer santrallerin herhangi bir siber saldırı yoluyla bir nükleer kazaya sebebiyet vereceği ihtimalini doğurmuştur. Geçmişte bununla alakalı somut örnekler mevcuttur. 2003'te ABD'deki Davis-Besse santraline karşı Slammer Solucan saldırısı, 2007'de Estonya'ya yönelik Stuxnet saldırısı ve Nisan 2016'da Almanya'da Gundremmingen santraline gerçekleştirilen saldırılar bunlardan sadece birkaçıdır.

Uluslararası hukuk ise nükleer santrallerin siber güvenliğine dair doğrudan kazuistik bir tanımlama ve düzenleme içermemektedir. Özellikle üçüncü bölümde bahsi geçen uluslararası düzenlemeler incelendiğinde, bu alanlardaki hukuki boşluğun siber saldırganları daha da teşvik etmesi yüksek muhtemeldir. BM Sözleşmesinin 51. maddesi uyarınca bir devlet herhangi bir devlete savaş ya da işgal etme girişiminde bulunması durumunda meşru müdafaa hakkı doğmaktadır. Santrallere ya da herhangi bir kritik altyapıya düzenlenecek siber saldırının da bu kapsama dâhil edilip edilmeyeceği, *jus ad bellum* ve *jus in bello* ile düzenlenmeye çalışılmıştır. *Jus ad bellum* ile bir devlete herhangi bir saldırı durumunda meşru müdafaa hakkı doğmaktadır ancak durum herhangi bir siber saldırı olduğunda saldırıyı kimin başlattığının tespiti zor olduğu için kesin çözüm getirmemektedir. *Jus in bellum* ise bir devletin kendisine karşı *jus ad bellum* doğması durumunda karşılık verme sürecinde riayet etmesi gereken kuralları kapsamaktadır. Ancak siber saldırıya karşı hangi ölçüde nasıl karşılık verileceği noktasında mutlak bir çözüm sunamamaktadır. Avrupa Konseyi, Siber Suçlar Sözleşmesi kapsamında doğrudan bir hukuki düzenleme içerse de nükleer santrallerin siber güvenliği konusunda kazuistik ve mutlak bir düzenleme içermemektedir.

Genel olarak, nükleer santrallerin siber güvenliği oldukça önemli ve kritik bir konu olmasına rağmen bu tezin ikinci ve üçüncü bölümünde açıklanmaya çalışıldığı üzere bu sorunsalı doğrudan mutlak bir şekilde giderecek uluslararası

düzenlemeler yoktur. Bu uluslararası hukuki boşlukta ise, bir devletin başka bir devlete nükleer silah geliştirme ya da siber tehdit algısıyla saldırısını mümkün kılmaktadır. Aynı şekilde bir teröristin herhangi bir nükleer santrale karşı siber saldırısı durumunda hangi uluslararası ceza ile mahkûm edileceği muğlaktır. Sonuç itibariyle bu hukuki boşluk muhtemel terör eylemlerinin artmasını teşvik etmektedir. Uluslararası kurum ve kuruluşlar bu boşluğu gidermek adına çeşitli çalışmalar yürütmektedir ancak bu gayretler uluslararası bağlayıcı ve tüm devlet ve aktörleri caydırıcı düzeyde değildir. Bu bulanıklık ve sorunsallık ikliminde bazı devlet ve aktörler somut olarak bu karmaşadan yararlanarak hukuki olmayan bir dizi eylem gerçekleştirmiştir. 6 Eylül 2007' de İsrail Orchard Operasyonu ile Suriye'deki bir santrali nükleer silah geliştirme algısıyla F-16' larla vurmuştur. Aynı şekilde 2010' da ABD-İsrail Müşterek operasyonu ile İran'daki Natanz nükleer santraline Stuxnet virüsü ile siber saldırı gerçekleşmiştir. Bu gibi durumlar ise nükleer santrallerin siber güvenliğinin ne denli önemli olduğunu ortaya koymaktadır.

Bu bağlamda, tezden çıkan sonuçları şunlardır:

- Siber suçlarla ilgili kapsamlı bir tanım oluşturulması. Nükleer santrallere karşı gerçekleşebilecek herhangi bir siber suç unsurunun kazuistik tanımlamasının yetersiz olmasından dolayı santrallere karşı siber suç işleyecek kişi ya da devletler için hangi durumla ne ile cezalandırılacaklarına yönelik bir yaptırım rejimi yoktur. Bu durum ise nükleer terörizm ve saldırganları teşvik edici düzeydedir. BM, UAEA ve özellikle UAD nezdinde siber saldırılara dair kapsamlı uluslararası hukuki tanım oluşturulmalıdır. Böylelikle taraf devletlerce esas alınıp uygulanacak bu tanım, taraf olmayan diğer devlet ya da devlet dışı aktörler tarafından emsal teşkil edecektir.

- Nükleer Santrallerin Siber Güvenliği Sözleşmesi Oluşturulması. BM nezdinde bu sözleşmenin ivedilikle oluşturulması gerekmektedir. 'Siber suç', 'siber savaş' ve 'siber saldırı' üçgeninde genel olarak 'siber uzay'a yönelik

uluslararası hukuki düzenlemelerin oluşturulması şarttır. Doğrudan bağlayıcı hükümler içermesi gereken bu sözleşme herhangi bir nükleer santrallere siber saldırı durumunda bu sözleşme dâhilinde BM tarafından yetkilendirilmiş bağımsız kuruluşlarca siber saldırı tespit raporları hazırlanmalıdır. Böylelikle *jus ad bellum* ve *jus in bello* daki saldırının nereden ve kimden geldiği sorunsalı da bağımsız kuruluşlarca tespit edilecektir. Amaç, ilke ve yöntemlerin BM üye ülkeleriyle oluşturulacağı bu kazuistik Sözleşme, böylelikle bu alandaki uluslararası hukuki boşluğu gidermiş olacak ve periyodik gelişim ve güncellemelerle daha bağlayıcı ve caydırıcı bir unsur haline gelecektir.

- Siber Karargâhların Oluşturulması. Yine BM bünyesinde yetkilendirilmiş bağımsız siber karargâhların oluşturulması şarttır. Bu bağımsız karargâhlar, kurulacak tüm nükleer santraller için himayelerinde bulundurması ön koşul olacak bir şartname haline gelmesi gerekmektedir. Böylelikle nükleer santraller bir yandan elektrik enerjisi üretirken diğer yandan bu karargâhlar, 7/24 doğrudan siber tehditler üzerine odaklanarak gerekli bilgilendirme ve uygulamaları yürütmekle mükellef olacaklardır.

- İstihbarat Sarmalının Oluşturulması. BM nezdinde yetkilendirilecek siber karargâhlar, Interpol ve diğer uluslararası istihbarat ağları ile sürekli koordinasyon halinde olarak muhtemel siber saldırıları önlemeye yönelik çalışmalar yürütmelidir. Bu sarmal, siber uzayda meydana gelen gelişmeleri sürekli takip ederek istihbarat akışını sağlamalıdır. Böylelikle devletler ve teröristler gibi devlet dışı aktörler için caydırıcı bir unsur oluşturmalıdır.

KAYNAKÇA

Kitap ve Makaleler

Ahn, Woogeun et al, Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs, International Journal of Distributed Sensor Networks, Vol. 2015, Article ID 836258, 2015, p.5.

Ali, A. M. , Legal Elements For Nuclear Security: Egyptian Nuclear Law As A Case Study, XI Radiation Physics & Protection Conference, 25-28 November 2012, Nasr City - Cairo, Egypt, p.323.

Alpna et al., Cyber Crime-Its Types, Analysis and Prevention Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 6, No. 5, May 2016, pp. 145-146.

Andress, Jason/Steve Winterfield, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Elsevier-Syngress, Waltham, MA, 2011, p.3.

Andrews, J. A, The Modern Law Review, The Modern Law Review, Vol. 30, No. 1, 1967, p. 111.

Anisimov, Aleksey Pavlovich / Anatoliy Jakovlevich Ryzhenkov, Thirty years after the accident at the Chernobyl nuclear power plant: historical causes, lessons and legal effects, Journal of Energy & Natural Resources Law, Vol. 34, No. 3, 2016, p. 265.

Arend, Anthony Clark, International Law and the Preemptive Use of Military Force, The Washington Quarterly Vol. 26, No. 2, p. 92.

Arora, Bhavna, Exploring and Analyzing Internet Crimes and their Behaviours, Perspectives in Science, Vol. 8, September 2016, p. 541.

Aslan, Yasin, Global Nature of Computer Crimes and the Convention on Cybercrime, Ankara Law Review, Vol.3 No.2, Winter 2006, p.139.

Avcı, Maya Ezgi, A Lawful Response to Cyber Attacks, Law & Justice Review, Year.7, Issue.12, June 2016, pp. 409-411.

Badea, Constantina et al., In The Aftermath Of Terrorism: Effects of Self Versus Group Affirmation on Support for Discriminatory Policies, Journal of Experimental Social Psychology, 2017, p.1.

Baron, Ryan M.F., A Critique of the International Cybercrime Treaty, Commlaw Conspectus, Vol. 10, 2002, p.273.

Baverstock, Keith, Chernobyl 25 Years on: Lessons Have Not Been Learnt and the Full Public Health Implications Are Unknown, BMJ: British Medical Journal, Vol. 342, No. 7804, 2011, p.936.

Beck, Louise Doswald, Some Thoughts on Computer Network Attack and the International Law of Armed Conflict, International Law Studies, Vol. 76, Computer Network Attack and International Law, Michael N. Schmitt & Brian T.. O'Donnell (Editors), 2002, p.65.

Beckrich, Amanda, The Green Room: The Pros and Cons of Nuclear Energy, The Science Teacher, Vol. 80, No. 3, 2013, p.10.

Berman, Franklin, The UN Charter and the Use of Force, Singapore Year Book of International Law and Contributors, 10 SYBIL, 2006, p. 12.

Bıçakcı, Salih, /F.Doruk Ergün/Mitat Çelikpala, Türkiyede Siber Güvenlik, EDAM, 1. Baskı, İstanbul, Mart 2016, s.30.

Bothe, Michael, The Peaceful Use of Nuclear Energy and the Protection of the Environment, Jonathan L. Black/Branch Dieter Fleck (eds), Nuclear Non-Proliferation in International Law: Volume III Legal Aspects of the Use of

Nuclear Energy for Peaceful Purposes, Canada, Asser Press- Springer,2016, p. 295.

Bowen, WYN Q., et al., Multilateral Cooperation and the Prevention of Nuclear Terrorism: Pragmatism over Idealism, International Affairs (Royal Institute of International Affairs 1944-), Vol. 88, No. 2, 2012, p.349.

Boyla, Mazhar/ Yılmaz Canküyer, Nükleer Enerji terimleri Sözlüğü, Ankara: Türk Dil Kurumu Yay., 1995, s. 118.

Brenner, S. / Bert-Jaap Koops, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, p.7.

Brenner, S., Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law, Murdoch University Electronic Journal of Law, Vol.8, No. 2, June 2001, p. 2.

Brenner, S./ LL Clarke, Distributing Security: Preventing Cyber Crime, John Marshall Journal of Computer and Information Law, Vol.23, No.4, Summer 2005, p. 6.

Brill, Kenneth C. / John H. Bernhard, A Convention on Nuclear Security: A Needed Step Against Nuclear Terrorism, Arms Control Today, Vol. 45, No. 5, 2015, p. 16.

Brill, Kenneth C. / John H. Bernhard, A Convention on Nuclear Security: A Needed Step Against Nuclear Terrorism, Arms Control Today, June 2015: https://www.armscontrol.org/print/6990 (E.T: 26.03.18).

Brown, Gary, and Keira Poellet, The Customary International Law of Cyberspace, Strategic Studies Quarterly, Vol. 6, No. 3, 2012, p. 129.

Bunn, Matthew /Martin B. Malin /Nickolas Roth William H. Tobey, Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?, Belfer Center for Science and International Affairs Harvard Kennedy School, Cambridge, MA, March 2016, p.4.

Burroughs, John, Looking Back: The 1996 Advisory Opinion of the International Court of Justice, Arms Control Association, 2016: https://www.armscontrol.org/ACT/2016_07/Features/Looking-Back-The-1996-Advisory-Opinion-of-the-International-Court-of-Justice (25.03.18).

Cadenas, Juan José Gomez, The Nuclear Environmentalist: Is There a Green Road to Nuclear Energy?, Springer-Verlag Mailand, New York, 2012, p.106.

Carl von Clausewitz, On War, Edited and Translated by Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976); Thomas Rid, Cyberwar and Peace: Hacking Can Reduce Real-World Violence, Foreign Affairs, Nov./Dec. 2013, pp. 77-87.

Carlton Stoiber/ Alec Baer/ Norbert Pelzer/ Wolfram Tonhauser., Hand Book on Nuclear Law, Austria IAEA Press, 2003, p. 4.

Cassim, Fawzia, Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players, The Comparative and International Law Journal of Southern Africa, Vol. 44, No. 1, 2011, p. 124.

Caşın, Mesut Hakkı, Modern Uluslararası Hukukun Temel Esasları, Legal Yayıncılık, Cilt I, İstanbul, 2013, s. 603 – 605.

Cheng, Bin, A New Era in the Law of International Carriage by Air: From Warsaw (1929) to Montreal (1999), The International and Comparative Law Quarterly, Vol. 53, No. 4, 2004, p. 855.

Cheng, Bin, The International and Comparative Law Quarterly, The International and Comparative Law Quarterly, Vol. 56, No. 2, 2007, p. 465.

Cho, Hyo Sung/Tae Ho Woo, Cyber security in nuclear industry – Analytic study from the terror incident in nuclear power plants (NPPs), Annals of Nuclear Energy, Volume 99, January 2017, p.47.

Cigoj, Stojan, International Regulation of Civil Liability for Nuclear Risk, The International and Comparative Law Quarterly, Vol. 14, No. 3, 1965, p. 809.

Cigoj, Stojan, International Regulation of Civil Liability for Nuclear Risk, The International and Comparative Law Quarterly, Vol. 14, No. 3, 1965, p.810.

Cimbala, Stephen J., Nuclear Deterrence And Cyber Warfare: Coexistence Or Competition?, Defense & Security Analysis, Vol. 33, No.3, 2017, p.193.

Couriel, Deborah Housen, Cybersecurity and Outer Space: Connected Challenges, Israel Defense, February 2, 2017 : http://www.israeldefense.co.il/en/node/28413 (E.T: 14.03.18).

Çakır, Hüseyin, Güncel tehdit: Siber Suçlar, Seçkin Yay., Ankara, 2014, s. 21.

Çelikpala, Mitat, Cyber Security and Nuclear Power Plants: International Frameworks, EDAM, 05.04.2016: http://edam.org.tr/en/cyber-security-and-nuclear-power-plantsinternational-frameworks/#_ftn4 (08.04.18).

Çetiner, Atıf/ Selim Sunal, Dünyada Nükleer Enerji Kullanımı ve Yeni Yaklaşımlar, 21yy Dergisi, 2008, s. 193.

Damrosch, Lori Fisler/ Bernard H. Oxman, Editors' Introduction, The American Journal of International Law, Vol. 97, No. 3, 2003, p. 555.

David Fischer, History of The International Atomic Energy Agency, Vienna, A Fortieth Anniversary Publication, September1997, p.9.

Demir, Ömer/ Mehmet Arıç/Halil Polat, Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar: Soruşturma ve Kovuşturma Yöntemleri, Adalet Yay. İstanbul, 2015, s. 195.

Denk, Erdem, "Bir Kitle İmha Silâhı Olarak Nükleer Silâhların Yasaklanmasına Yönelik Çabalar", Ankara Üniversitesi, SBF Dergisi, C. 66, S. 3, 2011. s. 115.

Dennis, Michael Aaron, Cybercrime, 3-9-2018: Encyclopedia Britannica: https://www.britannica.com/topic/cybercrime (E.T: 09.04.18).

Dhanapala, Jayantha, The United Nations' Response to 9/11, Terrorism and Political Violence, Vol. 17, No. 1-2, 2005, pp.17-18.

Dickstein, Phineas/ Sarah Vanunu, Nuclear Terror: The Essentials, Threats, Effects and Resilience, International Institute for Counter- Terrorism, 2016, p.4.

Dine, Alexandra Van/ Michael Assante / Page Stoutland, Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities, Nuclear Threat Initiative, 2016, p.1.

Dion-Schwarz, Cynthia, et al., Earlier Lessons from the Chernobyl Experience, Technological Lessons from the Fukushima Dai-Ichi Accident, RAND Corporation, Santa Monica, Calif., 2016, p. 45.

Döge, Jenny, Cyber Warfare: Challenges for the Applicability of the Traditional Laws of War Regime, Archiv Des Völkerrechts, Vol. 48, No. 4, 2010, p.488.

Driscoll Aimee O', 100+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2018 EDITION], February 15, 2018: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/ (E.T: 09.04.18).

Drumbl, Mark, et al., Self-Defense in an Age of Terrorism, Proceedings of the Annual Meeting American Society of International Law, Vol. 97, 2003, p. 141.

Duckwitz, C.A./ Taegder, K. Is The Euratom-US Cooperation Agreement Jeopardized?. Atw Atomwirtschaft, Atomtechnik, Vol.40, No.3., 1995, pp.159-163.

Duggal, Pavan, Cyber Security Law, its Regulation and Relevance for Outer Space, UNOOSA : http://www.unoosa.org/documents/pdf/hlf/HLF2017/presentations/Day2/Session_7b/Presentation5.pdf (14.04.18).

Dunlap, Charles J., Perspectives for Cyber Strategists on Law for Cyberwar, Strategic Studies Quarterly, vol. 5, no. 1, 2011, p. 93.

Dülger, Volkan, Bilişim Suçları ve İnternet İletişim Hukuku: 6518, 6526, 6527 ve 6552 Sayılı Yasa Değişiklikleri İle, Seçkin Yay., Ankara, 2014, s. 185.

Eaves, Elisabeth, What Does "Nuclear Terrorism" Really Mean?, 7 April 2016, Bulletin of the Atomic Scientists: https://thebulletin.org/what-does-nuclear-terrorism-really-mean9309 (E.T: 25.03.18).

El Baradei, Mohamed / Edwin Nwogugu / John Rames, International Law And Nuclear Energy: Overview of The Legal Framework, IAEA Bulletin, Vol.3, 1995, p.16.

Eliasson, Jan, Cyber Crimes, UNIS: http://www.unis.unvienna.org/unis/en/events/2015/crime_congress_cybercrime.html (09.04.18).

Ellingsen, Simen A., Safeguards Against Nuclear Terrorism: HEU vs Plutonium, Defence & Security Analysis, Vol.24, No.2, 2008, p.129.

Ellis, LTC Bryan W., The International Legal Implications and Limitations of Information Warfare: What Are Our Options?, U.S. Army War College, 10 April 2001, pp. 4-6.

Erdoğan, Yavuz, Türk Ceza Kanununda Bilişim Suçları: Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle, Legal Yay. , İstanbul, 2013, s. 47.

Farrell, Theo, / Hélène Lambert, Courting Controversy: International Law, National Norms and American Nuclear Use, Review of International Studies, Vol. 27, No. 3, 2001, p. 309.

Ferguson, Charles D., Nükleer Enerji: Herkesin Bilmesi Gerekenler, Ankara, Buzdağı Yayınevi, Birinci Baskı 2015, s.43.

Fidler, David P., Cybersecurity and the New Era of Space Activities, CFR, April 03, 2018 : https://www.cfr.org/report/cybersecurity-and-new-era-space-activities (E.T: 14.03.18).

Fidler, David P., American Society of Internatonal Law, International Convention for the Suppression of Acts of Nuclear Terrorism Enters into Force, Vol. 11, No. 18, July 05, 2007: https://www.asil.org/insights/volume/11/issue/18/international-convention-suppression-acts-nuclear-terrorism-enters-force (E.T: 03.04.18).

Fleming, T. Casey, et al., The Secret War Against the United States: The Top Threat to National Security and the American Dream Cyber and Asymmetrical Hybrid Warfare An Urgent Call to Action, The Cyber Defense Review, Vol. 2, No. 3, 2017, p.29.

Fovino IN, Guidi L, Masera M, Stefanini A. Cyber Security Assessment of A Power Plant, Electr Power Syst Res, Vol.81, 2011, p.26.

Furnell, Steven/ David Emm/ Maria Papadaki, The Challenge of Measuring Cyber-Dependent Crimes, Computer Fraud & Security, Vol. 2015, No. 10, October 2015, pp.6-7.

Gardam, Judith, The Place of Necessity and Proportionality in Restraints on the Forceful Actions of States, Cambridge University Press, 0521837529, December 2004, pp.1-4.

Geist, Edward, Deterrence Stability in the Cyber Age, Strategic Studies Quarterly, Vol. 9, No. 4, 2015, p. 49.

George Leloudas, The Cambridge Law Journal, The Cambridge Law Journal, Vol. 65, No. 2, 2006, p. 466.

Giaurov, Vesselin, The Cyber-Nuclear Security Threat:Managing the Risks, VCDNP, 2017, p.3.

Giladi, Rotem, The Jus Ad Bellum/Jus in Bello Distinction and the Law of Occupation, Israel Law Review, Hebrew University International Law Research Paper No. 18-08, Vol. 41, November 1, 2008, pp. 247-249.

Gjelten, Tom, Shadow Wars: Debating Cyber 'Disarmament', World Affairs, Vol. 173, No. 4, 2010, p. 33.

Gluschke, Guido, Cyber Security at Nuclear Facilities: National Approaches, The Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences, First ed., June 2015, p.18.

Goedde, Patricia, In Search Of A Civil Nuclear Liability Regime For North Korea, Asian Perspective, Vol. 27, No. 1, 2003, p.227.

Goldschmidt, Bertrand, The Atomic Complex, American Nuclear Society, 1982, pp. 257-62.

Gorove, Stephen, International Conventions on Civil Liability for Nuclear Damage, The American Journal of International Law, Vol. 62, No. 2, 1968, p.543.

Göçoğlu, Volkan, Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi, Hacettepe Üniversitesi, Yayınlanmamış Doktora Tezi, 2018, s.153.

Grandin, Karl, et al., Nuclear Energy, Ambio, Vol. 39, Sup.1, 2010, p.26.

Granville, Johanna, The British Journal of Criminology, The British Journal of Criminology, Vol. 43, No. 2, 2003, p. 452.

Green, Michael Hamel, The implications of the 2017 UN Nuclear Prohibition Treaty For Existing And Proposed Nuclear-Weapon-Free Zones, Global Change, Peace & Security, 2018, p.3.

Greenberg, Lawrence T. / Seymour E. Goodman / Kevin J. Soo Hoo, Information Warfare and International Law, National Defense University Press, 1998, p.8.

Grimmitt, Melanie, The Mena Nuclear Renaissance, Energy & Environment, Vol. 22, No. 1/2, 2011, p.42.

Grove, G./ S. Goodman / S. Lukasik, Cyber-Attacks and International Law, Survival, Vol. 42, No. 3, 2000, p.91.

Haataja, Samuli, The 2007 Cyber Attacks Against Estonia and International Law on the Use Of Force: an Informational Approach, Law, Innovation And Technology, Vol. 9, No. 2, 2017, p. 163.

Hafstad L.,Nuclear Reactor Developments, Stason E Lectures on Atomic Energy: Industrial and Legal Problems, 1952, pp. 3-16.

Hallwood, Paul / Thomas J. Miceli, The Economics of International Cooperation in the Apprehension and Prosecution of Maritime Pirates, Ocean Development & International Law, Vol. 43, No. 2, 2012, pp. 188-189.

Handrlica Jakub, [Я., ХЭНДРЛИКА], Ядерные Технологии И Международная Ответственность В Рамках Венской Конвенции О Гражданской Ответственности За Ядерный Ущерб: Правовые Проблемы [Nuclear Technologies and the İnternational Liability Framework of the Vienna Convention On Civil Liability For Nuclear Damage: Legal Problems Revisited], Вестник Омского университета. Серия «Право», No. 1 (46), 2016, p.113.

Haque, Adil Ahmad, A Theory of Jus in Bello Proportionality (May 4, 2015). Forthcoming in Weighing Lives: Combatants & Civilians in War (Jens David Ohlin, Larry May, Claire Finkelstein eds., 2015), pp.1-3.

Haque, Adil Ahmad, Necessity and Proportionality in the Law of War (August 22, 2016). Cambridge Handbook on Just War (Larry May ed, CUP 2016). August 22, 2016, p.18.

Hartley, Trevor C., Federalism, Courts and Legal Systems: The Emerging Constitution of the European Community., The American Journal of Comparative Law, Vol. 34, No. 2, 1986, p. 232.

Hashmi, Muhammad Jawad, Scenarios Of Nuclear Terrorism: An Analysis, Eurosia Review, 2012: https://www.eurasiareview.com/27012012-scenarios-of-nuclear-terrorism-an-analysis/ (E.T: 18.03.18).

Hassan, Daud/ Sayed M. Hasan, Origion, Development and Evolution of Maritime Piracy: A historical Analysis, International Journal of Law, Crime and Justice, Vol. 49, 2017, pp. 1-2.

Hathaway, Oona A. / Rebecca Crootof, The Law of Cyber-Attack, Faculty Scholarship Series, Paper 3852, Vol. 100, No. 817, 2012, p.833.

Heinegg, Wolff Heintschel von, Neutrality in Cyberspace, 2012 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012, NATO CCD COE Publications, Tallinn, pp. 35-37.

Heinonen, Olli, Nuclear Terrorism: Renewed Thinking for a Changing Landscape, Briefing at the Open Debate of the United Nations Security Council, Foundation for Defense Democracies, New York, 2017, pp.1-2.

Henderson, Christian, The United Nations and the Regulation Of Cyber-Security, Chapters, in: Research Handbook on International Law and Cyberspace, Chapter 22, Edward Elgar Publishing, 2015, p. 480.

Hmoud, Mahmoud, Are New Principles Really Needed? The Potential of the Established Distinction Between Responsibility for Attacks by Nonstate Actors and the Law of Self-Defense, The American Journal of International Law, Vol. 107, No. 3, 2013, pp. 57–578.

Hodge,Nathan, General: We Just Might Nuke Those Cyber-Attackers, WIRED, 13 May 2009, https://www.wired.com/2009/05/general-we-just-might-nuke-those-cyber-attackers/ (E.T: 11.04.18).

Hofmeister, Hannes, Watch What You Are Saying: The UN Charter's Prohibition on Threats to Use Force, Georgetown Journal of International Affairs, Vol. 11, No. 1, 2010, p. 107.

Högberg, Lars., Root Causes and Impacts of Severe Accidents at Large Nuclear Power Plants, Ambio, Springer On Behalf Of Royal Swedish Academy of Sciences, Vol. 42, No. 3, 2013, p. 269.

Hua, Jian / Sanjay Bapna,How Can We Deter Cyber Terrorism?, Information Security Journal: A Global Perspective, Vol. 21, No. 2, 2012, p.110.

Hubbert, M. King, Nuclear Energy and Fossil Fuels, Shell Development Company Exploration and Production Research Division, Houston, Texas, No. 95, June 1956, p.23.

Hughes, Rex, A Treaty for Cyberspace, International Affairs (Royal Institute of International Affairs 1944-), Vol. 86, No. 2, 2010, pp. 524.

Ingber, Rebecca, Untangling Belligerency from Neutrality in the Conflict with Al-Qaeda, Texas International Law Journal, Vol. 47, No. 1, pp. 80-89.

Janardhanan, Nandakumar, Transition to Energy Secure Future: Policies Enabling Energy Transition in India, Report, Institute for Global Environmental Strategies, 2012, p.4.

Jastram, Kate/ Anne Quintin, The Internet in Bello: Cyber War Law, Ethics & Policy, Seminar held 18 November 2011, Berkeley Law, pp. 20-26.

Jensen, Eric Talbot, Cyber Deterrence, 26 Emory International Law Review, Vol. 773, No. 773, 2012, p. 795.

Jha, Anupam, Dynamics of Legal Regime on Safety of Nuclear Power Plants In India After Fukushima Disaster, Journal of Risk Research, Vol. 17, No. 1, 2014, p. 147.

Johnson, Clifton M., Introductory Note To The International Convention For The Suppression Of The Financıng Of Terrorism, International Legal Materials, Vol. 39, No. 2, 2000, p. 268.

Johnson, Larry D., International Atomic Energy Agency: Diplomatic Conference To Adopt A Protocol To Amend The Vienna Convention on Civil Liability For Nuclear Damage And To Adopt A Convention on Supplementary Funding, International Legal Materials, Vol. 36, No. 6, 1997, pp. 1454–1455.

Kamminga, Menno T. , The IAEA Convention on Nuclear Safety, The International and Comparative Law Quarterly, Vol. 44, No. 4, 1995, pp. 872–882.

Karagülmez, Ali, Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri, Seçkin Yay. Ankara, 2014, s. 54.

Karauz, Ağâh Kürşat, Nükleer Santral İşletenin Hukukî Sorumluluğu, Nevşehir Barosu Dergisi, Yıl 1, Sayı 1, Mart 2014, s. 6.

Keeney, Spurgeon M. Jr. Chmn., Nuclear Power Issues and Choices, the USA, Nuclear Energy Policy Research Group, Sponsored by the Ford Foundation and Administered by the MITRE Corporation, 1977, p.44.

Kemp, Richard., Israel as a Strategic Asset of the West, Jewish Political Studies Review, Vol. 28, No. 1/2, 2017, p.23.

Kenneth V. Peifer, B.S, An Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy, December 1997 : http://iwar.org.uk/iwar/resources/usaf/maxwell/students/1997/peifer_kv.pdf (E.T: 11.04.18).

Kenney, Michael, Cyber-Terrorism in a Post-Stuxnet World, Orbis, Vol. 59, No. 1, 2015, p. 114.

Kettemann, Matthias C., Ensuring Cybersecurity Through International Law, Revista Española De Derecho Internacional, Vol. 69, No. 2, 2017, p. 289.

Kibaroglu, Mustafa, The Threat of Nuclear Terrorism Requires Concerted Action, Strategic Analysis, Vol. 38, No. 2, 2014, p.211.

Kim Heeeun et al., Identification of The Risk Induced By Malicious Attack On The NPP HMI System, Nuclear Safety and Simulation, Vol. 7, No. 2, December 2016, pp.153-154.

Kim, Do-Yeon, Cyber Security Issues Imposed on Nuclear Power Plants, Annals of Nuclear Energy, Vol. 65, March 2014, p.142.

Kim, Duyeon / Jungmin Kang, Where Nuclear Safety And Security Meet, Bulletin of the Atomic Scientists, Vol. 68, No.1, 2012, pp.86-87.

Kim, Hee Eun et al, Systematic Development of Scenarios Caused By Cyber-Attack-Induced Human Errors in Nuclear Power Plants, Reliability Engineering and System Safety, Vol. 167, 2017, p. 290.

Kimball, Daryl G., FOCUS: Eliminate NATO's Nuclear Relics, Arms Control Today, Vol. 40, No. 2, 2010, p.4.

Kizekova, Alica, The Shanghai Cooperation Organisation: Challenges in Cyberspace, The S. Rajaratnam School of International Studies, 22 February 2012 : https://www.rsis.edu.sg/rsis-publication/cms/1695-the-shanghai-cooperation-organ/#.WvNGVIiFNPZ (E.T: 13.04.18).

Kodar, Erki, Applying the Law of Armed Conflict to Cyber Attacks, ENDC Proceedings, Volume 15, 2012, pp. 108–109.

Kretzmer, David, The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum, The European Journal of International Law, Oxford University Press, Vol. 24, No. 1, 2013, p.239.

Kulesza, Joanna, International Internet Law, Global Change, Peace & Security, Vol. 24, No. 3, 2012, p.360.

Kushner, David, The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware That Stymied Iran's Nuclear-Fuel Enrichment Program, IEEE, 26 Feb 2013 : https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (E.T: 07.04.18).

Landau, Emily B./ Shimon Stein, On the Brink of Nuclear Terror? A Threat and Response Balance Sheet, the Institute for National Security Studies, INSS Insight No. 814, April 13, 2016: http://www.inss.org.il/publication/on-the-brink-of-nuclear-terror-a-threat-and-response-balance-sheet/ (26.03.18).

Larsen, Paul B, Recent Changes in Space Law's Concept of Sovereignty, Proceedings of the Annual Meeting (American Society of International Law), vol. 88, 1994, p. 266.

Larssen, Rolf Mowatt, Nightmares of Nuclear Terrorism, Bulletin of the Atomic Scientists, Vol.66, No.2, 2010, p.43.

Larssen, Rolf Mowatt, The Growing Threat of Nuclear Terrorism, IAEA Conference, 2009, p.5.

Leonard S. Spector., Nuclear Material and Commodity Trafficking as International Crimes: Current Status, Gaps in Coverage, and Potential Steps Forward, Proceedings of the Annual Meeting (American Society of International Law), Vol. 105, 2011, p.133.

Lilienthal, Gary/ Nehaluddin Ahmad, Cyber-Attack as Inevitable Kinetic War, Computer Law & Security Review, Volume 31, Issue 3, June 2015, pp. 391-392.

Limnéll, Jarno, The Command Imperative: Crafting Protocols for Cyber Conflict, Georgetown Journal of International Affairs, 2014, p.526.

Littlejohn, Allison, et al, Comparing Safety Culture and Learning Culture, Risk Management, Vol. 16, No. 4, 2014, p.273.

Lotrionte, Catherine, A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence, Georgetown Journal of International Affairs, 2013, p. 84.

Lucas, George R. Jr. Ethics and Cyber Conflict: A Response to JME 12:1 (2013), Journal of Military Ethics, Vol. 13, No. 1, 2014, p.21.

Mackby, Jenifer, Nonproliferation Verification and the Nuclear Test Ban Treaty, Fordham International Law Journal, Vol.34, No.4, 2011, pp.699-700.

Makowski, Andrzej, More on War, Israel Journal of Foreign Affairs, Vol. 11, No. 2, 2017, p. 308.

Malin, Martin B., and Nickolas Roth., A New Era for Nuclear Security, Arms Control Today, Vol. 46, No. 5, 2016, p. 8.

Mallard, Grégoire, Crafting the Nuclear Regime Complex (1950–1975): Dynamics of Harmonization of Opaque Treaty Rules, The European Journal of International Law, Oxford University Press, Vol. 25 No. 2, 2014, p.446.

Markoff, John, Step Taken to End Impasse Over Cybersecurity Talks, New York Times, July 2010 : https://www.nytimes.com/2010/07/17/world/17cyber.html (E.T: 13.04.18).

Martin, Brian, Opposing Nuclear Power: Past and Present, Social Alternatives, Vol. 26, No. 2, Second Quarter 2007, pp. 43-47.

Martinez, Jenny/Antoine Bouvier, Assessing the Relationship Between Jus in Bello and Jus Ad Bellum: An 'Orthodox' View, Proceedings of the Annual Meeting (American Society of International Law), Vol. 100, 2006, pp. 111-112.

Masters, Joshua, Nuclear Proliferation, Nonproliferation Review, Vol. 16, No. 3, 2009, p. 348.

Mattox, John Mark, Nuclear Terrorism: The 'Other' Extreme of Irregular Warfare, Journal of Military Ethics, Vol.9, No.2, 2010, p.160.

Maurer, Tim, Cyber Norm Emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-Security, Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project, Harvard Kennedy School Belfer Center for Science andd International Affairs, September 2011, pp. 10-11.

McBrayer, Sharon, Chernobyl's Legal Fallout, GA. Journal of International Law & Comparative Law, Vol. 17, No. 303, pp.304-305.

McDonald, Alan, Nuclear Power Global Status: A Look at Nuclear Power Generation Around The World and its Future Prospects, IAEA Bulletin Vol.49, Iss.2, March 2008, p.46.

McLaughlin, Kevin L.,Cyber Attack! Is a Counter Attack Warranted?, Information Security Journal: A Global Perspective, Vol.20, No. 1, 2011, p.61.

McMahon, Jeff, Morality, Law, and the Relation Between Jus ad Bellum and Jus in Bello, ASIL Proceedings, 2006, pp. 46-48.

Mégret, Frédéric, Jus in Bello and Jus Ad Bellum, Proceedings of the Annual Meeting (American Society of International Law), Vol. 100, 2006, pp. 121–123.

Melzer, Nils, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, ICRC, May 2009, pp. 43-45

Mertus, Julie, Assessing the NATO Intervention Under the UN Charter, Proceedings of the Annual Meeting, American Society of International Law, vol. 94, 2000, pp. 310–311.

Mertus, Julie, The Danger of Conflating Jus Ad Bellum and Jus in Bello, Proceedings of the Annual Meeting (American Society of International Law), Vol. 100, 2006, pp. 116–117.

Meulenbelt, Stephanie, The 'Worm' as a Weapon of Mass Destruction, The RUSI Journal, Vol. 157, No. 2, 2012, p. 64.

Meyer, Paul, Saving The Npt, Non-Proliferation Review, Vol.16, No.3, 2009, p.463.

Miriam F. Miquelon-Weismann, The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?, 23 The John Marshall Journal of Information Technology & Privacy Law, Vol. 23, No. 2, 2005, p. 337.

Miwao Matsumoto., 'Structural Disaster' Long Before Fukushima: A Hidden Accident, Development and Society, Vol. 42, No. 2, 2013, p.166.

Moore, George M., Out of Control: Why Mandatory International Reporting is Needed For Radioactive Sources and Materials, Bulletin of the Atomic Scientists, Vol. 70, No. 6, 2014, p.63.

Morris, Andrew, "Energy." Why Icebergs Float: Exploring Science in Everyday Life, 1st ed., London, UCL Press, 2016, p. 139.

Moslemzadeh, Pardis Tehrani/ Nazura Abdul Manap/ Hossein Taji, Cyber Terrorism Challenges: The Need for A Global Response to A Multi-Jurisdictional Crime, Computer Law & Security Review, Vol. 29, No. 3, June 2013, p. 208.

Moussa, Jasmine, Can Jus Ad Bellum Override Jus In Bello? Reaffirming the Separation of The Two Bodies of Law, International Review of the Red Cross, Vol. 90, No. 872, December 2008, pp. 965 – 966.

Moxley, Charles J. Jr./ John Burroughs / Jonathan Granoff, Nuclear Weapons and Compliance with International Humanitarian Law and the Nuclear Non-Proliferation Treaty, Fordham International Law Journal, Vol. 34, No. 4, 2011, pp. 612-614.

Nanda, Ved P. /Jon M. Van Dyke, International Nuclear Law: An Introduction, Nuclearintro_Macro, Vol. 35, No. 1, 2008, pp. 4-6.

Nguyen, Reese, Navigating Jus Ad Bellum in the Age of Cyber Warfare, California Law Review, Vol. 101, No. 4, 8-1-2013, p. 1112.

Nicholas Rostow, The World Health Organization, the International Court of Justice, and Nuclear Weapons, Yale Yale Journal of International Law, Vol. 20, No.1, 1995, p.154-155.

Nordyke, Mllo D., The Soviet Program For Peaceful Uses Of Nuclear Explosions, Science & Global Security, Vol.7, No.1, 2007, p.4.

Nunn, Sam., The Race between Cooperation and Catastrophe: Reducing the Global Nuclear Threat, The Annals of the American Academy of Political and Social Science, Vol. 607, 2006, pp.44-48.

Nye, Joseph S. Jr, From Bombs To Bytes: Can Our Nuclear History Inform Our Cyber Future?, Bulletin of the Atomic Scientists, Vol.69, No. 5, pp.8-9.

O'Connell, Mary Ellen/ Louise Arimatsu, Cyber Security and International Law Meeting Summary, Chatnam House, London, the UK, 29 May 2012, p. 10.

O'Connell, Mary Ellen, The Limited Necessity of Resort to Force, Imagining Law: Essays in Conversation with Judith Gardam, edited by Dale Stephens and Paul Babie, University of Adelaide Press, South Australia, 2016, pp. 48-49.

Obokata, Tom, Maritime Piracy as a Violation of Human Rights: A Way Forward for its Effective Prevention and Suppression?, The International Journal of Human Rights, Vol. 17, No. 1, 2013, p.21.

O'Neill, Kevin, The Nuclear Terrorist Threat, Institute for Science and International Security, August 1997, p.1.

Ozturk, Ilhan, Energy Dependency and Security: The Role of Efficiency and Renewable Energy Sources, IGC, April 2014, p.2.

Özdemir, Eyüp, Nükleer Güç Santrallarının Kurulmasına İlişkin Hukuki Esaslar, On İki Levha Yayıncılık, İstanbul, 2012, s.78.

Palliser, Janna, Nuclear Energy, Science Scope, Vol. 35, No. 5, 2012, p. 15.

Parlar, Ali, Türk Ceza Hukukunda Bilişim Suçları, Bilge Yay. Ankara, 2011, s.24.

Paust, Jordan J., Self-Defense Targetings of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan, Journal of Transnational Law & Policy, Vol. 19, No. 2, Spring 2010, p. 241.

Paust, Jordan J., Self-Defense, Laws of War, and Human Rights, Die Friedens-Warte, Vol. 81, No. 2, 2006, pp. 81-82.

Pavlischek, Keith, Proportionality in Warfare, The New Atlantis- Journal of Technology & Society : https://www.thenewatlantis.com/publications/proportionality-in-warfare (E.T: 15.04.18).

Peterson, Per F., et al., Nuclear Freeze: Why Nuclear Power Stalled—and How to Restart It, Foreign Affairs, Vol. 93, No. 3, 2014, p.28.

Petkis, Stephen, Rethinking Proportionality in the Cyber Context, Georgetown Law, pp. 1446-1447. : https://www.law.georgetown.edu/academics/law-journals/gjil/recent/upload/Petkis.PDF (E.T: 15.04.18).

Petras, Christopher M., The Use of Force in Response to Cyber-Attack on Commercial Space Systems - Reexamining SelfDefense in Outer Space in Light of the Convergence of U.S. Military and Commercial Space Activities, Journal of Air Law and Commerce, Vol. 67, p. 1251.

Pluta, Anna M. / Peter D. Zimmerman, Nuclear Terrorism: A Disheartening Dissent, Survival, Vol.48, No.2, 2006, p.55.

Pool, Phillip, War of the Cyber World: The Law of Cyber Warfare, The International Lawyer, Vol. 47, No. 2, 2013, p.303.

Ptasekaite, Rasa, The Euratom Treaty v. Treaties Of The European Union: Limits of Competence and Interaction, The Swedish Radiation Safety Authority, Vol. 2011, No. 32, 2011, p.37.

R. Krutz, Securing SCADA Systems, Wiley, Indianapolis, Indiana, 2006, p.10.

Radetzki, Marcus, Limitation of Third Party Nuclear Liability Causes, Implications and Future Possibilities. Nuclear Law Bulletin, Vol.63, 1993, pp.7-8.

Ramana, M. V., et al., A New Normal?: The Changing Future of Nuclear Energy in China, Learning from Fukushima: Nuclear Power in East Asia, edited by Peter Van Ness And Mel Gurtov, Anu Press, Australia, 2017, p. 104.

Ramey, James T., The Promise of Nuclear Energy, The Annals of the American Academy of Political and Social Science, Vol. 410, 1973, p.11.

Rasmussen, Morten., Establishing a Constitutional Practice of European Law: The History of the Legal Service of the European Executive, 1952—65, Contemporary European History, Vol. 21, No. 3, 2012, p. 382.

Richard A. Falkenrath, Robert D. Newman, and Bradley Thayer America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack, Cambridge Mass.:MIT Press, 1998, (Önsöz).

Richelson, Jeffrey T., Nuclear Terrorism: How Big a Threat?, The National Security Archive, the George Washington University, National Security Archive Electronic Briefing Book No. 388, 2012.

Robin Geiss, The Conduct of Hostilities in and via Cyberspace, Proceedings of the Annual Meeting (American Society of International Law), Vol. 104, 2010, pp. 372-373.

Roscini, Marco, World Wide Warfare Jus Ad Bellum and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, Vol. 14, 2010, p.90.

Rosenow, Patrick, United We Fight? Terrorismusbekämpfung Im Rahmen Der Vereinten Nationen Seit Dem 11. September 2001, Die Friedens-Warte, Vol. 86, No. 3/4, 2011, pp. 15-17.

Rrushi, J. and Campbell, R., 2008, in IFIP International Federation for Information Processing, Vol. 290; Critical Infrastructure Protection II, eds. Papa, M., Shenoi, S., (Boston: Springer), p.41.

Ruiz, Gaetano Arangio, Fifth report on State Responsibility, A/CN.4/453 and Add.1-3, United Nations, Extract from the Yearbook of the International Law Commission: 1993 Document, Vol. II (1), p.109.

Sagan, Scott D., The Global Nuclear Future, Bulletin of the American Academy of Arts and Sciences, Vol. 63, No. 2, 2010, p. 38.

Salik, Naeem, Nuclear Terrorism: Assessing the Danger, Strategic Analysis, Vol.38, No.2, 2014, p.182.

Sassòli, Marco; The Distinction and Relationship between Jus ad Bellum and Jus in Bello, Chinese Journal of International Law, Vol. 11, No. 3, 1 September, 2012, pp. 610-611.

Satapathy, C. , Impact of Cyber Vandalism on the Internet, Economic and Political Weekly, Vol. 35, No. 13, 2000, p.1060.

Schaap, Arie J., Cyber Warfare Operations: Development and Use Under International Law, Vol. 64, The Air Force Law Review, 2009, p.121.

Schmitt, Michael N, International Law and the Use of Force: The Jus Ad Bellum, Connections, Vol. 2, No. 3, 2003, p. 91.

Schmitt, Michael N., Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 Colum, Journal of Transnational Law & Policy, Vol. 885, No. 909, 1991, p.1041.

Shackelford, Scott, Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks, Journal of Internet Law, Forthcoming, November 4, 2009, pp. 5-6.

Sharma, Bhaskar, Cyber War and Jus in Bello, Foreign Policy Journal, Dec 3, 2012: https://www.foreignpolicyjournal.com/2012/12/03/cyber-war-and-jus-in-bello/ (E.T: 15.04.18).

Sharp, Walter Gary, CyberSpace and the Use of Force, Aegis Research Cooperation, The USA, p. 102.

Shea, Thomas E., The Verification Challenge: Iran and the IAEA, Arms Control Today, Vol. 45, No. 5, 2015, pp. 8-9.

Shen, Dan et al., Game Theoretic Solutions to Cyber Attack and Network Defense Problems, Twelfth International Command and Control Research and Technology Symposium (12th ICCRTS), 19-21 June 2007, Newport, RI, p.7.

Sieber, Ulrich, Bilgisayar Suçluluğu, Ünver Yener (ed.), İnternet Hukuku, (İstanbul: Seçkin Yay., Birinci Baskı, Nisan 2013,), s. 26.

Silver, Daniel B., Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, International Law Studies, Vol. 76, Computer

Networ Attack and International Law, Mitchal N. Schmitt & Brian T. O'Donnell (Editors), p. 74.

Simo, Augustin, What İf There's A Next Time? Preparedness After Chernobyl and Fukushima, Bulletin of The Atomic Scientists, Vol. 72, No. 4, 2016, p. 265.

Singer, P.W. / Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs To Know, Oxford, OUP, 2014, p.36

Smedt, Anne Boerger-De., Negotiating the Foundations of European Law, 1950—57: The Legal History of the Treaties of Paris and Rome, Contemporary European History, Vol. 21, No. 3, 2012, p. 339.

Sofaer, Abraham D., The Best Defense? Preventive Force and International Security, Foreign Affairs, Vol. 89, No. 1, 2010, pp. 111-113.

Sounnalat, Khamla, Cyber Crimes Legislation and Implementation, Cyber Crimes Conference 17-20 June, 2015, Strasbourg, France.

Suzuki, Tatsujiro, et al., Nuclear Energy Policy Issues in Japan after the Fukushima Nuclear Accident, Learning from Fukushima: Nuclear Power in East Asia, edited by Peter Van Ness and Mel Gurtov, Anu Press, Australia, 2017, p.10.

Sylves, Richard T. , Carter Nuclear Licensing Reform versus Three Mile Island, Publius, Vol. 10, No. 1, 1980, p.70.

Takada, Jun, Radiation Hazard and Protection for the Nuclear Weapon Terrorism, International Congress Series, Vol. 1276, February 2005, p245.

Tashbook, Linda, Nuclear Law Research Guide, Hauser Global Law School Program, New York University School of Law , June 2017: http://www.nyulawglobal.org/globalex/Nuclear_Research1.html#io (E.T: 27.03.18).

Taşdemir, Fatma / Gökhan Albayrak, The Law of Cyber Warfare in Terms of Jus Ad Bellum and Jus in Bello: Application of International Law to the Unknown?, December 23, 2017, E-Journal of Law, Forthcoming, pp. 4-6.

Temurçin, Kadir/Alpaslan Aliağaoğlu, Nükleer Enerji ve Tartışmalar Işığında Türkiye'de Nükleer Enerji Gerçeği, Coğrafi Bilimler Dergisi, Cilt.1, Sayı.2, 2003, s.25.

Ten, Chee-Wooi/ Manimaran Govindarasu / Chen-Ching Liu, Cybersecurity for Critical Infrastructures: Attack and Defense Modeling, IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, Vol. 40, No. 4, 2010, p.855.

Tessama, Zereay, et al. Mainstreaming Sustainable Energy Access into National Development Planning: The Case of Ethiopia. Stockholm Environment Institute, 2013, p.4.

Tikk-Ringas, Eneken, The Implications of Mandates in International Cyber Affairs, Georgetown Journal of International Affairs, 2012, p. 42.

Tom Ruys, The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are 'Minimal' Uses of Force Excluded from UN Charter Article 2(4)?, The American Journal of International Law, Vol. 108, Vo. 2, 2014, p. 161.

Trofimenko, Henry, SALT II: A Fair Bargain, Bull. Atomic Scientists, June 1979, p. 30.

Tsoukalas, Lefteri H., and Rong Gao., A Future Role for Nuclear Energy? Understanding the Global Energy Crisis, edited by Eugene D. Coyle and Richard A. Simmons, Purdue University Press, West Lafayette, Indiana, 2014, p.167.

Van Epps, Geoff, Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain, Connections, Vol. 12, No. 4, 2013, p. 15.

Varuttamaseni, Athi /Robert A. Bari/ Robert Youngblood, Construction of a Cyber Attack Model for Nuclear Power Plant, NPIC&HMIT 2017, San Francisco, CA, June 11-15, 2017, p.107.

Vatis, Michael, The Next Battlefield: The Reality of Virtual Threats, Harvard International Review, Vol. 28, No. 3, 2006, pp. 59–60.

Volders, Brecht, Nuclear Terrorism: What Can We Learn from Los Alamos?, Terrorism and Political Violence, 2017, p.3.

Warwick, Joanna, Public Acceptance of Nuclear Energy in Canada, Energy Exploration & Exploitation, Vol. 8, No. 5, 1990, p. 339.

Weber, Amalie M., The Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. ,2003, p. 427.

Wei, Yuxi, China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty, The Henry M. Jackson School of International Studies, University of Washington, June 21, 2016 : https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/ (E.T: 13.04.18).

Weiss, Peter, The American Journal of International Law, The American Journal of International Law, Vol. 94, No. 4, 2000, p. 816.

Wilkerson, Jordan, Reconsidering the Risks of Nuclear Power, Harvard University Graduate School of Arts and Sciences, Blog, Specıal Edition: Dear Madam/Mister President, 2016: http://sitn.hms.harvard.edu/flash/2016/reconsidering-risks-nuclear-power/ (E.T: 15.03.18).

Williams, Ja Rai A., The Legal Limits of Targeting the Cyber Capabilities of a Neutral State, Air Command and Staff College Air University, Yayınlanmamış Yüksek Lisans Tezi, 2015, s. 15.

Willis, Terry D., Criminal Liability in Cyberspace, GPSolo, Vol. 23, No. 1, 2006, pp. 37-38.

Witten, Samuel M., The International Convention for the Suppression of Terrorist Bombings, The American Journal of International Law, Vol. 92, No. 4, 1998, p. 774.

Wolter, Detlev, The UN Takes a Big Step Forward on Cybersecurity, Arms Control Today, Vol. 43, No. 7, 2013, p. 27.

Yergin, Daniel, The Prize: The Epic Quest for Oil, Money, & Power, Simon & Schuster, New York, 1991, p.23.

Zulkefli, Zakiah/ Manmeet Mahinderjit Singh/ Azizul Rahman Mohd Shariff/ Azman Samsudin, Typosquat Cyber Crime Attack Detection via Smartphone, Procedia Computer Science, Vol. 124, 2017, p.666.

Kurum Çalışmaları ve İnternet Kaynakları

AGECC: Energy for a Sustainable Future: Report and Recommendations, 28 April 2010, New York, p.7.

AKKUYU NÜKLEER, Akkuyu Nükleer Güç Santrali'nin temeli Rusya Federasyonu Devlet Başkanı ve Türkiye Cumhuriyeti Cumhurbaşkanı'nın tatıldığı törenle atıldı, 03.04.2018 : http://www.akkunpp.com/akkuyu-nukleer-guc-santralinin-temeli-rusya-federasyonu-devlet-baskani-ve-turkiye-cumhuriyeti-cumhurbaskaninin-tatildigi-torenle-atildi/update (16.04.18).

AKKUYU NÜKLEER, Projenin Tarihçesi: http://www.akkunpp.com/projenin-tarihcesi (E.T: 12.04.18).

AMACAD, Nuclear Liability: A Key Component of the Public Policy Decision to Deploy Nuclear Energy in Southeast Asia: https://www.amacad.org/content/publications/pubContent.aspx?d=1507 (E.T: 24.03.18).

ARENA, What is Renewable Energy?, https://arena.gov.au/about/what-is-renewable-energy/ (E.T: 13.03.18).

Armstrong, Martin, The Countries Holding The World's Nuclear Arsenal, Mar 2, 2018: https://www.statista.com/chart/8301/the-countries-holding-the-worlds-nuclear-arsenal/ (E.T: 14.03.18).

ASN, Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management : http://www.french-nuclear-safety.fr/International/International-reference-texts/International-conventions/Joint-Convention-on-the-Safety-of-Spent-Fuel-Management-and-Safety-of-Radioactive-Waste-Management (31.03.18).

Barnett, Sophie, Applying Jus Ad Bellum in Cyberspace, September 1, 2016 : http://www.e-ir.info/2016/09/01/applying-jus-ad-bellum-in-cyberspace/ (15.04.18).

BBC, Cybercrime and Fraud Scale Revealed in Annual Figures, 19 January 2017 : http://www.bbc.com/news/uk-38675683 (E.T: 08.04.18).

BBC, US President Barack Obama Warns of Nuclear Terrorism, 12 April 2010: http://news.bbc.co.uk/2/hi/middle_east/8614695.stm (E.T: 18.03.18).

BP, BP Statistical Review of World Energy, 66th Ed. 2017, p.43.

CAMBRIDGE: https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/dirty-bomb (E.T: 18.03.18).

CCDCOE, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: https://ccdcoe.org/tallinn-manual.html (E.T: 08.04.18).

CE, Convention on Cybercrime: Explanatory Report, 109th Session 38, November 8, 2001, : http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (E.T: 13.04.18).

CEF, What are Non-Renewable Sources of Energy? : https://www.conserve-energy-future.com/nonrenewableenergysources.php (E.T: 11.03.18).

Center for International Trade and Security, Nuclear Security Culture: The Case Of Russia, The University of Georgia, Athens GA, December 2004, p.5.

Center for the Study of Technology and Society, Hiroshima and Nagasaki at Sixty, The New Atlantis, No. 9, 2005, p.139.

CHECKPOINT, What is a Cyber Attack? : https://www.checkpoint.com/definition/cyber-attack/ (E.T:11.04.18).

CIA, The Chernobyl' Accident: Social and Political Implications, A Research Paper, Raport No: CIA-RDP08S01350R000300900002-4, 2012, p.5: https://www.cia.gov/library/readingroom/docs/CIA-RDP08S01350R000300900002-4.pdf (E.T: 16.03.18).

CIL, 2005 Protocol to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, National University of Singapore: https://cil.nus.edu.sg/2005-protocol-o-the-convention-for-the-suppression-of-unlawful-acts-against-the-safety-of-maritime-navigation/ (E.T: 05.04.18).

CISAC, Understanding the Risks and Realities of Nuclear Terrorism, Institute for International Studies, Stanford University, October 2002, p.2.

Clinton, Bill, EURATOM ve ABD Arasındaki Nükleer Enerji'nin İnsani Amaçla Kullanılması Anlaşması Hakkında 104. Meclisinin 1. Oturumunda İlettiği Yazılı Mesaj, Meclis Evrak No: 104-108, ABD Hükümeti Basın Ofisi, Washington, 29 Kasım 1995, s.2, bkz: https://www.gpo.gov/fdsys/pkg/CDOC-104hdoc138/pdf/CDOC-104hdoc138.pdf (E.T: 20.03.18).

Corporate Knights Inc. , Back Matter, Corporate Knights, Vol. 9, No. 1, 2010, p.2.

CPS, Cybercrime - Prosecution Guidance: Legal Guidance, Cyber / Online Crime : https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (E.T: 15.04.18).

CTBTO, : https://www.ctbto.org/the-treaty/article-xiv-conferences/2011/afc11-information-for-media-and-press/what-is-the-ctbt/ (E.T: 21.03.18).

CTBTO, General Overview of the effects of Nuclear Testing: https://www.ctbto.org/nuclear-testing/the-effects-of-nuclear-testing/general-overview-of-theeffects-of-nuclear-testing/ (E.T: 14.03.18).

CYBER WAR LAW, The Principles of Humanity and Military Necessity in Cyber War : http://cyberwarlaw.eu/the-principles-of-humanity-and-military-necessity-in-cyber-war/ (E.T: 15.04.18).

DİJİTAL DÖNÜŞÜM: Siber Güvenlik Mevzuatı: https://www.dijitaldonusum.gov.tr/siber-guvenlik-mevzuati/ (11.04.18).

DOD, Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, p.2.

DoS, 2015 NPT Gözden Geçirme Konferansı Ortak Bildirisi: https://2009-2017.state.gov/r/pa/prs/ps/2015/02/237273.htm (E.T: 21.03.18).

EC, Commission Recommendation of 4.4.2016 on the application of Article 103 of the Euratom Treaty : https://ec.europa.eu/energy/sites/ener/files/documents/1_EN_ACT_part1_v6_1.pdf (06.040.18).

EC, Communication From The Commission Nuclear Illustrative Programme Presented Under Article 40 of The Euratom Treaty for The Opinion of the European Economic and Social Committee : http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52016DC0177 (06.040.18).

EC, Reform of Cyber Security in Europe : http://www.consilium.europa.eu/en/policies/cyber-security/ (E.T: 13.04.18).

EF, Historical Development of the Word "Energy": http://home.uni-leipzig.de/energy/ef/01.htm (E.T: 05.04.18).

EIA, Nonrenewable and Renewable Energy Sources, February 9, 2017: https://www.eia.gov/energyexplained/index.php?page=nonrenewable_home (11.03.18).

EIA: https://www.eia.gov/energyexplained/index.cfm?page=nuclear_home#tab1 (E.T: 13.02.18).

El Baradei, Mohamed, Peaceful Uses of Nuclear Energy: Meeting Societal Needs, IAEA, Vienna- Austria, Nov. 15, 2014: https://www.iaea.org/newscenter/statements/peaceful-uses-nuclear-energy-meeting-societal-needs (20.03.18).

Emmerechts, Sam, General Principles of International Nuclear Law, OECD-NEA, 6 March 2008: http://qualidade.ipen.br/sq-cen/Atualizacao-CEN/4.14-Cursos/Curso-WNU/Main_Issues_of_Nuclear_Law-Sam_Emmerechts.pdf (E.T: 19.03.18).

Enerji ve Tabi Kaynaklar Bakanlığı: http://www.enerji.gov.tr/tr-TR/Sayfalar/Nukleer-Enerji (E.T: 13.10.18).

ERDA, Lyerly, Ray L./ Walter Mitchell, Nuclear Power Plants: https://www.osti.gov/includes/opennet/includes/Understanding%20the%20Atom/Nuclear%20Power%20Plants.pdf (E.T: 16.03.18).

FAS, Nuclear & Radiological Terrorism: https://fas.org/issues/nuclear-and-radiological-terrorism/ (E.T: 18.03.18).

FBI, 2016 Internet Crime Report, Internet Crime Complaint Center, 2016, p.17.

FORBES, How Does Cyber Warfare Work?, Jul 18, 2013: https://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/#2bda262044ce (E.T: 11.04.18).

FOREIGN RELATIONS LAW, Nuclear Nonproliferation, Congress Authorizes the President to Waive Restrictions on Nuclear Exports to India, Henry J. Hyde United States-India Peaceful Atomic Energy Cooperation Act of 2006, Pub. L. No. 109-401, Tit. I, 120 Stat. 2726 (to Be Codified at 22 U.S.C. §§ 2652c, 8001-8008, and 42 U.S.C. § 2153(d))., Harvard Law Review, Vol. 120, No. 7, 2007, p. 2021.

Fruhlinger, Josh, What is Stuxnet, Who Created it And How Does it Work?, CSO, AUG 22, 2017: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html (E.T: 06.04.18).

Furtado, Rebecca, A Brief Introduction to Nuclear Energy Laws, Pleaders, July 11, 2016 : https://blog.ipleaders.in/brief-introduction-nuclear-energy-laws/ (E.T: 19.03.18).

GREENPEACE, Nuclear Energy: https://www.greenpeace.org/usa/global-warming/issues/nuclear/ (E.T: 15.03.18).

Grimes, Roger A., Why it's So Hard to Prosecute Cyber Criminals: The Bad Guys Are Wreaking Havoc. Why Can't They Be Brought to Justice?, December 6, 2016: https://www.csoonline.com/article/3147398/data-protection/why-its-so-hard-to-prosecute-cyber-criminals.html (E.T: 09.04.18).

GUARDIAN: https://www.theguardian.com/environment/2006/may/26/energy.iran (E.T: 25.03.18).

GUARDIAN: https://www.theguardian.com/world/2009/apr/05/nuclear-weapons-barack-obama (E.T:25.03.18).

Henderson, Christian, The Use of Cyber Force: Is The Jus Ad Bellum Ready?, April 30, 2016 : http://www.qil-qdi.org/use-cyber-force-jus-ad-bellum-ready/ (15.04.18).

Hern, Alex, Cyber-Attacks and Hacking: What You Need to Know, The Guardian, 1 Nov. 2016 : https://www.theguardian.com/technology/2016/nov/01/cyber-attacks-hacking-philip-hammond-state-cybercrime (E.T: 15.04.18).

HS, Critical Infrastructure Sectors, 2017: https://www.dhs.gov/critical-infrastructure-sectors (E.T: 19.03.18).

HUMAN RIGHTS COMMITTEE, General comment No. 36 on article 6 of the International Covenant on Civil and Political Rights, on the right to life: Revised draft prepared by the Rapporteur: http://www.ohchr.org/Documents/HRBodies/CCPR/GCArticle6/GCArticle6_EN.pdf (25.03.18).

IAEA, 60 Years of "Atoms for Peace", 2013: https://www.iaea.org/newscenter/news/60-years-atoms-peace (25.03.18).

IAEA, Amendment to the Convention on the Physical Protection of Nuclear Material GOV/INF/2005/10-GC (49) INF/6, , Vienna, 2005, p.9.

IAEA, Code of Conduct on the Safety and Security of Radioactive Sources, Vieanna, Austria, 2004, pp. 4-5.

IAEA, Code of Conduct on the Safety and Security of Radioactive Sources, and Supplementary Guidance on the Import and Export of Radioactive Sources : http://www-ns.iaea.org/tech-areas/radiation-safety/code-of-conduct.asp (E.T: 06.04.18).

IAEA, Computer and Information Security : https://www.iaea.org/topics/computer-and-information-security (E.T: 12.04.18).

IAEA, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, Vienna, 2011, pp. 55-57.

IAEA, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, Vienna, 2011, p.2.

IAEA, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series, No. 17, 2011, p.14.

IAEA, Computer Security Incident Response Planning at Nuclear Facilities, Vienna, 2016, p.4.

IAEA, Computer Security Incident Response Planning at Nuclear Facilities, Vienna, 2016, pp. 11-16.

IAEA, Concept and Terms: IAEA Safety Standards: http://www-ns.iaea.org/standards/concepts-terms.asp (E.T: 18.03.18).

IAEA, Conducting Computer Security Assessments at Nuclear Facilities, Vienna, 2016, pp. 4-6.

IAEA, Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency :

https://www.iaea.org/publications/documents/treaties/convention-assistance-case-nuclear-accident-or-radiological-emergency (31.03.18).

IAEA, Convention on Early Notification of a Nuclear Accident : https://www.iaea.org/publications/documents/treaties/convention-early-notification-nuclear-accident (E.T: 30.03.18).

IAEA, Convention on Nuclear Safety: https://www.iaea.org/sites/default/files/infcirc449.pdf (E.T: 19.03.18).

IAEA, Convention on Physical Protection of Nuclear Material (CPPNM) and Amendment thereto : http://www-ns.iaea.org/conventions/physical-protection.asp?s=6&l=42 (E.T: 30.03.18).

IAEA, Convention on the Physical Protection of Nuclear Material : https://www.iaea.org/publications/documents/conventions/convention-physical-protection-nuclear-material (29.03.18).

IAEA, Country Nuclear Power Profiles: Turkey, 2017: https://cnpp.iaea.org/countryprofiles/Turkey/Turkey.htm (E.T: 16.03.18).

IAEA, Documents Produced by the Regulatory Body for a Specific Facility: Licence Document: https://www.iaea.org/ns/tutorials/regcontrol/docum/docum5124.htm# (24.03.18).

IAEA, General Conference: Resolution On Measures To Improve the Security of Nuclear Materials and Other Radioactive Materials, International Legal Materials, Vol. 41, No. 3, 2002, pp. 743–745.

IAEA, History: https://www.iaea.org/about/overview/history (25.03.18).

IAEA, IAEA Requirement for the Governmental Level and for the Operator: https://www.iaea.org/ns/tutorials/regcontrol/legis/legis113.htm# (E.T: 23.03.18).

IAEA, International Conference on Physical Protection of Nuclear Material and Nuclear Facilities : https://www-pub.iaea.org/iaeameetings/50819/International-

Conference-on-Physical-Protection-of-Nuclear-Material-and-Nuclear-Facilities (E.T: 06.04.18).

IAEA, International Status and Prospects for Nuclear Power 2017, Official Report, 2017, p.1: https://www.iaea.org/About/Policy/GC/GC61/GC61InfDocuments/English/gc61inf-8_en.pdf (18.03.18).

IAEA, Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management : http://www-ns.iaea.org/conventions/waste-jointconvention.asp (31.03.18).

IAEA, Joint Protocol Relating to the Application of the Vienna Convention and the Paris Convention: https://www.iaea.org/sites/default/files/infcirc402.pdf (25.03.18).

IAEA, Nuclear Energy Basic Principles, Nuclear Energy Series, No. EE-BP, Vienna, 2008, p.1.

IAEA, Nuclear Safety & Security: Conventions and Codes: http://www-ns.iaea.org/conventions/ (E.T: 25.03.18).

IAEA, Nuclear Security Culture: Implementing Guide, IAEA Nuclear Security Series No.7, Austria, 2008, pp.3-4.

IAEA, Nuclear Security Fundamentals: Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, Vienna, 2013, pp.3-10.

IAEA, Nuclear Terrorism: Threats and Risks, IAEA, 2017, p.4.

IAEA, Organization and Staffing of the Regulatory Body for Nuclear Facilities, Safety Series No. GS-G-1.1, IAEA, Vienna, 2002, p.23.

IAEA, Resolutions and Other Decisions of the General Conference: GC55/Res/10 Nuclear Security, Adopted by the General Conference on Fifty-fifth Regular Session 19-23 September 2011, p.3.

IAEA, Responsibilities and Capabilities of a Nuclear Energy Programme Implementing Organization, IAEA Nuclear Energy Series, No. NG-T-3.6, Vienna, 2009, p.3.

IAEA, Self-Assessment Of Nuclear Security Culture in Facilities and Activities: Technical Guidance, IAEA Nuclear Security Series No. 28-T, Vienna, 2017, p.6.

IAEA, The Convention on Nuclear Safety : http://www-ns.iaea.org/conventions/nuclear- safety.asp?s=6&l=41 (31.03.18).

IAEA, The Convention on the Physical Protection of Nuclear Material, IAEA - INFCIRC/274/Rev. 1, May 1980: https://www.iaea.org/sites/default/files/infcirc274r1.pdf (E.T: 26.03.18).

IAEA, The IAEA Mission Statement: https://www.iaea.org/about/mission (25.03.18).

IAEA, The International Legal Framework for Nuclear Security, IAEA International Law Series No. 4, Vienna, Austria, January 2011, p.3.

IAEA, Treaty on the Non-Proliferation of Nuclear Weapons (NPT): https://www.iaea.org/sites/default/files/publications/documents/infcircs/1970/infcirc140.pdf (E.T: 21.03.18).

IAEA, UN Security Council resolutions : http://www-ns.iaea.org/security/sc_resolutions.asp (31.03.18).

IAEA, Vienna Convention On Civil Liability For Nuclear Damage: https://www.iaea.org/sites/default/files/infcirc500.pdf (25.03.18).

IAEA: http://www-ns.iaea.org/conventions/nuclear-safety.asp?s=6&l=41 (E.T:25.03.18).

IAEA: http://www-ns.iaea.org/conventions/waste-jointconvention.asp?s=6&l=40 (E.T:25.03.18).

IAEA: https://www.iaea.org/newscenter/news/iaea-releases-projections-on-global-nuclear-power-capacity-through-2050 (E.T: 16.03.18).

IAEA: https://www.iaea.org/topics/conventions-on-emergency-preparedness-and-response#2 (E.T:25.03.18).

IAEA: https://www.iaea.org/topics/conventions-on-emergency-preparedness-and-response (E.T:25.03.18).

IAEA: https://www.iaea.org/topics/nuclear-security-conventions (E.T:25.03.18).

IATA, Montreal Convention 1999, 28 May 1999 : https://www.iata.org/policy/Documents/MC99_en.pdf (E.T: 13.04.18).

ICAN, Nuclear Arsenals: http://www.icanw.org/the-facts/nuclear-arsenals/ (E.T: 14.03.18).

ICAO, Convention on International Civil Aviation Done at Chicago, 7th Day of December 1944: https://www.icao.int/publications/Documents/7300_orig.pdf (E.T: 13.04.18).

ICAO, Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation : https://www.icao.int/secretariat/legal/List%20of%20Parties/VIA_EN.pdf (E.T: 13.04.18).

ICRC, What Are Jus Ad Bellum And Jus in Bello?, 22 January, 2015 : https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0 (E.T: 14.04.18).

IEA, http://www.iea.org/newsroom/news/2015/october/renewables-to-lead-world-power-market-growth-to-2020.html (E.T: 11.03.18).

IEAE, Eisenhower D., Atoms for Peace, 1953, https://www.iaea.org/about/history/atoms-for-peace-speech (E.T: 19.03.18).

IET, Legal Framework for the Nuclear Industry in Great Britain: https://www.theiet.org/factfiles/ (E.T: 18.03.18).

ILPI, ICJ's Advisory Opinion on Nuclear Weapons: A Brief Overview of The Conclusions of International Court of Justice in 1996, Nutshell Paper No 3/2011, pp.1-2.

IMO, Adopting A Convention, Entry into Force, Accession, Amendment, Enforcement, Tacit Acceptance Procedure : http://www.imo.org/en/About/Conventions/Pages/Home.aspx (04.04.18).

IMO, Brief History of IMO, http://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx (E.T: 03.04.18).

IMO, Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/SUA-Treaties.aspx (E.T: 05.04.18).

IMO, Maritime Security, http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Default.aspx (E.T: 05.04.18).

INFOSEC INSTITUTE, Jus in Cyber Bello: How the Law of Armed Conflict Regulates Cyber Attacks Part I, APRIL 10, 2014 : http://resources.infosecinstitute.com/jus-cyber-bello-law-armed-conflict-regulates-cyber-attacks-part/#gref (E.T: 15.04.18).

INLEX, Civil Liability for Nuclear Damage: Advantages and Disadvantages of Joining the International Nuclear Liability Regime, IAEA, pp.10-11.

International Convention for The Suppression of Acts of Nuclear Terrorism, International Legal Materials, Vol. 44, No. 4, 2005, p. 815.

INTERPOL, Cybercrime : https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (E.T: 08.04.18).

ITU, About International Telecommunication Union (ITU) : https://www.itu.int/en/about/Pages/default.aspx (E.T: 13.04.18).

ITU, Constıtutıon of The International Telecommunication Union : https://www.itu.int/council/pd/constitution.html (E.T: 13.04.18).

ITU, Global Cybersecurity Index 2017, p.13. : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (E.T: 13.04.18).

JAEA, International Forum on Peaceful Use of Nuclear Energy and Nuclear Security : https://www.jaea.go.jp/04/np/activity/2011-12-08/report_en.html (E.T: 18.0.18).

Jenden, James/ Ellen Lloyd/ Kailyn Stenhouse/ Jason Donev, Renewable and sustainable energy, Energy Education: http://energyeducation.ca/encyclopedia/Renewable_and_sustainable_energy (E.T: 11.03.18).

Kan, Naoto, Statement by Prime Minister Naoto Kan upon the General Resignation of the Kan Cabinet: https://japan.kantei.go.jp/kan/statement/201108/30danwa_e.html (E.T: 17.03.18).

Kantor, Moshe, We Must Face Up to the Threat of Nuclear Terrorism, The Telegraph, 8 June 2016: https://www.telegraph.co.uk/news/2016/06/08/we-must-face-up-to-the-threat-of-nuclear-terrorism/ (E.T: 26.03.18).

KASPERSKY, What is Cyber-Security? https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (06.04.18).

LAW INSIDER, Definition of Nuclear Laws: https://www.lawinsider.com/dictionary/nuclear-laws (E.T: 19.03.18).

Lowe, Christian, Kremlin loyalist says launched Estonia Cyber-Attack, Reuters, March 13, 2009: https://www.reuters.com/article/us-russia-estonia-

cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313 (E.T: 15.04.18).

Maehlum, Mathias Aarre, Non-Renewable Energy Resources, Energy Informative, May 3, 2013 : http://energyinformative.org/non-renewable-energy-resources/ (E.T: 14.03.18).

Maiese, Michelle, Jus in Bello, Beyond Intractability, June 2003 : https://www.beyondintractability.org/essay/jus_in_bello (E.T: 15.14.18).

Mariotte, Michael, Wishful Thinking: the Basis of New Nuclear Economics, March 28, 2016 : https://safeenergy.org/2016/03/28/wishful-thinking-the-basis-of-new-nuclear/#more-13790 (E.T: 15.03.18).

Markov, Sergei, Behind The Estonia Cyberattacks, March 06, 2009 : https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html (E.T: 15.04.18).

McCoy, Frank, Job Horizon: So You Want To Be A Cyber Security Professional, US Black Engineer and Information Technology, Vol. 36, No. 4, 2012, p. 6.

MFA, Press Release Regarding The Deposition of the Instrument of Ratification of the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) to UN, No: 223, 24 September 2012,: http://www.mfa.gov.tr/no_-223_-24-september-2012_-press-release-regarding-the-deposition-of-the-instrument-of-ratification-of-the-international-convention-for-the-suppression-of-acts-of-nuclear-terrorism-_icsant_-to-un.en.mfa (04.04.18).

MFAPRC, Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation, 2009/06/17 : http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t569701.shtml (E.T: 13.04.18).

MİLLİYET, Başbakan Yıldırım: Onbinlerce Siber Güvenlik Uzmanına İhtiyaç Olacak, 29.11.2017: http://www.milliyet.com.tr/basbakan-yildirim-teknolojiler-siyaset-2563498/ (E.T: 12.04.18).

NASA: Nuclear Weapon Effects In Space: https://history.nasa.gov/conghand/nuclear.htm (E.T: 14.03.18).

NATO Review Magazine, New Threats: The Cyber-Dimension: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm (E.T: 18.03.18).

NATO, NATO and the Non-Proliferation Treaty, Fact Sheet, 2017 : https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170323_170323-npt-factsheet.pdf (E.T: 21.03.18).

NATO, NATO Cyber Defence, February 2018 : https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf (E.T: 13.04.18).

NATO, North Atlantic Council Statement on the Treaty on the Prohibition of Nuclear Weapons, 2017: https://www.nato.int/cps/ua/natohq/news_146954.htm (E.T: 20.03.18).

NEWS: NEA/OECD Report on Radiological Impact of Chernobyl Accident, Current Science, Vol. 57, No. 9, 1988, p. 471.

NOBEL PRIZE, 2017 Nobel Barış Ödülü : https://www.nobelprize.org/nobel_prizes/peace/laureates/2017/ (E.T: 20.03.18).

NSGEG, Promoting Greater Transparency for Effective Nuclear Security: Summary Report & Initial Policy Recommendations, the Stanley Foundation, February 2013, p.4. : https://www.stanleyfoundation.org/nsgeg/NSGEGLondonReport022013.pdf (E.T: 20.03.18).

NTI, : http://www.nti.org/learn/treaties-and-regimes/comprehensive-nuclear-test-ban-treaty-ctbt/ (E.T: 21.03.18).

NTI, Addressing Cyber-Nuclear Security Threats: http://www.nti.org/about/projects/addressing-cyber-nuclear-security-threats/ (E.T: 19.03.18).

NTI, Global Nuclear Policy: http://www.nti.org/about/global-nuclear-policy/ (E.T: 18.03.18).

NTI, International Convention on the Suppression of Acts of Nuclear Terrorism: http://www.nti.org/learn/treaties-and-regimes/international-convention-suppression-acts-nuclear-terrorism/ (02.04.18).

NTI, Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management : http://www.nti.org/learn/treaties-and-regimes/joint-convention-on-the-safety-of-spent-fuel-management-and-on-safety-of-radioactive-waste-management/ (31.03.18).

NUCLEAR ENERGY, Brussels Convention 1971, The American Journal of Comparative Law, Vol. 20, No. 3, 1972, p. 533.

Nuclear Energy, History of Nuclear Energy, 2017: https://nuclear-energy.net/what-is-nuclear-energy/history (E.T: 12.03.18).

Nuclear Power Plant and Reactor Exporters, The Principles of Conduct: Compensation for Nuclear Damage : http://nuclearprinciples.org/principle/compensation-for-nuclear-damage/ (19.03.18).

OECD- NEA/IAEA, International Nuclear Law in the Post-Chernobyl Period, No.6146, 2006, pp. 74-75.

OECD: https://legalinstruments.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=197&Lang=en&Book=False (25.03.18).

OECD-NEA, Brussels Supplementary Convention: https://www.oecd-nea.org/law/brussels-supplementary-convention.html (25.03.18).

OECD-NEA, Convention of 31st January 1963 Supplementary to the Paris Convention of 29th July 1960, as amended by the additional Protocol of 28th January 1964 and by the Protocol of 16th November 1982 ("Brussels Supplementary Convention"), : https://www.oecd-nea.org/law/nlbrussels.html (25.03.18).

OECD-NEA, European Atomic Energy Community, Nuclear Law Bulletin, Vol. 2016/2, No.98, 2016, p.85.

OECD-NEA, History of the OECD Nuclear Energy Agency: https://www.oecd-nea.org/general/history/ (25.03.18).

OECD-NEA, Paris Convention on Nuclear Third Party Liability: https://www.oecd-nea.org/law/paris-convention.html (25.03.18).

OECD-NEA, The Nuclear Energy Agency: https://www.oecd-nea.org/general/about/ (E.T: 25.03.18).

OECD-NEA: Convention on Third Party Liability in the Field of Nuclear Energy of 29th July 1960, as Amended by the Additional Protocol of 28th January 1964 and by the Protocol of 16th November 1982 : https://www.oecd-nea.org/law/nlparis_conv.html (25.03.18).

Ponemon, Cost of Cyber Crime Study: Insights on the Security Investments that Make a Difference, 2017, s.12: https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50 (10.04.18).

PUI : https://www.iaea.org/newscenter/focus/peaceful-uses-initiative (E.T: 20.03.18).

PWC, Elektrik Piyasasında Kaynakların Kullanımına İlişkin bir Değerlendirme, https://www.pwc.com.tr/tr/sektorler/enerji-altyapi-madencilik/enerji-spotlights/elektrik-piyasasinda-kaynaklarin-kullanimina-iliskin.html (13.03.18).

PWC, Why Nuclear Power Plants Are More Vulnerable To Cyber Attacks Today : https://www.pwc.com/us/en/industries/capital-projects-infrastructure/asset-classes-sectors/nuclear-power-industry/nuclear-cyber-security.html (E.T: 06.04.18).

Ramsey, Carly / Ben Wootliff, China's Cyber Security Law: The Impossibility of Compliance?, Forbes, May 29, 2017 : https://www.forbes.com/sites/riskmap/2017/05/29/chinas-cyber-security-law-the-impossibility-of-compliance/#4ff0f4a7471c (E.T: 14.04.18).

REN21, Global Status Report, 2017: http://www.ren21.net/status-of-renewables/global-status-report/ http://energyinformative.org/non-renewable-energy-resources/ (E.T: 14.03.18).

ROSATOM, Benefits of Nuclear Energy: http://www.rusatom-overseas.com/nuclear-energy/benefits-of-nuclear-energy/ (15.03.18).

SCO, SCO Responds to Cyber Challenges, 09.06.2011: http://infoshos.ru/en/?idn=8349 (E.T: 13.04.18).

STATISTA, Proposed Budget of the U.S. Government for Cyber Security in FY 2016-2017 (in billion U.S. dollars) : https://www.statista.com/statistics/675399/us-government-spending-cyber-security/ (06.04.18).

T.C. Enerji ve Tabii Kaynaklar Bakanlığı, Türkiye'nin Nükleer Santral Projeleri: Soru-Cevap Nükleer Enerji Proje Uygulama Dairesi Yayın Serisi, 11 Ocak 2016, Yayın No.1, s.24.: http://www.enerji.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FT%C3%BCrkiyenin_N%C3%BCkleer_Santral_Projeleri_Soru-Cevap.pdf (E.T: 10.03.18).

TAEK, Nükleer Enerji Alanında Üçüncü Şahıslara Karşı Hukuki Sorumluluğa ilişkin Paris Sözleşmesi'ni Yenileyen 2004 Protokolü, 2011: http://www.taek.gov.tr/attachments/article/761/908_paris_2004_tr.pdf (E.T: 19.03.18).

TAEK: http://www.taek.gov.tr/nukleerguvenlik/nukleer-enerji-%20vereaktorler/169-%20nukleer-enerji/457nukleer-%20enerji-nedir (E.T: 13.03.18).

TBMM, Türkiye Cumhuriyeti Anayasası: https://www.tbmm.gov.tr/anayasa/anayasa82.htm (E.T:20.03.18).

TEİAŞ, Türkiye Kurulu Gücünün Yıllar İtibariyle Gelişimi, https://www.teias.gov.tr/tr/i-kurulu-guc (12.03.18).

The UK Office for Nuclear Regulation, Maintenance of a Robust Security Culture, Document ID: CNS-TAST-GD-2.1 Revision 0, Record Reference: TRIM Folder 4.4.2.19072. (2017/100113), March 2017, p.4.

The US Department of Defense, the DoD Cyber Strategy, April 2015: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (E.T: 07.04.18).

THE WORLD BANK: https://elibrary.worldbank.org/doi/10.1596/978-1-4648-0153-2_ch36 (E.T:17.03.18).

Thiele, Lisa, Introduction to Nuclear Law, Canadian Nuclear Safety Commission, July 13, 2017 : http://www.nuclearsafety.gc.ca/eng/pdfs/Presentations/VP/2017/20170713-lisa-thiele-WNU-Summer-Institute-eng.pdf (16.03.18).

U.N. Secretary-General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 4, UN, Doc. A/65/201, 30 July 2010, p.7. : http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf (E.T: 13.04.18).

U.S. Department of Energy Office of Nuclear Energy, Science and Technology, The History of Nuclear Energy : https://www.energy.gov/sites/prod/files/The%20History%20of%20Nuclear%20Energy_0.pdf (E.T: 13.03.18).

UAE, Renewable Energy, https://www.iea.org/about/faqs/renewableenergy/ (E.T: 11.03.18).

UAEK: https://www.iaea.org/topics/energy (E.T: 10.03.18).

UDHB, 2016-2019 Ulusal Siber Güvenlik Stratejisi, s.9 : http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (12.04.18).

UDÖ, A.584 (14) Sayılı Kararı: http://www.imo.org/blast/blastDataHelper.asp?data_id=22374&filename=A584%2814%29.pdf (E.T: 05.04.18).

UDÖ, MSC/Circ.443 Sayılı Kararı: http://www.imo.org/en/OurWork/Security/SecDocs/Documents/Maritime%20Security/MSC.Circ.443.pdf (E.T: 05.04.18).

UN, Atomic Energy: http://www.un.org/en/sections/issues-depth/atomic-energy/ (25.03.18).

UN, Chapter VII: Action With Respect To Threats To The Peace, Breaches Of The Peace, and Acts Of Aggression, Article 51: http://www.un.org/en/sections/un-charter/chapter-vii/ (25.03.18).

UN, Comprehensive Nuclear Test Ban Treaty, United Nations Audiovisual Library of International Law, p.3. : http://legal.un.org/avl/ha/ctbt/ctbt.html (21.03.18).

UN, Conference on Disarmament, Decision on Agenda Item 1 "Nuclear Test Ban" Adopted by the Conference on Disarmament, U.N. Doc. CD/1212 (Aug. 10, 1993): http://undocs.org/CD/1212 (E.T: 21.03.18).

UN, Cybersecurity: A Global Issue Demanding a Global Approach, 12 December 2011, New York : http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html (E.T: 11.04.18).

UN, Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX), 14 December 1974 : http://hrlibrary.umn.edu/instree/GAres3314.html (E.T: 12.04.18).

UN, Evrensel İnsan Hakları Beyannamesi: http://www.un.org/en/universal-declaration-human-rights/index.html (25.03.18).

UN, Funds, Programmes, Specialized Agencies and Others : http://www.un.org/en/sections/about-un/funds-programmes-specialized-agencies-and-others/index.html (04.04.18).

UN, Half of all Countries Aware but Lacking National Plan on Cybersecurity, UN Agency Reports, 5 July 2017 : https://news.un.org/en/story/2017/07/560922-half-all-countries-aware-lacking-national-plan-cybersecurity-un-agency-reports (E.T: 13.04.18).

UN, https://treaties.un.org/doc/publication/ctc/uncharter.pdf (E.T: 15.04.18).

UN, International Convention for The Suppression of Terrorist Bombings, International Legal Materials, Vol. 37, No. 2, 1998, p. 253.

UN, International Convention on Suppression of Acts of Nuclear Terrorism, 2005: http://www.un-documents.net/icsant.htm (E.T: 18.03.18).

UN, The Human Consequences of the Chernobyl Nuclear Accident: A Strategy for Recovery, A Report Commissioned by UNDP and UNICEF with the Support of UN-OCHA and WHO, 2002, p.14.

UN, The UN, Cyberspace and International Peace & Security-Side Event-October 5th, October 7th, 2016 : https://www.un.org/disarmament/update/the-un-cyberspace-and-international-peace-security-side-event-october-5th/ (E.T: 13.04.18).

UN, The United Nations General Assembly declared 2012 as the International Year for Sustainable Energy for All, 2012: https://www.un.org/press/en/2012/ga11333.doc.htm (E.T: 11.03.18).

UN, UN Climate Summit 2014: https://www.un.org/climatechange/summit/ (E.T: 05.04.18).

UN, United Nations Convention on the Law of the Sea : http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf (E.T: 14.04.18).

UN, United Nations General Assembly Adopts Global Counter-Terrorism Strategy: https://www.un.org/counterterrorism/ctitf/en/united-nations-general-assembly-adopts-global-counter-terrorism-strategy (06.04.18).

UN, United Nations Treaties and Principles on Outer Space, United Nations, New York, 2002, p.3.

UNODA, Nuclear Weapons: https://www.un.org/disarmament/wmd/nuclear/ (E.T: 12.03.18).

UNODA, Treaty on the Non-Proliferation of Nuclear Weapons (NPT) : https://www.un.org/disarmament/wmd/nuclear/npt/ (20.03.18).

UNODA: https://www.un.org/disarmament/wmd/nuclear/ctbt/ (E.T: 21.03.18).

UNODC, International Convention for the Suppression of Terrorist Bombings (New York, 15 December 1997) : https://www.unodc.org/documents/treaties/Special/1997%20International%20Convention%20for%20the%20Suppression%20of%20Terrorist.pdf (02.04.18).

UNODC, Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation 1988 (‘Montreal Protocol’) https://www.unodc.org/pdf/crime/terrorism/Commonwealth_Chapter_5.pdf (E.T: 13.04.18).

UNOOSA, International Space Law: United Nations Instruments, United Nations, New York, May 2017, p.100.

UNOOSA, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies :

http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html (E.T: 14.03.18).

UNSC, The Security Council : http://www.un.org/en/sc/ (31.03.18).

UNTC, 9. International Convention for the Suppression of Terrorist Bombings : https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-9&chapter=18&clang=_en (02.04.18).

US BUREAU OF INTERNATIONAL SECURITY AND NONPROLIFERATION, Protocol of 2005 to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation : https://www.state.gov/t/isn/trty/81728.htm (E.T: 06.04.18).

US DEPARTMENT OF ENERGY, Second National Report for the Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management : https://www.energy.gov/em/downloads/second-national-report-joint-convention-safety-spent-fuel-management-and-safety (31.03.18).

USAF, Cyberspace Operations: Air Force Doctrine Document 3-12 15 July 2010, Incorporating Change 1, 30 November 2011, pp. 9-14.

USCC, 2015 Report to Congress of the U.S.-China Economic and Security Review Commission: Executive Summary and Recommendations, One Hundred Fourteenth Congress First Session November 2015, p. 8. : https://www.uscc.gov/sites/default/files/annual_reports/2015%20Executive%20Summary%20and%20Recommendations.pdf (E.T: 14.04.18).

USLEGAL, Jus in Bello Law and Legal Definition: https://definitions.uslegal.com/j/jus-in-bello/ (E.T: 15.04.18).

USNRC, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71, January 2010, p.6.

USNRC, Backgrounder on the Three Mile Island Accident, 2013: https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html (E.T: 16.03.18).

USOM, USOM Hakkında : https://www.usom.gov.tr/hakkimizda.html (11.04.18).

Uyar, Fatih, Enerji Kaynakları Nelerdir? Kaça Ayrılır?, Enerji Beş Temiz Enerji Portalı, 1 Ocak 2017 : http://www.enerjibes.com/enerji-kaynaklari/ (E.T: 11.03.18).

Whitman, Christine Todd, The Case in Favor of Nuclear Power, Bloomberg Businessweek, 9.12.2007: http://www.nbcnews.com/id/20730356/ns/business-us_business/t/case-favor-nuclear-power/#.WwSRAEiFNPY (15.03.18).

WHO, Health effects of the Chernobyl accident: an overview, 2006: http://www.who.int/ionizing_radiation/chernobyl/backgrounder/en/ (E.T: 16.03.18).

WISE, Chernobyl: Chronology of a Disaster, No.724, March 11, 2011, p.4: https://www.wiseinternational.org/nuclear-monitor/chernobyl-chronology-disaster (19.03.18).

WNA, Liability for Nuclear Damage: http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/liability-for-nuclear-damage.aspx (25.03.18).

WNA, The Many Uses of Nuclear Technology, 2017: http://www.world-nuclear.org/information-library/non-power-nuclear-applications/overview/the-many-uses-of-nuclear-technology.aspx (E.T: 12.03.18).

WSIS, 2003 Tunis 2005 : http://www.itu.int/net/wsis/index.html (E.T: 12.04.18).

Birleşmiş Milletler Güvenlik Konseyi ve Genel Kurul Kararları

UNGA, A/RES/1653 (XVI), 24.11.1961: https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/167/06/IMG/NR016706.pdf?OpenElement (25.03.18).

UNGA, A/RES/29/3314, 14 December 1974 : http://www.un-documents.net/a29r3314.htm (E.T: 25.04.18).

UNGA, A/RES/47/68, 14 December 1992 : http://www.un.org/documents/ga/res/47/a47r068.htm (E.T: 19.03.18).

UNGA, A/RES/49/75, 15 December 1994 : http://www.un.org/documents/ga/res/49/a49r075.htm (E.T: 15.04.18).

UNGA, A/RES/50/53, 29 January 1996 : http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/50/53 (02.04.18).

UNGA, A/RES/51/210, 17 December 1996: http://www.un.org/documents/ga/res/51/a51r210.htm (02.04.18).

UNGA, A/RES/54/49, 4 December 1998 : https://gafc-vote.un.org/UNODA/vote.nsf/958591109a21b54c05256705006e0a5c/0e4088ff35d5505d0525681200673c74?OpenDocument&ExpandSection=5 (E.T: 12.04.18).

UNGA, A/RES/58/199, 30 January 2004: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (E.T: 12.04.18).

UNGA, A/RES/58/199, 30 January 2004: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (E.T: 12.04.18).

UNGA, A/RES/58/32, 18 December 2003 : https://undocs.org/A/RES/58/32 (13.04.18).

UNGA, A/RES/58/32, 18 December 2003 : https://undocs.org/A/RES/58/32 (13.04.18).

UNGA, A/RES/59/290, 13 April 2005 : : http://www.un-documents.net/a59r290.htm (02.04.18).

UNGA, A/RES/59/290, 15 April 2005, https://treaties.un.org/doc/source/docs/A_RES_59_290-E.pdf (E.T: 26.03.18).

UNGA, A/RES/59/61, 16 December 2004 : http://undocs.org/A/RES/59/61 (13.04.18).

UNGA, A/RES/60/45, 6 January 2006 : http://undocs.org/A/RES/60/45 (13.04.18).

UNGA, A/RES/61/54, 19 December 2006 : https://undocs.org/A/RES/61/54 (13.04.18).

UNGA, A/RES/61/54, 19 December 2006 : https://undocs.org/A/RES/61/54 (13.04.18).

UNGA, A/RES/62/17, 8 January 2008 : https://undocs.org/A/RES/62/17 (13.04.18).

UNGA, A/RES/63/37, 9 January 2009 : https://undocs.org/A/RES/63/37 (13.04.18).

UNGA, A/RES/64/211, 17 March 2010 : https://undocs.org/A/RES/64/211 (13.04.18).

UNGA, A/RES/64/25, 14 January 2010 : https://undocs.org/A/RES/64/25 (13.04.18).

UNGA, A/RES/67/97, 14 January 2013 : http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/67/97 (E.T: 19.03.18).

UNSC, https://www.un.org/sc/ctc/resources/databases/recommended-international-practices-codes-and-standards/united-nations-security-council-resolution-1373-2001/ (01.04.18).

UNSC, https://www.unodc.org/documents/treaties/Special/1997%20International%20Convention%20for%20the%20Suppression%20of%20Terrorist.pdf (02.04.18).

Uluslararası Adalet Divanı Kararları/Görüşleri

ICJ, Case Concerning Military and Paramilitary Activities in and Against Nicaragua, Judgement of 27 June 1986, p. 93. : http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (E.T: 12.04.18).

ICJ, Legality of the Threat or Use of Nuclear Weapons : http://www.icj-cij.org/en/case/95 (25.03.18).

ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, July 8, 1996, ICJ Rep. 1996, p. 226: http://www.icj-cij.org (25.03.18).

ICJ, Legality Of The Threat Or Use Of Nuclear Weapons, Reports Of Judgments, Advisory Opinions And Orders, 8 July 1996, pp.43-45.

ICJ, Reports Of Judgments, Advisory Opinions and Orders Legality of the Threat or Use of Nuclear Weapons, 1996 : http://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf (E.T: 18.04.18).

Resmi Gazete ve Avrupa Birliği Resmi Gazete Kaynakları

5710 Nükleer Güç Santrallarının Kurulması ve İşletilmesi ile Enerji Satışına İlişkin Kanun, 21.11.2007, Resmi Gazete, Sayı: 26707 Sayılı Resmî Gazete : http://www.resmigazete.gov.tr/eskiler/2007/11/20071121.htm (19.03.18).

Elektrik Piyasası Kanunu, Resmî Gazete, 30.03.2013, Sayı: 28603 : http://www.resmigazete.gov.tr/eskiler/2013/03/20130330-14.htm (12.03.18).

EURATOM ve ABD Arasındaki Nükleer Enerji'nin İnsani Amaçla Kullanılması Anlaşması, 20 Mayıs 1996, Avrupa Birliği Resmi Gazetesi, Sayı: L 120 : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:21996A0520(01)&from=EN (E.T: 20.03.18).

Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, Resmi Gazete, 11.03.13, Sayı: 28818 : http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm (E.T: 12.04.18).

Türkiye Atom Enerjisi Kurumu Kanunu, 13.07.1982, Resmi Gazete, Sayı:17753: http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/arsiv/17753.pdf&main=http://www.resmigazete.gov.tr/arsiv/17753.pdf (19.03.18).

Türkiye Cumhuriyeti Hükümeti İle Rusya Federasyonu Hükümeti Arasında Türkiye Cumhuriyetinde Akkuyu Sahasında Bir Nükleer Güç Santralinin Tesisine ve İşletimine Dair İşbirliğine İlişkin Anlaşmanın Onaylanmasının Uygun Bulunduğu Hakkında Kanun, 21.7.2010, Sayı: 27648 : http://www.resmigazete.gov.tr/eskiler/2010/07/20100721-34.htm (20.03.18).

Yüksek Lisans Kaynakları

Bills, Amanda, Cyber Warfare and Jus in Bello – The Regulation of Cyber 'Attacks' under International Humanitarian Law, Lund University, Yayınlanmamış Yüksek Lisans Tezi, s. 15-17.

Norouzi, Shiva, Uluslararası Hukukta Nükleer Programlar: İran Örneği, İstanbul Üniversitesi, Yayınlanmamış Yüksek Lisans Tezi, 2017, s. 6.

Reed, Samuel Thomas, The Nuclear Terrorism Disconnect : Electoral Incentives and U.S. Policy Responses, University of British Columbia, Yayınlanmamış Yüksek Lisans Tezi, 2013, s.18.

Sklerov, Lieutenant Matthew J., Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty To Prevent, The Judge Advocate General's School, United States Army, Yayınlanmamış Yüksek Lisans Tezi, 2009, s.86.

Valo, Janne., Cyber Attacks and the Use of Force in International Law, University of Helsinki, Yayınlanmamış Yüksek Lisans tezi, 2014, p.5.

Doktora Tezi Kaynakları

Gibson, A., The End, or Life in The Nuclear Age: Aesthetic Form and Modes Of Subjectivity, University of Minnesota, Yayınlanmamış Doktora Tezi, 2012, s. 1.

Kano, Chizu., Behavioral Change For Energy Conservation : Case Study of Post-Fukushima Experience İn Japan, Uppsala University, Yayınlanmamış Doktora Tezi , 2013, s.1.

Kilinc Ata, N., An Exploration of Renewable Energy Policies with an Econometric Approach, University of Stirling, Yayınlanmamış Doktora Tezi, 2015, s.14.

Lee, C. [**李卓穎**], 发展可再生能源行业的风险管理和投资战略。[Development of Risk Management and Investment Strategies in Renewable Energy Industry] , University of Hong Kong, Pokfulam, Hong Kong SAR, Yayınlanmamış Doktora Tezi, 2016, s.1.

Qasaymeh, K. A., South Africa's Peaceful Use of Nuclear Energy under the Nuclear Non-Proliferation Treaty and Related Treaties, University of South Africa, Yayınlanmamış Doktora Tezi, 2014, s.1.

Qasaymeh, Khaled Ahmed, South Africa's Peaceful Use of Nuclear Energy Under The Nuclear Non-Proliferation Treaty and Related Treaties, University Of South Africa, Yayınlanmamış Doktora Tezi, 2014. s. 39.

Sanchez, Victoria Justine, Radioactive Reversal?: The Fukushima Accident As A Focusing Event For Comparative Policy Change On Nuclear Energy, University of Delaware, Yayınlanmamış Doktora Tezi, 2017, s.4.

Särkikoski, T., Rauhan Atomi, Sodan Koodi : Suomalaisen Atomivoimaratkaisun Teknopolitiikka 1955-1970 [Peace Atom, War Code: Finnish Nuclear Atomic Solution Technology Policy 1955-1970], University of Helsinki, Yayınlanmamış Doktora Tezi, 2011, s. 4.

EKLER

EK 1: SOMUT NÜKLEER TERÖRİZM SENARYOLARI

SENARYO NUMARASI	SENARYO KONUSU	SENARYO/KURGU
1	**Nükleer Silahlı Terör Saldırısı**	Sabahın erken saatlerinde karanlık, sessiz saatlerde, kamufle teröristler, Belarus'ta kötü korunmuş bir nükleer araştırma reaktörüne sızdığını varsayılmıştır. Santralin içinde çalışanlar tarafından desteklenerek, teröristler elli kilogramdan oluşan zenginleştirilmiş uranyumu, nükleer bir cihaz için ihtiyaç duyulan el yapımı ham maddeyi çalmıştır. Makine araçları, kimyasallar, bomba tasarımları ve eski Sovyet bölgesinden uzakta kalan bir nükleer silah uzmanı ile donatılmış güvenli bir eve, yani bir terörist grubun nükleer enerjiye dönüştürülmesi için gerekli olan tüm malzemelere yönelmiştirler ve en sonunda amaçlarına ulaşmışlardır.
2	**Kirli Bomba (Dirty Bombs) ile Terör Saldırı**	Aynı şekilde yine bir terörist grup, içeriden yardım alarak, endüstriyel veya tıbbi bir tesisden tehlikeli miktarda sezyum-137 elde etmiştir. Teröristler, toz haline getirilmiş sezyum kloriti kirli bir bombayla birleştirmek için konvansiyonel patlayıcılar kullanmışlardır. Büyük bir metropolitan bölgenin finans bölgesindeki kirli bombayı patlatıp sezyum izotopunu altmış metrekarelik bir alana yaymışlardır. Patlamada birkaç düzine insan

		öldürülmüştür ve milyonlarca kişi şehri panik içinde tahliye etmiştir. Milyarlarca dolar gayrimenkulün yaşanmaz olduğu ilan edilmiştir. Bu durumda temizlemenin yıllarca ve daha pahalıya mal olduğu aşikâr olacaktır.
3	**Yanlışlıkla veya Yetkisiz Nükleer Füze Hava Saldırısı**	Rusya ve ABD arasındaki ilişki bozulmuştur. Eski rekabet ve şüpheler yeniden canlanmıştır. Rus Stratejik Roket Kuvvetleri'nin başkanı, gerginlikler arttıkça Rus devlet başkanına, Moskova'ya yönelik bir Amerikan nükleer füzesinin harekete geçtiğini tespit ettiklerini bildirmiştir. Ancak, Rus uyarı sistemi aşınmış olduğundan, alarmın yanlış olup olmadığını veya daha büyük bir saldırı olup olmadığını doğrulayamamıştırlar. Kargaşa, yanlış olan bilgilere dayanarak bir sonraki eylemi belirlemeye çalıştıkça ortaya çıkmıştır. Ancak artık çok geçtir ve nükleer bomba patlamıştır.
4	**Nükleer Silahlı Devlet Sayısında Keskin Bir Artış**	Kuzey Kore, harcanan nükleer yakıtını silah sınıfı plütonyuma dönüştürmeye devam etmektedir ve nükleer silah üretmektedir. Komünist rejim, 1998'de Hindistan ve Pakistan'ın yaptığı gibi bir silahı test etmektedir. Japonya ve Güney Kore'deki milliyetçiler, hükümetlerini nükleer olmayan statülerinden vazgeçmeye ve kendi cephaneliklerini geliştirmeye zorlamaktadır. Buna karşılık Çin, kendi nükleer programını genişletmektedir ve ABD ve Rusya ile birlikte silahlarını yüksek teyakkuz durumuna çekmiştir. Kuzey Kore'nin yaklaşımını inceleyen İran, birçok nükleer silah üretmek için yeterince

zenginleştirilmiş uranyum geliştirene kadar kedi ve fare oynamaya devam etmektedir. İran ve Kuzey Kore nükleer devletler haline geldikçe, diğer ülkeler seçeneklerini yeniden gözden geçirmektedirler. Bu süre zarfında, Mısır, Güney Kore, Japonya, Suudi Arabistan, Brezilya, Arjantin ve Endonezya, nükleer güçler haline gelmiştir ve nükleer enerji, teröristler elinde nükleer kazalar için daha yüksek bir ihtimal sunmaktadır.

EK 2: NÜKLEER ENERJİ PROGRAMI UYGULAMA OPERATÖRÜNÜN SORUMLULUK VE DEĞERLENDİRME KRİTERLERİ (Faz 1)

KAVRAM	AÇIKLAMA/TANIM
Ulusal pozisyon	Böyle bir programda var olan uzun vadeli taahhütlerin kapsamlı bir şekilde anlaşılmasına dayanan bir nükleer enerji programını üstlenir (veya üstlenmemeyi) ulusal bir karar için bir öneri sunar.
Nükleer güvenlik	Uzun süreli güvenliğin, bir nükleer tesisin tasarım, imalat, inşaat, işletme ve bakımı, kullanılmış yakıt ve atık yönetimi için hizmet dışı bırakma ve taahhütler ile ilgili tüm faaliyetlerin hayati bir parçası olduğunu ve bunun en iyi şekilde gerçekleştirildiğini açıkça ilgili tüm organizasyonlarda güçlü bir güvenlik kültürünün teşvik edilmesini vurgular.
Yönetim	Nükleer enerji programı ile ilgili her kurumda ihtiyaç duyulan yönetim uzmanlığının kapsamı ve derinliği ile bu uzmanlığı elde etme veya geliştirme stratejisini açık bir şekilde belirtir. Potansiyel sahibinin / operatör kuruluşunun formunu tanımlar ve yeteneklerini oluşturmaya yardımcı olur. Nükleer enerji programı ile ilgili her kuruluşun belirli sorumlulukları üzerine tahsisler için önerilerde bulunur.
Fonlama ve Finansman	İlgili kamu kurumlarının (düzenleyici kurum gibi) gelişmesini finanse etmek ve hizmet dışı bırakma ve atık yönetimi de dâhil olmak üzere belirli nükleer santral projelerini finanse etmek için bir strateji tasarlanır. Strateji, kamu finansmanı da dâhil olmak üzere, nükleer santral projesinin kendisine destek olmak için hükümet finansmanını da içerebilir.
Yasama Çerçevesi	Bir nükleer enerji programını desteklemek ve

	uygulamak için gerekli olan uluslararası hukuk araçlarını da içeren tüm mevzuatı belirlemek ve taslak hazırlama ve yürürlüğe koyma stratejisidir.
Koruma Önlemleri	Kapsamlı bir dizi önlemler anlaşmasının (CSA) UAEA ve nükleer malzemenin gerekli makamlarla birlikte denetlenmesi ve kontrolü (SSAC) için bir Devlet sisteminin kurulmasını kapsayan bir plan sağlar. Ulusal mevzuat, politikalar ve korunmalarla ilgili prosedürlerin hazırlanması ve uygulanmasını kapsayan bir plan oluşturur.
Düzenleyici yapı	Bağımsız ve etkili bir nükleer düzenleyici kurumun temel unsurlarını tanımlamak, geliştirmek ve finanse etmek için bir strateji geliştirir.
Radyasyon koruması	Tüm nükleer faaliyetler için kapsamlı bir radyasyondan korunma programının temel unsurlarını ve bunların her bir organizasyonda uygulanması için bir strateji tanımlar.
İnsan kaynakları geliştirme	Bir nükleer enerji programı için gereken çoklu disiplinlerin bilgi, beceri ve tutumlarını ve ihtiyaç duyulan personeli elde etme ve sürdürme stratejisini açıklar.
Paydaş katılımı	Ülkede nükleer enerjinin uygulanmasına ilişkin görüş anketleri yürütmek ve belirlenen paydaşlarla sürekli eğitim ve istişare planlarını yapar.
Site ve destekleyici tesisler	Potansiyel alanları ve nükleer tesislerin inşası ve işletilmesi için uygunluğunun ön değerlendirmesini belirlenmesidir.
Çevresel koruma	Nükleer enerji, mevcut çevre yasa ve yönetmeliklerinin değerlendirilmesi ve uygun revizyon için bir strateji için gerekli olan ek çevresel hususları değerlendirir.

Acil durum planlaması	Nükleer tesisler için acil durum planlamasının temel unsurlarını ve her kurumun ve örgütlerin bireysel rolünü tanımlar.
Güvenlik ve fiziksel koruma	Güvenlik ve fiziksel koruma programlarının temel unsurlarını tanımlar ve bu programlar için bir geliştirme stratejisi sağlar.
Nükleer yakıt döngüsü	Gerçekçi nükleer yakıt döngüsü planlarını tamamlamak için gerekli olan uzun vadeli nükleer yakıt döngüsü taahhütlerini sağlar. Çeşitli yakıt döngüsünü dikkate alarak, doğal kaynakların mevcudiyeti, kullanılmış yakıtın geçici depolanması ve kullanılmış yakıtın daha uzun süreli depolanması dâhil olmak üzere, nükleer yakıt döngüsünün bireysel adımlarında güvenli bir yakıt tedariği ve uygun ulusal katılımın sağlanması için strateji geliştirme seçenekleri sunar.
Radyoaktif atık	Düşük ve orta seviye atıkların elleçlenmesi ve bertaraf edilmesi için mevcut kapasitelerin bir değerlendirmesini, nükleer tesis işletimiyle ilişkili ek hacmi ele alma stratejisini ve yüksek seviyeli nükleer atıkların veya kullanılmış yakıtların nihai bertarafına yönelik yaklaşımı belirleme stratejisini gerçekleştirir.
Endüstriyel katılım	Yerel sanayi kabiliyetinin değerlendirmesini ve planlanan nükleer santral projeleri için sanayi katılımının istenen düzeyde yerelleşmesini veya desteklenmesini geliştirmek için strateji yürütür.
Tedarik	Yabancı tedarikçilerle yapılan ikili anlaşmaların gerekliliğini ve hem uluslararası hem de yerel tedarikçiler için kalite gerekliliklerini göz önünde bulundurarak, nükleer santral projesini desteklemek için ekipman ve hizmetleri temin etmek için bir

	strateji tasarlar.

EK 3: NÜKLEER ENERJİ PROGRAMI UYGULAMA OPERATÖRÜN SORUMLULUK VE DEĞERLENDİRME KRİTERLERİ (Faz 2)

KAVRAM	AÇIKLAMA/TANIM
Ulusal pozisyon	Diğerlerinin yanı sıra, gerekli yasaları ve uluslararası anlaşmaları uygulamak, uzun vadeli sorunlar ve bağımsız düzenleyici kurum için politikalar ve sorumluluklar oluşturmak ve nükleer altyapı gelişimini finanse etmek ve desteklemek için hükümet faaliyetlerini koordine eder. Teknolojik strateji geliştirme ve etkilenen kuruluşlar arasındaki etkileri koordine eder.
Nükleer güvenlik	Nükleer güvenliğe ilişkin sorumlulukların açık bir şekilde oluşturulmasını ve tüm katılımcı kuruluşların güvenlik sorumluluklarının farkında olduklarını ve ilgili tüm kurumlarda uygun bir kültür ve faaliyetlerin kurulmasını teşvik etmelerini sağlamaya çalışır.
Yönetim	Tanıtım, operasyonel, gözetim ve destek faaliyetlerini koordine etmek ve bağımsız düzenleyici kurumun oluşturulmasını ve görevlendirilmesini izler ve sahibi / işletici kuruluş, tekliflere ve lisans prosedürlerine hazırlanma sürecini yönetir.
Fonlama ve Finansman	Altyapı geliştirmek üzere yeterli finansmanı teşvik etmek için hükümet ile mal sahibi / işletmeci arasında ilk nükleer santral için gerçekçi bir finansman planı geliştirmeye çalışır.
Yasama Çerçevesi	Ülkenin kapsamlı bir yasal çerçeveyi uygulamaya yönelik sürecini izler.
Koruma Önlemleri	İlgili iştirak düzenlemelerine sahip bir CSA'nın UAEA ile yürürlükte olduğunu onaylar. Bir

	SSAC'nin kurulduğunu ve bu konuyla ilgili erken güvencelerin UAEA'ya sağlandığını onaylar.
Düzenleyici yapı	Bağımsız düzenleyici kurumun kurulduğunu ve görevlendirildiğini, uygun düzenlemeleri, kodları ve standartları içeren bir lisanslama süreci geliştirdiğini doğrular ve siteleri ve reaktör tasarımlarını gözden geçirip lisanslamaya hazır olduğunu onaylar.
Radyasyon koruması	Hükümet, düzenleyici kurum ve resmi radyasyon koruma programlarının sahibi / işletmecisi tarafından yürürlükteki kanun, yönetmelik ve programların geliştirilmesini ve uygulanmasını onaylar.
Güç Şebekesi	Bir nükleer santralin kurulması için şebeke sahibi ve / veya sahibi / işletmecisi tarafından gerekli planların, programların ve şebeke iyileştirmelerinin finansmanı onaylar.
İnsan kaynakları geliştirme	Tüm kuruluşların işlevlerini yerine getirmek için gerekli insan kaynağını elde ettiklerini ve ülkenin nükleer santralinin ve ilgili nükleer faaliyetlerin inşaat, işletme, bakım ve desteği ile ilgili planlarla tutarlı olarak insan kaynaklarını geliştirmek, muhafaza etmek ve değiştirmek için program ve planların yürürlükte olduğunu doğrular.
Paydaş katılımı	Hükümetin, düzenleyici kurumun ve mal sahibi / operatörün nükleer enerji programı geliştirme sürecindeki tüm uygun adımlarda halk eğitimi ve paydaş katılımı için programlar geliştirdiğini ve uyguladıklarını doğrular.
Site ve destekleyici tesisler	Sahibin / operatörün bir veya daha fazla uygun siteyi tanımladığını, güvenliğini sağladığını ve nitelendirdiğini ve site özelliklerinin teklif özelliklerine dâhil edildiğini onaylar.

Çevresel koruma	Çevre kanunundaki iyileştirmelerin yapıldığını ve çevre onayı ve gözetimi için sorumlulukların resmi olarak tayin edildiğini onaylar.
Acil durum planlaması	Hükümetin gerekli yasaları çıkardığını, düzenleyici kurumun düzenlemeleri geliştirdiğini ve mal sahibinin / işletmecisinin yerel ve ulusal makamlarla uygun acil durum planlarını ve protokollerini geliştirdiğini doğrular.
Güvenlik ve fiziksel koruma	Tüm nükleer malzeme ve tesislerin güvenliği ve korunması için hükümet, düzenleyici kurum ve mal sahibi / işletmeci tarafından uygun yasaların, yönetmeliklerin, protokollerin ve programların oluşturulduğunu onaylar.
Nükleer yakıt döngüsü	Nükleer yakıt döngüsü planlaması ve stratejisinin, yakıt döngüsünün tüm kısımlarını kapsadığını, nükleer yakıt ve yakıt hizmetlerinin güvenli bir şekilde tedarik edilmesine yönelik stratejiler de dahil olmak üzere ve yerinde harcanan yakıt depolama kapasitesinin geliştirildiğini ve sahibi / operatör nükleer santral teklif talebini onaylar. Santral yapım programı ve ulusal nükleer silahların yayılmasını önleme taahhütleriyle uyumlu yakıt döngüsü tesisleri teklif ve inşa etmek için entegre bir planın varlığını doğrular.
Radyoaktif atık	Düşük seviyeli atık (LLW) ve orta düzey atıkların (ILW) elleçlenmesi, taşınması ve depolanması için uygun yasaların, yönetmeliklerin ve tesislerin yerinde veya planlanmış olduğunu doğrular. Buna ek olarak, hükümete üst düzey atıkların (HLW) ve kullanılmış yakıtın nihai olarak bertaraf edilmesi konusunda strateji ve politikalar geliştirmesine

	yardımcı olur.
Endüstriyel katılım	Ülke sahibi / işletmeci, düzenleyici kurum ve belirlenmiş sektörlerin, 1. fazda geliştirilen ülke politikaları ile öngörülen endüstriyel katılımı geliştirmede işbirliği yaptığını onaylar.
Tedarik	Sahibinin / operatörün, 1. fazda geliştirilen ülke politikaları ile tutarlı olarak nükleer santral işletimini ve bakımını desteklemek için ekipman ve hizmet alımları için resmi planlar geliştirdiğini doğrular.

EK 4: BELİRLİ BİR TESİS İÇİN DÜZENLEYİCİ KURULUŞ TARAFINDAN ÜRETİLEN BELGELER

Lisans Belgesi

Yetkilendirme süreci (bkz. 2.2), düzenleyici sistemin yasal çerçevesini (yasa ve yönetmelikler) düzenleyici sistemden etkilenen ana tarafların (düzenleyici kurum ve operatör) sorumlulukları ile ilişkilendiren başlıca mekanizmadır. Nükleer tesis için düzenlemelerin başlıca amacı, nükleer programa dâhil olan kişiler, faaliyetler ve tesisler için geçerli olan teknik ve idari gereklilikleri tesis etmektir. Bu tür düzenlemeler, lisanslara dâhil edilen daha ayrıntılı gereksinimlere temel oluşturur. Ruhsat, zorunlu olmayan teknik kılavuzlara veya endüstriyel standartlara kısmen veya bir bütün olarak atıfta bulunarak, bunları zorunlu hale getirebilir. Lisans, doğrudan veya referans olarak, bu faaliyetlerin güvenli performansını yöneten koşulları oluşturur.

Lisans formatı

Lisansın formatı, yetki sürecinin belirli bir aşaması için ulusal yasal prosedürlere uygun olarak düzenleyici kurumun gerekli gördüğü yetki ve şartların içeriğine bağlıdır. Örneğin, lisans, temel belgelere atıfta bulunabilir ve yalnızca başka bir yerde tarif edilmemiş olan temel terimleri tanımlamak için gerekli olan malzemeleri sağlayabilir. Dolayısıyla, bir lisansın biçimi sadece ülkeler arasında değil, aynı zamanda bir ülke içinde, aşamadan aşamaya ve lisanstan lisans verilen bir aşama için de değişecektir. Lisans aşağıdaki gibi bilgiler içermektedir:

Yasal otorite: Lisans, dayanağı olan yasa ve yönetmeliklere açıkça atıfta bulunur.
Düzenleyen otorite: Lisans, lisansı vermek için yasa veya yönetmelikle yetkilendirilen kişilerin resmi isimlerini belirler; lisansı üzerinde imzası ve kaşesi bulunacak olan ve operatörün lisans şartlarına göre hesap vereceği kanaatindedir.
İhtiyaçların yerine getirilmesi: Ruhsat, ruhsat verme yasası kapsamında tüm yasal ve teknik gerekliliklerin yerine getirildiği ve önerilen faaliyetlerin işçiler, kamu

veya çevre için aşırı radyolojik risk olmaksızın gerçekleştirilebileceği bir özet beyanı içermektedir.

Belge tabanı: Lisans, başvuruyu desteklemek için operatör tarafından sağlanan belgeleri ve gözden geçirme ve değerlendirme süreci sırasında düzenleyici personel tarafından geliştirilen ve lisansın verilmesine temel oluşturan belgeleri tanımlar.

Diğer lisanslarla ilişki: Lisans, önceden izin verilip verilmediğini veya gelecekteki bir izin için ön şart olup olmadığını gösterir.

Operatör: Lisans, lisanslı faaliyet için yasal olarak sorumlu olan ve tesisin günlük kontrolünde bulunan kişi veya kuruluşun kesin bir kimliğini içerir.

İzin süresi: Ruhsat, geçerli bir yetkilendirme tarihini belirtir. Aynı zamanda, örneğin, sabit bir terminale dayandırılabilen bir sonlandırma tarihi de içerebilir. Alternatif olarak, lisanslama kararının altında yatan varsayımların geçerli kalacağı ve sonunda lisanslama için temelin yeniden gözden geçirileceği bir dönem belirtilecektir.

Lisanslı faaliyet: Lisans, nükleer tesis, yeri ve yetkili faaliyeti yeterli derecede kesin bir şekilde açıklar.

İşletmecinin uyumluluk sorumluluğu: Lisans, İşletmecinin, lisansta atıfta bulunulan veya yer alan veya başka bir şekilde uygulanabilecek yasal şartlara, yönetmeliklere ve koşullara uygunluğundan sorumlu olduğu konusunda uygun bir beyan içermektedir. Lisans ayrıca bu sorumluluğun devredilemeyeceğini belirtmelidir.

Lisans koşulları

Lisans, düzenleyici kurum tarafından belirlenen ve başvuru sahibinin uymak zorunda olduğu yükümlülükleri açıkça belirttiği gibi, referans veya eki tarafından dayatır. Ruhsat ile ilgili kanun ve uygulamalar devletlere göre değişiklik göstermektedir. Bazı devletler Kanun'da ve düzenleyici kurumun yönetmeliklerinde yalnızca Lisans'a atıfta bulunurken, diğer devletler Lisans'da açıkça veya bazı koşullar içerdiğine dair koşulları belirtmektedir.

Lisans koşulları, etkili düzenleyici kontrolün sağlanması için nükleer tesislerin yerleşimini, inşasını, işletmeye alınmasını, işletilmesini ve hizmet dışı bırakılmasını veya kapatılmasını etkileyen tüm güvenlikle ilgili gereklilikleri uygun şekilde kapsamaktadır. Bunlar aşağıdaki gibi önemli yönleri içerir: tasarım gereksinimleri; radyolojik koruma; acil Durum prosedürleri; modifikasyonlar; kalite güvencesi; operasyonel sınırlar ve koşullar; işlemler; ve personelin yetkilendirilmesi.

Koşullar format olarak değişebilirken, koşulları anlaşılabilir ve etkili kılmak için koşulların niteliğini belirleyen bazı temel nitelikler vardır. Her koşul, bir kişinin yerine getirilmesinin diğerinin yerine getirilmesi veya başka herhangi bir yasal zorunluluk ile çelişmemesi bakımından diğer tüm koşullarla tutarlıdır. Koşulları teknik sınırlar ve eşikleri belirleyen koşullar, prosedürleri ve çalışma şekillerini belirten koşullar, idari hususlarla ilgili koşullar, denetim ve uygulama gerekliliklerine ilişkin koşullar ve bunlara yanıtla ilgili koşullar gibi koşulları mantıksal tiplere gruplamak yararlı olabilir.

Aşağıdaki tablo genel ve aşamalı özel lisans koşullarının örneklerini sunar.

Genel ve Aşamalı Özel Lisans Koşulları Örnekleri.

Genel lisans koşulları aşağıdaki unsurları içermektedir:
• Operatör, düzenleyici kurumun yetkili temsilcilerini, operatörün kontrolü altındaki personel, tesisler ve kayıtlara tam erişim ile sağlar; bu düzenlemeler, uygunluğu belirlemek ve güvenliği değerlendirmek için gerçekleştirilir. • Operatör, düzenleyici kurumun, önemli veya potansiyel olarak önemli olaylar ya da lisansın dayandığı hususlar, bilgiler, varsayımlar veya beklentilerdeki değişikliklerle ilgili olarak tam ve sürekli bilgilendirilmesini sağlar. • Operatör, düzenleyici kurumun güvenlik çıkarları için talep edebileceği düzeltici önlemleri veya önlemleri alır. • Operatör, faaliyetlerini, düzenleyici kurumun önceden onayı olmaksızın, lisansa özel olarak yetki verilmiş olanların ötesine genişletmez. • İşletmeci, başvurularda başvurulanlar dahil olmak üzere düzenleyici kurum, tesisin güvenliği ile ilgili yasalar, yönetmelikler ve lisansın gerektirdiği tüm güvenlik kayıtlarını geliştirmekte, muhafaza etmekte, güncellemekte ve sürdürmektedir. • Operatör, faaliyetlerini, her adımın emniyete uygun olarak gerçekleştirilmesini sağlamak için temel bir çerçeve sağlamak üzere, yetkilendirme sürecinin tüm aşamalarını kapsayan onaylanmış bir kalite güvence programına uygun olarak yürütmektedir. • Operatör, tesis değişikliklerini düzenleyici kurum tarafından belirlenen şartlara uygun olarak rapor etmelidir. • Operatör, düzenleyici kurumun gerektirdiği emniyetle ilgili tüm kazaları, olayları ve olayları rapor etmelidir.
Aşamaya özel lisans koşulları şu unsurları içermektedir:
Saha hazırlığı: Bir siteyi yetkilendirirken, düzenleyici kurum, işletmecinin sitenin kullanımı üzerinde kullanmak zorunda olduğu kontrolleri ve

operatörün siteyi hazırlayabilme ehliyeti, yasaların ve yönetmeliklerin izlencesinde, bir inşaat ruhsatı gerektirir.

İnşaat: İnşaatı yetkilendirirken, bu safhanın nükleer tesisin güvenli bir şekilde işletilmesini sağlayacak şekilde ilerlemesini sağlamak için gerekli olan birkaç koşul vardır. Bu koşullar şunları içermektedir:

- Nükleer tesis, düzenleyici kurum tarafından onaylanan ilgili saha parametrelerine uygun olarak tasarlanmış ve inşa edilmiştir.
- Nükleer tesis, düzenleyici kurum tarafından onaylanmış tasarıma uygun olarak inşa edilmiştir. Operatör, onaylanmış tasarımdan, düzenleyici kurumun önceden onayı olmadan güvenliği etkileyebilecek herhangi bir şekilde sapmaz.
- Operatör, uygun bir zemin araştırması da dahil olmak üzere bölgenin ön-radyolojik çalışmasını başlatır.

Ayrıca, inşaatın yetkilendirilmesi sırasında, nükleer tesisin belirli bölümlerinin tasarımına ilişkin düzenleyici kuruluştan ek onay almasını gerektiren operatöre şartlar getirilebilir.

Hizmete alma: Nükleer tesisin işletmeye alınmasına yetki verirken, düzenleyici kurum aşağıdakileri de içeren bir dizi koşulu belirler:

- Hizmete alma, düzenleyici kurum tarafından onaylanmış bir programa uygun olarak gerçekleştirilir.
- Güvenlik için önemli olan tamamlanmış yapılar, sistemler ve bileşenler, lisans koşullarına uygun olarak denetlenmiş, test edilmiş ve onaylanıncaya kadar hizmete sunulmamıştır.
- Operatör, nükleer materyaller için onaylanmış depolama tesisleri sağlar. Düzenleyici kurum, nükleer malzemenin tesise getirilmesinden önce etkili olması için uygun fiziksel güvenlik önlemleri talep edebilir.
- Kısmi veya radyoaktif malzeme, yasal izin olmaksızın siteye getirilmez.

- Bölünmüş ve radyoaktif malzemenin tesise girmesiyle birlikte, işletmeci, yalnızca yetkili personelin denetim ve gözetimi altında, düzenleyici kurum tarafından onaylanan işletim limitleri ve koşullarına uygun olarak yazılı prosedürleri kullanarak işletir. Bu sınırlar ve şartlarda yapılan herhangi bir değişiklik, düzenleyici kurumun önceden onayını almıştır.
- İşletmeci, acil durum hazırlığına katılan diğer yetkililerle koordine edilmiş onaylanmış bir acil durum planına sahiptir.

Operasyon: Rutin Operasyonda yetkilendirmede, işletmeye alma sırasında getirilen koşullar, faaliyete geçirme sonuçları ışığında uygun şekilde değiştirilir. Düzenleyici kurum, gerekli görüldüğü takdirde, bu lisansa aşağıdaki gibi koşullar ekler:

- Operatör, tesisi düzenleyici kurum tarafından yetki verilen maksimum kapasite seviyesinden fazla çalıştırmaz.
- İşletmeci, düzenleyici kurum tarafından önceden onay alınmaksızın, güvenlik için önemli olan onaylanmış tesisin hiçbir parçasının değiştirilmemesini sağlamak için düzenleyici kurum tarafından onaylanmış bir değişiklik prosedürüne sahiptir.
- Operatör, nükleer tesisin, denetleyici kurum tarafından onaylanmış bir zaman çizelgesine göre güvenlik için önemli yapılar, bileşenler ve sistemler için belirtildiği şekilde gerçekleştirilmesi için hizmet içi denetim ve testlere tabi tutulmasını sağlar.
- Operatör, güvenlikle ilgili ekipman ve sistemlerin bakımının düzenleyici kurum tarafından onaylanan bir programa uygun olarak yapılmasını sağlar.
- Düzenleyici kurum tarafından onaylanmış düzenlemeler, çizelgeler, prosedürler veya kurallarda, aynı kuruluş tarafından önceden onay verilmeden değişiklikler yapılmaz.
- Operatör, nükleer tesisin sadece yetkili personelin kontrol ve gözetimi altında düzenleyici kurum tarafından kabul edilebilir yeterli sayıda

olmasını sağlar. Kaza durumunda operatörün sorumluluğu gibi diğer olası lisans koşulları dahil değildir.
Hizmetten Çıkarma: Bir tesisin devreden çıkarılması izin verirken lisans tesisi kapatılır veya iptal etme yaptırımı bu aşamada çok etkili olması pek mümkün değildir çünkü, düzenleyici kurum, uyum sağlamak için yasal olarak bağlayıcı gereksinimleri belirterek özellikle ilgilenir.
Kapanış: Bir atık bertaraf tesisinin kapatılmasının ardından, çevresel izleme dahil, sürekli kontrol gerekli olabilir. Ulusal mevzuata bağlı olarak, gereklilikler, operatör tarafından tutulan bir Kapanış sonrası lisans kapsamında bulunabilir veya kapanış anlaşması öncesinde ilgili bir ulusal makam tarafından sorumluluklar alınabilir.

EK 5: SİBER SUÇ KATEGORİLERİ VE ÇEŞİTLERİ

1) Bireylere Karşı Siber Suçlar

a. ***E-Posta Dolandırıcılığı (E-Mail Spoofing):*** Bu saldırı, sahte bir e-postanın bir kaynaktan yayıldığı zannedilip, başka bir kaynaktan gönderilmiş olduğu anlaşılan e-posta anlamına gelmektedir. Ayrıca e-posta dolandırıcılığı (E-Mail forging) olarak da adlandırılabilmektedir. Bu durumda saldırganın ana hedefi, kurbanın e-posta hizmetini çok sayıda e-posta göndererek engellemektir.

b.*Yemleme (Phishing)*: Yemleme, insanları paralarıyla dolandırmaya çalışmaktır. Kimlik avı, finansal kuruluşların müşterileri tarafından talep edilmemiş e-postaların alınmasından, hesaplarına erişmek için kullanıcı adlarını, şifrelerini veya diğer kişisel bilgilerini girmelerini talep etmektedir. Suçlu, daha sonra müşterinin çevrimiçi banka hesabına ve bu hesapta bulunan paralara erişebilmektedir. Müşteriler, bilgilerini girmek için e-postadaki bağlantıları tıklarlar ve böylece dolandırıcılığın gerçekleştiğinden habersiz kalmaktadırlar.

c. İstenmeyen Posta (Spamming): İstenmeyen toplu iletileri göndermek üzere elektronik mesajlaşma sisteminin kötüye kullanılması anlamına gelmektedir.

d. Siber Karalama (Cyber Defamation): Kişinin haysiyetini / imajını düşürmek ve posta hesaplarını ele geçirerek bilinmeyen kişilerin posta hesabına kaba dil kullanarak bazı postalar göndermek suretiyle herhangi bir kişiyi karalamaya yönelik bir saldırı türünü kapsamaktadır.

e. ***Siber Takip ve Taciz (Cyber Stalking and Harassment)***: Başka bir kişi grubunu veya örgütü defalarca taciz etmek üzere interneti vasıta olarak kullanımak anlamına gelmektedir. Bu taciz, cinsel olabilmekle birlikte diğer motivasyonlara da sahip olabilmektedir.

f. *Bilgisayar Sabotajı (Computer Sabotage):* İnternetin bilgisayar sisteminin normal işleyişini durdurmak için solucanların, virüslerin veya mantıksal bombaların kullanılması yoluyla kullanılması, bilgisayar sabotajı olarak adlandırılmaktadır.

g. Kötü Amaçlı Yazılımlar (Malware): Kötü amaçlı yazılımlar, bir bilgisayar sisteminin sahibinin bilgisi veya izni olmadan sisteme zarar veren herhangi bir kişinin bilgisayarını diğer insanların aygıtlarına veya sosyal ağ profillerine sızmak için denetimini ele geçiren bir yazılımdır. Bu tür bir yazılım, bir korsan tarafından spam veya virüsleri yaymak için uzaktan kontrol edilen bilgisayarlardan oluşan bir _botnet‘ - ağ oluşturmak için de kullanılabilir.

2) Mülkiyete Karşı Siber Suçlar

a. Fikri Mülkiyet Suçları (Intellectual Property Crimes): Sahibinin tamamen veya kısmen haklarından yoksun bırakıldığı herhangi bir yasa dışı işlem suçudur. En yaygın suç türü yazılım korsanlığı, telif hakkı ihlali, ticari marka, bilgisayar kaynak kodu hırsızlığı, vb.dir.

b. Siber Ganimet (Cyber Squatting): Aynı Alan Adı için hak talebinde bulunduklarını iddia ederek bir üründe hak sahibi etmektedir. Örneğin iki benzer isim yani www.yahoo.com ve www.yahhoo.com gibi…

c. Siber Vandalizm (Cyber Vandalism): Vandalizm, bir kişinin diğer bir kişinin malına zarar vermek anlamına gelmektedir. Böylece siber vandalizm, bir ağ hizmeti durduğunda veya bozulduğunda bilgisayarda saklanan veriyi veya bilgiyi yok etmek veya zarar vermek anlamına gelmektedir.

d. Bilgisayar Sisteminin Hacklenmesi (Hacking Computer System): Basit terimlerle korsanlık, bir bilgisayar sistemine ve / veya ağa bir 'yasadışı izinsiz giriş' anlamına gelmektedir. Hackleme saldırıları, Facebook, Twitter, blog platformu gibi ünlü sosyal ağ sitelerini bilgisayar üzerinden yetkisiz erişim /

kontrol ile ele geçirilmesini içermektedir. Hack etkinliğinden dolayı bilgisayar sisteminin yanı sıra veri kaybı da olmaktadır. Ayrıca özellikle araştırmalar, bu saldırıların esas olarak finansal kazanç amaçlı olmadığını ve belirli bir kişinin ya da şirketin itibarını azaltmadığını göstermektedir.

e. Yetkisiz Bir Şekilde Değişim Yapmak (Altering in an Unauthorized Way): Bu saldırı türü, çok az teknik uzmanlık gerektirmektedir ve çalışanların girmeden veya yanlış veri girmeden önce verileri değiştirerek veya yetkisiz talimatlar girerek veya yetkisiz işlemler kullanarak çalışanların çaldığı hırsızlıkların yaygın şeklidir; Genellikle yetkisiz işlemleri gizlemek için çıktıyı değiştirmek, yok etmek, bastırmak veya çalmak şelinde uygulamaları görülmektedir.

3) Örgütlere Karşı Siber Suçlar

a. Hacking (Hackleme): Bilgisayar sistemi üzerinde yetkisiz kontrol / erişim ve bilgisayar korsanlığı gibi tüm programların tamamen imha edilmesi anlamına gelir.

b. Şebeke Trafiğinin Dinlenmesi (Sniffing): Şifre hackerları, ağ kullanıcılarının siteye giriş yaptıkları sırada adını ve şifresini izleyen ve kaydeden programlardır.

c. Hizmet Engelleme Saldırısı (Denial of Service Attacks): Suç mağdurun ağının bant genişliğini arttırmaktadır. Saldırganlar genellikle banka, kredi kartı ödeme ağ geçitleri, cep telefonu ağları ve hatta kök ad sunucuları gibi yüksek profilli web sunucularında barındırılan siteyi veya hizmeti hedefler. Hizmet dışı saldırıların engellenmesi, diğer kullanıcıların kaynakları kullanamayacağı ve bu nedenle hizmet sağlandığı için kaynakları tüketecek şekilde tasarlanmıştır. Bir bilgisayar ağ ortamında, temel kaynaklar CPU, bellek ve bant genişliğidir.

d. Virüs saldırısı (Virus Attacks): Bilgisayar virüsü, çalıştırıldığında, kendi kopyalarını (muhtemelen değiştirilmiş) başka bilgisayar programlarına, veri dosyalarına veya sabit sürücünün önyükleme sektörüne ekleyerek çoğaltan kötü

amaçlı bir yazılım programıdır; Bu çoğaltma başarılı olduğunda, etkilenen alanların "enfekte" olduğu gözlemlenmektedir.

e. E-posta Bombardımanı / Posta Bombası (E-mail bombing/Mail bomb): Kurbanın e-posta hesabına veya sunucusuna çökmesi için büyük ölçekte e-posta gönderilmesi anlamına gelmektedir.

f. Salam Saldırısı (Salami Attack): Bu suçlar mali suç işlemek için kullanılır. Burada önemli olan değişiklik, tek bir teşebbüste tamamen fark edilmeden saldırının gerçekleştirilmesi ya da önemsiz kılınarak saldırının gerçekleşmesi anlamına gelmektedir. Örneğin, bir banka çalışanı, her müşterinin hesabından küçük bir miktar kesen bankaların sunucularına bir program eklemesi gibi...

g. Mantık Bombası (Logic Bomb): Mantıksal bir bomba, belirtilen koşullar mevcut olduğunda kötü amaçlı bir işlevi başlatan bir yazılım sistemine kasıtlı olarak sokulmuş bir kod parçasıdır. Örneğin, bir programcı, dosyaları şirketten sonlandırılmadan önce silmeye başlayan bir kod parçasını gizleyebilir.

h. Truva atı (Trojan Horse): Truva atları kendilerini kopyalayabilen, bilgi çalabilecek veya bilgisayar sistemine zarar verebilecek e-posta virüsleridir.

EK 6: GÜNCEL SİBER SALDIRI LİSTESİ

TREND 1: Ulus devlet siber silahları şu anda suçluların elinde olması

-Mart 2017: CIA'nin iPhone'lara, Android cihazlara ve Akıllı TV'lere nasıl sızdığını gösteren binlerce belge yayınlanmıştır.

-Nisan 2017: The Shadow Brokers tehdit grubu, en tahrip edici sürüm olduğu düşünülen Ulusal Güvenlik Ajansı (NSA) istismar ve saldırı araçlarını içeren bir döküm yayınlamıştır. Neredeyse 300 megabaytlık bir malzeme içeren sızdırılmış önbellek, Windows işletim sisteminin çoğunun sürümlerini ve ayrıca Orta Doğu'daki en büyük SWIFT hizmet sağlayıcısı olan EastNets'un hack kodlarını hedeflemiştir.

-Mayıs 2017: WannaCry fidye yazılımı eksik yazılmış, paketlenmemiş, gizlenmemiş bir 'Kill Switch' (Kilitleme) içeriyordu. Yine de, bu kötü amaçlı yazılım büyük ölçüde Shadow Brokers'ın NSA araçlarının sızmasını sağlamıştır. Sızan kod, basit bir fidye yazılımını, sayısız kamu ve sivil tesisleri etkileyen çok etkili bir küresel saldırıya neden olmuştur.

-Haziran 2017: WannaCry saldırısında açık olan aynı NSA kapasiteleri, tüm ağları ele geçiren Ukrayna örgütlerine yönelik bir saldırı olan NotPetya'da yeniden kullanıldı.

TREND 2: Reklam yazılımı ve kötü amaçlı yazılım arasındaki çizgi kaybolmaktadır ve mobil reklam botnetleri yükselmektedir.

-Fireball malware: Reklamları çalıştırmak için tasarlanmış bir tarayıcı, aynı zamanda kurbanın makinesinde herhangi bir kodu çalıştırabilir.

-**HummingWhale:** Yeni sürüm, reklam gelirlerini ele geçirmek için yeni bir taktik oluşturmuştur; Google'ın güvenliğine sızmak; Google Play'e düzinelerce uygulama yükleyebilir hale getirmiştir.

-**Judy**: Google Play'deki en büyük kötü amaçlı yazılım enfeksiyonu olabilecek otomatik tıklama reklamıdır.

-CopyCat: Yaklaşık 14 milyon Android cihazını etkileyen bir mobil kötü amaçlı yazılımdır. Hackerlar, iki ay içinde sahte reklam gelirlerinde yaklaşık 1.5 Milyon Dolar kazanabilmişlerdir.

TREND 3: Büyük siber ihlaller tüm coğrafyaları etkilemektedir.

AMERİKA

23 Şubat 2017: Araştırmacılar, web güvenlik şirketi Cloudflare'nin merkez sunucularında kritik bir güvenlik hatası bulmuşlardır. Bir arabellek hatası, Uber, 1Password ve çevrimiçi bir arkadaşlık sitesi olan OKCupid dahil olmak üzere, 3,400 web sitesinden hassas kullanıcı bilgilerinin büyük bir sızıntısına neden olmuştur.

7 Mart 2017: WikiLeaks, Merkezi İstihbarat Teşkilatı'na (CIA) ait olduğu iddia edilen 8.000'den fazla dosya ve belge yayınlamıştır. "Vault7" olarak adlandırılan yayın, web tarayıcıları, Windows, Android, Apple ürünleri ve güvenlik ürünleri de dahil olmak üzere çeşitli platformlar için düzinelerce açıktan yararlanma ve güvenlik açıkları içermekteydi. Sızıntı ayrıca, CIA tarafından kullanıldığı iddia edilen uygulama ve yöntemler hakkında ayrıntılı bilgi içermektedir.

7 Nisan 2017: Kimliği tespit edilemeyen bilgisayar korsanları, Teksas eyaletindeki Dallas şehrinin acil durum siren sistemine sızdılar ve Cuma gecesi yaklaşık bir saat boyunca şehrin tüm 156 sirenlerini tekrar aktif hale getirmişlerdir.

14 Nisan 2017: Daha önce NSA'ya ait olduğu iddia edilen korsan araçları serbest bırakan Shadow Brokers grubu, hem Windows hem de SWIFT bankacılık sistemi için sıfır-gün güvenlik açıklarından yararlanan ek araçlar sızdırdımıştır. Bir ay sonra, küresel saldırı, bu sürümden yararlanmıştır ve Windows OS SMB EternalBlue iletişim protokolündeki bir güvenlik açığı kullanarak WannaCry ve Ransomware ile on binlerce makineden etkilenmiştir. Kurbanlar arasında hastaneler, telekomünikasyon şirketleri, otomobil üreticileri ve diğerleri bulunmaktaydı.

11 Mayıs 2017: Kaliforniya merkezli popüler bir eğitim teknolojisi şirketi olan Edmodo, öğrencilere, velilere ve öğretmenlere ait yaklaşık 77 milyon kullanıcı hesabı için kişisel verileri kaybetti. Çalınan veriler e-posta adreslerini, kullanıcı adlarını ve karma şifrelerini içermekteydi. Hackerin, karanlık bir web forumunda satış verilerini 1.000 $ karşılığında teklif ettiği bildirilmiştir.

AVRUPA, ORTA DOĞU VE AFRİKA (EMEA)

7 Ocak 2017: Almanya merkezli E-spor şirketi Turtle Entertainment GmbH'nın sahip olduğu popüler bir video oyun topluluğu olan E-Sports Entertainment Association League, 1,5 milyon kullanıcının kişisel verilerini ortaya çıkarabilecek bir sızıntıyla karşılaşmıştır.

12 Ocak 2017: Mobil adli tıp ve hacker araçları geliştirmekle tanınan bir İsrailli şirketi olan Cellebrite, 900 GB müşteri verilerinin çalınmasına yol açan bir sızıntı ile karşı karşıya kaldı.

9 Nisan 2017: İngiltere merkezli bir kredi firması olan Wonga, çoğu İngiltere'de bulunan 270.000 müşteriyi etkileyen bir sızıntı yaşadı. Wonga'ya göre, sızan veriler e-posta adreslerini, ev adreslerini, telefon numaralarını, kısmi kredi kartı numaralarını ve banka hesap numaralarını içermekteydi.

ASYA PASİFİK (APAC)

13 Şubat 2017: McDonald's India uygulaması, McDelivery, isim, e-posta adresi, telefon numarası, ev adresi ve sosyal profiller dahil olmak üzere 2.2 milyondan fazla müşterinin kişisel verilerini sızdırmıştır. McDelivery, 13 Şubat'taki meseleyi kabul etmiştir ancak 17 Mart itibarıyla sorun düzeltilmemiş ve müşteri verileri açıkta kalmaya devam etmiştir.

14 Mart 2017: Japon ödeme ödeme hizmetleri tedarikçisi olan GMO Payment Gateway, şirketin sistemindeki bir güvenlik kusurunun, müşterilerinden iki tanesinin web sitelerinden kişisel ve finansal veri sızıntısına yol açtığını doğrulamıştır: Tokyo metropol hükümeti ve Japonya Konut Finans Ajansı.

13 Nisan 2017: Bir Avustralya İnternet şirketinin DNS sunucuları büyük bir DDoS saldırısına uğradıktan sonra, yaklaşık 500.000 Avustralya web sitesine bir buçuk saat boyunca erişilememiştir.

24 Nisan 2017: Kimliği belirsiz bir hacker, Avustralya merkezli kurumsal Atlassian'ın sahibi olduğu grup sohbet platformu olan HipChat'e girmiştir. Adlar, e-posta adresleri ve karma şifreler gibi kullanıcı hesabı bilgileri, sohbet odası meta verilerinin yanı sıra çalınmıştır.

EK 7: NÜKLEER SANRALLEREE KARŞI SİBER SALDIRI SENARYOLARI

Her biri korunmak zorunda olan bilgisayar tabanlı saldırıların yapısı ve şekli önemli ölçüde değişebilmektedir. Saldırılar farklı türlerde olabilirken, yüksek seviyedeki sonuçlar şunları içermektedir:

- Bilgiye yetkisiz erişim veya engelleme (**gizlilik** kaybı);
- Bilginin, yazılımın, donanımın vb. Yetkisiz bir şekilde değiştirilmesi (**bütünlük** kaybı);
- Veri iletim hatlarının bloklanması ve / veya sistemlerin kapatılması (**kullanılabilirlik** kaybı).

Bilgisayar saldırılarına karşı önleyici tedbirlerin geliştirilmesinde, saldırıların ve saldırı veya saldırganların ilgili bilgileri elde etmek ve hedef bilgisayar sistemlerine erişmek için kullanabilecekleri potansiyel mekânları anlamak önemlidir. İyi organize edilmiş bir bilgisayar saldırısı birden fazla aşamadan oluşur. Bu aşamalar şunları içermektedir:

- Hedef tanımlama;
- Keşif;
- Sistem erişimi / uzlaşma ve
- Saldırı yürütmedir.

Aşağıdaki alt bölümler üç kurgusal bilgisayar saldırı senaryosunu listelemektedir. Hedeflerden biri olarak bilgi toplayan ilk senaryo, aşağıdaki iki senaryo için bir başlangıç olarak uygulanabilmektedir.

SENARYO I - Kötü amaçlı bir eylemi gerçekleştirmek için bilgi toplama

Saldırının amacı - sonraki saldırıları gerçekleştirmek için tesisin kontrollü (sınırlı erişim) alanlarına fiziksel erişim kazanmaktır.

İlgi alanları ise, erişim kartlarını yöneten ve erişim imkânı olan kişilerdir. Kısıtlı alanlara fiziksel erişim kazanmak, hem kart yöneticisinin bilgisayarından ödün vermeyi hem de erişim kodu sisteminin güvenliğini içermektedir. Saldırgan, donanım parçaları temin eden taşeron olarak seçmeyi tercih etmektedir. Saldırıyı desteklemek için olası bilgi toplama hedefleri şunları içermektedir:

- Muhtemel gasp veya “sosyal mühendislik” için personel bilgisi;
- Erişim kontrol sistemi için tasarım dokümantasyonu;
- Güvenlik sistemlerinin veya tesisin diğer ilgili alanlarının politika ve mühendislik planları;
- Operasyonel çizelgeler - fabrika takvimi, günlük rutin, çalışmakta olan, çalıştıkları zaman, tatilde olan, belirli değişiklikler olduğunda;
- Tedarikçilerin listesi ve donanım üzerinde çalışırken;
- Ekipman ve parça envanteri;
- Şifre ve erişim kontrol önlemleri;
- Erişim kontrol idari ve teknik önlemler;
- Yazılım geliştirici ve mevcut proje bilgileri;
- Ağ mimarisi;
- Telekomünikasyon mimarisi. Bu bilgileri toplamak için potansiyel yöntemler şunlardır:
- 'Sosyal mühendislik';
- Genel bilgi için Web aramaları;
- Veri Madenciliği;
- Savaşı başlatacak bahane arama;
- E-posta saldırıları - ağ erişimi, anahtar kaydediciler kazanmak için "kimlik avı";
- Yazılım veya cihazların ana makine üzerinde kurulumu - disk, hafıza kartı veya CD;

- Şifre girişi veya erişim kodu girişi (el, ses veya video gözetimi) üzerinde dinlemeyi kesme.

Saldırının bileşenleri şunları içerebilmektedir:
- Erişim kartı (çalıntı kartı) ve kodu alma;
- Mevcut erişim kartının çalınması / çoğaltılması;
- Yeni kart oluşturmak için kart makinesine erişim;
- Yeni çalışan girişinin oluşturulması;
- Son zamanlarda işten ayrılan çalışanın kimliğini varsayarak;
- İstenen erişim düzeyini temin etmek.

Kart ve kodlar elde edildikten sonra, saldırgan, donanım parçalarını teslim eden kişi olarak dikkat çekmeyecek şekilde tesise girmek için organizasyonel etkinlik için edinilen bilgileri kullanır.

SENARYO II - Bir veya birkaç bilgisayar sistemini devre dışı bırakma veya karşı tarafı uzlaşmaya zorlama saldırısı

Saldırının hedefi - bir nükleer enerji santralini sabote etmek ve tesisin yeniden başlatılmasını önlemektir.

Bu örnekte, kapatma süresi boyunca bir taşeron, besleme suyu kontrol sistemi üzerinde testler yürütmektedir. Yüklenici, sistemi kendi ofisinden izlemek ve test etmek için uzaktan erişim noktası kurar. Yüklenici işi tamamladıktan sonra erişim noktası yanlışlıkla yerinde kalır. Saldırgan, alt yükleniciyi fabrikada daha önce bir işçi olarak tanımlayan santral bilgilerini ve santralle ilgili bilgi için birincil hedefi toplamıştır. Saldırgan, alt yüklenicinin ofisine karşı bir e-posta "sızma- phishing" saldırısı gerçekleştirir ve sistemde bir yönetimsel kontroller sağlayan bir temel aygıt implante eder. Saldırgan, yüklenicinin bilgisayar ağına erişir ve tesis

tarafından test planlarını keşfeder ve aynı zamanda tesis tarafından devre dışı bırakılmayan uzaktan erişim portunu keşfeder.

Bu bilgilerle, saldırgan, şebekeye sistem arızasına yol açan trafiği besleme suyu kontrol sistemine bir hizmet engeli (DDoS) saldırısı gerçekleştirebilir ve sistem sel altında kalabilir. Sistem en az trafik yükünü işleyecek şekilde tasarlanmıştır. Saldırgan erişim sağladıktan sonra, ağı eşleştirir ve iletişim protokolünü belirler, saldırıyı gerçekleştirir. Saldırı, tesisin elle karıştırılmasına neden olan besleme suyu kontrol sistemindeki yanıt kaybına neden olur. Besleme suyu kontrol sistemi arızasının nedeni hemen belirlenemez ve tesis soruşturma için kapatılır.

SENARYO III - Koordineli saldırı aracı olarak bilgisayar sistemi üzerine uzlaşma

Saldırının hedefi - depolama tesisleri arasında geçiş yaparken nükleer malzemenin hırsızlığıdır. Çalıntı malzemenin kaybını gizlemek için envanter ve izleme sistemini değiştirmek için bir bilgisayar saldırısı gerçekleşmesi gerekmektedir.

Keşif ve istihbarat toplama, depolama tesisleri arasındaki radyoaktif malzeme sevkiyatlarının etiketlenmesi ve takibi için süreci tanımlamaktadır. Buna, bileşeni tanımlayan ve içeriği listeleyen öğelerdeki Radyo Frekansı Tanımlama (RFID) etiketleri dâhildir.

Saldırı planı, yoldaki malzemenin kaldırılması için içeriden yardımı içermektedir. Saldırının aşamaları şunlardır:

- Yolda taşımanın durdurulması;
- Gönderilen radyoaktif malzemenin az miktarda çıkarılması;
- Geri kalan gerçek miktarı yansıtmak için RFID çipinin yeniden programlanması;

- Envanter izleme sisteminin yeni tutarı yansıtacak şekilde değiştirilmesidir.