Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı

Kamu Yönetimi Doktora Programı

TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARININ KAMU POLİTİKASI ANALİZİ ÇERÇEVESİNDE DEĞERLENDİRİLMESİ

Volkan GÖÇOĞLU

Doktora Tezi

Ankara, 2018

TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARININ KAMU POLİTİKASI ANALİZİ ÇERÇEVESİNDE DEĞERLENDİRİLMESİ

Volkan GÖÇOĞLU

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı

Kamu Yönetimi Doktora Programı

Doktora Tezi

Ankara, 2018

KABUL VE ONAY

Volkan GÖÇOĞLU tarafından hazırlanan "Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi" başlıklı bu çalışma, 28.12.2017 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Doktora Tezi olarak kabul edilmiştir.

Prof. Dr. Doğan Nadi LEBLEBİCİ (Başkan)

Prof. Dr. Mehmet Devrim AYDIN (Danışman)

Prof. Dr. Hikmet KAVRUK

Prof. Dr. Mete YILDIZ

Yrd. Doç. Dr. Cenay BABAOĞLU

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof. Dr. Musa Yaşar SAĞLAM
Enstitü Müdürü

BİLDİRİM

Hazırladığım tezin/raporun tamamen kendi çalışmam olduğunu ve her alıntıya kaynak gösterdiğimi taahhüt eder, tezimin/raporumun kağıt ve elektronik kopyalarının Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü arşivlerinde aşağıda belirttiğim koşullarda saklanmasına izin verdiğimi onaylarım:

☒ Tezimin/Raporumun tamamı her yerden erişime açılabilir.

☐ Tezim/Raporum sadece Hacettepe Üniversitesi yerleşkelerinden erişime açılabilir.

☐ Tezimin/Raporumun ..... yıl süreyle erişime açılmasını istemiyorum. Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin/raporumun tamamı her yerden erişime açılabilir.

[Tarih ve İmza] 09.01.2018

[Öğrencinin Adı Soyadı] Volkan GÖĞÜŞ

YAYINLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanması zorunlu metinlerin yazılı izin alarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

- [x] **Tezimin/Raporumun tamamı dünya çapında erişime açılabilir ve bir kısmı veya tamamının fotokopisi alınabilir.**
  (Bu seçenekle teziniz arama motorlarında indekslenebilecek, daha sonra tezinizin erişim statüsünün değiştirilmesini talep etseniz ve kütüphane bu talebinizi yerine getirse bile, tezinin arama motorlarının önbelleklerinde kalmaya devam edebilecektir)

- [ ] **Tezimin/Raporumun ..... tarihine kadar erişime açılmasını ve fotokopi alınmasını (İç Kapak, Özet, İçindekiler ve Kaynakça hariç) istemiyorum.**
  (Bu sürenin sonunda uzatma için başvuruda bulunmadığım taktirde, tezimin/raporumun tamamı her yerden erişime açılabilir, kaynak gösterilmek şartıyla bir kısmı ve ya tamamının fotokopisi alınabilir)

- [ ] **Tezimin/Raporumun ..... tarihine kadar erişime açılmasını istemiyorum, ancak kaynak gösterilmek şartıyla bir kısmı veya tamamının fotokopisinin alınmasını onaylıyorum.**

- [ ] **Serbest Seçenek/Yazarın Seçimi**

09 / 01 / 2018

.....

(İmza)

Öğrencinin Adı Soyadı

Volkan Göğüş

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, Prof. Dr. Mehmet Devrim AYDIN danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

Volkan GÖÇOĞLU

İTHAF

Canım Annem ve Babam

Günay ve Tayfun GÖÇOĞLU'NA …

TEŞEKKÜR

Çalışma konumun belirlenmesi ve bu sürecin sonuçlandırılmasına kadar geçen süreçte çok büyük emeği ve desteği olan, her türlü fikir alış verişinde bulunduğum, değerli yorumları ve yönlendirmeleriyle çalışmamı emin adımlarla sürdürmeme olanak sağlayan çok değerli tez danışmanım Sayın Prof. Dr. Mehmet Devrim AYDIN'a tüm samimiyetimle teşekkür ederim.

Tez jürimde yer alarak değerli görüş ve fikirlerini benimle paylaşan Prof. Dr. Doğan Nadi LEBLEBİCİ'ye, Prof. Dr. Hikmet KAVRUK'a, Prof. Dr. Mete YILDIZ'a ve Yrd. Doç. Dr. Cenay BABAOĞLU'na teşekkürü borç bilirim.

Eğitim hayatıma başladığım günden beri her türlü yardım ve fedakârlığı sağlayan, bana destek olan anneme, babama ve kardeşlerime; süreçte motivasyonumu hep yüksek tutan arkadaşlarıma teşekkürlerimi sunarım.

ÖZET

Volkan GÖÇOĞLU. *Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi*, Doktora Tezi, Ankara, 2018.

Siber güvenlik, kritik altyapılar olan iletişim, enerji, su, finans, ulaşım ve gıda üretim gibi sistemlerinin yanında önceki dönemlerde fiziki olan ancak içinde bulunulan dönemde büyük oranda (özellikle yönetim mekanizmaları) siberleşmiş endüstriyel kontrol sistemlerinin güvenliğini de içeren bir alan haline gelmiştir. Özellikle ulusal güvenliklerinin sağlanması ve kritik altyapılarının korunması noktasında ülkeler, geleneksel güvenlik yöntemlerinin yanı sıra gelişen teknolojiler ve bu teknolojiler beraberinde dönüşen kritik altyapılarla birlikte siber güvenlik konusunda da farkındalık kazanmışlardır. Bu noktada siber güvenliği bir kamu politikası konusu olarak ele almak ve ile kamu politikası analizi yaklaşımları çerçevesinde düşünmek gerekmektedir. Bu tezde öncelikle, ele alınan bir örnek olay ve beş ülke incelemesinden çıkarılan sonuçlar yardımıyla kamu politikası ve siber güvenlik arasındaki sıkı ilişki belirlenmiştir. Akabinde, Türkiye'nin siber güvenlik politikalarını tanımlayan toplamda 28 adet resmi belge (kalkınma planları, strateji ve eylem belgeleri, hukuki belgeler ve raporlar) araştırma kapsamına alınmış, bu belgelerin içerikleri NVivo 11 nitel veri analizi programı yardımıyla kodlanmış ve analiz edilmiştir. Araştırmanın sonuç kısmında, Türkiye'nin siber güvenlik ve kritik altyapı politikalarının kamu politikası analizi yaklaşımları ve karar verme modelleri çerçevesindeki yönelimleri, üretilen politikaların özellikleriyle birlikte ortaya konulmuştur.

Anahtar Sözcükler

Kamu Politikası Analizi, Siber Güvenlik, Karar Verme Modelleri, Kritik Altyapı, Ulusal Güvenlik.

ABSTRACT

Volkan GÖÇOĞLU. *The Assessment of Turkey's Cyber Security Policies in the Context of Public Policy Analysis*, Doctoral Thesis, Ankara, 2018.

Cyber security has become a field that includes the security of industrial control systems that is used to be physical, but it is now substantially cybered, besides the critical sub-structures such as communication, energy, water, finance, transportation and food production systems. Particularly at the point of ensuring national security and protecting critical sub-structures, countries have become aware of cyber security, along with traditional security methods, as well as emerging technologies and critical infrastructures that have evolved with these technologies. At this point, it is necessary to address cyber security as a public policy topic and evaluate it in the context of public policy analysis. In this thesis, firstly, the close relationship between public policy and cyber security was determined through the results of a case study and five country reviews. Then, 28 official documents defining the cyber security policies of Turkey were included in the scope of the research, coded by the help of qualitative research analysis software NVivo 11 and analyzed. In the conclusion part, tendencies of Turkey's cyber security and critical sub-structure policies and their features were revealed within the context of public policy analysis approaches and decision making models.

Keywords

Public Policy Analysis, Cyber Security, Decision Making Models, Critical Sub-structures, National Security.

İÇİNDEKİLER

KISALTMALAR DİZİNİ

AB: Avrupa Birliği

ABD: Amerika Birleşik Devletleri

AR-GE: Araştırma ve Geliştirme

BM: Birleşmiş Milletler

BTK: Bilgi Teknolojileri Kurumu

BTSEP: Bilgi Toplumu Stratejisi ve Eylem Planı

CEO: Chief Executive Officer

CIA: Central Intelligence Agency

CMF: Cyber Mission Force

CPT: Cyber Protection Team

CRS: Congressional Research Service

DBS: Defense Science Board

DHS: Department of Homeland Security

DOD: Department of Defense

DPT: Devlet Planlama Teşkilatı

EGM: Emniyet Genel Müdürlüğü

EHK: Elektronik Haberleşme Kanunu

EUC: European Comission

FBI: Federal Bureau of Investigation

FSB: Federal Security Service

GÖÇMER: Göç ve Sınır Güvenliği Araştırma Merkezi

GRU: Main Intelligence Directorate

HP: Hewlett Packard

IRGC: Islamic Revolutionary Guard Corps

ITU: International Telecommunications Union

KB: Kalkınma Bakanlığı

KPA: Kamu Politikası Analizi

NASA: National Aeronautics and Space Administration

NATO: North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması Örgütü)

NICE: The National Initiative for Cybersecurity Education

NPC: Standing Committee of the National People's Congress

NS: New Scientist

PLC: Programmable Logic Controllers

RNS: Russian National Security

SCADA: Supervisory Control and Data Acquisition

SOME: Siber Olaylara Müdahale Ekibi

SVR: Foreign Intelligence Service

TBMM: Türkiye Büyük Millet Meclisi

UBGKT: Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı

UBGMD: Uluslararası Bilgi Güvenliği Mühendisliği Dergisi

UDHB: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

UK: United Kingdom

UN: United Nations

USCYBERCOM: United States Cyber Command

USOM: Ulusal Siber Olaylara Müdahale Merkezi

WHOPS: White House Office of the Press Secretary

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

GİRİŞ

II. Dünya Savaşı'nın sona ermesiyle birlikte, kapitalist ve sosyalist sistemler arasında kıyasıya bir rekabet başlamış, bu rekabete bağlı araştırma ve geliştirme ataklarının da uzay çağını başlattığı ileri sürülmüştür. Söz konusu rekabetin en önemli sonucu özellikle bilgisayar ve iletişim sistemleri alanlarında ortaya çıkardığı büyük teknolojik gelişmeler olmuştur. Bu gelişmeler insanlık tarihinde yeni bir toplumsal gelişmenin habercisi olarak algılanmıştır (Çelik, 1998: 54). Bilgisayar ve iletişim teknolojilerinin gelişmesiyle birlikte ortaya çıkan bu toplumsal değişmede, bilgiyi üretme, dağıtma, kullanma şekilleri ve araçlarının yanı sıra toplumun bilgiye karşı olan algısı ve bilginin toplum üzerindeki yansıması da değişmiştir. Söz konusu toplumsal dönüşüm, dünyanın bilgi toplumuna (Webster, 2014: 19) geçişini tasvir etmektedir. Bilgi toplumunda özellikle ülkeler adına ortaya çıkan en önemli kavramlardan birisi siber güvenlik olmuştur.

Kelime kökeni itibariyle hayvan ve makine sistemlerinde kontrol ve iletişim konusunda öne çıkan "sibernetik" kavramının (Wiener, 1948) "siber" kökünden ileri gelen ve günümüzde daha çok elektronik kontrol sistemlerini nitelerken, bir nesne olarak değil, ağlar ile erişilen bir elektronik sistemi destekleyen ve niteleyen bir kavram olarak nitelendirilen siber güvenlik, son yıllarda ülkeler açısından üzerinde durulması gereken en önemli konulardan biri haline gelmiştir. Bu doğrultuda ülkeler siber güvenlikle ilgili stratejiler, geliştirmeye, politikalar üretmeye başlamışlardır. Özellikle ulusal güvenliklerinin sağlanması ve kritik altyapıların korunması noktasında ülkeler, geleneksel güvenlik yöntemlerinin yanı sıra gelişen teknolojiler ve bu teknolojiler beraberinde dönüşen kritik altyapılarla birlikte siber güvenlik konusunda farkındalık kazanmaktadırlar. Zira siber güvenlik, kritik altyapılar olan iletişim, enerji, su, finans, ulaşım, gıda üretim gibi sistemlerinin yanında önceki dönemlerde fiziki olan ancak içinde bulunulan dönemde büyük oranda (özellikle yönetim mekanizmaları) siberleşmiş endüstriyel kontrol sistemlerinin güvenliğini de

içeren bir alan haline gelmiştir. Bu noktada siber güvenliği bir kamu politikası olarak ele almak ve kamu politikası ile kamu politikası analizi kuramları çerçevesinde düşünmek, anlamak ve ele almak gerekmektedir. Kamu politikası, son yıllarda Türkiye'de de araştırmacılar tarafından bir çalışma alanı olarak ilgi gören bir kavramdır (Yıldız vd., 2011: 358). Kavram biraz daha detaylı olarak tasvir edilmeye çalışıldığında kamu politikası; devletin yasalardan gelen otorite gücünün nüfuz ettiği herhangi bir konuda yetki sahibi olan kamu kurumu ya da kamu görevlisinin yaptığı iş ve eylem olarak değerlendirilebilir. Buna göre, bakanlar kurulu kararıyla yürürlüğe giren ve tüm vatandaşları etkileyen bir vergi indirimi gibi, küçük bir köydeki ihtiyar heyeti ve muhtarın köy ile ilgili aldıkları bir karar, kamu politikası kavramını ifade edecektir (Akdoğan, 2011: 75). Öyleyse, ilk anlamıyla kamu politikası kavramını devlet ve bağlı kuruluşları aracılığıyla karar verilen ve uygulanması belirli bir kitleyi ya da topluluğu etkileyen karar ya da kararlar bütünü olarak düşünmek yanlış olmayacaktır. Siber güvenliğe kamu politikası çerçevesinde bir yaklaşım, ülkeler adına siber güvenlik alanında üretilecek kamu politikaların daha amaca yönelik bir şekilde oluşturulmasını sağlayacaktır. Siber güvenlik politikalarının çözüm arayacağı problemlerin daha doğru bir şekilde belirlenmesi ve problemin çözümüne yönelik üretilecek politikalardaki yöntem, katılım, uygulama süreci, uygulama ardından elde edilen sonuç ve çıktıların değerlendirilmesi adımlarında kamu politikası analizi yaklaşım ve karar verme modellerinin karar vericilere sağlayacağı katkı yadsınamaz niteliktedir.

Bu tez, kamu politikası analizi yaklaşımlarını ve bu yaklaşımlar içerisinde yer alan karar verme modellerini derinlemesine ele alarak, Türkiye'nin siber güvenlik ve onunla bağlantılı olarak kritik altyapılarla ilgili politikalarını belirleyen ve belirten resmi belgelerde uyguladığı ya da uygulamayı öngördüğü politikaları söz konusu yaklaşım ve modeller çerçevesinde analiz etmektedir.

Çalışma sonucunda altı çizilen hususlar ve eksik gösterilen noktalara karar vericiler tarafından ilgi gösterildiği takdirde, siber güvenlik konusunda daha verimli

politikalar oluşturulabileceği düşünülmektedir. Zira üretilecek siber güvenlik politikalarının çalışmada yer verilen yaklaşım ve modeller içerisinde ele alınarak düşünülmesi, karar vericilere problemler, öncelikler, ortaya çıkacak sonuç ve dışsallıklar konularında farklı bakış açıları kazandırabilecektir.

Tezin Amacı ve Kapsamı

Çalışma, ülkeler açısından önemli bir konu haline gelen siber güvenliği kamu politikası analizi yaklaşımları ve karar verme modelleri çerçevesinde ele alarak, Türkiye'nin siber güvenlik politikalarını bu analiz ve modeller çerçevesinde değerlendirmekte ve politikaların söz konusu çerçeve içerisindeki yönelimlerini belirlemek üzere yapılmıştır. Bu amaç doğrultusunda Türkiye'nin siber güvenlik politikalarını belirleyen ve belirten resmi belgeler (strateji ve eylem belgeleri, kalkınma planları, hukuki belgeler ve raporlar) incelenerek ve belirli bir yöntem temelinde kodlanarak analiz edilmiştir. Analiz sonucunda Türkiye'nin siber güvenlik politikalarına dair bulgular yorumlanarak söz konusu politikalar, kamu politikası analizi ve karar verme yaklaşımları çerçevesinde değerlendirilmiştir. Yorumsamalar sonucunda resmi belgelerde belirlenen ve belirtilen, Türkiye'nin siber güvenlik politikalarının hangi yaklaşımlar çerçevesinde şekillendiği belirlenmiştir. Bu yönüyle çalışma, Türkiye'nin siber güvenlik politikalarının hangi kamu politikası analizi yaklaşımları çerçevesinde, hangi karar verme modelleri temel alınarak, hangi yönelimlerde (altyapısal, teknolojik, statükocu vb.) olduğunu belirlemeyi amaçlamaktadır. Türkiye'de, yeni bir akademik çalışma alanı olan kamu politikasının kuramsal kısmını yine Türkiye açısından yeni bir kavram olan siber güvenlik ve onun politikalarıyla ilişkilendirerek somut politika önerileriyle tek tek analiz eden bu çalışmanın, kamu yönetimi alan yazınına katkı sağlayacak bir nitelikte olduğu düşünülmektedir. Çalışmada siber güvenliğin ticari, siyasi (demokrasi) ve devlet (idari) boyutlarından devlet boyutuna odaklanmaktadır. Dolayısıyla yapılan yorumsama ve çıkarsamalar da bu açıdan olacaktır.

Tezin Araştırma Sorusu

Yukarıda belirtilen amaç doğrultusunda tezin araştırma sorusu şu şekilde belirlenmiştir:

““Türkiye’nin siber güvenlik politikalarının kamu politikası analizi yaklaşımları çerçevesindeki yönelimleri nelerdir?”

Tezin Çalışma Planı

Çalışma beş bölümden oluşmaktadır. Çalışmanın ilk dört bölümü, bölümlerde ele alınan konular dâhilinde yapılan alan yazını taramaları doğrultusunda oluşturulmuştur. Çalışmanın beşinci bölümünde ise veri toplama tekniklerinden doküman analizi tekniği kullanılarak yapılmış nitel bir araştırmaya yer verilmiştir. Çalışmanın bölümleri ve bölümlerin kapsamları şu şekildedir:

Birinci bölümde, kamu politikası ve kamu politikası analizi kavramları, kamu politikası analizi içerisinde yer alan yaklaşımlar ve karar verme modelleri alan yazını temelinde derinlemesine ele alınmıştır. Bölümün sonunda, alan yazınında dağınık bir şekilde ele alındığı gözlemlenen bu yaklaşım ve modellere dair bir sınıflandırma yapılmıştır.

İkinci bölümde, siber güvenlik detaylı olarak incelenmiştir. İlk olarak ulusal güvenlik konusu ele alınmış, akabinde siber güvenlik, bir bilgi toplumu yansıması olarak incelenmiştir. Bölümün ilerleyen kısımlarında siber güvenlikle ilgili diğer kavramlar olan siber saldırı, siber sömürü, risk, tehdit ve güvenlik açığı kavramları, kritik altyapılar ve ilgili alt sistemler ele alınmıştır. Aynı başlık altında, siber güvenliğin ülkelerin ulusal güvenlikleri açısından önemini somut olarak ortaya koymak üzere Stuxnet örnek olayına yer verilmiştir.

Üçüncü bölümde ülkelerin siber güvenlik politikaları ile ilgili bilgiler verilmiş bu doğrultuda Clarke ve Robert'ın (2010) araştırmalarında siber güvenlik odağında incelenen ABD, Rusya, Çin, İran, Kuzey Kore ile bunlara ek olarak İsrail ve Almanya'nın siber güvenlik politikaları incelenmiştir.

Dördüncü bölümde, Türkiye'nin siber güvenlik politikalarının hukuki ve kurumsal dayanaklarını ortaya koymak üzere Türkiye'de siber güvenlik ile ilgili yapılan hukuki düzenlemeler ve kurulan kurumlar ele alınmıştır.

Çalışmanın araştırma bölümünü oluşturan beşinci bölümde, Türkiye'nin siber güvenlik politikalarının kamu politikası analizi yaklaşımları ve karar verme modelleri çerçevesindeki yönelimlerini belirlemek üzere veri toplama tekniklerinden doküman analizi tekniği kullanılarak yapılan nitel araştırmaya yer verilmiştir. Bu araştırma kapsamında Türkiye'nin siber güvenlik politikalarını belirleyen ve belirten strateji belgeleri ve eylem planları, kalkınma planları, meclis araştırma ve Emniyet Genel Müdürlüğü raporları, hükümet planları ve hukuki belgeleri inceleme dâhiline alınmıştır. Araştırmanın yöntemi, sınırlılıkları ve örneklemi gibi bilgilerine bu bölüm içerisinde yer verilmiştir.

1. BÖLÜM: TEMEL KAVRAMLAR VE YAKLAŞIMLAR ÇERÇEVESİNDE KAMU POLİTİKASI

Çalışmanın girişi niteliğindeki bu bölümde öncelikle çalışmayı oluşturan temel kavramlar olan kamu politikası ve kamu politikası analizi üzerinde durulmuş olup söz konusu kavramlar ortaya konulan ilgili yaklaşımlar çerçevesinde ele alınmıştır. Daha sonra kamu politikası yaklaşımları içerisinde yer alan ve politika üretim sürecinin önemli bir bölümünü oluşturan karar verme modelleri incelenmiş ve bölümün sonunda tüm bu yaklaşım ve modeller sınıflandırmaya tabi tutulmuştur.

1.1. KAMU POLİTİKASI KAVRAMI VE TANIMLARI

Resmi süreçler sonucunda göreve gelen siyasi iktidarların asli görevleri, vatandaşların iktidardan beklentilerini karşılamak, kamu düzenini muhafaza ederek bir uzlaşı ortamı sağlamak ve kamu hizmetlerini yürütmektir. Söz konusu asli görevlerin çıktılarından birisi de kamu politikasıdır (Yıldız ve Sobacı, 2013: 17). Kamu politikasının ilgili alan yazınındaki belirli isimlerden tanımlarına değinmeden önce bu kavramın genel olarak neyi ifade ettiğine değinmekte yarar vardır. Kamu politikası, vatandaşların taleplerini karşılamak, hizmetlerin yürütülmesinde ve kamu düzeninin sağlanmasında, aynı şekilde hizmetlerin ve düzenin her türlü fonksiyonunun iyileştirilmesinde ortaya çıkan bir kavramdır. Vatandaşın bir konu ya da soruna yönelik talebinin karşılanmasında kamu politikaları oluşturularak bu taleplere cevap, sorunlara ise çözüm bulunmaya çalışılmaktadır. Talep ve sorunlara yönelik müdahale, siyasi iktidar ve ona bağlı devlet organlarında yapılmaktadır. Bu yönüyle kamu politikası, devletin yasalardan gelen otorite gücünün nüfuz ettiği herhangi bir konuda yetki sahibi olan kamu kurumu ya da kamu görevlisinin yaptığı iş ve eylem olarak değerlendirilebilir. Buna göre, bakanlar kurulu kararıyla yürürlüğe giren ve tüm vatandaşları etkileyen bir vergi indirimi veya küçük bir köydeki ihtiyar heyeti ve muhtarın köy ile ilgili aldıkları bir karar, kamu

politikası kavramını ifade edecektir (Akdoğan, 2011: 75). Yöneticilerin verdikleri talimatlar, hükümetlerce yayınlanan politika yazıları ve açıklamaları, yönetsel düzenleme ve yönetmelikler, mahkemelerce verilen kararlar kamu politikasının ifade ve ilan biçimlerindendir. Alınan ulusal bir karardan, bir köydeki hane halkını ilgilendiren bir karara kadar geniş bir nüfuz alanına sahip olan kamu politikası, bu yönüyle karmaşık bir süreci ve güçler ilişkisini barındırmaktadır. Bu kararlar dizisi biraz daha detaylı düşünüldüğünde, devletten, herhangi bir konuda yüksek bilgi birikimine sahip bir kişinin, sahip olduğu tüm seçenek ve değerleri ortaya koyarak en iyi kararı verdiği akla gelmektedir. Graham Allison, "Essence of Decision (Kararın Özü)" isimli kitabında, bahsi geçen ve geleneksel yönetim anlayışında yer alan tek bir resmi görevlinin verdiği bu kararı *model 1* olarak tanımlamıştır. Aynı kitapta Allison, kararın kurumsal olarak alındığı durumu model 2 ve kararın bürokratik çekişmeler sonucu alındığı durumu ise model 3 olarak isimlendirmiştir (akt. Heymann, 2008: 8). Kitapta, karar vericilerin en iyi kararı vermek için sahip olması gereken bilgi ve değerler bütününün lobiler, çıkar grupları ve çeşitli faktörlerce bulanıklaştırılarak en doğru kararın alınmasının güçleşebildiği de vurgulanmaktadır.

Anderson (2003) çalışmasında kamu politikalarını bir takım kategorilere ayırarak incelemiştir. Söz konusu kategoriler yazarın çalışması üzerinden incelendiğinde, kamu politikalarında ilk grup, asli ve prosedürel politikalardır. *Asli politikalar* direkt olarak, uygulanmaları sonucunda fiyat ve maliyete etki eden, politikanın ilgililerine avantaj ya da dezavantaj sağlayan politikalardır. Örneğin, devletin yollar yapması, alkollü bir içeceğin perakende satışını yasaklaması gibi politikalar bu politikalara örnektir. *Prosedürel politikalar* ise bir uygulamanın nasıl ve kimler tarafından yürütüleceğini belirleyen politikalardır. Yazar bu politikalara uygun bir örnek olarak 1946 yılında çıkarılan federal Yönetsel Prosedür Düzenlemesi'ni (Administrative Procedure Act) örnek vermektedir. Söz konusu düzenleme devlet ve sivil kuruluşlara yönetmelik ve prosedürel düzenlemeler çıkarma konusunda yol

gösterici bir nitelik taşırken, aynı zamanda kamu politikası oluşturma süreçlerine ilgili diğer aktörlerin nasıl ve ne şekilde katılabileceklerini de tarif etmektedir.

Diğer politikası kategorileri, dağıtıcı, düzenleyici, özdenetimci ve yeniden dağıtıcı kamu politikası kategorisidir. Bu kategorilerdeki politikalar, sonuçlarından etkilenen ve politikanın formülasyonunda yer alan aktörlere göre değişiklik göstermektedir. *Dağıtıcı politikalar,* toplumun bireyler, gruplar, sektörler, cemiyetler gibi belirli kısımlarına etki eden politikalardır. Ev kredileri için geliştirilen vergi indirimi politikaları, tarımla uğraşanlar için gelir vergisi indirimleri ve bedava devlet eğitim-öğretim programları gibi politikalar dağıtıcı politikaları oluşturmaktadır. *Düzenleyici politikalar*, etkide bulunduğu aktörlere yönelik uygulamaların ve çıkarların sınırlarını oluşturan ve belirleyen politikalardır. Bu yönleriyle dağıtıcı politikalardan ayrılırlar. Dağıtıcı politikalar etkide bulundukları çıkar gruplarının özgürlük alanlarını genişletirken düzenleyici politikalar bu sınırları daraltır ya da netleştirirler. Düzenleyici politikaların örnekleri daha çok iş hayatını ve sektörel işleyişi odak alan politikalardır. Sektörlerdeki şirketler ve çıkar grupları arasındaki rekabeti düzenleyen politikalar bu kategoriye girmektedir. Diğer yandan, kişi-kişi, kişi-grup ya da şirket arasındaki ticaret ilişkilerini düzenleyen düzenleyici politikalar olabileceği gibi, istismar, pornografi ve bireysel silahlanma gibi kişisel davranışları düzenleyen politikalar da olabilecektir. Düzenleyici politikalar, etkide bulunması beklenen odaklara direkt olarak ve kısa vadede yarar sağlamayabilir. Örneğin, temiz hava ve çevre üzerine üretilecek politikalar bireylere uzun vadede etki edecek düzenleyici politikalar olacaklardır.

Özdenetimci Politikalar, haksız rekabeti önlemek üzere oluşturulan düzenleyici politikalara benzer politikalardır. Bu ikisi arasında ufak bir farklılık vardır. Özdenetimci politikalarda, haksız rekabeti önleyici düzenlemelerin çıkar gruplarının, bünyelerinde bulunan üyelerinin çıkarlarını korumak adına düzenleme haklarının kendilerine bırakılması söz konusudur. Örneğin, meslek odalarının

üyelerine verdikleri profesyonel lisanslar ve bu lisansları vermek için uyguladıkları prosedürler bu kuruluşların kendi düzenleme alanlarındandır.

Yeniden dağıtıcı politikalar zenginden alıp fakire verme politikaları olarak ele alınabilir. Ancak bunu sadece para ve gelir olarak görmemek gerekir. Aynı zamanda bir konudaki haklar ve nüfuz gücü de yeniden dağıtılabilir. Örneğin, bir alanda vergi toplama hakkının merkezi kurumlardan alınarak yerel yönetim kuruluşlarına verilmesi gibi bir politika, örnek olarak düşünülebilir. Çıkar grupları arasında çatışma ve hatta savaşlara neden olan politikalar genellikle yeniden dağıtıcı politikalardır. Mülkiyetin ve gelirin yeniden paylaştırılması, yoksullara yardım, ABD'de siyahilere verilen hakların genişletilmesi, seçme ve seçilme hakkı gibi hakların yeniden dağıtılması, özellikle ülkelerdeki liberal, muhafazakâr, sosyal demokrat gibi siyasi grupların tartışmalarına ve farklı görüşlerine konu olan yeniden dağıtıcı kamu politikalarıdır. Bir diğer kategori ise politikaları somut ve soyut olarak sınıflandıran *maddesel ve sembolik* kamu politikaları grubudur. Maddesel kamu politikaları etkide bulunduğu kişi ya da gruplara gelir artışı, hak kazancı gibi somut kazanımlar ya da bunların tam tersi olarak dezavantajlar sağlarken, sembolik politikalar daha çok vatanseverlik, demokrasi, barış gibi soyut kazanımlar sağlayan politikalardır. Kamu politikalarının sınıflandırılmasında son kategori ise ortak çıkarlara ve kişisel çıkarlara yönelik oluşturulan politikalardır. Ortak çıkarlara yönelik politikalar, ilgili tüm vatandaşlara, herhangi bir ayrım ya da beklenti gözetmeksizin etki eden kamu politikalarıdır. Örneğin, mahalleye yapılan bir çocuk parkı, çocuğu olan tüm vatandaşlar için bir kazanımdır. Bireysel çıkarlara yönelik politikalar ise politikanın belirlediği karşılığa, beklentiye ya da özelliğe sahip vatandaşlara, karşılığını ödemek koşuluyla fayda sağlayabilecektir. Posta servisi, çöp toplama, sağlık bakımı gibi hizmetler bu tip politikalara örnek olarak gösterilebilecektir.

Goodin ve arkadaşlarının (2006: 3-4) belirttiği üzere yönetmek bir arzunun uzantısıdır ve kontrolü sağlamayı, bir dünyayı şekillendirmeyi amaçlamaktadır.

Kamu politikaları da bu yönetme arzusunun birer uzantısı olarak özellikle II. Dünya Savaşı sırasında yapılan yön-eylem araştırmalarının bir türevi niteliğinde çalışılmaya başlanmış ve ilk başlarda "Yüksek Modernizm" anlayışıyla yoğurularak daha çok analitik düşünce ve teknik problemlere bir çözüm arayışı olarak ele alınmıştır. Özellikle bu anlayış, savaş yıllarında Pentagon[1] ve diğer Amerika Birleşik Devletleri (ABD) kurumlarında uygulanmıştır. 1970'li yıllarda yüksek modernizmin etkileri halen sürerken, sosyal bilimciler kamu politikasının limitlerine ışık tutarak, modern anlayışın bir yansıması olan "en iyi yol" görüşünün politika üretim sürecindeki hâkimiyetini eleştirerek uygulama, yönetim ve kontrol fonksiyonlarında alternatif düşünceler geliştirmeye başlamışlardır (Cooper ve Burrel, 1988: 94-102; Lyotard, 1994; Saylan ve Boybeyi, 1994: 313; Göçoğlu, 2014). Bu düşünceler modern düşüncenin aslında gizliden gizliye var olan keskin limitlerini daha yumuşak bir hale getirmeyi hedeflemiştir. 20. yüzyılın ikinci yarısı bu etkilerle, kamu politikaları açısından yeni bir dönem sayılabilecektir. Söz konusu dönemden sonra kamu politikası özellikle sosyal bilimciler tarafından çeşitli şekillerde ve çeşitli fonksiyonları ön plana çıkarılarak tanımlanmıştır.

Alan yazınında yer alan kamu politikası çalışmalarının büyük bir kısmında olduğunun aksine Dye (1972: 2), "Understanding Public Policy" isimli kitabında kamu politikasını henüz ilk paragrafta kamu politikasını "devletin yapmayı ya da yapmamayı seçtiği her şey" olarak tanımlamıştır. Bu tanım, özellikle kamu yönetimi alan yazınında genel kabul gören bir tanım olmuştur. Lasswell ve Kaplan (1971: 71), kamu politikasını (ya da politikayı) amaçların, değerlerin ve uygulama pratiklerinin projelendirilmiş bir programı olarak tanımlarken, bu projelendirilmiş programı özel ya da sosyal olarak ayırmaktadırlar. Onlara göre bu söz konusu programlar bir kişiye ya da o kişinin diğer kişilerle ilişkilerine etki edebilmektedir. Dolayısıyla politikalar da, onlardan etkilenen bu kişilerin beklentileri neticesinde

[1] ABD'nin Savunma Bakanlığı ve Genelkurmay Başkanlığı'nın genel adıdır.

oluşturulur ve şekillendirilir. Bu noktada kamu politikası kavramı, bir kişiyi etkileyen değil, kişiler arası bir etkileşime etkide bulunan bir kavramı ifade etmektedir. Lasswell ve Kaplan (1971: 73) politika kavramını açıklarken özellikle "etki", "etki ağırlığı", "etki boyutu" gibi kavramları da kullanarak, oluşturulan politikaların hangi diğer politikaları ve kimin politikalarının etkilediği, ne ölçüde geniş bir kitleyi ilgilendirdiği, hangi değerleri barındırdığı gibi soruları beraberinde taşıdığını vurgulamaktadırlar. Politikaların önem dereceleri de bu sorulara verilecek cevaplara göre değişecektir.

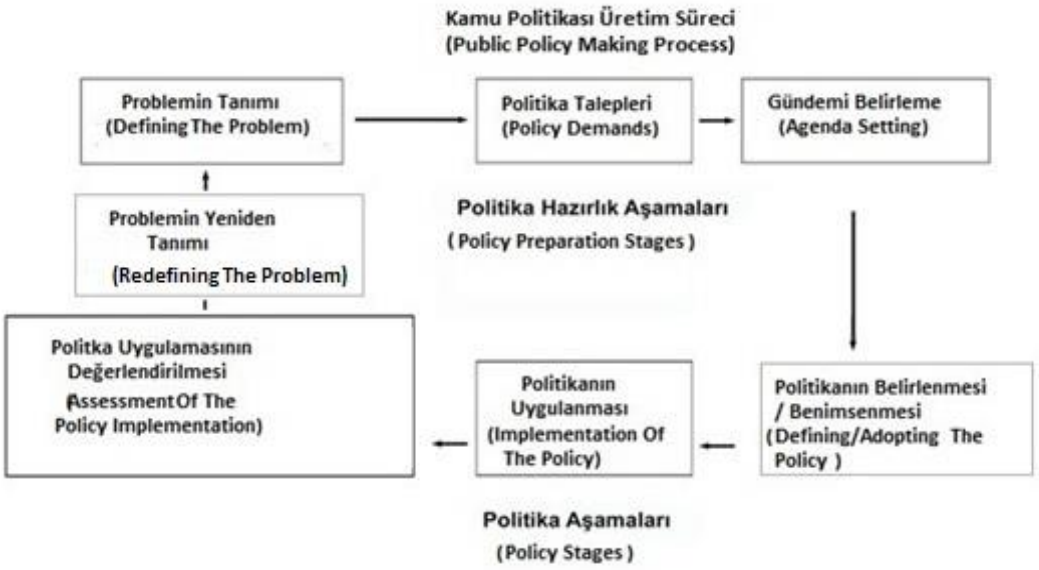
James Anderson (1994: 5'den akt: Yıldız ve Sobacı, 2013: 18) politikayı "belirli bir soruna ilişkin bir aktörün veya aktörler topluluğunun yürüttüğü faaliyetler bütünü ya da hareketsizliği" olarak tanımlamaktadır. Faaliyetler konusuna paralel olarak Wildavsky (1980: 25), kamu politikasının en derin ve gerçek anlamıyla ne ifade ettiğini anlamak için onu "koordinatörü olmayan bir koordinasyon" şeklinde düşünmenin gerektiğini vurgulamaktadır.

Kamu politikasını daha geniş bir düzleme oturtarak ele alan Eyestone kavramı; devlet kurumlarının ve bu kurumların etrafında onlarla ilişki halinde bulunan çevresinin etkileşimi olarak tanımlamıştır. Bu yönüyle Eyestone kamu politikasını, kamu yönetiminin ekolojik bir etkisi olarak görmektedir ancak yazar, söz konusu ekolojik çevrenin ne olduğunu ve kimlerden ya da nelerden oluştuğunu açıklamamıştır (Huang, 2002: 276). Diğer bir tanım olarak ise Easton (1953'den akt. Çevik, 1998: 110), kamu politikasını, siyasal sistemin çevresinden gelen beklenti ve isteklere verdiği tepki olarak tanımlamaktadır. Easton, bu tanımı özellikle ortaya koyduğu "siyasal sistem" kavramı üzerinden geliştirirken, siyasal sistemi, toplumu birbirine bağlayan idari kararları ve toplumun ortak değerlerini muhafaza eden, karşılıklı ilişkiler geliştiren kurum ve çalışmaların bir uzlaşması, kamu politikasını ise söz konusu bu siyasal sistemin bir çıktısı olarak ele almaktadır.

Alan yazınında yer alan diğer çalışmalarda, kamu politikalarını bir eylemler bütünü olarak ele alındığına rastlanırken (Akdoğan, 2011: 75; Anderson, 2003: 2), kamu politikasını bir süreç olarak inceleyen çalışmalar da (Jones, 1977; Young, 2006: 844) bulunmaktadır. Bu yönde bir bakış açısında, kamu politikası tanımlarını tamamlayıcı bir nitelikte olan bu kavramı anlamak için kamu politikasının üretim sürecini incelemekte yarar vardır. Kamu politikası üretimi sürecini döngüsel olarak basamaklara ayıran rasyonel yaklaşım çerçevesinde oluşturulmuş politika yapım süreci modeli, alan yazınında yer bulduğu formatlarda ve başlıklarda ufak değişmeler söz konusu olsa da aşağıdaki tabloda yer alan şekli ile kalıplaşmıştır. Bu kalıba benzer şekilde Jenkins (1978: 30), alan yazınında yer alan ve politika üretim süreci basamaklarından oluşan rasyonel kamu politikası analiz süreci döngüsünün Harold Lasswell'in temelini attığı kalıbın geliştirilmesiyle ortaya çıktığını vurgulamaktadır. Türkiye'de yapılan kamu politikası analizi çalışmalarında da benzer kalıptaki süreç döngüsüne rastlamak mümkündür.[2] Söz konusu tablo aşağıda yer almaktadır.

[2] Sözü edilen model çerçevesinde yapılmış iki çalışma örneği için; Semiz, Ö. (2009). "Bir Kamu Politikası Analizi: Türkiye'de Korsanla Mücadele Odaklı Fikri Haklar Politikası", Ankara Barosu Dergisi, Erişim Tarihi: 20.09.2015, http://www.ankarabarosu.org.tr/siteler/ankarabarosu/frmmakale/2009-4/1.pdf ve Çalı, H. H. (2012). "Aile İçi Şiddet: Bir Kamu Politikası Analizi", Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi 2012 16 (2): 1-25 künyeli çalışmalara bakılabilir.

Şekil 1: Bir Süreç Olarak Kamu Politikası



Kaynak: Cochran vd., 2009.

Kamuya ilişkin bir konunun ilgili aktörlerce çözülmek üzere bir amaç haline gelmesi, o konunun bir kamu politikası problemine dönüşmesine bağlıdır. Problemin tanımlanması olarak nitelendirilen bu ilk basamak, kamu politikası analizi sürecini başlatan basamak olması dolayısıyla çok önemlidir. Yıldız'ın (2011: 2) değimiyle, "kamu politikası üretim süreci büyük bir çembere benzetilirse, saatin 12'yi gösterdiği noktada "problemin tanımı" vardır". Politika taleplerinin oluşturulması, problem tanımından sonra, tanımlanan probleme ilişkin çözüm önerilerinin ortaya konulması aşamasıdır. Bu aşamada en önemli kriterlerden birisi aktörlerin sürece katılımıyla soruna farklı açılardan yaklaşılabilmesidir. Söz konusu aktörlere ilerleyen kısımda daha detaylı değinilecektir.

Kamu politikası sürecinin bir diğer önemli aşaması ise gündem belirleme aşamasıdır. Medya ve sosyal medya aktörleri hem politika taleplerinin karar vericilere ulaşmasında hem de gündem belirlenmesinde işlevi olan en önemli aktörlerdir. Gündem belirlemede bir takım farklı amaç odakları ve bu odakların

oluşturulmasında rol alan aktörler olabilmektedir. Örneğin, hükümetin seçtiği politika alternatiflerinin ön planda olduğu “hükümet gündemi”, karar listesine alınan ve farklı aktörlerin önerilerinin de yer aldığı “karar gündemi” ve medyada ilgi toplayan politika alternatiflerinin bulunduğu “medya ve kamuoyu gündemi” birbirlerinden farklı içeriğe sahip olabilecektir. Birer aktör olarak hükümet gündeminde hükümet yetkililerinin; karar gündeminde özel sektör yetkililerinin, uzmanların ve teknik ekiplerin; medya ve kamuoyu gündeminde ise sivil toplum kuruluşlarının ağırlığı daha baskın şekilde hissedilecektir (Kingdon, 2014: 4). Gündemde yer bulan bu aktörlerin politika alternatiflerinin kabul edilebilirliğinde, çözüm önerilerinin niteliğinin beraberinde oluşturdukları baskınında etkisi olacaktır. Özellikle 2000’li yıllardan itibaren önemli bir iletişim aracı haline gelen internet ve sosyal medya, aktörlerin politika alternatiflerini geniş kitlelere duyurabilecekleri birer araç haline gelmişlerdir (Göçoğlu, 2014).

Belirlenen ve benimsenen bir kamu politikasının ilgili kuruluşlarca yürütülmeye başlandığı aşama politikanın uygulama aşamasıdır. Bu aşama genellikle, politika için gereken kanunun çıkarılmasıyla sona eren bir süreç olarak düşünülse de, daha dinamik ve aksiyona dayalı bir aşama şeklindedir (Jann ve Wegrich, 2007: 51). Uygulanan kamu politikalarının değerlendirme aşamasında, belirlenen probleme yönelik bir çözüm olarak benimsenen politikaların amaçlarına ulaşıp ulaşmadığı sorgulanmaktadır. Söz konusu amaçların gerçekleşip gerçekleşmediği ve belirlenen sorunun çözülüp çözülmediğinin yanı sıra, asıl sorunun çözülen sorun mu yoksa bu soruna yol açan başka bir sorun mu olduğu da saptanmalıdır (Yıldız, 2011: 7). Bu, genel olarak kamu politikaları sonucunda saptanması zor ve zahmetli bir durum olmaktadır. Problemin yeniden tanımlanması aşaması ise uygulanan politika sonucu çözüm bulmuş ya da bulamamış bir problemin geldiği son noktanın belirlenmesi ya da ürettiği yeni problemlerin saptanmasına dayanmaktadır. Son aşama olarak, yeni sorunların ortaya çıkma ihtimali

doğrultusunda, üretilen kamu politikalarının tam anlamıyla başarıya ulaşması için problemin yeniden tanımlanması aşaması da büyük önem taşımaktadır.

Kamu politikası analizinde, basamaklarda bir başlık olarak yer almamasına karşın sürecin bütününde etkiye ve önemli bir role sahip olan "aktörler", üzerinde özellikle durulması gereken bir konudur. Aktörler, problemin tanımlanmasından, politika taleplerinin ve alternatiflerinin belirlenmesinde, gündemin oluşturulmasında, politikaların belirlenerek uygulanmasında ve politika sonuçlarının geribildirimlerle değerlendirmesinde rol alan paydaşlardır.

Kamu politikası üretim sürecine etkide bulunan aktörler, Meier'in (1991) oluşturduğu şemayı yüksek lisans tezinde[3] geliştirerek veren Keeley'e (akt. Sutton, 1999: 26) göre "devlet merkezli" ve "toplum merkezli" olmak üzere iki gruba ayrılmaktadır. Keeley, devlet merkezli kamu politikası aktörlerini hükümet kabinesi, teknokratlar, bürokratlar ve devlet çıkarları olarak sıralamıştır. Aynı çalışmada, toplum merkezli aktörler; sınıflar, çıkar grupları, partiler ve seçmenler olarak gruplandırılmıştır. Bunun yanında söz konusu ayrımı resmi - gayri resmi aktörler (Birkland, 2010) olarak yapanlar da vardır. Birkland (2010: 92-93) özellikle 1950'lerden bu yana kurumsalcılık anlayışını domine eden davranışsalcılık anlayışıyla birlikte bireylerin, grupların ve bunların meydana getirdikleri kurumların birbirleri arasındaki iletişim ve etkileşimlerin sosyal bilimciler tarafından incelenmeye başladığını vurgulamaktadır. Daha sonra siyaset bilimi alanında da önemli yer tutan yeni kurumsalcılık anlayışı da bu iki akımın bir sentezi olarak türemiştir. Söz konusu ilişkilerin sonucunda kamu politikası sürecinde etkide bulunan aktörler ortaya çıkmaktadır. Yazara göre kamu politikası üretim sürecinde rol alan resmi aktörler, yasama organı (parlamento), yürütme organı (bakanlar

[3] Şema ve daha fazlası için; James Keeley'nin 'Conceptualising the policy process' in Reconceptualising Policy Processes, The Dynamics of Natural Resource Management and Agricultural Intensification Policymaking in Ethiopia' isimli tezine başvurulabilir.

kurulu), mahkemeler, devlet kurumları ve bürokratlar; gayrı resmi aktörler ise çıkar grupları, siyasi partiler, düşünce kuruluşları, araştırma şirketleri, medya, sivil toplum kuruluşları, mesele ağları ve politika ağlarıdır. Birkland'a karşıt bir görüş olarak Angelov (2002), devlet, toplum ve uluslararası kuruluşların birer aktör olmadıklarını savunmaktadır. Ona göre bu yapılar, "kurum ve kuruluşlar" olarak sınıflandırılmalıdır. Aktörler ise bireysel ya da grup çıkarlarını savunan oluşumlardan meydana gelmektedir. Bu yönde bir ayrım, "aktör" olabilme özelliğinin politikayı, "kendi ya da mensubu olduğu kitlenin çıkarları doğrultusunda etkileme amacında olması" koşul şartına bağlaması yönünden dikkat çekicidir.

Araştırmacı, yüksek lisans tezinde (Göçoğlu, 2014: 10-19) kamu politikası aktörlerini devlet ve diğer kamu politikası aktörleri olarak daha genel bir şekilde gruplandırmıştır. Yıldız'a (2011) göre; devlet olarak tanımlanan politika aktörü devletin yönetim sistemine göre değişiklik gösterebilir. Federal sistemlerde federal ve federe devlet ya da diğer bir yerel yönetim birimi olabilir. Örneğin, İspanya gibi federal ile tekçi sistemin ortasında bir yerde bulunan sistemlerdeki özerk bölge yönetimleri de federe devlet benzeri aktörler arasında sayılabilir. Devleti bu şekilde soyut bir yapı olarak tanımlarken, onun bünyesinde bulunan devlet kurumları, kuruluşları, organları, bu organları oluşturan bireyler ve çalışanlar da bu tanımlamanın içine girebilir. Araştırmacıya (Göçoğlu, 2014: 10-19) göre diğer kamu politikası aktörleri ise muhalefet partileri, bireyler (vatandaşlar), sivil toplum kuruluşları, baskı grupları, üniversiteler, uluslararası kuruluşlar, düşünce üretim kuruluşları ve danışmanlık kurumlarıdır.

Bu başlıkta görüldüğü üzere kamu politikası kavramsal olarak bir karar, bir tasarı, bir süreç, eylem ve işlemler bütünü olarak ele alınabilmektedir. Kamu politikasından ve kamu politikasının ele alınan bu yönlerinden farklılaşan ve daha çok kamu politikasını çözümlemeye ve anlamaya eğilen kamu politikası analizi ise bir sonraki başlıkta detaylı olarak incelenecektir.

1.2. KAMU POLİTİKASI ANALİZİ YAKLAŞIMLARI

Kamu politikası analizi, uygulanacak politikanın çeşitli şekillerde, çeşitli araçlarla çözümlenmesini ifade etmektedir. Bu bağlamda, politika analizi terimi, sistem analizi ile siyasal anlamdaki politika kavramını bir biri ile ilişkilendiren profesyonel bir disiplin için kullanılabilecektir (Dror, 1967: 200). Bu tanım doğrultusunda kamu politikası analizi hükümetlerin dış politika, savunma, konut, sağlık, eğitim gibi bütün kamu hizmetleriyle ilgili olarak olumlu ya da olumsuz yaptıkları şeyleri öğrenmek olarak da tanımlanabilecektir (Çevik, 1998: 105).

Kamu politikası analizine farklı yaklaşımlar penceresinden bakmak, politika analizinin şeklini ve öne çıkan unsurlarını değiştirmektedir. Alan yazını genelinde bu yaklaşımlar, karar alma/verme sürecinin eklektik bir uzantısı olarak gelişmektedir. Söz konusu kamu politikası analizi yaklaşımlarının düşünce sistemleri farklı olsa da aslında birbirleri ile çeşitli şekillerde (öğrenci-öğretmen, aynı dönem meslektaşı vb.) bağları bulunan kişiler tarafından ortaya atılan ya da geliştirilen, destek ve eleştiri boyutlarıyla birbirlerinden ayrılan yaklaşımlardır (Çorbacıoğlu, 2008). Bu yaklaşımlar en genel anlamda rasyonalist bakış açısı, post-pozitivist ya da yorumsamacı ve karma kamu politikası analizi bakış açısı içerisinde gruplandırılabilir (Smith ve Larimer, 2009: 103, Hill, 2005: 16-22).

Rasyonalist yaklaşım, karar almada akılcı davranılması, politika analizinde elde edilecek bilgiler doğrultusunda çözümlemeler yapılıp, refahın artırılması, kamu tercihine bağlı kalınması, verilerin multidisipliner bir şekilde değerlendirilmesi ve halk katılımının sağlanması amaçlarına sahiptir (Andrews, 2007: 161). Yaklaşım, kökenlerini rasyonel ve pozitivist kökenler temelinden almakta ve toplumsal politikaların probleme ilişkin tüm verilerin elde edilmesi ve akabinde analiz edilmesiyle mümkün olacağı ön kabulüne dayandırmaktadır (Leoveanu, 2013: 43). Burada, duygu ve değerler geri plana itilmektedir. Dönemsel olarak ikinci dünya savaşı sonrası Keynesyen politikalar ve refah devleti eğiliminin etkisindedir.

Rasyonel Kamu politikası analizinin temelleri, Easton'ın (1965: 77) sistem analizi yaklaşımında yer alan analiz sürecinin Jenkins (1978: 17) tarafından başlama, bilgilenme, düşünme, karar verme, uygulama, değerlendirme ve sonlandırma basamakları olarak belirlenmesi ve nihayet bu basamakların geliştirilerek Lasswell (1971) tarafından kamu politikası analizine uyarlanmasıyla oluşmuştur. Yaklaşıma göre, kamu politikası maksimum toplumsal kazanımlı sonuca ulaşmayı amaçlamaktadır. Bu da demektir ki "hükümetler, topluma en yüksek miktardaki maliyetleri aşan kazançları sonuç veren kamu politikalarını seçmelidirler ve hükümetler kazançların maliyetleri karşılayıp geçemediği politikaları terk etmelilerdir" (Çevik, 1998: 109). Lasswell'in ortaya koyduğu bu geniş kapsamlı bilgiye dayanan rasyonel yaklaşım, zamanla eleştirilere uğramıştır. Bu eleştiriler yeni bir yaklaşım doğurmamış, rasyonellik modelinin gerçek dünyadaki politika üretim sürecine uymasını sağlayacak bir takım farklı görüşler getirmiştir.

Rasyonel kamu politikasına eleştiri niteliğinde olan görüşlerin başında Simon'ın (1957) "sınırlı rasyonalite" kavramı gelmektedir. Ona göre karar vericiler, uygulanacak politika ile ilgili sınırlı bilgiye sahiptir ve diğer politika alternatifleri ile ilgili tüm seçenekleri aynı anda düşünememektedir. Sonuç olarak karar vericiler "en iyi" kararı değil, en "memnun edici" kararı vereceklerdir (Enserink, vd., 2013: 20). İkinci bir eleştirel görüş ki bu görüş eleştirel olmaktan çok rasyonel modele karşı çıkan bir görüştür; Linblom'a (1959) aittir. Lindblom (1959: 80-81), o döneme dek alan yazınını esir almış olan rasyonel kamu politikası analizi yerine, yazında bir hayli ihmal edilen ve geri planda bırakıldığını vurguladığı ve "ikinci metot" olarak adlandırdığı "ardışık sınırlı mukayese" kavramını formüle etmeyi amaçlamıştır. Ona göre birinci metot olan rasyonel metot yalnızca çok basit ve tek amaçlı ya da değişkenli problemlere çözüm olabilecek politikalarda bir nebze başarıya ulaşabilecektir ancak bunun yanında karmaşık kamu politikalarında başarılı olmayacaktır. Karar vericiler asla tüm değerleri, tüm politika alternatiflerini ya da tüm politika çıktılarını aynı anda düşünemeyeceklerdir. Göz ardı edilen değer,

alternatif ya da sonuçlar olacaktır. Ayrıca, geçmişte üretilen politikalar yeni üretilecek olan politikaları da sınırlayacaktır. Politika üreticisinin bilgileri önceden üretilmiş politikalarla önemli bir derecede sınırlandırılmıştır. Bu yüzden uzun dönemde çözüm getirecek politikalara ulaşılamayacak, bunun yerine önceden uygulanmış politikaların üzerine küçük eklemeler yapılarak kısa vadede çözüm sunacak politikalar üretilecektir. Buna artırımcı, inkrementalist ya da tedrici (Çorbacıoğlu, 2008: 36) model denilmektedir.

Wildavsky'nin (1979) savunusu, görüşü Lindblom'dan çok da ayrılmasa da kamu politikası analizinde özellikle devlet ve vatandaşlar arasındaki çıkar ve fayda dengesinin kurulması ya da arzulanan amaçların ortak bir noktada buluşması üzerine kurulmuştur (Hoppe, 1999: 206). Düşüncesinin çoğulcu bir temele yönelmesinde demokrasi üzerine derin çalışmaları bulunan Robert Dahl'dan etkilenmesi önemli bir rol oynamıştır. Diğer yandan Lindblom'um inkrementalist modelinden etkilenmiş ve dahi bunu devlet bütçesine uyarlamıştır. Devlet bütçelerinde yeni yıl için ayrılacak finansman kaynakları bir önceki yılın verileri dâhilinde oluşturulmakta ve bu kararın verilmesinde siyasi mekanizmaların diğer çıkar gruplarıyla birlikte tartışmaları etkili olmaktadır. Alınan kararlar bu gruplardan hangisinin galip geleceğine bağlıdır (Çorbacıoğlu, 2008: 40).

Kamu politikası analizinde post-pozitivist ya da yorumsamacı yaklaşım, rasyonel yaklaşımdaki daha çok ekonomik temeller üzerine kurulmuş olan politika üretim sürecine karşı çıkan ve gerçekler-değerler ayrımını yaparak değerlerin önemini vurgulayan bir yaklaşımdır (Fischer, vd., 2007: 19). Postmodernizmin ve yorumsamacı paradigmanın etkilerini taşıyan yaklaşım, politika analizinin yapısını lineer, süreçsel, ve akılcı bir kalıptan çıkararak; karmaşık, çok sesli, keskin çizgileri olmayan ve çoğunlukla tartışmacı bir kalıba taşımıştır (Lejano, 2013: 98-112). Çok seslilik konusunu destekler bir şekilde rasyonel yaklaşıma getirdiği temel eleştiri, rasyonel politika analizinin demokratik bir sistemin ihtiyaçlarına cevap veremiyor olmasıdır. Bunu yanında politika analizinin amaçları arasında sosyal değerler göz

ardı edilmektedir. Örneğin, eğitim kalitesini artırmak üzere üretilen bir kamu politikasında para kaynağının ve dolayısıyla maddi imkânların artırılmasına rağmen okulun eğitim kalitesi artmayabilir. Bu durumda paranın bir önemi yoktur. Gerekli olan şey kurumsal ve maddi olmayan bir değişimdir. Bu değişimdeki girdiler ve ölçütler ampirik veri olarak değil, sosyal değer olarak hesaba katılacaktır. İstatistiksel olarak bir değeri olmayan faktörler göz önüne alınmalıdır. Böylece politika analizinin sonuçları yorumlayıcı bir şekilde değerlendirilecektir (Smith ve Larimer, 2009: 118).

Çevik (1998: 108-111), çalışmasında bazı kamu politikası analizi yaklaşımlarına yer vermiştir. Bu yaklaşımlar *kurumsal yaklaşım*, grup yaklaşımı, elit (seçkinci) yaklaşımı, ussal (rasyonel) yaklaşım, artırımcı yaklaşım (inkremental), sistem yaklaşımı ve süreç yaklaşımıdır. Kurumsal yaklaşım; parlamento, hükümet, bakanlıklar, mahkemeler ve belediyeler gibi kurumların ve bunlar arasındaki ilişkilerin daha çok biçimsel ve hukuki yönlerini tanımlamak ve incelemekle ilgilenen bir yaklaşımdır. Yaklaşıma göre kurumsal yapı, düzenleme ve işlemler kamu politikası açısından önemli faktörlerdir. *Grup yaklaşımı*; kamu politikasını grup mücadelelerinin bir sonucu olarak gören yaklaşımdır. Bireyler, amaçlarını gerçekleştirmek üzere ortak ya da benzer amaçları taşıyan grupların içerisine girerek kamu politikalarına etki güçlerini artırmaktadırlar. Kamu politikası ise bu mücadeleler sonrası oluşan dengeden ibarettir. Bu yaklaşımın en kritik ve kamu politikası açısından tehlikeli sayılabilecek noktası şudur; siyasal sistem ve kamu politikaları kurumlar, ideolojiler ve personel gibi faktörler göz ardı edilerek yalnızca bir grup mücadelesi olarak düşünülürse, ortaya çıkacak açıklama verimsiz ve yanlış yönlere giden bir açıklama olabilir. Dolayısıyla sayılan faktörler de göz önüne alınmalıdır. *Elit yaklaşım*a göre, kamu politikalarını şekillendirenler gücü ellerinde bulunduran seçkin gruptur. Kamu politikalarına halk ve aktörler değil bu grup yön vermektedir. Yine de, bu görüşe göre elitler halkın zararına kamu politikaları üretiyor değildir. Halkın refahı kamu politikalarını oluşturan bu söz

konusu elit sınıfın omuzlarında yükselmektedir. Yazara göre kamu politikalarının karar verme kısmını en iyi şekilde açıklayan *ussal yaklaşım* ise en yüksek düzeyde kamu yararını sağlayan politikaya ulaşmayı amaçlamaktadır. Maliyetleri kazanımlarından yüksek olan kamu politikaları bu yaklaşıma göre terk edilmelidir. Ussal yaklaşımın detayları ve basamakları başlığın ilk bölümlerinde farklı bir sınıflandırmada (rasyonel ve post-pozitivist) verilmiştir. Linblom'un (1959) ortaya koyduğu *artırımcı yaklaşımın,* rasyonalizme tepki olarak ortaya çıktığı savunulabilir. Bu yaklaşımda, yeni sorunlar için önceden uygulanmış kamu politikalarının üzerine yapılan ilavelerle oluşturulmuş kamu politikaları vardır. Easton (1953) tarafından ortaya konulan *sistem yaklaşımı*nda, sisteme karşı gelen politika istemleri insanlardan ve gruplardan gelmektedir. Yaklaşımda sistem ve sistemin çevresi bir bütün olarak görülmekte ve kamu politikalarının sistemin çevresinin isteklerine verdiği tepkinin bir sonucu olarak ortaya çıktığı düşünülmektedir. Bu anlamda istekler birer girdi olarak sistemin içerisine girer ve birer çıktı, kamu politikası olarak çıkar. Son yaklaşım olan *süreç yaklaşımı*nda ise kamu politikası bir siyasal faaliyetler serisi olarak ele alınmaktadır. Bu faaliyetler bir sürecin kısımlarından oluşmaktadır. Sürecin kısımları; sorunların tespiti, kamu politikası amaçlarının formüle edilmesi, kamu politikalarının meşruiyetini gerçekleştirme, kamu politikalarını uygulama ve kamu politikalarının değerlendirilmesi olarak sıralanmaktadır. Süreç yaklaşımı, kamu politikası çalışan yazarlarca sıklıkça ele alınan bir yaklaşımdır. Kamu politikası analizi üzerine yapılacak olan alan yazını taramalarında, özellikle Türkçe kaynaklarda isimleri sıkça geçen, kamu politikası alanında uluslararası yazında ismi bilinen yazarların önemli bir kısmının kamu politikası analizine bir süreç olarak yaklaştığı gözlemlenebilecektir (bkz. Sabatier, 1991;, Hill, 1997; Hill ve Hupe, 2009;. Lasswell, 1956; Jones, 1977; Jenkins, 1997). Çalışmada, bir önceki başlık olan "kamu politikası" başlığında, kamu politikası sürecine değinilmiştir. Bu anlamda kamu politikası süreci hem kamu politikasını tanımlamaya yarayan bir süreç hem de kamu politikası analizinde kullanılan bir yaklaşım olarak ele alınabilecektir.

Kamu politikası analizi diğer bilimsel çalışmalarda olduğu gibi nitel ya da nicel bir nitelik taşıyabilmektedir. Gül'ün (2015: 12-13) belirttiği üzere nicel bir nitelik taşıyan kamu politikası analizlerinde deney, test, anket, ikincil veri analizi gibi sayısal ağırlık taşıyan, verilerin sayısal değerlerle ifade edildiği ve değişkenler arasındaki ilişkinin daha net olarak belirlendiği iddia edilen yöntemler kullanılmaktadır. Bu anlamda nicel nitelik taşıyan kamu politikaları pozitivist epistemolojiye dayanmaktadır. Nitel nitelikteki kamu politikası analizinde ise olaylar, sorunlar ve olgular kendi doğal süreçlerinde ve ortamlarında, kapsamlı ve bütüncül bir biçimde ortaya koymayı ve daha derinlemesine anlamayı hedefleyen, anlama, anlatma[4] (Hampton, 2009: 228) betimleme, yorumlama ve açıklamanın öne çıktığı analiz çeşididir. Nitel kamu politikası analizi nicel olana göre daha esnek bir yöntem anlayışını içermektedir. Nitel analizler, programda ya da politikada değişkenler arasındaki sınırların karmaşık olduğu ya da iç içe geçtiği ve kesin olarak saptanamadığı, dolayısıyla değişkenler arasındaki ilişkilerin ölçümlenmesinin ve yönünün saptanmasının güç olduğu durumlarda kullanılır. Bu yönüyle nitel kamu politikası analizinde ilişkilerin belirlenmesinin nicel yöneteme göre daha belirsiz ve tutarsız olabileceği düşünülebilecektir. Diğer yandan dikkat edilmesi gereken nokta, nitel kamu politikası analizinde sayısal verilerle ifade edilebilecek bir değerde ziyade toplumsal, kültürel, kitlesel değerler gibi değerlerin optimizasyonunun ön planda tutulduğudur. Bu yönüyle yukarıda ele alınan ve "değerler" vurgusuyla tasvir edilen post-pozitivist kamu politikası analizi yaklaşımına işaret etmektedir. Post-pozitivist kamu yönetimi analizi bir yaklaşım türü olmakla birlikte nicel ve nitel ayrımındaki kamu politikası analizi daha çok bir metodolojik yaklaşımı ifade etmektedir. Konuya benzer bir örnek olarak da Smith ve Larimer (2009: 22) kamu politikası analizine metodolojik yaklaşımlar sınıflandırması gösterilebilir. Yazarlar, ilgili tabloda bu analize yaklaşımları nitel, nicel, işlem maliyeti, risk değerlendirmesi

[4] Buradaki anlatma ile yabancı alan yazınında "narrative public policy analysis" (açıklayıcı politika analizi) anlaşılmalıdır.

ve Delphi tekniği[5] şeklinde sıralayarak bu sınıflandırmayı bir metodolojik sınıflandırma olarak nitelemişlerdir.

Babaoğlu'nun (2017: 522) belirttiği üzere, artırımcı modelin yenilikçi politikalara olan karşı duruşu, var olmayan problemlere karşı yetersizliği ve ani gelişen meselelerde yeterli manevra kabiliyetine imkân tanımaması durumu eleştirilere uğramıştır. Yukarıda bahsedilen, rasyonel kamu politikası analizinin eleştirileri ile bu eleştiriler sonucunda yeni bir yaklaşım eğilimi ortaya çıkmıştır. Bu yaklaşım "karma kamu politikası analizi yaklaşımı" olarak isimlendirilmektedir (Çevik ve Demirci, 2009: 37). Karma model yaklaşımında iki önemli temsilciden söz etmek gerekir. Bu isimler Etzioni (1967) ve Dror (1964)'dur. Her iki isim de yorumsamacı ve rasyonel kamu politikası analizi yaklaşımlarının argümanlarını eleştirmiş ve kendi görüşleri doğrultusunda hem analiz hem de karar verme yöntemlerine eklemelerde bulunmuşlardır. Söz konusu eleştiri ve görüşlere çalışmanın ilerleyen kısımlarında ayrı başlıklar halinde daha detaylı yer verilecektir.

Çalışmanın bu başlığında kamu politikası analizine yaklaşımlar, alan yazınında da sıkça başvurulduğu üzere "girilen bir patikanın gittiği yönde" açıklanmıştır. Alan yazını taramasında incelenen ve yukarıda belirtilen çalışmalarda genel olarak kamu politikası analizinin, belirlenen bir yaklaşım çerçevesinde (örneğin, rasyonel, pozitivist, yorumsamacı, elitist, süreç vb.) ele alınarak, ele alınan belirsiz çerçeveler sınırlarında açıklandığı görülmüştür. Farklı çalışmalarda aynı kavram ve kuramların farklı üst başlıklarla altında, farklı yaklaşımlar çerçevesinde verildiği gözlemlenmiştir. Bazı çalışmalarda kamu politikası analizi yaklaşımları (rasyonel,

---

[5] Delphi tekniği, özellikle politik ya da duygusal ortamlarda karar verme durumunda kalındığında ya da verilecek kararların güç ve baskı grupları tarafından etkilenme ihtimalinin olduğu durumlarda kullanılması gereken bir tekniktir. Özellikleri; karara etkide bulunan düşüncenin kime ya da kimlere ait olduğunun bilinmemesine dayanan "katılımda gizlilik", "grup tepkisinin istatistiksel analizi" ve katılımcıların belirli dönemlerde yapılan ardışık anketlerle diğerlerinin ve kendi düşüncelerini karşılaştırma imkânı bulduğu "kontrollü geri besleme" şeklinde sıralanabilmektedir (Şahin, 2001: 215-216).

yorumsamacı ve karma) kapsayıcı yaklaşımlar olarak verilirken, bazılarında bu yaklaşımlar altında yer verilen karar verme modellerine benzer şekilde “model” olarak isimlendirilmişlerdir (bkz. Leoveanu, 2013). Bu karmaşa, hangi isim ve kavramın bir metodolojiyi, bir kök felsefeyi içeren genel bir yaklaşım olduğunu, hangi kavramların bu yaklaşımlar içerisinde yer alan ve belirli eleştiriler ya da eklenimler doğrultusunda oluşmuş sadece birer karar verme modeli olduğunu iyiden iyiye muğlaklaştırmış gözükmektedir. Bu hususların yanında, kamu politikası analiz ya da modellerini kavramak üzere bir çizgi belirleyebilmek için üzerinde durulması gereken, birçok çalışmanın kesişim noktası haline gelmiş isimler ve konular da göze çapmıştır. Çalışmanın ilerleyen kısımlarında söz konusu isimler ve ortaya koydukları görüşlere detaylı olarak yer verilecek ve akabinde, kamu politikası analizi yaklaşımları ve modellerinin açıklanmasında, anlatılmasında ve sınıflandırılmasında alan yazınında göze çarpan belirsizliği azaltmak niyetiyle araştırmacı tarafından önerilen bir sınıflandırmaya yer verilecektir.

1.3. KAMU POLİTİKASI ANALİZİNDE KARAR VERME MODELLERİ

Kamu politikaları çalışmalarında ve ilgili alan yazınında, kökenlerini çeşitli disiplinlerden temel alan bazı kuram ve modeller yer almaktadır. Bu modeller, uygulamada kamu politikaları üretim sürecinde, özellikle karar verme biçimlerinde kullanılmak üzere bir takım düşünceleri, reçeteleri ve metotları barındırmaktadır. Bu başlık altında, kamu politikaları çalışma alanında yer almış söz konusu model ve yaklaşımlar ele alınmıştır.

1.3.1. Karar Vermede Sınırlı Rasyonalite

Geleneksel karar verme yaklaşımında var olduğu kabul edilen kapsamlı rasyonalitenin, “en iyi ve optimal karara tüm unsurlar ve alternatiflerin değerlendirilmesi ile ulaşılacağı” görüşü Herbert A. Simon tarafından sorgulanmış

ve bu sorgunun çıktısı olarak “Sınırlı Rasyonalite” (Bounded Rationality) kavramı alan yazınına girmiştir. Sınırlı rasyonalite kavramı genel olarak, karar vericinin sahip olduğu bilgi ve analitik yeterliliklerinden kaynaklanan bilişsel sınırlılıklarını, rasyonel karar verme yaklaşımı içerisinde hesaba katan bir anlayışı tanımlamaktadır. Yaklaşım, verilen kararların karar verme sürecinden nasıl ve ne şekilde etkilendiği ile ilgilenen, ekonomiye davranışsal yaklaşım içerisinde ana bir tema olarak da ele alınmaktadır (Simon, 1997: 291). Söz konusu yaklaşım, rasyonel karar alma karşısında, onu eleştiren ve farklı bakış açıları ortaya koyan farklı modellerin de geliştirilmesine öncülük etmiştir.

Simon, karar vermenin doğasında aktörler, değerler, önyargılar, kültür, tarih ve deneyim gibi unsurların iç içe olduğunun kabulünde, rasyonel karar vermenin organizasyonel ve psikolojik bir bağlamda anlaşılması gerektiğini savunmaktadır. Simon’un düşüncesinin temelini oluşturan normatif mikroekonomiye göre, gerçek dünyada “en iyi” ya da “en uygun” kararı almak mümkün değildir ve ekonomik insan aslında “yeteri kadar iyi” ve “tatmin edici” kararları almaktadır. Karar vericiyi optimum karar almaya götürecek sürecin maddi olarak külfetli ya da imkansız olduğu durumlarda ekonomik insan, tatmin edici kararı almaktadır (Simon, 1992: 36’dan akt. Köseoğlu, 2013: 249). Karar vericiler, verecekleri kararların sonuçlarını önceden kesin olarak belirleyip bu sonuçlar arasında karşılaştırma yapamamaktadırlar. Dolayısıyla kararların sonuçları ile bu kararların içerdiği amaçları gerçekleştirmek üzere kullanılan araçlar arasında direkt bir ilişki bulunmamaktadır. Bu minvalde, karar vericiler değerler ve amaçların yoğurulmasından meydana gelen “tatmin edicilik” ile ilgilenirler (Köseoğlu, 2013: 249).

Simon (1972: 161-164), rasyonel karar verme yaklaşımını betimleyici ya da normatif olan, insanların ya da örgütlerin verilen amaçları belirgin olan durumlarda nasıl ve ne şekilde aldıklarını açıklayan bir yaklaşım olarak ele almaktadır. Karar almada, kararların birey ya da örgüt tarafından alınmasından ziyade, kararların

sonucunda ulaşılmak istenen ve bu yönde ortaya konulan hedefler ile içinde bulunulan ve tanımlanan durumların belirgin olması önem taşımaktadır. Tam manasıyla rasyonel olabilmek bir örnek dâhilinde düşünülürse; risk ve belirsizlik gibi unsurlar, aktör tarafından karar almada talep ya da maliyet kalemleri içerisinde yer alabilir. İlk varsayımda aktör, söz konusu unsurlar ile ilgili belirli bir durumda, mevcut durum ile ilgili rastgele bilgiye sahiptir. Daha sonra aktörün söz konusu fonksiyonları ilgili mükemmel bilgiye sahip olduğu varsayımı, aslında aktörün o parametrelerin o durumdaki dağılımları ile ilgili mükemmel bilgiye sahip olduğu şeklinde değişir. Varsayımda meydana gelen bu değişiklik düşünüldüğünde, karar vericinin en iyi kararı vermede yapacağı hesap formülü değişmiş, işlem daha basit ya da daha karmaşık hale gelmiştir. Hesabın durumun belirliliğine göre değiştiği düşünüldüğünde, işlemin genelde daha karmaşık ve zor bir duruma geleceği aşikârdır. Karar vericinin değişen çevre ve şartlarda hesapladığı maliyet unsuru da değişebileceğinden ve karar vericinin çevrede var olan ve kullanabileceği tüm diğer alternatifleri bilmesi de imkânsız olduğundan, bu alternatiflerin de bir belirsizlik ve değişim içerisinde olacağından dolayı en rasyonel kararı almak da imkânsız bir duruma gelmektedir.

Simon (1976), rasyonel ve sınırlı rasyonel karar alma durumlarını iki figür üzerinden betimlemiştir. Bunlardan birincisi “ekonomik insan” figürüdür. Ekonomik insanı tanımlarken hesaba katılacak olan gerçekler ve değerler ayrımının üzerinde özellikle durmuş ve bu ayrımı bir park-bahçe ustası üzerinden örneklendirmiştir. Buna göre (Simon, 1976: 198), ustanın yapacağı işte alternatif olarak değişebilecek fonksiyonlar otların kesimi, bitki ekimi ve temizlik gibi fonksiyonlarken; değerler ise kanunlarca ve sosyal yapı tarafından belirlenen genel görünüm, temizlik düzeyi, rekreasyon ve kullanım biçimidir. Ustanın hesaba katacağı gerçekler; bütçe, çalışma metotları ve birim maliyetlerdir. Bu figürde tasvir edilen ekonomik insanın alacağı kararların da rasyonel ölçüde alındığı

varsayılmaktadır. Bakka ve Fivesdal (1986'dan akt. Simonsen, 1994: 3) söz konusu ekonomik insanı beş maddede şu şekilde özetlemektedir:

-Alternatiflerin olduğu durumlarda, her zaman bir karar verilebilecektir.

-Alternatiflerin sonuçları kişinin değer ölçütlerine göre değerlendirilebilecektir.

-Öncelikli olan işlemler geçişlidir (A>B>C'dir ancak C>B) değildir.

-Her zaman kişinin değer ölçütlerinde en yüksek gelen alternatif seçilecektir.

-Aynı durumlar tekrarlandığında, yine aynı seçimler yapılacaktır.

Ekonomik insan modeli, ideal olarak nitelendirilen rasyonel karar verme yaklaşımını temsil etmektedir. Rasyonel olmak, tam bir bilgi sahipliğini ve eldeki tüm alternatiflerin sonuçlarının tam anlamıyla öngörülebilmesini gerektirmektedir. Uygulamada, bu modelin bir takım sınırlılıkları vardır. Bilinçsizlik, yetenekler, alışkanlıklar, değer yargıları, arz edilen bilgilerdeki sınırlılıklar ve kavrama yetileri gibi unsurlardaki sınırlılıklar buna örnek olarak gösterilebilecektir. Dolayısıyla Barros 'un (2010: 459) belirttiği gibi, ekonomik insanı yönetsel kararlar verme eyleminde ele alırken, onu bir miktar esnekleştirmek gerektiği kabul edilmelidir. Aksi takdirde, ekonomik insanı özne olarak alan bir yönetsel kuram kullanışsız kalacaktır.

Simon'a göre (Simon, 1976'dan akt. Simonsen, 1994: 4) ekonomik insan ve yönetsel insan birbirinden iki ana özellik bakımından ayrılmaktadır. Birincisi, ekonomik insan sahip olunan bütün alternatifler arasından "en iyi" olanı seçerken, onun kuzeni olan yönetsel insan ise memnuniyet verici ya da diğer bir ifadeyle "yeterince iyi olan" alternatifi seçecektir. İkinci olarak ise, ekonomik insan gerçek dünyanın tüm karmaşasıyla uğraşırken, yönetsel insan onu zorunlu bir basit kalıba indirgenmiş bir model olarak kavrar. Ekonomik insanda olduğu gibi dünyanın tüm

karmaşıklığını ve o karmaşıklıktaki faktörlerin birbirleriyle olan ilişkilerini değil, sadece içerisinde bulunduğu karar alma safhasında, ilgili ve önemli gördüğü durumları hesaba katarak bir seçim yapacaktır. Dolayısıyla yönetsel insan (Bakka ve Fivesdal, 1986'dan akt. Simonsen, 1994: 4), sınırlı alternatifler ve bu alternatiflerin olası sonuçları hakkında sınırlı bir bilgiyle ve yeterince iyi alternatifi seçerek karar verecektir. Sınırlı bilgi ile memnun edici seçimleri yapacak olan yönetsel insan, aynı zamanda bağlantılı seçimler arasından, kapsamlı bir gözlem ve içeriğe dayanmayan, kendi sezgilerince belirlenmiş seçimler de yapabilecektir.

Sınırlı rasyonalite yaklaşımı, karar verme çalışmaları açısından bir dönüm noktası olarak görülebilecek bir yaklaşımdır. Özellikle modernizmin bir yansıması olarak bilimsel alanda uzun bir dönem başat olarak hüküm süren pozitivist ve rasyonel yöntem ve yaklaşımların eleştirilmeye başlanması, eleştirilerin akabinde tamamlayıcı ya da tersine yapıbozumcu olarak tanımlanabilecek farklı karar verme yaklaşımları ortaya çıkmıştır. Bu yaklaşımların ortak noktaları, karar vermede tam anlamıyla bir rasyonalite durumuna karşı çıkmaları ve bunu eleştirmeleri olarak ele alınabilecektir. Bunun yanında rasyonel kamu politikası analizine getirdiği eleştirilerin yanında, sınırlı rasyonalite yaklaşımı; rasyonel açıdan tam olarak bağımsız olamayan, onu eleştiren ve bir diğer yönüyle tamamlayan, daha sonraki dönemlerde güçlenen yorumsamacı kamu politikası analizi açısı ile arasında bir köprü olan düşünce sistematiği olarak ele alınabilecektir.

1.3.2. Savunma Koalisyonu Modeli

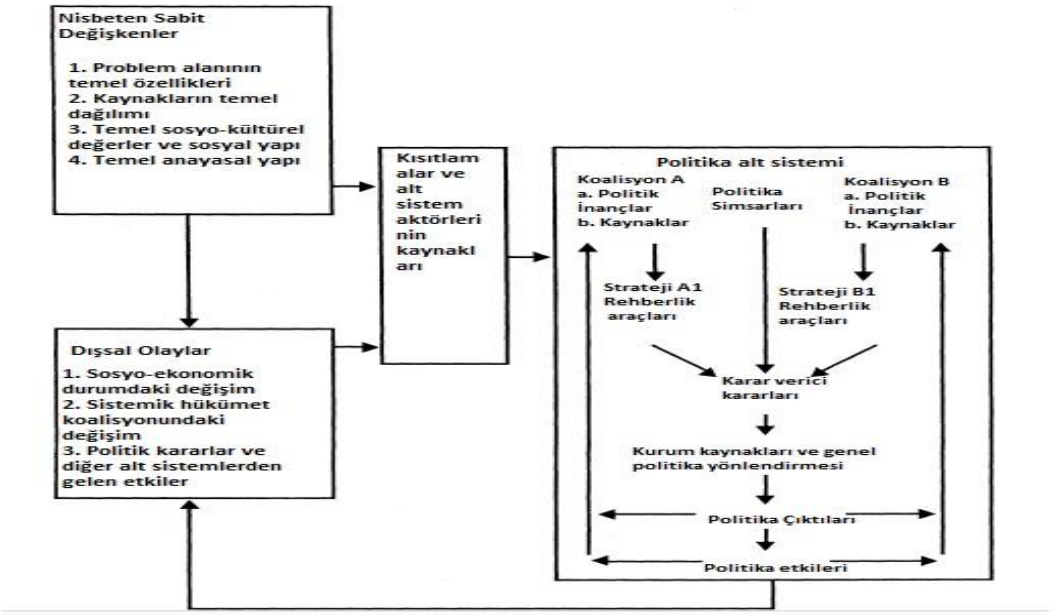
Savunma koalisyonu modeli Sabatier'in (1987) ortaya koyduğu bir modeldir. Sabatier, ortaya koyduğu modelden önceki dönemlerde kamu politikası analizinin daha çok kamu politikalarında karar verici pozisyonlarda bulunan üst düzey yöneticilerin teknik yaklaşımlarına dayandığını vurgulamaktadır. Kamu politikası üzerine olan bu algı ve yaklaşım tarzı son yıllarda, aynı gelenekten gelen

yazarlarca “verilen belirli bir resmi yapıda, değişen sosyo-ekonomik bir çevrede, farklı değer ve çıkarlara sahip grupların bir güç mücadelesi” (Sabatier, 1987: 650) olarak popülerlik kazanmıştır. Sabatier’in ortaya koyduğu bu model o zamana dek alan yazınında yer alan ve “bilginin kullanımı” ve “politika değişimi” üzerine ortaya atılan görüşlerin bütünleşmesine yönelik bir çerçeve sunmaktadır. Ayrıca bu çerçeve, politika analizinin politika odaklı öğrenme üzerindeki rolü ile politika değişimi üzerindeki rolünün ayrıştırılabilmesinde kullanılabilecektir. Sabatier (1987: 650) kurduğu bu iskeletin özellikle şu konular üzerinde kuramsal tartışmalara ve ampirik bulgulara yer vereceğini vurgulamaktadır:

- Politika analizi, örgütsel pozisyonların ve çıkarların açığa vurulmasında sık olarak bir savunma üslubuyla kullanılmaktadır.
- Bunun etkileri genellikle uzun vadede, günlük ilişkilerindeki algılarına ve iç dünyalarına kadar yayıldığında görülebilmektedir.
- Bilişsel olmayan (kavramak ya da idrak etmekle ilgili olmayan), kurumsal düzenlemeler, politik kaynaklar ve örgütsel çıkarlar gibi faktörler politika değişiminde büyük rol oynamaktadır.

Yukarıdaki sıralanan tartışmalara göre, yazarın ortaya koyduğu model en iyi şekilde, belirli politik arenada faaliyet gösteren ve güçlü bir inanç sistemi olan örgütlerde gözlemlenebilecektir. Politika odaklı öğrenme, örgütün belirli bir politik alanda, belirli inanç ve değer sistemiyle birlikte politikalara etki etme eylemindeki süreç, fonksiyon ve araçları kapsamaktadır. Bu durum aşağıdaki şekilde daha net görülebilecektir.

Şekil 2: Politika Alt Sistemlerindeki Rekabetçi Savunma Koalisyonlarına Odaklı Politika Değerlendirmesi Genel Modeli.



Kaynak: Sabatier, 1987: 653.

Şekilde görüldüğü üzere politikanın seyrini etkileyen, politikanın üzerine kurulduğu örgüt yapısı, sosyo-kültürel değerler, sosyal yapı, anayasal yapı gibi önceden belirli olan değişkenler vardır. Sabatier bu değerleri politika odaklı öğrenmenin bir unsuru olarak ele almaktadır. Söz konusu değişkenlerin dışında bir de gerçek dünya vardır ve bu dünya herhangi bir zaman diliminde (politika sürecinin içinde ya da dışında) değişebilecek değişkenleri içermektedir. Sabatier, politika odaklı öğrenme ve diğer dışsal değişimler üzerinde meydana gelebilecek değişikliklerin arasındaki bu ayrımı net bir şekilde vurgulama çabasındadır. Sabatier, bu vurgulamayı yaparken Heclo'ya (1974, 1978) verdiği atıflarda, Heclo'nun politika odaklı öğrenmede, bireysel ve örgütsel çıkarlar, sistemin yapısal dinamikleri, problem parametreleri gibi unsurları göz önüne aldığını, kendi ortaya koyduğu ayrımda ise daha geniş bir bakış açısıyla savunma koalisyonları ve grubun inanç değerleri gibi unsurların da hesaba katıldığını vurgulamaktadır. Heclo ile arasındaki bu ayrım farklılığını üç

sütunda toplamaktadır. Bunlardan birincisi, Sabatier'in politika alt sistemlerini, politika analizinde birer ünite olarak toplamasıdır. İkincisi bu modelin savunma koalisyonlarına odaklanmasıdır. Son olarak sistem dinamiğinin anlaşılmasında politika odaklı öğrenmenin kritik bir faktör olduğunun kabulüdür (Sabatier, 1987: 654).

Sabatier (1987: 660-661), ABD'nin hava kirliliği politikaları üzerinden tasvir ettiği modelinde aktörlerin önemini de vurgulamaktadır. Örneğin, ABD hava kirliliği politikalarında yer alan aktörler; Çevre Koruma Ajansı, farklı ajansların politika ile ilgili başkanlıkları, tüketici birlikleri, ilgili diğer birlikler, konu ile ilgili araştırma enstitüleri, araştırmacı gazeteciler ve diğer ülkelerdeki aktörlerdir. Yazar bu aktörlerin farklı kökenlerden ve farklı kurumlardan gelerek ortak bir inanç sistemini paylaşan grup liderleri, araştırmacılar ve memurlar olduklarını belirtirken bu farklı aktörlerin bir koalisyon oluşturduğunu ve buna "savunma koalisyonu" adını verdiğini belirtmektedir. Sabatier'e göre belirli bir politika için uzun dönemde (on yıllar) meydana gelen tekrarlı koalisyonlar zamanla sayıca azalarak daha etkili hale gelebileceklerdir. Diğer yandan yeni bir politika üretmek için kısa vadede birden çok koalisyon oluşabilecektir. İlk durumda koalisyonlar sayı ve yoğunluk bakımından daha küçük kalabilecektir. Bu durum, orta ve uzun vadede politikayı etkileyecek olan koalisyonların inanç sistemlerinin benzeşerek koalisyonların birleşmesinin sonucudur. ABD'de 1970'lerden bu yana hava kirliliği konusunda kurulan koalisyonlar son durumda iki ye ayrılmaktadır. Birinci koalisyon, koşulsuz şartsız hava temizliğine ve buna bağlı olarak insan sağlığı ve ekosisteme odaklanan gruptur. İkinci grup ise daha çok uygulanacak olan politikaların ekonomik fizibilitesine odaklanan ve kar-zarar, işlem maliyeti gibi unsurları bu politikada ön plana alan gruptur.

Sabatier, kendi modelinin farkını "inançların çıkarlardan daha iyi bir birleştirici olması" tezine dayandırmaktadır. Ona göre, Sierra Club liderlerinden de verdiği örnekle; bir örgütte mensupların algısındaki örgüt amaçları ve çıkar tanımları

değişebilmektedir. Bunun yanında örgütün inanç sistemi yani sahip olduğu ideoloji, örgüt mensupları tarafından daha çok içselleştirilmiştir. Örgütü bir kamu politikası üretiminde, politikayı etkilemek bakımından bir arada tutan yapıştırıcı çıkar ve amaçlardan çok bu inanç sistemidir. İnanç sistemleri, ideolojiler amaçlar ve çıkarlar gibi çabuk değişen unsurlar değillerdir. Kısa dönemli amaçlar ve kar hedefleri olabileceği gibi bu amaç ve hedefler kısa bir dönem içinde de değişebilecektir. Yine de bir koalisyondaki tüm inançların bir olduğunu düşünmek gerçeklikten uzaktır. Önemli olan (ki bu aynı zamanda Sabatier'in ikinci tezidir) inanışların genelinin, özünün aynı olmasıdır ve politikaların özüne de bu ortak olan inanışlar etki edecektir. Üçüncü tezi ise; koalisyonların, uyuşmayan ya da farklılık gösteren ikincil görüşlerinin, bir politikanın zayıf yönleri üzerinde çatışmaya girmeden yok olmasıdır. Böylece bir politika üzerindeki görüş birliğinin sağlanmasında, farklı olabilecek ikincil görüşlerin etkisi de yok olabilmektedir (Sabatier, 1987: 668). Sabatier'in dördüncü tezi, hükümet eylem planlarının ve genel politikaların onların alt sistemlerinde yer alan ve politikalara etkide bulunan savunma koalisyonları değişmedikçe önemli ölçüde aynı kalacağı ve büyük bir revizyona uğramayacağı üzerine kurulmuştur (Sabatier, 1987: 670). Buradaki vurgu, koalisyonların temel ve genel inançlarının değişmeyecek olmasına dayanmaktadır. Ona göre, koalisyonlar politikalara özlerindeki inançlar doğrultusunda etki etmektedirler. Savunma koalisyonlarının politika üzerindeki ikincil tavırları değişken olabilecekse de bu koalisyonlar öz inançlarını sadece politikaya etkide kalabilmek adına değiştirmeyeceklerdir. Beşinci tezinde ise dördüncü tezine paralel bir şekilde, alt sisteme dışarıdan sosyo-ekonomik değişimler, iktidar koalisyonları ve başka politikaların çıktılarını etkisi gibi önemli endişe verici unsurlar gelmedikçe hükümet eylem planlarının genel politikalarının değişmeyeceğidir.

Usta'nın da (2013: 78) belirttiği üzere Sabatier, kamusal eylemlerde ve kamu politikası üretim sürecinde her sektörü ayrı bir koalisyon kabul etmektedir. Kamu politikasının oluşturulmasında büyük ya da küçük çaplı farklı koalisyonlar yer

alabilecektir. Bir koalisyon kendi inanç ve görüşlerini diğerlerine kabullendirebilecek bir güçte ise bu koalisyonlar dominant olarak nitelendirilmektedir. Koalisyonların yalnızca somut kaynakları değil aynı zamanda fikir ve inanışları da kamu politikalarına etki etmektedir. Dahi bu faktörler, örgüt adına politikalara yön vermekte daha dirençli dayanaklardır. Buradaki inanış sistemi problemlerle ilgili olarak algılanan gerçekler, sosyal tasvirler ve temel değerler bütünüdür. Bir politika ancak bir inanış sistemi ile ileri sürülebilmektedir. Sabatier'in ortaya koyduğu bu yaklaşım, modernist dönemin rasyonel ve sayısal değerlerine değil, inanış sistemlerine ve değerlere önem verirken, bu yönüyle post-pozitivist ya da yorumsamacı ya da post-modern kamu politikası analizi içerisinde yer alabilecek bir yaklaşım olarak değerlendirilebilecektir.

1.3.3. Artırımcı (İnkrementalist) Karar Verme Modeli

Charles Lindblom tarafından geliştirilen bu model, rasyonel kamu politikası analizi yaklaşımına bir muhalefet olarak ortaya çıkan karar verme modellerinden birisidir. Bu model, amaçlar ve amaçları gerçekleştirmek üzere uygulanması gereken eylemleri birbirinden bağımsız değil, birbirlerine yakın unsurlar olarak görmektedir. Dolayısıyla araç ve amaç çözümlemesi bir kamu politikası için yeterli değildir ve sınırlı kalmaktadır. Rasyonel politika analizini eleştirdiği nokta ise soruna yönelik sınırlı sayıda politika seçeneği vardır ve bu doğrultuda sınırlı sayıda sonuç göz önüne alınmalı ve öngörülmelidir (Erat ve Kaçer, 2014: 62). Lindblom'un modelinin ortaya çıkışında etkili olan temel düşünce, insan problemlerinin inanılmaz derecede karmaşık bir yapıya sahip olmasının yanında, bunların çözümü için yine insan tarafından üretilecek politikalarda, insan aklının analitik kapasitesinin ve kaynakların çok sınırlı oluşudur (Lindblom, 1959). Lindblom (1959: 81), ortaya koyduğu modele, o zamana dek politika analizi için var olmuş iki metodun bir analize bakış açısının karşılaştırması ile başlamaktadır. Söz konusu karşılaştırma aşağıdaki tabloda verilmiştir.

Tablo 1: Politika Analizi İçin Metot Karşılaştırması

Rasyonel – Kapsamlı (Kök)	Ardışık Limitli Karşılaştırma
Amaçların veya değerlerin alternatif politikaların ampirik istatistiki verilerden ayrı ve belirgin olarak açıklanır.	Değerler, amaçlar ve gereken eylemin ampirik verileri belirgin şekilde ayrılmaz ve birbirleriyle iç içe geçmiştir.
Politika formülasyonu sebep – sonuç analizi için kullanılır. Öncelikle sonuçlar sebeplerden yalıtılmıştır, sebepler daha sonradan sonuçları gerçekleştirmek için kullanılır.	Sebepler ve sonuçlar belirgin, açık ve ayrılmış olmadıkça, sebep-sonuç analizi uygunsuz ve kısıtlıdır.
İyi bir politika, arzulanan sonuçlara en uygun sebeplerin belirlenmesi olarak kabul edilmektedir.	İyi bir politika, analizcilerin üstünde en çok uzlaştığı politikadır (bu uzlaşı, en uygun sebep ve sonuçların belirlenmesi üzerindeki bir uzlaşı olarak görülmemelidir)
Analizin kapsamlı olduğu ver her detayı hesaba kattığı düşünülür.	Analizler çok ciddi ölçüde kısıtlıdır. En önemli olası sonuçlar, alternatif olabilecek politikalar ve etkilenebilecek değerler göz ardı edilir.
Kurama sıkı bir şekilde güvenilir.	Başarılı bir karşılaştırma, kuramı arka plana itebilir.

Lindblom'un (1959: 82) özetlediği üzere yukarıda tabloda verilen iki bakış açısı arasındaki fark, analizlerde yer alan amaçlar ve değerler arasında yapılan seçimlerdir. İlk bakış açısında ilerleyen bir analizci öncelikle ampirik verileri ve değerlendirmeyi iç içe alarak, değerler ve amaçlar arasından önemli göreceği amaçların kendisine yönelik politikayı seçecektir. İkinci bakış açısında ilerleyen bir analizci de bir seçim yapacaktır ancak birinci analizciden ayrı olarak amaçlardan çok marjinal ya da artırımcı değerler üzerine odaklanacaktır. Bu analizci, amaçların genel formülasyonunu yararlı görmeyerek marjinal ve artırımcı kıyaslamalar yapacaktır. Bu kıyaslamaları yaparken şu yol izlenecektir; iki alternatif politikanın var olduğu düşünüldüğünde, birinci politika gerçekleştirilmesi gereken beş adet amaçtan üçüncüsünü daha büyük oranda gerçekleştirecektir. İkinci politika ise üçüncüye nazaran dördüncü amacı daha çok gerçekleştirmektedir. Burada analizci, iki politikadan birini seçerken gerçekleştirilen ve birbirinden farklılaşan bu amaçlardan (üçüncü ve dördüncü) hangisinin marjinal değerlerinin fazla olduğunu belirleyerek seçimini fazla olandan yana kullanacaktır.

Rasyonel bakış açısına sahip analizde, önemli olan her şeyin hesaba katıldığı görüşü hâkim olsa da, neyin "önemli" olduğu kapsamlı bir şekilde açıklanmadığı,

açıklanmaya gerek duyulmadığı için bu analiz çeşidinin çok sınırlı olduğu belirtilmelidir (Lindblom, 1959: 84).

Artırımcı karar vermek, problemlere yönelik daha önceden belirlenmiş, uygulanmış ve sonuca ulaşmış politikaların, yine benzer ve bir yönüyle problemler karşısında revize edilerek yeniden üretilmesi ve uygulanması olarak düşünülebilecektir. Bu yönde verilen kararlar, politikaya etki etmek isteyen aktörlerin ya da grupların, politika sonuçlarını daha kolay öngörebilmesini sağlayacaktır (Lindblom, 1959: 86). Bu yüzden karar vericiler, sonuçlarını ve aktörlerin tepkilerini kestiremeyecekleri sıfırdan politikalar üretmek yerine, önceden uygulanmış politikaları farklı ya da benzer sorunlar için yeniden değerlendirerek, hedeflenen marjinal fayda ya da değerlere yönelik revizeler yaparak benzer politikaları uygulayacaklardır. Söz konusu artırımcı kararlar yukarıdaki tabloda verilen birinci ve ikinci metottan ikicisine uymaktadır. Rasyonel metot ile üretilecek olan politikalar, kuramı bir politika üretmede tek yol olarak görür ve kurama sıkı sıkıya bağlı kalarak bir yönüyle de yeni baştan bir politika üretmeyi kabul ederken; karşılaştırmalı analiz yönteminde kuram sadece sistematik karşılaştırma yerine kullanılacak bir alternatif olarak kalabilmektedir. Bu karşılaştırmada, rasyonel ve kök olan analizdeki savunulan “en iyi” olan politika ve karar yerine, yeniden tanımlanan ve semptom problemlerden türeyen yeni problemlerin çözümü için “makul” politikalar üretilecektir. Lindblom daha sonra yaptığı çalışmalarda da artırımcı karar verme üzerine olan yorumlarını geliştirmiş ve bu karar verme modelinde siyaset ile analizi birbirinden ayırmıştır. Artırımcı karar vermenin kendi içindeki üç türünden bahsetmiştir. Siyaset kısmında basit ve küçük adımlarla siyasal değişmeyi anlatan “siyasal bir örüntü olarak artırımcılık”, analiz kısmında ise basit artırımcı analiz, parçalı artırımcı analiz ve stratejik analiz olmak üzere bölümlendirilmiştir. Basit artırımcı analiz; artırımcı olarak farklılaşan alternatif politikaları seçimi, parçalı artırımcı analiz; belirli taktiklere ve metotlara odaklanarak politika seçimi, stratejik analiz ise karmaşık olan politika problemlerinin daha basite indirgenmesi için

hesaplanan ya da dikkatle seçilen taktiklerin bir setini ifade etmektedir (Köseoğlu, 2013: 251).

Duruma ülke yönetimleri ve hükümetler açısından bakıldığında, önceki iktidarların yerine gelen yeni iktidarlarda, baskı gruplarının çok tepkisini çekmemek adına, oluşan ya da yeniden tanımlanan problemler karşısında bir önceki iktidar döneminde uygulanan politikalara benzer politikalar uygulayacaklardır. Böylece, önceden ölçülen ve halen korunan değerlere karşı, politika neticesinde oluşacak olan tepkiler de kontrol altında tutulmuş olacaktır. Sonuç olarak karar vericiler yeni sorunlar tanımlamak ve amaçlarlar belirlemek yerine önceki benzer sorunlar için belirlenmiş amaçların üzerine ilave sorunlar ve amaçlar belirleyerek politika üreteceklerdir.

1.3.4. Normatif Optimum Karar Verme Modeli

Rasyonel karar alma modelinin eleştirisi üzerine kurulan artırımcı karar alma modeli, Yehezkel Dror tarafından eleştirilmiş ve bu eleştiri sonucunda ortaya Normatif Optimum Karar Verme Modeli ortaya çıkmıştır. Dror'un (1964) temel eleştirisi, artırımcı modelde savunulduğu üzere kararların her zaman önceden alınmış kararlar üzerinden tasarlanmayacağı, geçmiş politikaların sonuçlarının arzulandığı gibi olmadığı durumlarda ve yeni bir politika sorunu çıkması ve geçmiş dönemlerde benzer bir soruna yönelik üretilmiş bir politika bulunmadığı durumlarda yeni ve radikal politikaların üretilebileceğidir (Köseoğlu, 2013: 253).

Dror (1964: 154), çalışmasına öncelikle artırımcı karar verme modelinin sınırlı kaldığı durumları açıklamakla başlamıştır. Bu durumlardan ilki, alınacak kararların genel memnuniyeti sağlaması gerektiği durumlardır ve bu durumlarda politikalar üzerinde radikal değişiklikler yapmak önemlidir. Eski politikaların, oluşan yeni durumlar için (yeni sosyo-ekonomik yapı, değişen bilgi, teknoloji ve kültürel unsurlar) çözüm üretemediği noktalarda, yeni politikalar tasarlanmalıdır. Örneğin,

ekonomik olarak gelişmekte olan ülkelerde, önceki dönemlerde üretilen ekonomi politikaları, içinde bulunulan dönemde çözüm üretemeyebilecektir. İkinci durumda, artırımcı politikaların uygulanabilmesi, problemlerin doğasının yüksek derecede benzerlik göstermesine bağlıdır. Yeni kaynaklardan oluşan problemler, ya da kökü itibari ile geçmişte edinilen tecrübelerden bağımsız olan problemlere karşı artırımcı politikalar üretilemeyecektir. Söz konusu problemlere karşı yeni politikaların geliştirilmesi gerekecektir. Son durumda ise artırımcı kararlar alınabilmesi için problemlerin çözümü için mevcut olan araçların da devamlı olması gerekmektedir. Önceden ortaya çıkmış problemlerin çözümünde kullanılan araçlar, yeni oluşan problemlerin çözümünde kullanılmak üzere, halen mevcut olmayabilecektir. Gelişen ve değişen teknolojiye bağlı olarak çıkan yeni altyapı ve teknik problemlere karşı üretilecek çeşitli politikalar da son iki duruma yönelik örnekler olarak düşünülebileceklerdir. Bu eleştirileriyle birlikte Dror (1964: 156), geleneksel olan rasyonel model ve Lindblom'un (1956) artırımcı modelini yeniden değerlendirerek Normatif Optimum Modelini ortaya koymuştur. Normatif optimum modelin özellikleri ise aşağıdaki şekilde sıralanabilecektir:

-Değerler, amaçlar ve karar kriterleri belirlenmesi.

-Eldeki verilerin, araştırma sonuçlarının ve deneyimlerin kullanılması ve bilinçli bir çabayla, yenilikçi ve yaratıcı alternatiflerin düşünülmesi.

-Minimal risk stratejisi ya da yenilik stratejisinin tercih edilmesi konusunda alternatiflerin ve kararların ortaya çıkaracağı sonuçların tahmin edilmesi.

-Yukarıdaki madde yer alan ilk strateji izlenecekse artırımcı model kullanılır. İkincisi tercih edilecek olursa, bir sonraki aşamada sonuçların tahmini için eldeki bilgi ve sezgiye dayanılır ve öngörülen sonuçlar tanımlanır.

-Optimum politikanın sağlaması, yukarıda sıralanan ve 1'den 4'e kadar olan aşamaların çeşitli analistler tarafından tartışılarak üzerinde uzlaşması şeklinde gerçekleştirilmektedir.

-Analizi daha kapsamlı bir şekilde gerçekleştirip gerçekleştirmemeye karar vermek için problemin yeterince önemli olup olmadığına karar vermek.

-Kuram, tecrübe ve rasyonalitenin tümünün bunların karışımının kullanılabilirliğine ve problemin doğasına dayanması.

-Deneyimlerden öğrenme, öncülük ve yaratıcılığın uyarımı, personelin geliştirilmesi ve entelektüel çabanın teşvik edilmesi gibi politika üretiminin kalitesini artırıcı açık anlaşmalar yapmak.

Dror (1968), yukarıda özellikleri sıralanan normatif optimum politika yapım modelini daha sonra geliştirip üç ayrı aşamaya ayırarak açıklamıştır. Köseoğlu'nun (2013: 255-256) belirttiği üzere bu aşamalar; meta politika yapımı, politika yapımı ve post politika yapımı aşamalarıdır. Sayılan aşamalardan farklı bir aşama olmasına karşın onlarla yakın ilişkide olan karmaşık bir iletişim ve geri besleme ağı bulunmaktadır. Meta politika yapımı, politikanın oluşturulmasının öncesinde, değerler, kaynaklar, sorunlar ve stratejilerin oluşturulması aşamasıdır. Bu aşamada hesaba katılan "değerler" modelin post-pozitivist kamu politikası analiziyle, bir yönüyle kesişim noktası sayılabilecektir. Politika yapım aşaması ise kaynakların dağılımı ve amaçların belirlenmesini içerirken, en iyi alternatif politikanın seçildiği aşamadır. Son olarak post-politika yapım aşaması ise politika uygulamasını ve uygulama sonuçlarının değerlendirmesini içerir. Söz konusu aşamalar, bir yönüyle de rasyonel, basamaklı politika analizi modelini anımsatmaktadır. Dror'un bu yaklaşımı politika analizi yaklaşımlarının daha genel sınıflandırması üzerinden düşünülecek olursa, hem rasyonel hem de post-pozitivist kamu politikası analizinin izlerini taşıdığı söylenebilecektir.

1.3.5. Karma - Tarama Karar Verme Modeli

Karma - tarama karar verme modeli, Amitai Etzioni (1967) tarafından, karar vermede bir "üçüncü yaklaşım" olarak ortaya konulmuştur. Etzioni (1967: 385-387), modelini ortaya koyduğu çalışmasında öncelikle karar vermede rasyonalist yaklaşım ve artırımcı yaklaşımın varsayımlarını sıralamıştır. Bu sıralamanın ardından rasyonalist yaklaşımı bir kenara bırakarak artırımcı yaklaşımın farklı boyutlardaki eleştirileri üzerinde durmuştur. Bu eleştirileri aktardıktan sonra ise kendi ortaya koyduğu model olan Karma – Tarama Karar Verme Modelini açıklamıştır.

Etzioni (1967: 385-386), rasyonalist modeli ele alırken, onun en iyi kararı almak adına bağlı olduğu, belirlenmiş bir süreci vurgulamaktadır. Yazara göre, rasyonel modelde karar vericilerin politika ile ilgili tüm unsurlara hâkim olduğu varsayılırken, artırımcı modelin rasyonel modeli eleştirdiği nokta da bu noktadır. Diğer yandan rasyonel modelde önceden belirlenmiş olarak var olduğu kabul edilen amaçlar, değerler ve beklenen sonuçlar gibi unsurların, sosyal hayattaki karar alma sürecinde değişken olduklarını vurgulanmaktadır. Yazar, bu unsurların birbirlerinden açık bir şekilde ayrıldığı rasyonel karar verme modelini uygulanabilir bulmamaktadır. Rasyonel modelin en büyük handikabı olarak ise, karar vericilerin, rasyonel ve optimum olan, en iyi kararı vermek için gereken bilgiyi edinecek ne zamanları, ne de imkanlarının olmaması durumunu göstermektedir.

Etzioni (1967: 386-387) artırımcı modeli, onun en belirgin altı özelliğini sayarak belirtmiştir. Yazar bu altı özelliği kısaca şu şekilde belirtmektedir:

-Karar vericiler, politika üretmek için yeni baştan politika üretim sürecine girmezler ve kapsamlı bir araştırma yapmazlar. Bunun yerine benzer problemlere karşı önceden üretilmiş politikaları üzerinden, yeniden tasarlanmış politikalar üretirler.

-Tüm politika alternatifleri değil yalnızca sınırlı sayıda politika alternatifi hesaba katılır.

-Hesaba katılan her bir politika alternatifi için yalnızca sınırlı sayıda sonuç öngörüsü değerlendirilir.

-Karar verici, karar verme sürecinde problemle birden çok kez yeniden karşılaşır. Bu karar vericiye, hem sebep-sonuç ilişkilerini sayısız şekilde açığa kavuşturma şansı hem de karar verme sürecini daha iyi kontrol etme imkânı vermektedir.

-Yalnızca tek bir doğru politika ya da çözüm yoktur, bunun yerine konular üzerinde seri şekilde yapılan ve sonu gelmeyen analizler ve değerlendirmeler vardır.

-Artırımcı politikalar, gelecekteki sosyal hedefleri gerçekleştirmekten çok dönemsel sosyal kusurları gidermek şeklinde tanımlanmaktadır.

Etzioni (1967: 387), artırımcı yaklaşımın normatif eleştirisini yaparken, özellikle artırımcı kararlarda katılımcılık sorununa vurgu yapmaktadır. Katılımcılık sorunu, partizanların farklı güç ve pozisyonlarda bulunmasından ve bu unsurlar dolayısıyla politikalara farklı derecelerde etki etmelerinden ileri gelmektedir. Yazara göre, ikinci temel sorun ise artırımcı politikaların, günü kurtarma politikaları ve geçmiş politikaların yeniden inşasına odaklanırken temel toplumsal yenilikleri göz ardı edebilmesidir.

Etzioni'nin (1967: 388) artırımcı karar verme modeline getirdiği ve kendi modelini de onun üzerine kurduğu eleştiri ise "artırımcı" kavramına getirdiği eleştiridir. Yazara göre, ABD'nin geçmiş politikalarında, artırımcı olarak alınmış gibi gözüken kararların çoğu aslında daha öncesinden alınmış temel bir politikanın adımları niteliğindedir. Örnek olarak; ABD'de 1950-1960 yılları arasında bütçe üzerine her dönem alınan kararlar bir önceki döneme göre çok az miktarda değişiklikler içermesi ve önceki alınan kararın bir devamı olması itibarı ile artırımcı bir politika

gibi gözükmektedir. Daha detaylı düşünüldüğünde ise bu artırımcı politikaların temeli aslında ABD'nin Kore savaşına girmesi gibi temel bir politikanın uzantısı olarak gelişmiştir. Diğer yandan artırımcı kararlar daha küçük, güvenli ve doğru politika adımları olarak nitelendirilirken, karar vericinin, bu adımların gerçekten doğru ve güvenli olup olmadığını değerlendirmesi de onu artırımcı düşünceden çıkarıp daha kapsamlı ve temel bir düşünce sistemine itecektir.

Etzioni (1967: 289), Kendi ortaya koyduğu Karma - Tarama Karar Verme Modelini anlatmak için okuyucudan bir simülasyon hayal etmesini istemektedir. Buna göre, dünyanın tümündeki iklim hareketlerini takip etmek üzere iklim panelleri kullanılarak bir gözetim sistemi kurulacaktır. Böyle bir durumda rasyonalist yaklaşım, detaylı bir gözlem için kamera sistemleri kurarak tüm alan üzerindeki iklim değişikliklerini bu cihazlarla sürekli kayıt altında tutacak ve bu raporlama sistemini mümkün olduğunca sıkı şekilde kontrol altında tutarak iklim hareketlerini döngüsel olarak inceleyecektir. Böyle bir incelemede, analiz edilmek üzere bir veri yığınıyla karşı karşıya kalınacağı ve bu analizin sağlıklı yapılabilmesi için belirli bir kapasiteye ihtiyaç duyulacağı önceden kestirilebilecektir. Artırımcı yaklaşım ise böyle bir durumda, önceki zamanlarda ölçümlenmiş benzer örnekleri hatta benzer bölgelerdeki ölçümleri analiz ederek çıkarsamalar yapma yoluna gidecektir. Böyle bir durumda artırımcı yaklaşım, farklılık gösterecek oluşumları göz ardı edebilecektir. Yazarın ortaya koyduğu Karma- Tarama Modelde ise iki tip kamera kullanılacaktır. Bu kameraların ilk türü geniş açılı kameralar olup, alanın tümünü gözlemde tutan ancak detaylı gözlemlemeye olanak vermeyen kameralardır. İkinci tür kameralar ise daha dar açılı ancak odaklandığı bölgeye sıfır noktasına kadar görüş sağlayarak en ince detayları dahi gözlemlemeye olanak sağlayan kameralardır. Yukarıda bahsedilen, artırımcı politikaların büyük çoğunluğunun aslında daha genel ve rasyonel özellik gösteren radikal politikaların bir uzantısı oluşu savunusunun çözümlenmesi de bu örnekte yansıtılmıştır. Diğer yandan artırımcı ve geneli görmeyen ve amaçtan uzaklaşan bir karar, geniş açılı bir

gözlemle doğru yöne yöneltilebilecektir. Geniş açıdan bakan kameralar radikal kararları, dar açıya odaklanan kameralar ise artırımcı olan ya da gözüken kararları oluşturabilecek ya da gözlemleyebileceklerdir. Modelin aldığı "tarama" ismi bu gözetim ve gözlem sisteminden ileri gelmektedir. Etzioni (1967: 389), alınacak karar için harcanacak kaynak, zaman ve çabanın da taramanın genişliğine bağlı olduğunu vurgulamaktadır. Kararların uygulanabilirliği de söz konusu taramanın niteliğine ve sonuçlarına göre değişecektir. Değişen ortam, ortamın değişmesinin kararın sonucuna muhtemel etkileri gibi unsurlar da karar almak üzere politika üretim sürecine yapılacak olan yatırımları belirleyecektir.

Etzioni'nin (1967: 390-391) modelinde, sürece dâhil olan aktörler de verilecek kararı hem etkileyebilecek hem de değerlendirebilecektir. Verilecek kararlar bir ya da birden fazla ana hedefle ilgili olabilecektir. Bu durumda farklı aktörler kendilerinin ilgili oldukları ana hedefler üzerinde özellikle duracaklardır. Verilecek bir kararda, bir aktörü birinci ana hedef ilgilendirirken, diğer bir aktörü ikinci ya da üçüncü ana hedef daha çok ilgilendirebilecektir. Böyle durumda aktörler, verilecek kararlarda kendi odaklandıkları ana hedeflerin ne derecede gerçekleştirileceği üzerinde duracaklardır. Bu noktada, politika alternatifleri devreye girmektedir. Herhangi bir politika alternatifi, aktörün önem verdiği ana hedefi daha fazla gözetiyorsa, aktörün seçimi ve baskısı da bu politikadan yana olacaktır.

Karma tarama modele morfolojik bir açıdan bakıldığında, modelin artırımcı karar verme modeline göre daha esnek yapıda olduğu söylenebilecektir (Etzioni, 1967: 391). Artırımcı karar verme modeli çevrenin ve şartların daha stabil olduğu durumlarda uygulanması daha yerinde olan bir modeldir. Eskiye dönük ve benzer başka sorunlar için üretilmiş politikaların üzerinde ufak değişikliklerle yeni sorunlara adapte edilen politikalar, çevrenin ve şartların dinamik bir şekilde değişim içinde olduğu durumlarda yetersiz kalacaklardır. Karma - tarama modelde yapılacak geniş açılı taramalar, değişen çevre ve şartların yerinde ve zamanında anlaşılmasına imkân sağlayarak, alınacak kararların, söz konusu durumlara uygun şekilde

tasarlanmalarını sağlayacaklardır. Ele alınan yönleriyle bu model, artırımcı yaklaşımın yeniliklere ve gelişmelere karşı olan katı tutumunu bertaraf ederken, diğer yandan da rasyonel yaklaşımın[6] gerçekçi sayılamayacak yanlarını törpülemeye çalışan (Altunok ve Metin, 2003: 99), karar verici ve analizcilere daha geniş hareket imkânı sağlayan bir model olarak nitelendirilebilecektir.

1.3.6. Çöp Kutusu Karar Verme Modeli

Örgütlerde gözlemlenen karmaşık ve çok yönlü yapı, örgütün hiyerarşi mekanizması ve sosyal dinamizmine bağlı olarak ortaya çıkan çapraz ilişkilerin varlığı odak alınarak geliştirilen bir diğer model ise Çöp Kutusu Karar Verme Modelidir. Söz konusu model, Cohen, March ve Olsen (1972) tarafından ortaya konmuş olup, kamu politikalarında sürecin, sorunların ya da çözümlerin lineer bir sırayla belirlenmediğini, karar vericinin politika üretimine sürecin herhangi bir kısmından direkt olarak başlayabileceğini savunmaktadır (Bakioğlu ve Demiral, 2013: 12).

Daft' ın (2008: 470-471) belirttiği gibi artırımcı karar verme modeli örgütlerde tekil sorunların çözümü üzerine odaklanırken, çöp kutusu karar verme modeli ise çoklu

---

[6] Altunok ve Metin (2003), karar verme modellerini ele alırken bu modelleri iki ana başlık altında ele almıştır. Bunlardan ilki Weberci Ussal Davranış Yaklaşımıdır. Bu yaklaşımın en büyük temsilcisi olarak Herbert Simon gösterilmektedir. Simon'un dışında March ve Gross Da söz konusu yaklaşımı desteklemişlerdir. Diğer ana yaklaşım ise Smithci Ussal Davranış Yaklaşımıdır. Bu yaklaşımın temelleri Charles Lindblom ve David Braybrooke tarafından Weberci Ussal Yaklaşımın eleştirisi mahiyetinde geliştirilmiştir. Birinci yaklaşım kapsamında yer alan Simon ve onu destekleyen yazarların görüşleri bir tez olarak kabul edilirse, ikinci yaklaşım kapsamında yer alan Lindblom ve onu destekleyen yazarların görüşlerinin de antitez sayılabileceği Altunok ve Metin (2003: 98) tarafından vurgulanmıştır. Bu durumda, Etzioni'nin (1967) Karma Tarama Modeli ise bu görüşlere karşılık bir antitez sayılabilecektir.

ve çok yönlü sorunların çözümüne odaklanmaktadır. Yazar bu vurguyu, Cohen ve arkadaşlarının (1972) “organize olmuş anarşi” olarak adlandırdıkları, örgütün yüksek belirsizlik durumunda olduğu ve belirsizliğin organik bir yapıda olan örgüt tarafından üretildiği durum üzerinden pekiştirmektedir. Organize olmuş anarşiler, dikey örgüt yapısı, hiyerarşi ve bürokratik kararlarla kontrol edilemeyeceklerdir ve bu anarşiler üç karakteristik özelliğin sonucu olarak ortaya çıkmaktadır (Daft, 2008: 471):

1. *Problematik Tercihler:* Amaçlar, problemler, alternatifler ve çözümler tam olarak tanımlanmamış ya da karmaşık tanımlanmıştır. Karar verme sürecinin her bir adımında belirsizlik mevcuttur.

2*. Belirsiz ve Tam Anlaşılmamış Teknoloji:* Örgüt içindeki sebep-sonuç ilişkilerinin tanımlanması ve belirlenmesi zor bir iştir. Kararlara etki eden belirgin bir veri seti bulunmamaktadır.

3. *Devir:* Örgütsel pozisyon deneyimleri çalışanların değişimine ve devir daimine bağlıdır. Örgüt içindeki çalışanlar kendilerine verilen görevlerle meşgul olmaktan dolayı alınacak kararlara etki edecek ve katılacak zamanı bulamamaktadırlar. Bu yüzden alınan kararlarda katılımcılık kısıtlı bir şekilde sağlanmaktadır.

Yukarıda sayılan ve organize olmuş anarşinin özelliklerini belirten unsurlar özellikle son yıllarda gelişen teknoloji ve küreselleşmeye bağlı olarak değişen (internet tabanlı ve çok uluslu bir hale gelen) örgüt yapılarında giderek daha ön plana çıkan unsurlar haline gelmiştir.

Modeli ve modeldeki politika üretim sürecini anlamak için sorunların ve çözümlerin bir arada bulunduğu çöp kutuları düşünülebilir. Bir çöp kutusu içinde önceden ortaya çıkmış sorunlar, sorunlar için üretilmiş alternatifler ya da bunların her iki taraflı bir karışımı bulunabilir. Üretilecek politikanın üretim hızı da bu çöp kutularının ne şekilde elde bulunduğuna bağlı olarak değişmektedir (Cohen, vd.,

1972: 2). Politikanın ortaya çıkmasında ise dört ana akım ve bu akımların ne şekilde kombine edileceği önem taşımaktadır. Yazarlara göre bu dört akımdan ilki *problemler* akımıdır. Problemler örgütün içinden ya da dışından gündeme getirilebilirler. Bunlar örgüt üyelerinin yaşam tarzı, aile hayatları, işle ilgili sorunları, kariyerleri, grup ilişkileri, maaşları, ideolojileri gibi sebeplerden doğabilir. İkinci akım ise *çözümler* akımıdır. Çöp kutusunun içindeki çözümler, sorusunu arayan cevaplar niteliğindedir. Bunun için çözümlerin hangi sorunlar için tasarlandığına dikkat edilmelidir. Aksi takdirde cevabın iyi tasarlanmadığı durumlarda, onun örgütsel bir problemi çözmek ya da başka bir sorunun cevabı olarak orada var olduğu bilinemeyecektir. Diğer bir akım, *katılımcılar* akımıdır. Katılımcılar, gelip geçicidir. Katılımcılar tarafından karar sürecine yapılacak olan her girdi aynı zamanda bir çıktı olacaktır. Burada karara etki derecesi, alınacak kararın özelliklerine göre değişim gösterecektir. Önceden belirtildiği üzere, katılımcıların yeni üretilecek politika için harcadıkları/harcayabildikleri zaman da onların politikaya etki derecesini belirleyecektir (Cohen, vd., 1972: 4).

Çöp kutusu karar verme modeli, sorunları tam manasıyla ve kökten bir çözüme ulaştırmasa da, amaç ve hedeflerin belirsiz olduğu durumlarda, daha iyi kararlar alabilmeyi olanaklı kılan bir modeldir. Bunun yanında, modelin geleneksel ve konvansiyonel olan rasyonel karar alma biçimine karşı daha patolojik bir duruş sergilediği ileri sürülebilecektir. Bu yönüyle çöp kutusu karar verme modeli, rasyonel karar verme modeline göre daha detaycı, sorunları daha ayrıntılı ve farklı boyutlarda ele alarak, semptom sorunların da verilecek kararlarda hesaba katılmasını sağlayabilecektir. Modelin geçerliliğini, ilk bölümlerde katılımcıların kararlara farklı ilgi ve enerji düzeylerindeki katılımlarını açıklayan ve çalışmanın son bölümlerinde üniversiteler ve kolejler üzerinden inceleyen Cohen ve arkadaşları (1972), söz konusu modelleriyle kamu politikası alanında kayda değer bir yer edinmişlerdir.

Bu yaklaşıma rasyonel ya da yorumsamacı kamu politikası analizi çerçevesinden bakıldığında, modelin daha çok rasyonel yaklaşımda bulunan belirsiz ve tam anlaşılmamış teknoloji, problematik tercihler ve devir gibi rasyonel yaklaşımın bileşenlerini daha ayrıntılı bir şekilde içerdiği ve yorumlayamaya çalıştığı kanısına varılmıştır. Bu yönüyle model, rasyonel kamu politikası analizi yaklaşımları içerisinde yer alabilecek niteliktedir.

1.3.7. Çoklu Akımlar Modeli

"Çoklu akımlar" ya da diğer bir ismiyle "politika fırsat pencereleri" modeli, John Kingdon tarafından geliştirilen ve özellikle sorunların gündeme gelmesiyle ilgilenen bir modeldir. Kingdon, ABD federal yönetiminde sorunların nasıl gündeme geldiğini açıklamak üzere bu modeli ortaya koymuştur. Model, genel olarak belirsizlik şartlarında politika oluşturma sürecini açıklarken, Cohen ve arkadaşları (1972) tarafından ortaya konulan çöp kutusu karar verme modelinin geliştirilmesine ve revize edilmesine dayanmaktadır.

Kamu politikası üretiminin eyleme geçmesi için öncelikle politika oluşturmaya sebep teşkil edecek sorunların gündeme gelmesi gerekmektedir. Söz konusu sorunların hangi durumlarda ve ne şekilde gündeme geldiğini anlamak ve yorumlamak, bu noktada önem taşımaktadır. Sorunların gündeme gelmesinde ilk akla gelebilecek senaryolardan birisi, ilgili sorunun artık kriz seviyesine ulaşmış olması durumudur. Bu durumda sorun artık görmezden gelinemeyecek ve ötelenemeyecek bir duruma ulaşmıştır. İkinci durum, sorunun ilgili tüm unsurlarıyla birlikte net bir şekilde belirginleştiği durumdur. Üçüncü durum, bir sorunun medya tarafından odak alınarak gündeme taşındığı durumdur. Dördüncü durumda, üretilecek kamu politikasının geniş bir kitleyi etkilemesi söz konusudur. Dolayısıyla bir kitleyi ya da bir baskı grubunu etkileyecek olan kamu politikasının ilgilileri tarafından gündeme getirilmesi daha kolay olabilecektir. Son durum ise ilgili

problemlerin, toplumda güç ve meşruiyeti sorgulatacak hale gelmesidir. Böyle bir ortam da konunun gündeme gelmesine neden olacaktır (SU, t.y.: 4). Kingdon, çöp kutusu karar verme modeli temelinden ürettiği ve uyarladığı modelinde, gündem oluşturmada üç ayrı akımdan bahsetmektedir. Bu akımlar sırasıyla aşağıdaki şekilde özetlenebilecektir (Kingdon, 2014; Köseoğlu, 2013: 259).

Problemler Akımı: Problemler, yönetimlerde bulunan yöneticilerin ilgisini çekmektedir. Bu problemler hükümetin rutin gözetimleri sonucu yöneticilerin gündemine gelebileceği gibi onların ilgilerine bir takım etkiler sonucu da gelebilmektedir. Problemlerin yöneticilerin gündemine gelmesinde etkili olacak aktörler kamusal olabileceği gibi, sivil toplum kuruluşları ya da akademisyenler gibi aktörler de olabilecektir. Kingdon (2014: 91), söz konusu akımı ele alırken özellikle problemlerin gerçekte problem olup olmadıklarının tespitinin de önemi üzerinde durmaktadır.

Politika Önerileri Akımı: Kamu politikalarının oluşturulmasında çeşitli aktörler politikalara yön vermektedir. Bu aktörler planlama, değerlendirme ve bütçe gibi konularda yetkili birimlerde bulunan bürokratlar, kuram ve kamu politikası önerisi geliştirmeye çabalayan akademisyenler, araştırmacılar ve çeşitli çıkar gruplarından oluşan aktörlerdir. Çeşitli politika alanlarında uzmanlaşmış olan bu aktörleri Kingdon (2014: 20), “politika girişimcileri” olarak adlandırmaktadır. Bu girişimciler kendi amaçlarını ve kaynaklarını politikaya etki etmek üzere kullanmanın yanı sıra, hem problem ve çözümleri bir araya getirmeye, hem de bir araya getirdikleri problemler ve çözümleri politikaya yansıtmaya çabalamaktadırlar. Bahsi geçen etki ve çabalar sonrası, bir takım fikir ve öneriler karar vericiler tarafından politika üretim sürecine dahil edilirken, bazıları da göz ardı edilebilecektir. Fikir ve önerilerin karar vericiler tarafından kamu politikası üretim sürecine alınması, uygulanabilir olmasına, beklenen değerleri içermesine ve sahip olunan bütçeye uygunluğuna bağlı olacaktır.

Siyaset Akımı: Siyaset akımı, Kingdon'un çoklu akımlarından en değişken ve hassas olan akım olarak değerlendirilebilecek niteliktedir. Akım, farklı değişkenler boyutunda ele alınabilecektir. Bu değişkenlerden ilki, "ülke gündemi"dir. Ülke gündemi ya da Kingdon'un (2014: 147) adlandırmasıyla "ülkenin modu" (ülkenin içinde bulunduğu ruh hali) ülkenin farklı zaman dilimlerinde, farklı değerlerin ya da problemlerin çeşitli neden-sonuç ilişkilerine göre ön plana çıkması ve kamuoyunun bunlara karşı daha hassas bir hale gelmesini ifade etmektedir. Söz konusu hassasiyete ve ortama göre hangi politikaların gündeme (daha kolay) gelebileceği değişebilmektedir. Örneğin, ülkelerin kimi dönemlerde sol kimi dönemlerde ise sağ politikalara yönelmesi ve uygulaması bu durum içinde değerlendirilebilecektir. Akımın diğer değişkenlerinden olan hükümetin değişmesi (Kingdon, 2014: 153) unsuru da, aynı zamanda verilen örnekteki sağ-sol politikalar yönelme eğilimini belirleyen bir unsurdur. Politika üretim sürecine etkide bulunan en üst merci sayılabilecek yasama organı ve ülke gündemini kolayca değiştirebilme imkânına sahip iktidar yöneticilerinin değişmesi, siyaset akımını da değiştirecektir. "Organize olmuş politik baskı grupları" (Kingdon, 2014: 150) ise siyaset akımını etkileyen bir diğer unsurdur. Kingdon, bu unsurun özellikle kamu politikası alanında çalışan araştırmacı ve akademisyenlerin en çok ilgilendikleri unsur olduğunu vurgulamaktadır. Bu baskı grupları, amaçları ve politika görüşlerine yön veren kaynaklarının yanı sıra sahip oldukları oy potansiyeli ile de siyaset akımını değiştirme potansiyeline sahiplerdir. Bu potansiyelin kullanılabilmesinde ve kamu politikasına etki gücünde, söz konusu baskı gruplarının sahip olduğu güç, diğer baskı grupları ile çatışmasından arda kalan güç gibi etmenler önemlidir. Diğer yandan, baskı gruplarının hükümetlerce desteklenip desteklenmemesi de onların kamu politikasını etkileyebilme derecesini belirleyecektir.

Kingdon modelini, Amerikan eyalet yönetimi sisteminde, kamu politikası üretim süreçlerinin karmaşıklığını ve bu süreçlerde bir sorunun gündeme ne şekilde gelerek bir kamu politikası halini alabileceğini açıklayarak kurmuştur. Fırsat

penceresi olarak adlandırılan ve sorunlar, politika önermeleri ve siyaset akımlarının bir araya gelmesiyle bir kamu politikasının oluşması temeline dayanan bu modelin içinde bulunulan dönem ve şartlarda da geçerliliğini koruduğu söylenebilmektedir (Larkin, 2012: 30). Söz konusu görüş, kamu politikası alanında yapılacak politika analizi çalışmalarında ayrı bir odak noktası olarak test edilebilecektir. Modelin temelini aldığı çöp kutusu karar verme modeli düşünüldüğünde ve modelin özellikle politikanın gündeme gelmesi ve hayata geçirilmesi basamaklarını irdelemesi ile politikanın nihayeti için rasyonel çözümler önermesi göz önüne alındığında, rasyonel kamu politikası analizi yaklaşımı içerisinde düşünülebilecektir.

1.3.8. Guy. B. Peters ve Politika Formülasyonu

Politika formülasyonu, politika problemlerinin kamu politikası karakteristiklerine göre sınıflandırılmasını ifade etmektedir. Politika sınıflandırması, çeşitli alanlarda çalışan çeşitli yazarlar tarafından farklı şekillerde yapılagelmiştir. Immergut'un (2011: 69) belirttiği üzere Theodore J. Lowi (1972), kamu politikasını doğası gereği dağıtıcı, düzenleyici ve yeniden dağıtıcı olmak üzere üçe ayırmıştır. James Q. Wilson (1980), kamu politikasından doğan fayda ve maliyet dağılımlarını inceleyerek farklı düzenleme çatışmalarının analizini yapmıştır. B. Guy Peters (2005) ise politikaların problemleri üzerinde odaklanarak bu problemler için belirli bir tipoloji ortaya koymuştur. Tipolojiye göre politika problemleri çözülebilir, karmaşık ya da bölünebilir olabileceklerdir ve çözüm için kullanılacak araçlar problemin tipine göre değişiklik göstereceklerdir.

Peters (2005: 350) politika tasarımı konusunda, politika araçları temelindeki alan yazınından bahsederken; öncelikle politika araçları çalışmalarının Bardach, Salamon ve Hood gibi isimlerce politikanın "uygulama" kısmından incelendiğini vurgulamaktadır. Bu yöntem ise özyineleme ve özgönderimsellik yaklaşımlarıyla eleştiriye uğramıştır. Son olarak ise geleneksel yaklaşımlara olan eleştirileri de ele

alarak geliştirilen, “araçların formüle edilmesi” durumuna yönelik bir yaklaşım ortaya çıkmıştır. Araçların formüle edilmesi konusunda çeşitli unsurlardan yola çıkılmıştır. Bu alanda yapılan çalışmalarda, araçların hizmet üretimindeki politik doğasına, değerlere karşı olan taraflı olma durumlarına ve dahi hangi araçların kullanılacağına karar vermeye etki edecek olan ulusal politik kültür üzerine odaklanılmıştır. Araçların yanı sıra alan yazınında, onların kullanımı ile “çözülmüş” olan politika problemleri arasındaki ilişkiyi araştıran çalışmalar da yapılmıştır.

Politika problemleri ile bu problemlerin çözümü, dolayısıyla politika tasarımı için kullanılacak araçları seçme arasındaki ilişkiyi inceleyen Peters (2005: 351), çıkış noktası olarak “durumsallık” yaklaşımını ele almıştır. Buradan hareketle Peters, politika problemlerinin onların değişkenliğini belirleyen doğasını ve bu değişkenliğe göre de politika tasarımı için yapılacak seçimlerin “duruma bağlı” olmasını vurgulayarak, politika problemlerinin formüle edilmesine dayanan modelini ortaya koymuştur.

Peters’e (2005: 352) politika problemlerinin tanımlanması süreci iki basamaktan oluşmaktadır. Basamaklardan birincisi problemin hangi konu ya da alan hakkında olduğunun belirlenmesidir. Bir problem, çevresel, tarımsal, sosyal ya da başka bir konuda olabilecektir. Özellikle kamu politikası oluşturmada gündem belirlemeye etki edecek olan problemin kimliğinin belirlendiği bu birinci basamakta, problemin çözümüne yönelik kullanılacak olan aracın belirlenmesi için büyük bir adım atılmış olacaktır. İkinci basamak ise problemi sınıflandırmaya yarayacak olan araçların seçilmesidir. Bu basamakta, kimliği tanımlanmış olan problem, çözüm için hazır hale getirilmektedir. İlk basamakta kimliği belirlenen (örneğin tarımsal olan bir problem) problem için ikinci basamakta, ilgili olduğu alana yönelik olarak politika araçları belirlenecektir. Diğer bir anlatımla, ilk basamakta problemler etiketlenmekte ve problemin hangi alanda olduğu ve eğer kamusal bir problemse hangi kamu kuruluşunun bu problemle ilgileneceği belirlenmektedir. İkinci basamakta ise daha karmaşık bir süreç olarak problemin karakteristiğinin

belirlenmesi için problemin içinde yer alan değişkenlerin ve bu değişkenler doğrultusunda kullanılacak politika aracının belirlenmesi söz konusudur. Politika problemlerinin nesnel ya da öznel olabileceğini, onların doğal olarak ya da sosyal olarak yapılandırılmış bir şekilde oluşabileceğini vurgulayan Peters, Rochefort ve Cobb'un (1994) çalışmalarında gündem belirlemeye yönelik olarak ayrıştırdıkları politika problemlerinin karakteristiklerine[7] atıf yaptıktan sonra, kendi ortaya koyduğu politika problemlerinin karakteristiklerini sıralamaktadır. Peters'a (2005: 356-365) göre politika problemlerinin karakteristikleri aşağıdaki gibidir:

Problemin Çözülebilirliği: Politikaların oluşturulup uygulanması için ilk ve belki de en önemli karakteristik, politika probleminin çözülebilir olmasıdır. Hükümetin politik anlamda bir sorun üzerine yoğunlaşması ve harekete geçmesi için bazı politik realitelerin bulunması gereklidir. Hükümet, harekete geçmek için bir program belirleyecektir. Programın uygulamaya geçmesi için de politikanın bir çözümle sonuçlanabileceğine dair bir öngörüsü ya da daha önce benzer bir politikada ulaşılmış çözümleri içeren deneyime sahip olması gibi etkenler gerekecektir. Bazı problemler de tekrar tekrar çözülmesi gereken ve geçici çözümleri olabilecek problemlerdir. Buna örnek olarak, hükümetin harcamalarını ne yönde ve nasıl ayarlayacağına karar verilen ve her yıl yapılan bütçe görüşmeleri gösterilebilecektir. Diğer yandan çözülmüş sayılan problemler daha sonradan yeniden beklenmedik şekilde ortaya çıkabileceklerdir. Bu türdeki problemler kronik problemler olabilir. Ekonomiler, genel olarak hükümetleri rahatsız eden kronik bir problem olarak görülebilecek olan, beklenmedik zamanlarda beklenmedik krizlere girebilen, daralabilen ve büyüyebilen sistemlerdir.

---

[7] Söz konusu karakteristikler, nedensellik (causality), ciddiyet (severity), etki alanı (incidence), yakınlık (proximity), yenilik (novelty), ortaya çıkardığı buhran (crisis) ve çözümlere uygunluğu (availability of solutions) şeklinde sıralanmaktadır (Rochefort ve Cobb, 1994).

Problemin Karmaşıklığı: Peters (2005: 358-360) karmaşıklığı tanımlamak için öncelikle karmaşıklığı politik karmaşıklık ve programatik karmaşıklık olarak ikiye ayırmaktadır. Politik karmaşıklık, politika üretiminde yer alan aktörlerin ve bu aktörlere ait olan çıkarların sayısını ve çeşitliliğini belirtmektedir. Bu unsurlar ve unsurların politika üretim sürecinde içerilme miktarı politika üretilmesinde yaşanacak olan karmaşıklığı ve çözüme yönelik tartışmaları etkilemektedir. Programatik karmaşıklık ise farklı boyutları içermektedir. Bu boyutlardan biri politikanın teknik içeriği olarak düşünülebilecektir. Bir vatandaş ya da aktör için üretilecek olan politikanın teknik içeriği karmaşık olabilecektir. Programatik karmaşıklığın diğer boyutları, neden sonuç ilişkileri ve politika yürütmesi için kullanılacak araçların seçimi olarak sıralanabilecektir.

Problemin Ölçek Sorunu: Politika problemlerinin diğer bir karakteristiği, ölçek sorunudur. Problemin ölçeği, onun etkilediği alanı belirtmektedir. Etki ettiği gibi problemler ve problemlere karşı üretilecek olan çözümler bütüncül (holistik) bir özellik taşıyabileceği gibi artırımcı (inkremental) bir özellik de taşıyabilecektir. Örneğin NASA (National Aeronautics and Space Administration) aya insan yollayacağında bu politikayı "ya hep ya hiç" mantığıyla sürdürecektir. Gönderilen insanın ayın yarı yoluna kadar gidip geri dönmesi, gerçekleştirilmek istenen amacı karşılamayacaktır. Diğer yandan kanserle ya da AIDS'le (Acquired Immune Deficiency Syndrome) mücadeleye dayanan politikalar ulusal, bölgesel ya da yerel şekilde yürütülebilecek (problemlerin çözülmeye çalışılacak olmasına göre) bölünebilir ve artırımcı bir özellik gösterecektir. Problemlerin ölçeğini görebilmek adına verilebilecek en somut örneklerden birisi de AB (Avrupa Birliği) politikalarıdır. Belirlenen problemler karşısında parlamento tarafından üretilen politikaların uygulandığı AB ülkeleri de problemin ölçeğini yansıtmaktadır (Peters, 2005: 360-362).

Problemin Bölünebilirliği: Peters (2005: 362-363) problemin bölünebilirliğini, hükümetin ekonomik problemlere ürettiği çözümler ve bu yönde uyguladıkları kamu

politikaları üzerinden ele almaktadır. Hükümetlerin izleyecekleri uygulamalar bir problemin çözümü için direkt olarak bir fayda sağlayamayabilecektir. Bu gibi durumlarda hükümetler, problemi bölerek geçici çözümler arayabileceklerdir. Örneğin, özel sektörün herhangi bir alanına ilişkin bir üretim hacmi probleminde, söz konusu alanı desteklemek için doğrudan adımların atılması yerine bu alandaki vergilendirmeler, girişimcilerin lehine olacak şekilde yeniden düzenlenebilecektir. Diğer yandan ülke ekonomisinin konu aldığı cari açığın fazlalığına yönelik bir problem, sektörlere bölünerek sektörlerdeki ihracatlar ayrı ayrı teşvik edilerek büyük problem olan cari açık küçük problemlere bölünerek çözülmeye çalışılabilecektir.

Problemin Parasallaştırılabilirliği: Peters'in (20005: 363) "saçma" olarak nitelendirdiği "parasallaştırılabilme" terimi, problemlerin bir para ile ifade edilebilmesini ve problemlerin çözümlerinin parasal bir değerle sağlanabilmesini ifade etmektedir. Örneğin, insan hakları ihlalleri ve cinsiyet eşitliği gibi problemlerin çözümleri finansal araçlarla sağlanamayacaktır. Bunun yanında, emeklilikten sonra yoksulluk, düşük gelirli evlerdeki su tesisat kalitesine bağlı olarak meydana gelen sağlık riskleri gibi problemlerin çözümleri finansal araçlar kullanılarak gerçekleştirilebilecektir. Bazı durumlarda hükümetler parasallaştırılmaması gereken bazı problemleri finansal araçlarla gidermeye çalışmakta ya da sadece bu eylemleri birer çözüm çabası olarak lanse etme gayretine girmektedirler. AB'nin, üye ülkelere göç ve yine cinsiyet eşitliği gibi problemlere yaklaşımı, genel olarak problemlerin çözümü için fonlar oluşturup bu fonları hedef ülkelere aktarma politikaları geliştirme şeklinde gerçekleştirilmektedir.

Etkinliğin Kapsamı: Politika problemlerinin, kullanılan politika araçlarının ve bu problemleri meydana getiren davranış farklılıklarını anlayabilmek için düşünülmesi gereken diğer bir potansiyel unsur da etkinliğin kapsamıdır. Etkinliğin kapsamı konusu doğrudan doğruya yönetimlerin kapasitesi ile ilgilidir. Örneğin, bir ülkedeki nükleer tesislerin güvenliğini sağlamak ve onları yeniden düzenlemek, ülkede hane

halkı tarafından pişirilen yemeklerin hava sağlığına etkilerini bir düzenlemeye tabii tutmaktan daha kolay olacaktır. Nükleer tesis örneğinde, düzenleme yapılacak olan tesis ve program sayısı kuvvetle muhtemel daha az olacaktır ve bu işlemlerde hesaba katılacak olan risk, maliyet gibi unsurlar kestirilebilir ve birbirine benzer olacaktır. Hane halkı yemek pişirme örneğinde ise birçok ev, yemek menüsü, pişirme şekli, kullanılan malzeme gibi değişken olacaktır (Peters, 2005: 364).

Karşılıklı Bağımlılıklar: Bu karakteristik ise politika problemlerinin ilgili oldukları kurumları ve bu kurumların arasındaki koordinasyon meselesi ile ilgilidir. Bir politika problemi ve bu problemin çözümü yalnızca bir kurumla ilgili olabilir. Böyle durumlarda, politika üretim süreci dairesel döngüye sahip bir süreçten oluşmaktadır. Buna örnek olarak, vatandaşların sosyal güvenlik ile ilgili problemleri ve bu problemlerin çözümü için akla gelen ilk ve tek devlet kurumu olarak Çalışma ve Sosyal Güvenlik Bakanlığı gösterilebilecektir. Diğer yandan bazı problemler ise birden fazla kurumun koordinasyonunu gerektirecek nitelikte olabilecektir. Örneğin, tarımsal üretim ve ihracat problemi öncelikli olarak Gıda, Tarım ve Hayvancılık Bakanlığının ilgili bir problemi olarak görülebilecektir. Fakat problemin daha detayına inildiğinde bunun Gümrük ve Ticaret Bakanlığı ve dahi Dışişleri Bakanlığı ile ilgili bir problem olduğu sonucuna varılabilecektir. Peters (2005: 365-366) söz konusu problemin çözüm noktası (kurumu) ve çözüm aracı ile ilgili olma durumunu "problemin tek uzantılı ve çok uzantılı" olması şeklinde açıklamaktadır.

Model genel olarak ele alındığında, izlenen düşünsel yolun, genel olarak problemlerin doğasına karşı getirilen analitik bir yaklaşıma dayandığı söylenebilecektir. Böyle bir yol, problemlerin çözümü için rasyonel kapasiteyi artırma çabası olarak kabul edilebilecek bir niteliktedir. Problemlerin çözümü için kullanılan araçlar, problemin doğasına göre nitel ya da nicel bir anlam taşısa da, modelin genel hatlarındaki analitik duruşun, onu rasyonel kamu politikası analizi yaklaşımı sınırlarına koyduğu söylenebilecektir. Zira modeli açıklamak için alan

yazınında ele alınan ve bu çalışmada sunulan örnekler de genel olarak nicel verilere dayanmaktadır.

1.3.9. Kamu Politikası Analizi Yaklaşımlarının ve Karar Verme Modellerinin Sınıflandırılması

Kamu politikası analizinde yaklaşımlar ve kamu politikası karar verme modelleri, alan yazınında yer alan çalışmaların büyük çoğunluğunda "girilen bir patikanın gittiği yönde" açıklanmıştır. Söz konusu yaklaşım ve modeller kimi çalışmalarda çalışmanın odağı konusunda belirli yaklaşımlar etrafında sınırlı olarak ele alınırken, kimi çalışmalarda ise belirli yaklaşımların ön plana alındığı ve diğer yaklaşımların ise ön planda tutulan yaklaşımların gölgesinde kaldığı gözlemlenmiştir. Diğer yandan, farklı çalışmalarda aynı kavram ve kuramların farklı üst başlıklar altında, farklı yaklaşımlar çerçevesinde verildiği gözlemlenmiştir. Bazı çalışmalarda kamu politikası analizi yaklaşımları (rasyonel, yorumsamacı ve karma) kapsayıcı yaklaşımlar olarak incelenmiştir. Bazılarında ise aynı kavramlar, bu kapsayıcı yaklaşımlar altında yer verilen karar verme modellerine benzer şekilde "model" olarak ele alınmıştır (bkz. Leoveanu, 2013). Bu karmaşa, hangi isim ve kavramın bir metodolojiyi, bir kök felsefeyi içeren genel bir yaklaşım olduğunu, hangi kavramların bu yaklaşımlar içerisinde yer alan ve belirli eleştiriler ya da eklenimler doğrultusunda oluşmuş birer karar verme modeli olduğunu iyiden iyiye muallaklaştırmış gözükmektedir. Bu hususların yanında, kamu politikası analiz ya da modellerini kavramak üzere bir çizgi belirleyebilmek için üzerinde durulması gereken, birçok çalışmanın kesişim noktası haline gelmiş isimler ve konular da göze çapmıştır. Bu kesişim noktaları, kamu politikası analizinin çerçevesini ve kamu politikası analizi yaklaşımlarının haritasını belirlemek üzere gereken çizgileri araştırmacıya verebilecek niteliktedir. Çalışmanın hemen önceki kısımlarında söz konusu isimlere ve ortaya koydukları görüşlere hem kamu politikası analizi yaklaşımları hem de kamu politikasında karar verme modelleri içerisinde yer

verilmiştir. Çalışmanın bu başlığı altında söz konusu karmaşıklığı derlemek adına, kamu politikası analizine daha bütüncül bir açıdan bakılarak yaklaşımlar ve kamu politikasında karar verme modelleri çeşitli yönlerden ele alınacak ve bunlara bir sınıflandırma uygulanmaya çalışılacaktır. Sınıflandırma içerisine yapılan alan yazını taramasında ön plana çıkan ve "kesişim noktası" olarak nitelendirilen isimler ve görüşleri alınmıştır. Ele alınmayan isimler ve görüşlerinin istenildiği ve uygun görüldüğü taktirde farklı araştırmacılarca söz konusu sınıflandırmanın içine alınabileceği düşünülmektedir.

Goodin ve arkadaşlarına (2006: 3-4) göre kamu politikası analizi, yönetmek arzusunun bir uzantısı olarak kontrolü sağlamayı, bir dünyayı şekillendirmeyi amaçlamayan; kökenleri antik çağlara kadar götürülebilecek olmasına rağmen özellikle II. Dünya Savaşı sırasında yapılan Yön-Eylem araştırmalarının bir türevi niteliğinde sistematik olarak çalışılmaya başlamış ve ilk başlarda "Yüksek Modernizm" anlayışıyla yoğurulan bir çalışma alanı olarak ele alınmıştır. Bu yönde bir yaklaşımı destekleyen Smith ve Larimer (2009: 7-8), kamu politikası ve analizi ile ilgili eylem ve çalışmaların devletlerin ortaya çıktığı çağlara kadar götürülebileceğini belirtmektedirler. Yazarlara göre, ideal devlet tipini ve işleyişini bir eser ile anlatan Platon'dan, Prens adlı eseriyle devletin başındaki yöneticiye öğütler veren Machiavelli'ye ve nihayet devlet politikaları ile ilgili eserleri olan Hobbes, John Locke, James Madison, Adam Smith ve John Stuart Mill'e kadar birçok isim, kamu politikaları alanı çalışanı sayılabilecektir. Bu isimlerin her biri kamu politikasının tanımına uygun olarak devletlerin neleri yapması ya da yapmaması konusundaki görüşlerini alana kazandırmışlardır. Diğer yandan kamu politikası alanı çalışanları, kamu politikası analizi çalışmalarının başlangıcını işlem maliyeti yaklaşımı ve bu yaklaşım doğrultusunda analizlerin federe devletlerde yapılmaya başlandığı 1930'lara götürürken, bazıları da başlangıcı 1960'lardan itibaren almaktadır. Yine de açıklamalarının sonunda Smith ve Larimer (2009: 8), kamu politikası analizinin başlangıcını 20. yüzyılın ortasında, Lasswell'in (1951)

politika bilimlerini metodolojik açıdan incelemeye başladığı tarih olarak kabul etmektedirler. Kamu politikası analizinin ortaya çıkış tarihine ilişkin savları ortaya koyan bu bilgiler, başlığın ilerleyen bölümlerinde kamu politikası analizi yaklaşımlarının sınıflandırılmasında tekrar ele alınacaktır.

Smith ve Larimer (2009) kamu politikası analiz yaklaşımlarını metodolojik olarak nitel, nicel, işlem maliyeti, risk değerlendirmesi ve Delphi tekniği şeklinde sınıflandırdıklarından çalışmanın önceki kısımlarında bahsedilmişti. Kitabın geneline bakıldığında, yazarların ele aldıkları tüm kamu politikası analizi yaklaşımlarını temelde var olan iki yaklaşım temelinde ve bu yaklaşımlar arasındaki çatışma üzerinden ele aldığı gözlemlenmektedir. Bu iki yaklaşım; rasyonel yaklaşım ve post-pozitivist yaklaşımdır. Bir önceki başlıkta da değinildiği üzere rasyonel yaklaşım, karar almada akılcı davranılması, politika analizinde elde edilecek bilgiler doğrultusunda çözümlemeler yapılıp refahın artırılması, kamu tercihine bağlı kalınması, verilerin multidisipliner bir şekilde değerlendirilmesi ve halk katılımının sağlanması amaçlarına sahipken (Andrews, 2007: 161), post-pozitivist yaklaşım daha çok ekonomik temeller üzerine kurulmuş olan, politika üretim sürecine karşı çıkan ve gerçekler-değerler ayrımını yaparak değerlerin önemini vurgulayan bir yaklaşımdır (Fischer, vd., 2007: 19). Politikaların üretimi, bu üretim sürecine katılım ve demokrasi kavramları çerçevesinden bakıldığında rasyonel kamu politikası analizi bakış açısının post-pozitivist olana göre daha az demokratik ve katılımı daha az teşvik eden bir bakış açısı olduğu söylenebilir. Özellikle işlem maliyeti, kamu tercihi kuramı gibi düşünceleri içerisinde barındıran rasyonel analiz, politikalara daha teknik, bütüncül, fayda-maliyet odaklı baktığı ve değer, farklılık gibi faktörleri politika üretim sürecine katmadığından dolayı "yukarıdan aşağıya" politika üretim modelini uygulamaktadır. Post-pozitivist analiz ise toplumsal ve kimi zaman bireysel değerleri, nicel faydalardan daha ön planda tuttuğu için, katılımı teşvik eden, mikro düzeydeki farklılıklara üretilecek politikaya etki bakımından ilgi gösteren, "aşağıdan yukarıya" politika üretim modelini

uygulamaktadır. Michael Lipsky'nin (1971, 1980) "street-level bureaucrat" olarak kavramsallaştırdığı (Smith ve Larimer, 2009: 167) ve "halka en yakın düzeyde, vatandaşla birincil muhatap olan bürokrat" anlamına gelen bürokrat tipi de bu yukarıdan aşağıya politika üretim sürecinin önemli araçlarından biri olarak görülmektedir.

Smith ve Larimer (2009) kitabın ilk bölümlerinde Lasswell'in politika analizini politika üretim basamaklarından oluşan bir sürece göre sistematikleştirdiği modelini ele almışlar ve bu modelin diğer kamu politikası analizi çalışmalarını etkilediğini vurgulamışlardır. Çalışmanın bir önceki başlığında değinildiği üzere söz konusu yaklaşım, rasyonel kamu politikası analizi yaklaşımının içerisinde yer alan bir modeldir. Çalışmanın kalan bölümlerinde bu modelden "basamaklar modeli" olarak bahsedilecektir. Yazarlar, Lasswell'in basamaklar modelinin yanında tam bir kamu politikası analizi yaklaşımı sayılmayacak olsa da, Lowi'nin (1972) politikaları dağıtıcı (distributive), kurucu (consituent), düzenleyici (regulatory) ve yeniden dağıtıcı (redistributive) olmak üzere sınıflandıran modelini ele almışlardır (Smith ve Larimer, 2009: 48). Onlara göre bu model, politikaların türlerini önceden belirleyerek ona göre bir takım analizler yaparak, politika analizinin sonuçlarını etkileyebilecek bir modeldir. Yazarlar bu modeli de rasyonel kamu politikası analizi yaklaşımı çerçevesinde yer bulan bir model olarak ele almışlardır. Yazarlar bu modelin de rasyonel yaklaşım içinde bulunmasının yanı sıra basamaklar modelini destekler bir nitelikte olduğunu vurgulamışlardır. Yazarların kitabında yer alan ve rasyonel kamu politikası analizi içerisinde yer alan bir diğer yaklaşım ise kamu tercihi kuramının kamu politikası analizinde kullanılmasına dayanan modeldir. (Smith ve Larimer, 2009: 57).

Post-pozitivist kamu politikası analizi yaklaşımı, kamu yönetimi alan yazınında aynı zamanda "yorumsamacı" kamu politikası analizi yaklaşımı olarak da isimlendirilmektedir. Orhan (2013: 66-87), zamanla geleneksel bilimsel yaklaşımın sınırlılıklarının farkına varılarak ortaya konulması, bu bakış açısıyla alınan

kararların aslında çok sınırlı bir çerçevede alındığını ve ussal karar alma sürecinin varsayımlarının tam olarak hayata geçirilemediğini vurgulamaktadır. Yorumsamacı yaklaşımlar ise geleneksel yönteme karşı onun ussallık ve nesnellik varsayımlarına bir eleştiri olarak ortaya çıkmış ve karmaşıklığa bir düzen getirme çabası olarak görülebilecek yaklaşımlardır. Bu yaklaşımlar kökenlerini genel olarak sosyal bilimlerden almakla birlikte; öznelerin anlam dünyalarını ve dilsel düzenliliklerin çalışılmasının kamu politikası üretiminde katkıda bulunacağını savunmaktadırlar. Yazar, yorumsamacı yaklaşımların içerisine tam ve net olarak sayılamayacak olsa bile "savunma koalisyonu"[8], "söylemsel kuramcılık", ve "anlatıcı/söylemsel" politika analizini almaktadır. Diğer yandan rasyonel karar verme biçimlerinin sorgulanarak sınırlılıklarının ortaya konmasında büyük öneme sahip olan düşünceler de bir geçiş niteliğinde olarak yorumsamacı bakış açısı içerisine alınabilecektir. Herbet Simon tarafından geliştirilen sınırlı ussallık ve Charles Lindblom tarafından ortaya konulan artırımcılık (inkrementalizm) bu geçişi sağlayan fikirlerden kavramsallaşmış olanlar arasındadır. Yazar, yorumsamacı yaklaşımın özellikle beşeri bilimlerde yaygın hale gelerek görüngübilim (phenomenolgy) ve yorumbilgisinden (hermeneutics) etkilendiklerini belirtmektedir. Tarihsel olarak düşünüldüğünde, yorumbilgisinin başlangıcını 18. yüzyıla, kutsal metinlerin, metinlerin, yasaların, yönetmeliklerin, haberlerin, konuşmaların ve mülakatların yorumlandığı ve bunları yorumlayanların aynı zamanda birer kamu politikası aktörü sayılabileceği zamana kadar götürülebilecektir. Görüngübilim ise pozitivist açının varsayımlarının göz ardı ettiği değerler ve yerel bilgi değişkenlerini ön plana alarak alındığı ve 20. yüzyılda ortaya çıkan bir yaklaşımdır. Yorumsamacı yaklaşım, özellikle post-yapısalcılık ve post-modernizm kökenlerinden beslenen Foucault, Derrida, Lavan, Lyotard ve Roty'nin

---

[8] Savunma koalisyonu (Advocacy Coalition Framework), Paul Sabatier ve Hank Jenkins- Smith tarafından geliştirilen ve inanışların, kamu politikası ve kamu politikası üretim sürecini etkileyen bir değişken olarak kullanıldığı bir yaklaşımdır (Orhan, 2013: 78).

kullandığı çerçeveleri politika analizine adapte eder. Karmaşıklık, belirsizlik ve kutuplaşmanın, tartışma ve açıklamalarla giderilebileceğini savunan "anlatıcı politika analizi"; post-yapısalcı sosyolojik ve siyasal çözümleme sürecini kamu politikası sürecine uyarlamaktadır. Bahsi geçen analiz "politika söylemi", ya da "söylemsel politika analizi" şeklinde daha parçalı isimlerle anıldığı gibi, sön dönemlerde yapılan çalışmalarda daha genel bir çatı kurmak amacıyla "eleştirel politika analizi" ya da "yorumsamacı politika analizi" şeklinde isimlendirilmiştir.

Son yıllarda kamu politikası analizi ve yönetimi alanına yeni bir yaklaşım getiren, alana bütünsel ve kapsamlı uygulamalarıyla etki eden diğer bir yaklaşım da "karmaşıklık kuramı" olmuştur. Morçöl (2013: 88-113) bunu açıklarken, çeşitli alan yazınlarında yer edinmiş ve Newton, Einstein, Ferguson (fen bilimleri) ve Diamond (sosyal bilimler) gibi isimlerin kuramlarından örnekler verirken, aslında kuramın kavram olarak basite indirgemeci tavrını vurgularken, "kuram" ve "karmaşıklık" kavramları arasında olan bu yöndeki çelişkiyi ele almaktadır. Yazar, doğa temelinde düşünüldüğünde doğanın içindeki var olan karmaşıklıkla onun insan zihnince algılanması arasında bir örtüşmeme durumunun olduğunu, aslında doğa ile onun bilgisi arasında bir karmaşıklık ilişkisi olduğunu vurgulamaktadır. Karmaşıklık kuramı köklerini, kaos kuramı, genel sistem kuramı, grup kuramı, dinamik sistemler kuramı, bilişim kuramları, biyolojik verim ve genetik kuramı, sibernetik, oyun kuramı, ağbağ kuramı ile ajan temelli simülasyon, toplumsal ağbağ analizi konularındaki gelişmelerden almaktadır. Kurama kamu politikası analizi açısından bakılacak olursa, kimi kamu politikası karar vericileri ve çalışanları kamu politikası analizine basite indirgemeci bir bakış açısıyla yaklaşırken, kimileri ise kamu politikalarının karmaşık süreçlerden meydana geldiklerini savunmaktadırlar. Yazarın belirttiği üzere; kamu politikası süreci ve kamu politikası analizinde, değişkenler arasında doğrusal olmayan, asimetrik ilişkilerin esas olması ve bağımsız değişkenlerin mevcut olmadığı durumlarda da sistemin kendi kendini değiştirebileceği ve biçimlendirebileceği düşünülerek, kamu politikasının

geleneksel kuramlarda olduğundan farklı bir biçimde kavramsallaştırılması gerekmektedir. Son yıllarda gündemde yer tutan ve kamusal kuruluşların karar ve uygulamalarının tek başına, talep edilen sonuçlara ulaşamayacaklarını ve hizmetlerin yürütülmesinde yeterli olmayacaklarını savunarak buna bir çözüm getiren kavram olan "yönetişim" de bu savı desteklemektedir. Yazar karmaşıklık kuramının kendini biçimlendirme, kendiliğinden oluşum ve birlikte evrim özellikleriyle kamu politikasını ilişkilendirirken, kamu politikası analizi ve çözümleme yöntemlerinin genişleyerek karmaşıklık kuramı çalışanlarının kullandıkları aktör temelli simülasyonlar ve toplumsal ağ analizi gibi yöntemlerin bu analizlerde kullanılabileceğini belirtmektedir. Yazarın anlatımlarından karmaşıklık kuramının nitel, yorumsamacı bir kamu politikası yaklaşımı olduğu çıkarılmıştır. Bu yönüyle karmaşıklık kuramı, öz konusu sistemlerin anlaşılma ve youmlanma çabası olarak görülebilecektir. Bu çıkarsamaya dayanak olarak verilebilecek cümlelerden biri şudur (Morçöl, 2013: 104):

> *"… Bu noktada vurgulanması gerekenler şunlardır: toplumsal ilişkilerdeki karmaşıklık doğadakinden daha fazladır; bunun nedeni toplumları oluşturan bireylerin her birinin karmaşık sistemler olmalarıdır. Her bireyin biyolojik özelliklerinin yanı sıra, kişilik yapısı (psikolojik özellikleri), toplumsal ilişkiler içindeki yerleri vb. onun sistemik özelliklerini belirlemektedir. Kendilerini karmaşık sistemler olan bireylerin ve onların oluşturdukları toplumsal birimlerin (özel ve kamusal örgütlenmeler, dernekler, etnik kümelenmeler vb.) birlikte hareket ettikleri ve iletişimde bulundukları toplumların karmaşıklığının derecesi, oksijen ve hidrojen moleküllerinin etkileşimleri ile ortaya çıkan karmaşıklığın derecesinden çok daha yüksektir"*

Öyleyse yukarıdaki alıntılanan paragrafta da altı çizilen şekilde; iletişim, kişilik, psikoloji, sosyo-kültür gibi değer tabanlı bileşenlerin ön plana çıktığı karmaşıklık kuramına aşağıda yapılacak olan sınıflandırmada, yorumsamacı kamu politikası analizi yaklaşımları arasında yer vermek daha doğru olacaktır.

Yukarıda bahsi geçen kuramlardan genel sistem kuramı ve siyasal grup kuramını biraz daha detaylı ele almak, kamu politikası analizi yaklaşımlarını daha iyi anlamak için faydalı olacaktır. Zira söz kamu politikası analizinin nesnelerinden olan sistemleri ve sosyal grupların kamu politikalarına etkilerini bu kuramlar irdelemektedir.

Genel Sistem Kuramı, Ludwig von Bartalanffy tarafından 1930'lu yıllarda ortaya atılarak temellendirilen ve sonraki yıllarda geliştirilen (1954'te kuramı geliştirme cemiyeti kurulmuştur) bir kuramdır. Kuramın amacı kapsayıcı yapısı ve tüm disipline uygulanabilirliği ile ilimler arası işbirliğini sağlamaktır (Dicle ve Dicle, 1969: 87). Bertalanffy (1968: 33), kuramda kapalı mekanik sistemlerden, çevresiyle etkileşimde olan mikro-organizmalara, termodinamik yasalarından sosyal yapılara, doğal ve sosyal hayatın tüm sistemlerini ele almıştır. Bu sistemleri çevresiyle etkileşimde olan (açık sistemler) ya da olmayan (kapalı sistemler) olarak ayırmıştır. Ona göre sistem, birbiri ve aynı zamanda bulundukları çevre ile ilişkide olan belirli parçalardan yani alt sistemlerden oluşmaktadır. Genel sistem kuramını siyasal sisteme ve kamu yönetimine uygulayarak Siyasal Sistem Kuramı haline getiren David Easton, siyasal kararların belirlenmesinde "girdi-çıktı" analizleri ile dışsallık değerlendirmelerinin de kamu politikası analizine dâhil olmasını sağlamıştır. Ona göre siyasal sistem içerisine, sistemin bulunduğu çevreden giren talepler ve destekler, bu sistem içerisinde bir uzlaşı sağlanmasının ardından kararlar ve politikalar şeklinde olarak yine çevreye bir çıktı olarak yansırlar. Buna göre kamu politikaları, çevresiyle etkileşim içerisinde olan siyasal sistemdeki uzlaşılar sonrası ortaya çıkan karar çıktıları olarak düşünülmektedir (Easton, 1957: 384; 1965). Tüm bu yönleriyle Siyasal Sistem Kuramı, Rasyonel Kamu Politikası Analizi yaklaşımının temellerini oluşturan kuramlar arasında yer almaktadır.

Grup Kuramı ise kökenlerini matematikten (cebir) alan bir kuram olup, siyaset bilimi ve kamu yönetimi disiplinine uygulanması sonucu Siyasal Grup Kuramı olarak anılmaya başlamakla birlikte, siyasal sistem içerisindeki grup çatışmalarını odak

alan bir kuramdır. Çevik'in (1998: 108) vurguladığı üzere bu kuram kamu politikasını grup mücadelelerinin bir ürünü olarak görmektedir. Yazara göre bu kuramın kamu politikaları açısından en büyük eksikliği kurumlar, ideolojiler ve personel gibi unsurların dikkate alınmamasıdır. Buradan anlaşılacağı üzere ilk bakışta kuram, daha önce ele alınan Savunma Koalisyonu Karar Verme modelinin temel özelliklerini yansıtıyor gibi gözükse de aslında tam tersi olarak bu özellikleri dışarıda bırakmakta ve Rasyonel Kamu Politikası Analizine yaklaşmaktadır. Yazarın da belirttiği üzere içinde bulunulan dönemde, baskı grupları ve sivil toplum kuruluşlarının birçok gelişmiş ülkede etkili olarak, gelişmekte olan ülkelerde ise göreceli olarak kamu politikalarına etki ettiği göz ardı edilmemelidir. Bu yönüyle siyasal grup kuramı, kamu politikası analizi çalışmalarında da yer verilmesi gereken bir kuramdır.

Buraya kadar yapılan açıklamalar ve kamu politikası analizine getirilen yaklaşımlar çerçevesinde, kamu politikası analizi yaklaşımları en üst kategoride rasyonel ve yorumsamacı (ya da post-pozitivist) kamu politikası analizi yaklaşımları olarak ele alınabilecektir. Öyleyse; rasyonel kamu politikası analizi yaklaşımının içerisinde değerlendirilebilecek olan, sırasıyla metodoloji, kuram ve karar verme modelleri; nicel analiz yöntemi, baş vurulan kuramlar olarak **işlem maliyeti** ve **kamu tercihi kuramı**, **sibernetik**, **siyasal sistem kuramı, siyasal grup kuramı** ve **yön-eylem kuramı** (daha önce değinilen), modeller olarak; yaklaşımın ana modeli olan **basamaklar** modeli, daha çok rasyonel görüşün bileşenlerini daha detaylı ancak farklı bir açıdan ele alan **çöp kutusu karar verme modeli,** hem temelini çöp kutusu karar verme modelinden alan hem de rasyonel ve pragmatist bir duruş sergileyen **çoklu akımlar modeli**, analitik bir çözümleme taktiğine sahip olarak, dayandığı örneklerle de bunu destekleyen **politika formülasyonu modeli** gruplandırılabilecektir. Yorumsamacı ya da bir diğer adlandırma ile post-pozitivist kamu politikası analizi yaklaşımı ana kategorisinde ise metodolojik olarak nitel analiz yöntemi, başvurulan kuramlar olarak **post-modernist kuramlar** ve

karmaşıklık kuramı, modeller olarak ise; kamu politikası analizinde inançların ve değerlerin rasyonel çıkarlardan daha önemli bir belirleyici olduğunu savunan **savunma koalisyonu modeli**, rasyonel görüşe tepki olarak ortaya çıkan **artırımcı karar verme modeli** gruplanabilecektir. Son olarak her iki kamu politikası analizi yaklaşımını da aynı anda içeren ya da bunlar arasında bir geçiş niteliğinde olan ara kategoride, rasyonalitenin sınırlarının karar vermenin tüm sınırlarını kapsamadığını savunarak onu eleştiren **sınırlı rasyonalite**, artırımcı karar verme modelinin eleştirisi üzerine kurularak karar vermede hem bu kuramı hem de yeri geldiğinde rasyonel yaklaşımı kullanan **normatif optimum karar verme modeli**, hem rasyonel yaklaşımı hem de yorumsamacı yaklaşımın bir modeli olarak belirlenen artırımcı karar verme modelini birleştirerek daha kapsamlı ve verimli bir model ortaya koymayı amaçlayan **karma karar verme modeli** gruplanabilecektir.

Daha derleyici olması ve daha kolay anlaşılması açısından yukarıda yapılan sınıflandırmayı bir tablo aracılığıyla anlatmaya çalışmakta yarar vardır.

Tablo 2: Kamu Politikası Analizi Yaklaşımlarının Sınıflandırılması

	Kamu Politikası Analizi (KPA) Yaklaşımları		
	Rasyonel KPA	**Karma KPA**	**Yorumsamacı KPA**
Analiz Yöntemi	Nicel Analiz	Nicel-Nitel Analiz	Nitel Analiz
Temel Alınan Kuramlar	-İşlem Maliyeti -Kamu Tercihi -Yön-Eylem - Siyasal Sistem Kuramı - Siyasal Grup Kuramı	-Sınırlı Rasyonalite	-Post-Modernist Kuramlar -Karmaşıklık Kuramı
Karar Verme Modelleri	-Basamaklar Modeli -Çöp Kutusu Karar Verme Modeli -Çoklu Akımlar Modeli -Politika Formülasyonu Modeli	-Normatif Optimum Karar verme Modeli-Karma-Tarama Karar VermeModeli	-Savunma Koalisyonu Modeli -Artırımcı Karar Verme Modeli

Yukarıdaki tablo ile daha sistematik bir şekilde tasvir edilmeye çalışılan kamu politikası analizi yaklaşımları sınıflandırmasının hatları ve sınırlarını katı bir şekilde

düşünmemek gerekmektedir. Farklı disiplinler çerçevesinde yer alan daha birçok kuram ve model, kamu politikası analizinde kullanılabilecek ve dolayısıyla yukarıdaki sınıflandırma içerisinde yer alabilecektir. Söz konusu sınıflandırma, kuram ve modellerinin alan yazınında genel olarak verilen özellikleri, kamu politikası analizi yaklaşımlarının özellikleri ve metodolojik bağıntılılar kullanılarak yapılmaya çabalanmıştır. Dolayısıyla, farklı savunular, ele alınan özelliklerin farklı yorumlanışı ya da araştırma sırasında gözden kaçırılmış olabilecek farklı noktalar kuram ve modellerin yer aldığı konumları değiştirebilecektir. Bu yönüyle sınıflandırma yapılacak diğer akademik çalışmalar ve eleştiriler doğrultusunda geliştirilmeye açık olarak düşünülmüş, tasarlanmış ve sunulmuştur. Tüm bu istisnalarla birlikte sınıflandırmanın, kamu politikası alan yazınında bir bilgi yığını şeklinde, hatları olabildiğince belirsiz olarak gözlemlenen kamu politikası analizi yaklaşımlarını ve modellerini daha bütüncül bir şekilde kavramak adına yararlı olabileceği düşünülmektedir.

2. BÖLÜM: ULUSAL GÜVENLİK TEMELİNDE SİBER GÜVENLİK, BAĞLANTILI KAVRAMLAR VE KONULAR

Çalışmanın bu bölümü altında siber güvenlik kavramı derinlemesine ele alınacak ve bu kavramın bağlantılı olduğu kavramlar incelenecektir. Bu yönde yapılacak bir kavramsal bilgi taraması, çalışmanın daha sonraki bölümlerinde sıkça yer verilecek olan siber güvenlik konularında geçecek olan kavramların daha iyi anlaşılmasını sağlayacaktır. Bu bölümde, ilk olarak ulusal güvenlik konusu ele alınmış, akabinde siber güvenlik, bir bilgi toplumu yansıması olarak incelenmiştir. Bölümün ilerleyen kısımlarında siber güvenlikle ilgili diğer kavramlar olan siber saldırı, siber sömürü, risk, tehdit ve güvenlik açığı kavramları, kritik altyapılar ve ilgili alt sistemler ele alınmıştır. Aynı başlık altında, siber güvenliğin ülkelerin ulusal güvenlikleri açısından önemini somut olarak ortaya koymak üzere Stuxnet örnek olayına yer verilmiştir.

2.1. BİR MAKRO KAMU POLİTİKASI OLARAK ULUSAL GÜVENLİK POLİTİKASI

Ulusal güvenlik politikası, bir ulusun askeri ve sivil tüm kaynakları ve araçlarını topyekûn ve koordineli bir şekilde savunma görevlerini gerçekleştirmesi ve milli çıkarlarını korunması adına atılan adımları kapsayan bir planı ifade etmektedir. Her ülke örtülü ya da açık bir şekilde bir güvenlik stratejisine sahiptir. Açık olan güvenlik stratejileri belgelerden ve planlardan okunurken, örtülü stratejiler ise ülkelerin güvenlikleri ile ilgili zaman içinde attıkları adımların ayak izlerinden okunarak gideceği yönün öngörülmesi suretiyle tahmin edilebilecektir (Doyle, 2007: 624). Devletlerin atacakları bu adımlar daha geri planda, toplumlarının sosyal karakteristiklerine ve onun ötesinde de stratejik kültürlerine göre şekil alacak

(Lantis, 2002: 87-88) ve ulusal çıkarların itici kuvveti ile küresel sahadaki hareket alanlarının durumuna göre ilerleyebilecektir.

Gohlert'e (1974: 174) göre, ülkeler ulusal güvenlik politikalarını oluştururlarken iki bakış açısında ilerleyen bir güvenlik algısı üzerinden politika yürütürler. Birinci bakış açısında hayati unsurlar söz konusudur ve algı müzakere ya da uzlaşma fonksiyonlarından ziyade, ülke sınırlarındaki askeri kontrollerle sağlanan güvenliği niteler. İkinci bakış açısı ise dış ilişkiler politikaları ile ulusal güvenlik arasında nitel bir farklılığın olduğunun altını çizen bir yaklaşım sergilemektedir. Buna göre ulusal güvenlik, sıradan dış ilişkiler politikalarına göre çok daha yüksek önceliğe sahip bir politika türüdür. Yazar, güvenlik konusunda önemli gördüğü iki kaynağa atıf vermekte (Wolfers, 1957; Rosenau, 1971) ve buradaki iki tartışmaya dikkat çekmektedir. Söz konusu kuram bazlı araştırmalar ulusal güvenliği araçsal bir hedef ve spesifik bir alan olarak görmektedir. Örneğin Wolfers (1957'de akt. Gohlert, 1974: 174) ulusal güvenliği "önceden kazanılmış değerler"e karşı bir tehdidin olmaması durumu ve bu değerlere karşı gelecek saldırıların kaygısı olarak nitelerken, Rosenau (1971'den akt. Gohlert, 1974: 175) ulusal güvenliği, birbirine karşı olan tavırların şekillendiği ve önceden hesaplanmış hamlelerin yapıldığı, ulusal sınırlar arasında var olan bir etkileşim süreci olarak nitelemektedir.

Gohlert'in (1974: 174) ulusal güvenliği irdelemek üzere vurguladığı "neyin güvenliği ve ne için?" sorusuna aynı zamanda bir yanıt niteliğinde olarak soruya Kamu Tercihi Kuramının penceresinden yaklaşan, ülkelerin ulusal güvenliği ne için ve ne şekilde sağlamaya çalıştığını sorgulayan Lehman ve Willett (1986) ABD güvenlik politikalarını incelemişlerdir. İncelemelerinin sonucunda, ulusal güveliği sağlamak üzere yürütülen politikalarda dikkat çeken iki tip probleme rastlanmıştır. Birinci tip problemdeki konu özel sektörün ulusal güvenlik politikası doğrultusunda üretime nasıl teşvik edileceği konusudur. Kamu tercihi kuramının ilkelerinden olan fayda maksimizasyonu (Buchanan, 1984) ulusal güvenlik konusunda devlet ve özel sektör arasında da kendini göstermekte ve özel sektörün üretim hedefleri buna

göre şekil almaktadır. Lehman ve Willett'in (1986: 45-46) ortaya koydukları birinci tip probleme göre, devletler ulusal güvenliği sağlamak adına farklı araştırma ve geliştirme (ar-ge) çalışmalarını (örneğin siber güvenlik) desteklemek isteyebilir. Bu çalışmalar özel sektör açısından bir kar getirmeyecekse özel sektör bunun yerine daha çok para kazandığı spesifik bir silah üretimine yönelebilecektir. Söz konusu silah üretimi, devlet açısından ülkenin ulusal güvenliği için bir öncelik değilse, burada bir çatışma söz konusu olmaktadır. Bu problemin çözümü için ar-ge ve fiziki üretim için yapılacak kontratların ayrı şekillerde düzenlenmesi ve dahi ar-ge faaliyetleri için hizmet satın alma teşviklerinin iyileştirilmesi politikası yararlı görülmektedir. İkinci ve diğerine nazaran daha temel olan problem tipi ise ulusal güvenlik politikasında yer alan aktörlerin daha iyi sonuçlar alınması adına teşvik edilmesi problemidir. Söz konusu aktörler, devletin farklı kurumları, özel sektör, ilgili sivil toplum kuruluşları (STK) ve vatandaşlar olarak ele alınabilecektir. Bu problemin çözüm önerisi olarak ise yapılacak kurumsal reformlar ön planda tutulmuştur. ABD'de üzerinden ortaya konulan, ulusal güvenlik ile ilgili bu çatışmalar, liberal bir bakış açısı etrafında şekillenmiştir. "Totaliter yönetimlerin olduğu ülkelerde söz konusu çatışmaların olmayacağı ya da daha az olacağı kabul edilirse, ulusal güvenliğin daha kolay ve sağlam bir şekilde sağlanabileceği söylenebilir mi?" sorusu başka bir akademik araştırmanın konusu olabilecek niteliktedir.

Yukarıda birinci bakış açısı olarak ele alınan ulusal güvenliğin ülke sınırlarına yaptığı vurgu, 20. yüzyılın son dönemlerinde ortaya çıkan küreselleşme olgusu ve süreci ile birlikte önemini yitirmeye başlamıştır. Küreselleşmenin ortaya çıkardığı ulus devletlerin sınırlarının belirsizleşmesi tartışmaları, ulusal güvenlik kavramına yönelik algıya da etki etmiştir. Diğer yandan küreselleşme dünyada, ülkelerin güç dağılım kanallarını yeniden şekillendirmiş, asimetrik güç ilişkilerini ortaya çıkarmış ve ülkelerin ulusal güvenlik ihtiyaçlarını yeniden tanımlamalarına neden olmuştur (Kay, 2004). Genel geçer bir anlamda ulusal güvenlik, en az bir ülkenin hayati çıkarlarını ya da değerlerini korumak üzere organize edilmiş politikaları

barındırmaktadır. Savaşlar ve iç isyanlar bir kenarda tutulduğunda, küreselleşmenin sonucunda ülkeler arası güç dengeleri, savunma-saldırı dengeleri ve güvenlik ikilemlerini etkileyen diğer unsurlar değişime uğramış, ülkelerin kendi çıkarlarını korumaları küreselleşme öncesi döneme göre daha zor bir hale gelmiştir (Kirshner, 2006: 2). Ülke sınırlarını aşan, insanlar, bilgiler ve fikirler beraberinde kontrolsüz silahlanma, siber saldırılar, etnik ayaklanmalar, küresel suçlar, uyuşturucu ticareti ve kaçakçılığı, çevresel belirsizlik, bulaşıcı hastalıkların yayılımı[9] (Davis, 2003: 1), küresel terör gibi ulusların güvenliklerini riske sokan yeni tehditleri beraberinde getirmiştir. Bu tehditlerden biri de küreselleşme sonucunda ortaya çıkan ya da ortaya çıkan diğer olumsuzlukların bir sonucu olan demografik hareketlilikler yani göçlerdir. 2000'li yıllardaki göç hareketleri 1970'li yıllardakinin iki katından fazla bir sayıya ulaşmıştır (Simmons, 2007: 3). Göç hareketleriyle birlikte gündeme gelen sınır güvenliği konusu da ulusal güvenlikle birebir bağlantılı bir konudur. Türkiye'nin Helsinki süreci ile hukuki zemine taşınan Avrupalılaşma süreci ile AB'nin güvenlik sorununa ilişkin endişesi, bir bakıma göçün AB tarafından güvenlikleştirilmesi, Türkiye'nin göç ve sınır yönetimi politikalarının da bir şekilde Avrupalı bakış açısı kazanmasına neden olmuştur. Türkiye tarafından yürürlüğe konulan önemli hukuksal değişiklikler (6458 sayılı Yabancılar ve Uluslararası Koruma Kanunu gibi) ve yapısal düzenlemeler, AB ülkeleri ile imzalanan projeler, geri kabul anlaşmaları göç ve sınır yönetimi konusunda Avrupalılaşma sürecinin politika anlamında etkisiyle gerçekleşen önemli adımlar olarak gösterilebilecektir (PA, 2016: 24). Yine de, özellikle son dönemin ana gündem maddesi olan Suriye

---

[9] Bulaşıcı hatalıkların yayılımı, küreselleşme ve aynı paragrafta değinilen demografik hareketliliklerin sonucu olarak da ulusal güvenlikleri tehdit eden bir silah olarak kullanılmaktadır. Bunu "bioterör" olarak ele alan ve derinlemesine araştırıp tartışan bir kaynak için bkz. Report. (2002). Challenges For The Chemıcal Scıences In The 21st Century Natıonal Securıty & Homeland Defense, Washington: The Natıonal Academıes Press.

krizi sonrasında Türkiye'ye gelen Suriyeli mülteciler olayından sonra Avrupa'nın da Türkiye'den örnek alacağı mülteci ve sınır güvenliği politikaları ortaya çıkmıştır

Küreselleşme, devletlerin içişleri ve dışişleri alanında yürüttükleri politikalar arasındaki çizgileri aşındırarak, onları küresel görmeye, düşünmeye ve hareket etmeye itmiştir (Flanagan, v.d., 2001: 7). Böyle bir bakış açısı ve ortamda ülkeler nasıl bir ulusal güvenlik politikası izleyeceklerini daha çok tartışır hale gelmişlerdir. Bu bağlamda, çeşitli karar verme yaklaşımları ulusal güvenlik politikalarının üretiminde kullanılır hale gelmiştir. Redd ve Mintz (2013), karar verme yaklaşımlarının ulusal güvenlik politikaları üretiminde kullanılması üzerine yaptıkları kuramsal temelli çalışmalarında, rasyonel karar verme kuramı (rational choice theory), sibernetik kuramı (cybernetic theory), beklenti kuramı (prospect theory), çoklu buluşsal kuram (poliheuristic theory), grup düşünümü (groupthink), çoklu düşünme (polythink), kurumsal süreç modeli (organizational process model), bürokratik politikalar (bureaucratic politics), analojik sebeplendirme (analogical reasoning) gibi kuram ve modellerin ulusal güvenlik politikasındaki uygulamalarını örnek olaylar beraberinde çalışmalarında sunmuşlardır.

Akdoğan'ın (2011: 75) tanımıyla, bakanlar kurulu kararıyla yürürlüğe giren ve tüm vatandaşları etkileyen bir vergi indiriminden, küçük bir köydeki ihtiyar heyeti ve muhtarın köy ile ilgili aldıkları bir kararın kamu politikası olarak nitelendirilebileceğine çalışmanın ilk bölümünde değinilmiştir. Ulusal güvenlik politikası, kamu politikası bağlamında düşünüldüğünde makro bir kamu politikası olarak düşünülebilecektir. Bunun ötesinde ulusal güvenlik politikasının "makro" bir kamu politikası olarak ele alınmasının gerekliği yukarda atfedilen küreselleşme ile birlikte devletlerin içişleri ve dışişleri alanında yürüttükleri politikalar arasındaki çizgileri aşınması (Flanagan, v.d., 2001: 7) yaklaşımıyla daha da pekişmektedir.

Güvenlik konusu, askeri ve parlamenter güçleri, istihbarat servisi, ulusal ve yerel kolluk güçlerini, sınır güvenliğini, gümrük ve sahil koruma alanlarını da içermektedir

(Bearne, v.d., 2005: iii). Ulusal güvenlik ve bu sayılan alanlar üzerine üretilecek kamu politikalarının, çalışmanın ilk bölümünde yer verilen kamu politikası analizi yaklaşımları çerçevesinde düşünmenin ve analiz etmenin politikanın etkin ve etkili olması açısından fayda sağlayacağı düşünülmektedir. Bu bağlamda makro bir kamu politikası olarak ele alınacak olan ulusal güvenlik, gerek temelleri, Easton'un (1965: 77) sistem analizi yaklaşımında yer alan analiz sürecinin Jenkins (1978: 17) tarafından başlama, bilgilenme, düşünme, karar verme, uygulama, değerlendirme ve sonlandırma basamakları olarak belirlenmesi ve nihayet bu basamakların geliştirilerek Lasswell (1971) tarafından kamu politikası analizine uyarlanmasıyla oluşan rasyonel kamu politikası, gerekse ekonomik temeller üzerine kurulmuş olan politika üretim sürecine karşı çıkan ve gerçekler-değerler ayrımını yaparak değerlerin önemini vurgulayan post-pozitivist (Fischer, vd., 2007: 19) açısından dizayn edilebilecektir. Her iki bakış açısından düşünüldüğünde, ulusal güvenliğin aynı zamanda kamu güvenliği sağlaması dolayısıyla, hem kamu yararı boyutu hem de devlet bütçesine getirdiği yük bağlamında bir de ekonomik yönü bulunmaktadır. Bu bağlamda Redd ve Mintz'in (2013) ulusal güvenlik politikalarını yürütürken kullanılan yaklaşımlar olarak sıraladıkları ve iki önceki paragrafta yer verilen kuram ve modeller daha çok politikaya yöntemsel olarak yön verecek olan yaklaşımlar olarak ele alınabilir. Diğer yandan ulusal güvenliğe makro bir kamu politikası olarak yaklaşıldığında, kamu politikası analizi yaklaşımları ve kamu politikası üretiminde kullanılan, bu çalışmanın ilk bölümünde de ayrı başlıklarda yer verilen karar verme yaklaşımları bir araç olarak kullanılabilecektir. Öncelikle ulusal güvenliğin sağlanmasında ya da korunmasında tanımlanan problemin doğasına, izlenecek yönteme (ki burada Redd ve Mintz'in yaklaşımları ele alınabilecektir) ve elde edilmesi beklenen sonuçlara göre rasyonel ya da post-pozitivist bir açı geliştirilerek üretilecek kamu politikasına etki eden diğer unsurlar (değişkenler, ortama ilişkin belirsizlik vb.) da göz önünde bulundurulacaktır. Söz konusu faktörler belirlendikten sonra üzerinde karar kırılan kamu politikası analizi sistemi ile politika üretilebilecektir. Kamu politikası analizi ve kamu politikası üretim sürecinde yer

alan çeşitli karar alma modellerinin kuramsal altyapıları karar vericiler için çeşitli faydalar sağlayacaktır. Örneğin; ulusal güvenlik ile ilgili problemlerin net ve doğru bir şekilde belirlenmesi, oluşturulacak politikaların radikal ya da önceden uygulanmış politikaların bir türevi olması (artırımcı karar alma), Lehman ve Willett'in (1986) kamu tercihi kuramına gönderme yaptığı üzere belirlenen politika hedeflerine yönelik olarak ekonomik çıkarlar ya da milli değerlerin ön planda tutulması, politikayla ilgili tüm aktörlerin sürece dâhil edilip edilmemeleri, alternatif politikaların analizi gibi konular daha sistematik ve kuramsal altyapı temelinde tasarlanabilecektir.

Ulusal güvenliğin makro bir kamu politikası olarak ele alınması, geleneksel olarak güçlü bir algı şeklinde beliren ve gelinen dönemde değişen "ulusal güvenlik algısı"nın bir gerekliliğidir. Devlet yönetimlerinin, özellikle Dünya Savaşları'ndan sonra ulusal güvenliği sadece ülkeye yönelik askeri saldırılar ve bu saldırılara karşı alınacak askeri-politik stratejiler olarak görmesi, içinde bulunulan dönemde yanlış bir tutum olarak kabul görecektir. Bello'nun (2011: 68) da belirttiği üzere artık ulusal güvenlik sadece fiziki ve askeri saldırılara yönelik tedbir ve bu saldırıların engellenmesi değil, siber saldırılar, ekonomik büyümenin sekteye uğraması, terör, salgın hastalıklar, iç ayaklanmalar, göçler, küreselleşe beraberinde gelen ve gelecek yeni tehditler gibi birçok tehdide karşı sağlanan bir güvenliktir. Bu bağlamda ulusal güvenlik sadece askeri stratejiler geliştirmek üzerine odaklanan bir politika olarak değil, kamu düzeni ve kamu yararını, insan haklarını, ekonomik fayda-maliyet analizleri yanında milli, kültürel ve insani değerleri de göz önünde bulundurarak ele alınması gereken "makro bir kamu politikası" olarak düşünülmesi gereken bir olgudur.

2.2. BİLGİ TOPLUMUNDA YENİ BİR KAVRAM OLARAK SİBER GÜVENLİK

Siber güvenlik kavramına giriş yapmadan önce genel olarak “güvenlik” kavramı üzerinde bir nebze yoğunlaşmakta yarar vardır. Güvenlik kavramı, alan yazınında üzerine kesin bir uzlaşmanın sağlanamadığı, tartışmalı kavramlardan biri olarak görülebilecektir. Baylis (2008: 73), kavram üzerinde tartışmada bulunan yazarların birçoğunun güvenliğin temel değerlere (hem bireysel hem kitlesel) yönelik tehditlerden özgür olunması anlamına gelmesi olduğu noktasında fikir birliğinde olduklarını, ancak analizlerin temel odağının bireysel, ulusal ya da uluslararası ölçeklerden hangisi olduğu konusunda farklılaştıklarını vurgulamaktadır. Yazarların güvenlik tanımı geliştirmek üzere odak aldıkları ölçeklerin farklılaşmasının yanında, güvenlik kavramının tanımı yapılırken birçok değişkenin dikkate alınması gerekliliği ve değişen şartlara göre kavramın çerçevesinin yeniden belirlenmesi durumu herkes tarafından kabul gören ve her dönem geçerli olan bir tanımın ortaya çıkmasına engel olmaktadır (Sancak, 2003: 124).

Kelimenin etimolojik kökenine inilecek olursa, Türkçede güvenlik kelimesi itimat etmek veya inanmak manasına gelen “küven” kökünden türemiş olup, kelimenin kökü 8. ve 11. yüzyıllar arasında Orta Asya Türkçesinde ün, nam, iktidar anlamında kullanılan “küve” ya da “küv” kelimelerine dayanmaktadır. Küven kelimesi aynı zamanda böbürlenmek ve mağrur olmak anlamına da gelirken, bu anlamlarından dolayı özellikle 19. yüzyılda olumsuz bir kavram olarak kullanılmış, daha sonra sıfatları soyut bir ada ya da adları bir işleve dönüştüren “-lık” ekiyle birleştirilerek kullanılmıştır (Nişanyan, 2009: 219’dan akt. Birdişli, 2011: 151). Kelime anlamına yakın olarak, geleneksel manada güvenlik; askeri tehditleri vurgulayan, statüko odaklı ve devletler üzerine odaklanan bir kavram olarak kullanılmıştır (Booth, 1991: 318). Daha dar bir açıyla bakıldığında ise dönemsel olarak, küresel etkilerin uzantısı olarak güvenlik kavramının anlamsal

yoğunlaşmalara maruz kaldığı gözlemlenebilmektedir. Örneğin, Dünya Savaşlarından sonra ülkelerin birbirlerine karşı askeri tehditleri olarak algılanan ulusal güvenlik, Soğuk Savaş döneminde ülkelerin birbirleri arasında olan stratejik ilişkileri ve dengeler, ABD'deki 11 Eylül olaylarından sonra ise daha çok terörizme karşı alınan tedbirler olarak algılanmaya ve tasvir edilmeye başlamıştır (Booth, 2007: 96). Tüm bu algısal farklılıkların doğrultusunda güvenlik kavramını irdelemek Birdişli'nin (2011: 150) vurguladığı üzere bir dikotomiye ihtiyaç duymaktadır. Zira ontolojik güvenliği kavramak sezgilere dayalıdır ve bu nedenle zihin göreceli bir etkinliğe ihtiyaç duyar. Nasıl ki güzeli anlamak ya da tasvir etmek için bir çirkinliğe, gece için bir gündüze ihtiyaç duyuluyorsa güvenlik için de tehditlere ihtiyaç duymaktadır.

Siber güvenlik kavramına gelindiğinde bu kavram, son yıllarda bilgisayar ve iletişim teknolojilerinin gelişmesine ve bu teknolojilerin insanların sosyal hayat, iş hayatı ve kamusal hayat gibi yaşam alanlarının büyük bir kısmında yer kaplamasına paralel olarak sıkça kullanılır hale gelen kavramlardan biri olmuştur. Siber güvenlik kelime kökeni itibariyle hayvan ve makine sistemlerinde kontrol ve iletişim konusunda öne çıkan "sibernetik" kavramının (Wiener, 1948) "siber kökünden ileri gelmekte olup, günümüzde daha çok elektronik kontrol sistemlerini nitelerken, kelime bir nesne olarak değil, ağlar ile erişilen bir elektronik sistemi destekleyen ve niteleyen bir sıfat olarak anlaşılmalıdır. Siber güvenliği çalışan ve sağlamayı görev ya da meslek edinmiş uzmanların amaçları ve görevleri, ilgili aktörler ve konular genel olarak siber güvenliğin konu sahasını çizebilir. Söz konusu araç ve görevler üç sütunda toplanabilecektir. Birinci sütunda yer alan amaçlar; önlemek, tespit etmek ve cevap vermektir. İkinci sütunda siber güvenlik konusunun nesneleri yer almaktadır. Bu nesneler, insanlar, süreç ve teknolojidir. Son sütunda ise siber güvenliğin gizlilik, bütünlük ve kullanılabilirlik gibi özellikleri yer almaktadır (Bayuk, vd., 2012). Diğer yandan siber güvenlik kavramı ile birlikte en sık kullanılan ve yine kavrama temel oluşturan bir kavram da "siber uzay" (cyberspace)'dir. Siber alan fiziki donanımların

ortaya çıkardığı ve barındırdığı bir alan olmasına karşın somut bir alan değildir. Siber alan sadece internetle birlikte var olan bir alan değildir. İnternete bağlı olmayan bilgisayarlar ya da farklı ağlar da siber alan oluşturabilir. Son olarak siber alan birden fazla soyut olgunun bir araya gelmesinden de oluşabilmektedir. Yazılımlar, bilgiler ve ağlar buna örnek olarak verilebilecektir (Clark, vd., 2014).

II. Dünya Savaşı'nın sona ermesiyle birlikte, kapitalist ve sosyalist sistemler arasında kıyasıya bir rekabet başlamış, bu rekabete bağlı araştırma ve geliştirme ataklarının da uzay çağını başlattığı ileri sürülmüştür. Söz konusu rekabetin en önemli sonucu özellikle bilgisayar ve iletişim sistemleri alanlarında ortaya çıkardığı büyük teknolojik gelişmeler olmuştur. Bu gelişmeler insanlık tarihinde yeni bir toplumsal gelişmenin habercisi olarak algılanmıştır (Çelik, 1998: 54). Bilgisayar ve iletişim teknolojilerinin gelişmesiyle birlikte ortaya çıkan bu toplumsal değişmede, bilgiyi üretme, dağıtma, kullanma şekilleri ve araçlarının yanı sıra toplumun bilgiye karşı olan algısı ve bilginin toplum üzerindeki yansıması da değişmiştir. Bu değişim ve beraberinde gelinen dönem genel olarak "bilgi toplumu" olarak isimlendirilmeye başlanmıştır.

Webster (2014: 8), bilgi toplumunu tam anlamıyla anlamak için farklı boyutlarını ayrı ayrı değerlendirmek gerektiğini belirtmektedir. Bu boyutlar; teknolojik, ekonomik, mesleki, uzaysal ve kültüreldir. Yazarın çalışmasında, kavramın teknolojik boyutu daha çok bir ülkenin internet ve bilgi teknolojilerine adaptasyon kapasitesine dayandırılmıştır. Buna göre, ülkenin sahip olduğu internet ve iletişim altyapısı ve bu alanlarda sunduğu hizmet kapasitesi ülkenin bilgi toplumunu yakalayabilmesinin temel faktörleridir. Ekonomik boyutu, ülke ekonomisi içinde ya da gayri safi milli hasılada, bilgi ve hizmet temelli sektörlerden elde edilen gelirlerin artmasını odak almaktadır. Bu boyutu Daniel Bell (1973), post-endüstriyel toplum içerisinde ele almıştır. İngiltere'de Sanayi Devrimi öncesi ve sonrası şeklinde ele aldığı ve buna bağlı olarak endüstrileşme öncesi ve sonrası olarak ayırdığı toplumu inceleyen Bell, post-endüstriyel toplum olarak tanımladığı toplumda, artık kas gücü

değil, bilginin önemli olduğunu vurgulamış ve bunu ekonomi üzerinden incelemiştir. Castells de (1999: 37) Bell'e benzer şekilde, bilgi toplumunu endüstri devriminden sonra devrim niteliğindeki yapısal ve teknolojik gelişmelerden sonra ortaya çıkan "endüstriyel toplum" gibi bilgi ve internet teknolojilerin yaşamın her evresine etki ettiği toplumu "bilgi toplumu" (informational society) olarak isimlendirmenin uygun olacağı görüşündedir. Lax (2001: 34), bilgi toplumunun ekonomik boyutunu küreselleşme ve ticaret ağları açısından ele almış ve bilgi toplumunun küçük ve hibrid üreticilere de teknolojinin avantajlarıyla gelişme ve iş yapma fırsatı verirken, büyük ticari işletmelerin rekabet gücünü düşürdüğü için onlara olumsuz etkide bulunduğunu vurgulamıştır.

Bilgi toplumunun kendi değimiyle en fazla gözle görülen fakat en az ölçümlenebilen boyutu olan kültürel boyutunu ele alan Webster (2014: 19), özellikle televizyon, akıllı telefon, bilgisayar ve gazete gibi kitle iletişim araçları ile insanlara yansıtılan bilginin yoğunluğuna dikkat çekmektedir. Söz konusu bilgi yoğunluğu, bilgi toplumundaki insan hayatını pek çok sembole yüklemektedir. Örneğin, giyim modası ve moda bilgisi doğrultusunda belirli bir giyime sahip olan insan, etrafına hakkındaki bu entelektüel bilgiyi yansıtmaktadır. Bireyin giydiği giysiler sahip olduğu moda bilgisinin ve yansıttığı tarzın sembolleridir. Webster, bilgi toplumunun beraberinde getirdiği kültürel değişimi örnekte betimlenmeye çalışıldığı üzere toplum yaşamının sembolleşmesine dayandırmaktadır. İnsan yaşamında var olan bilgi yoğunluğu nedeniyle, bilgiler sembollerin ardına sıkıştırılmakta ve insanlara semboller aracılığıyla hatırlatılmakta ya da karşılarına çıkarılmaktadır.

Webster'in (2014: 17) ele aldığı uzaysal boyut, bilgi toplumunda gelişerek çoğalan bilgi ağlarını ifade etmektedir. İnternet ve iletişim teknolojilerinin gelişmesiyle birlikte farklı lokasyonlardaki farklı bireyler zaman ve mekân fark etmeksizin oluşturdukları ağlar sayesinde bilgi üretmekte ve üretilen bu bilgileri birbirleriyle paylaşabilmektedir. Çalışmasında Amerika, Rusya ve Çin'i bilgi ağları çerçevesinde inceleyen Castells (2004: 3), sosyal yapısı mikro elektronik araçlarla

kurulan bilgi ve iletişim tabanlı ağlardan oluşan toplumu “bilgi ağı toplumu” olarak tanımlamaktadır. Uzaysal boyut, ortaya çıkan bilgi ağı toplumu sonucunda iş dünyası, akademik dünya, idari yönetimler ve daha birçok alanda sürekli gelişmeyi amaçlayan bilgi ağlarının zaman ve mekânın önüne geçerek son derece etkin bir hale gelmesini nitelemektedir. Webster’ın uzaysal boyutuna paralel olarak Albrechts ve Mandelbaum (2007: 15), Habermas’ın kişiler arası diyalog yaklaşımı ile Castells’in ağ toplumu yaklaşımı arasında ilişki kurarak, gelişmiş olan bilgi ağlarının sadece resmi ve çıkara dayalı ilişkiler değil, aynı zamanda insanların günlük hayatının ve sosyal yaşamının bir parçası olduğunu vurgulamaktadırlar.

Bilgi ağlarının yoğun olarak sanal ortamlarda oluştuğu ve geliştiği bilgi toplumunda bu ağların güvenliği konusu da önemli bir faktör olarak gündeme gelmektedir. Söz konusu sanal tüm oluşumların ve dolaylı olarak da oluşumlarda saklanan, yayınlanan, üretilen bilgilerin güvenliği genel olarak “siber güvenlik” olarak isimlendirilmektedir. Siber güvenlik, bireysel, kitlesel, bölgesel ya da ulusal ve dahi uluslararası anlamda bir güvenliği ifade etmektedir. Bu yönüyle hem bir vatandaş olarak bireyi hem de bireyin güvenliğinden sorumlu olan ve bir politika üreticisi, uygulayıcısı olan devletin yaşam alanına giren bir konudur.

Siber güveliğin genel olarak üzerinde uzlaşılmış belirli bir tanımı yoktur. Korff (t.y., 1-4), çalışmasında siber güvenliğin çeşitli kurumlarca yapılmış tanımlarına yer vermiştir. Buna göre NICE (The National Initiative for Cybersecurity Education) siber güvenliği, bilgi ve iletişim sistemleri ile bu sistemlerin içerisinde yer alan bilgilerin herhangi bir zarara, saldırıya ya da yok edilmeye karşı korunduğu, savunulduğu bir faaliyet ya da süreç olarak tanımlamaktadır. Kurum, daha detaylı yaptığı tanımda unsurları artırarak; siber uzaydaki operasyonlar ve güvenliğe bağlı politika, strateji, standartlar ile her türlü tehdit, güvenlik açığı, caydırıcılık, uluslararası bütünleşme, olaylara karşı hazırlıklı olma, direnç, kurtarma politikaları, askeri, diplomatik ve istihbarat ile ilgili küresel bilgi ve iletişim altyapısının güvenliği gibi unsurları eklemiştir. ITU (International Telecommunications Union) ise siber

güvenliği “siber çevre, kurumlar ve bireylerin varlıklarını korumak adına kullanılabilecek araçların, politikaların, güvenlik kavramlarının, güvenlik talimatlarının, risk yönetim yaklaşımlarının, eylemlerin, kursların, en iyi örneklerin, güvence ve teknolojilerin toplamı” olarak tanımlamaktadır.

Siber güvenlik kavramının daha iyi anlaşılabilmesi için siber güvenliğin kullandığı araçlara da değinilebilir. Bundan önce belirtmekte yarar vardır ki; siber güvenlik siber uzayda sağlanan güvenlik olarak düşünülmelidir. Siber uzay ise tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortam olmakla birlikte bu terim ilk defa, bilim kurgu romanlarıyla tanınan William Gibson tarafından 1980’lerin başında kullanılmıştır (Kara, 2013: 4). Birleşik Krallığın siber güvenlik strateji belgesinde ise siber uzay “bilgileri saklamaya, düzenlemeye ve birbiri arasında alışveriş yapmaya imkân veren, bilgisayar, internet ve diğer sistemleri içeren altyapısal ve sektörel sistemleri destekleyen, dijital ve interaktif bir bağlantı ağı” (GCHQ, 2012: 3) olarak tanımlanmıştır. Günümüzde siber uzayla eş anlamlı olarak “siber ortam” terimi de kullanılmaktadır. Siber güvenliğin kullanıldığı araçlara geri dönülecek olursa; Yue (2003: 566-568), siber güvenliğin araçlarını üç kategoriye ayırmaktadır. Birinci kategori “optimal tasarım” kategorisidir. Optimal tasarım; ağın kendini yenilemesi, onarması ve restore etmesini ifade etmektedir. Aynı zamanda bu ağın ne kadar bağlanılabilir ya da kapsayıcı (kapasite) olduğu ve bu kapasitenin arttıkça kapsadığı bağlantı sayısıyla birlikte tehditlere karşı ne kadar güvenli olduğu konusu da optimal tasarımla ilgilidir. İkinci kategori “sürekli ağ denetimi” kategorisidir. Burada ağın sürekli ve devamlı olarak gözlemlenmesi ve zayıf yönlerinin belirlenmesi söz konusudur. Ağda meydana gelecek problemler için teknik çözümler de kullanılabilecektir. Bu kategori aynı zamanda ağın güvenilirliği hakkında referans veren kategoridir. Son kategori ise “sonraki nesillerin güvenliği” kategorisidir. Söz konusu siber ortam ağlarında, birçok farklı güvenlik kriptoları kullanılabilmektedir. Ağlarda yer alan kriptolama sistemlerinin kalitesi ya da

fazlalığı, ağ için katlanılacak olan maliyetin yanı sıra ağın gelecek siber saldırılara karşı dayanıklılığını da artıracaktır. Dolayısıyla ağı kullanacak olan gelecek neslin güvenliği de de artmış olacaktır.

Siber güvenlik, yukarıda da bahsedildiği siber bir ortamın, uzayın ya da ağların güvenliğini nitelemektedir. Bu ağlar çeşitli amaç ve fonksiyonda kişiler ve kurumlar tarafından kullanılmakla birlikte siber güvenlik de hem bireyleri, hem kurumları ve dahi devletleri ilgilendirmektedir. Öyleyse, siber güvenliğin bireysel, kurumsal ve ulusal boyutlarından söz edilebilecektir. Bu çalışma, siber güvenliğin kurumsal (kamu sektörü) ve ulusal boyutu üzerinde odaklanmaktadır. Dolayısıyla çalışmanın ilerleyen kısımlarında siber güvenlik özellikle ulusal bir perspektiften ele alınacak olup, zaman aman bireysel boyutuna değinilecektir.

Dünyanın önde gelen ağ teknolojileri firmalarından olan CISCO, siber güvenliği Avustralya üzerinden incelerken, onu bir “ulusal öncelik” olarak tanımlamakta ve internete olan bağımlılığın hem bireysel hem ulusal düzeyde artması mukabilinde önemini vurgulamaktadır (CISCO, 2017: 2). Bir denetim, vergi ve danışmanlık hizmetleri sağlayıcısı olan ve alanında ileri gelen dört büyük firmadan biri olan KMPG de siber güvenliğin önemini vurgularken, siber güvenlik konusunda devlet kurumlarının ve özel sektörün edindiği deneyim ve tecrübelerin birbirleri arasında paylaşılarak kamu-özel işbirlikleri kurulması gerektiği üzerinde durmaktadır. Şirketin raporunda yer alan sonuçlara göre (KMPG, 2016: 4); 2014 yılında Avustralya kayıtlarına göre 1131 siber güvenlik vakası meydana gelmiştir. Bu vakalardan dolaylı ya da dolaysız olarak 21.5 milyon insan etkilenmiştir. Küresel boyutta ise özel sektörde siber güvenlik için saldırılara karşı 565 milyar dolar bütçe harcanmıştır. Araştırmanın odak aldığı Avustralyalı CEO’ların (Chief Executive Officer) %25’i siber güvenliği şirket yönetimine etkide bulunan en önemli konulardan biri olarak görürken, %29’u bilgi güvenliğini üzerinde durulan en büyük risk faktörü olarak görmektedir. Tüm bunların yanında CEO’ların %35’i kendilerini herhangi bir siber güvenlik olayına karşı hazırlıklı olarak görmektedirler.

Başlığın bu noktasına kadar ele alınan konu ve açıklamalarda görüldüğü üzere siber güvenlik, bireylerin, şirketlerin ve özellikle vurgulandığı üzere devletlerin bütüncül güvenlikleri açısından önem taşıyan ve onlar tarafından da önem gören bir konu haline gelmiştir. Bu yönüyle siber güvenlik konusunda yapılacak olan akademik ve teknik çalışmaların, düzenleme ve geliştirmelerin de gelenekselleşmiş güvenlik anlayışının dışında sanal (siber), aslında bir o kadar da reel olan, farklı bir güvenlik anlayışının oluşması yönünden önem taşıdığı düşünülmektedir.

Siber güvenlik konusu hakkında genel bilgi ve açıklamalara yer verdikten sonra onun olumsuz unsurları olan siber atak, siber sömürü, risk, tehdit ve güvenlik açığı kavramlarına değinmenin, siber güvenliği daha iyi anlamak açısından uygun bir adım olacağı düşünülmektedir. Bu doğrultuda çalışmanın devamında bahsi geçen kavramlar hakkında genel bilgiler verilecektir.

2.3. SİBER GÜVENLİK İLE BAĞLANTILI KAVRAMLAR VE KONULAR

Bu başlık altında, siber güvenlik ile bağlantılı kavramlar ve konular sırası ile ele alınmıştır.

2.3.1. Siber Atak / Siber Saldırı

Siber güvenliğin en önemli tehdit unsuru siber ataklardır. Siber ataklar, bilgi barındıran sanal ağlara, bilgileri çalmak, değiştirmek ya da yok etmek amacıyla yapılabilmektedir. Söz konusu saldırılar bilgisayardan bilgisayara, cihazların ya da onların içerisindeki bilgilerin gizlilik, bütünlük ve ulaşılabilirliğini tahrip etmek için yapılmaktadır (O'Shea, 2003: 6). Özellikle internet teknolojilerinin gelişmesi ve internet kullanımının yayılmasıyla birlikte, bilgisayarların büyük çoğunluğu internete bağlı bir hale gelmiştir. Bu durum, siber atakların nüfuz edebileceği alanı da

genişletmiştir. Zira siber saldırılar, bilgisayar ve ağların oluşturdukları sanal ortamda yön ve hedef bulmaktadırlar. Böylece siber saldırılar için gelişen zemin, akabinde saldırıların da artmasına neden olmaktadır (Zhang, v.d., 2010: 56). Artan saldırıların beraberinde siber güvenlik konusunun önemi de pekişmektedir.

Siber saldırılar, temelde insan kaynaklı eylemlerdir. Her ne kadar kullanılan araçlar ve hedef alınan noktalar sanal ortam ve verilerden oluşsa da saldırıların sonuçları insanları etkilemekte ve amaçları da insanların oluşturdukları amaçlara dayanmaktadır. Lu (2014: 11) siber saldırıların klasik hackerlar, paralı hackerlar, hacktivistler, iç mihraklar (kötü niyetli olmalarına gerek olmaksızın) ve ulus devletlerce yapılabileceğini belirtmektedir. Siber saldırıları gerçekleştiren bu unsurlar hedef olarak bireyleri, firmaları ve devlet kurumlarını hedef alarak onların ağlarına girmeyi deneyebileceklerdir. Bu çalışma da, özellikle ulus devletlerin ve devlet kurumlarının siber güvenliğini odak almakta ve onlara yönelik siber saldırılarla ilgilenmektedir.

Geers (2010) siber atakları, Soğuk Savaş döneminde önem kazanan ve üzerinde durulan “caydırıcılık kuramı” üzerinden düşünmüş ve yorumlamıştır. ABD ve Sovyetler Birliği arasında olan psikolojik savaş, geleneksel askeri savaş mantığını sona erdirmiş ve bu iki gücün ellerinde bulundurdukları ve insanlığın sonunu getirebilecek nükleer silahlar savaş potansiyeli taşıyan ülkeleri bir eylemsizlik durumuna getirmiştir. Siber saldırılar da bu minvalde düşünülürse, büyük bir askeri strateji olabilecek ve ülkelerin kitle imha silahları gibi teknolojilerinin çalınması, ya da imha edilmesine kadar zararlar verebilecektir. Ülkeler, siber saldırılardan korunmak üzere uluslararası askeri bir savunma politikası izleyebileceklerdir. Caydırıcılık kuramında, ulus devletler iki temel caydırma stratejisine sahiptirler; reddetme ve cezalandırma. Söz konusu iki strateji, üç temel gereksinimi içermektedir; kapasite, iletişim ve kredibilite. Geers’e (2010: 301) Siber saldırılar aslında ülkelerin ellerinde bulundurdukları nükleer silahları kendi ülkeleri içerisinde patlatacak bir potansiyele sahip olarak düşünülse bile şuan için bu düşünce bir

bilim kurgu olarak görülmektedir. Bu yüzden siber ataklar, nükleer saldırılardan daha alt tehlikede görülen saldırılardır. Bu yüzden caydırıcılık kuramında, tarafların eylemsiz kaldığı “reddetme” stratejisi es geçilmekte ve “cezalandırma” stratejisi uygulanmaktadır. Cezalandırma stratejisi için ise ülkelerin siber saldırılardan korunacak, onlara karşılık verebilecek ya da saldırı düzenleyebilecek bir siber altyapı, tehditleri caydırıcı bir iletişim yönü ve cezalandırıcı bir caydırıcılık stratejisi uyguladığında ayakta kalabilecek bir kredibilitesi olması gerekmektedir.

Bir siber ortama yapılacak saldırılar sistemin güvenliğinin kırılabileceği birçok güvenlik zaafı ya da hatasından kaynaklanabilmektedir. Bu doğrultuda bir bakış açısını öncelikli olarak benimseyen Fovino ve arkadaşları (2009), siber saldırılarla “kusur ağaçları” (fault trees) yaklaşımıyla birlikte ele almışlardır. Yaklaşımda “petri net tabanlı” ve “saldırı ağaçları” isimli iki model yer almaktadır. Petri net tabanlı yaklaşım, saldırıların çeşitli aşamalardan geçerek eyleme dönüştüğünü vurgularken, saldırı ağaçları yaklaşımı ise bu hazırlıkların sistemin sahip olduğu kusurlara (kusur ağaçları yaklaşımı) göre gerçekleştirildiğini anlatmaktadır. Buna göre bir sistem, sahip olduğu tüm bileşenlere ve bu bileşenlerin ortaya çıkardığı ya da potansiyel olarak kalan kusurlara bağımlı bir şekilde güvenliğini muhafaza etmektedir. Sistemin güvenliği sahip olduğu kusurlar oranında risk altındadır.

Siber saldırıların dünya gündemine gelmiş belli başlı bazılarına bakılacak olursa, NATO kronolojik olarak bir sıralama yapmıştır (NATO, 2016). 1988 yılında şuan Massachusetts Institute of Technology’de Profesör olarak çalışan Robert Tapan Morris’in yazdığı solucan özellikle Amerika Birleşik Devletleri’nde (ABD) internet aracılığıyla tüm bilgisayarlarda yayılarak onları neredeyse çalışamaz halde getirmiştir. Bunu yapma amacının internetin ne kadar büyük olduğunu anlamak olduğunu söyleyen Morris, ABD tarafından ulusal siber suçla yargılanan ilk kişi olmuştur. 2006 yılında National Aeronautics and Space Administration’a (NASA) bir siber saldırı gerçekleşmiş ve uzay araçlarının planları davetsiz misafirlerce ele geçirilmiştir. 2007 yılında Estonya’ya gerçekleştirilen siber saldırıda ülkenin internet

sistemleri zarar görmüş ve özellikle bankacılık sistemi bundan etkilenmiştir. Estonya hükümeti bu saldırıya karşı hemen pozisyon almış ve sistemlerini saatler içinde düzeltmiştir. Yine bu yılda ABD Savunma Bakanlığının e-meal adresi hacklenmiş ve böylece Pentagon'a sızılmaya çalışılmıştır. Aynı yıl içerisinde Çinli yetkililer, geneli Tayvan ve ABD'den olan hackerların stratejik birimlerinden bilgiler çalmak amacıyla ülkelerinin siber alanına saldırdıklarını açıklamıştır. 2008'de ABD'de Cumhuriyetçi ve Demokrat Partinin her ikisinin de bilgileri hacklenmiştir. 2009'da Gazze Şeridi'nde operasyonlar düzenleyen İsrail'in internet altyapısına yaklaşık 5 milyon bilgisayarla saldırıda bulunulmuştur. 2010'da İran Siber Ordusu adı verilen bir grup Çin'in Baidu ara motoruna saldırıda bulunmuştur. Saldırının bir sonucu olarak, arama motoruna giren kullanıcılar İran Siber Ordusunun politik mesajı ile karşılaşmışlardır. Aynı yıl Stuxnet isimli Siemens firmasının endüstriyel kontrol sistemlerine müdahale etmek için geliştirilmiş yazılımın aslında İran Nükleer Programını hedef alan bir silah olduğu spekülasyonları ortaya çıkmıştır. 2011 yılında Kanada'nın kamu kurumlarına büyük bir siber saldırı girişiminde bulunulduğu devletçe açıklanmış ve saldırı sonucunda birçok kurumun internet bağlantısı kesilmiştir. 2011'de ABD Savunma Bakanlığı siber saldırıya uğrayarak kurumdan 24.000 dosyanın çalındığını açıklamıştır. 2012'de Rus firması Kaspersky 2007'den beri süren bir siber saldırıyı keşfederek gün yüzüne çıkarmış ve bu saldırıya "Kızıl Ekim" ismini vermiştir. Bu saldırıda hackerların Asya, Avrupa ve Amerika'daki devlet kurumlarını hedef alarak buralardan bilgi ve belge kaçırdıkları belirlenmiştir. Sitedeki son açıklanan siber saldırı ise 2013 yılında Kuzey Kore'nin Güney Kore'ye yaptığı siber saldırıdır.[10]

---

[10] Diğer örnek siber saldırılar için bkz. Peretti, K. Slade, J. State-Sponsored Cybercrime: From Exploitation to Disruption to Destruction, http://www.alston.com/Files/Publication/0470bf82-1589-4200-be02-de03a3aea95b/Presentation/PublicationAttachment/35553890-a8a6-4eb5-b7bf-e6397539d409/14-183-State-Sponsored-Cybercrime.pdf

İçinde bulunulan dönemde siber saldırılar, sistemlere sızma, bilgi çalma, bilgi yerleştirme, mevcut bilginin bozulması gibi durumların ötesinde, bir ülkenin haberleşme sistemlerine, sağlık sistemlerine, bilgi sistemlerine, enerji ağlarına, ulaşım ağlarına, komuta ve kontrol sistemlerine zarar verecek ölçüde asimetrik bir harp türü olarak (Doğançay, t.y.: 6) karşımıza çıkmaktadır. Saldırıların ne zaman ve ne şekilde gerçekleşeceği, yönü ve faili alan savaşlarında olduğu gibi gözle görülememekte ve önceden kestirilememektedir. Diğer yandan, bu saldırılar ve saldırılar sonucunda hedefe yaşatılacak olan tahribatın büyüklüğü de geleneksel savaşlarda olduğu üzere mühimmata yapılan yatırımların büyüklüğü ile orantılı olmayıp, tahribat sadece bir bilgisayar ve bir insan beyninin birleşimi ile meydana getirilebilmektedir. Tüm bu yönleriyle siber saldırılar, sahip oldukları çeşitli boyutlarıyla, özelikle teknik uzmanlar tarafından detaylı şekilde araştırılmakta, çeşitli savunma yöntemleri geliştirilmekte ve bunlar siber güvelik sistemlerine entegre edilmektedir.

2.3.2. Siber Sömürü

Siber sömürü, bir siber ortamdaki siber güvenlik kusurlarından ortaya çıkan ve güvenlik açıklarının kullanılması sonucu ortamdaki bilgilerin çeşitli amaçlar doğrultusunda istismarına dayanan bir eylem ve aynı zamanda bilişsel bir suçtur. Kaliforniya hukuk bürosunun yayınladığı, siber sömürü hakkındaki hukuki düzenlemeleri anlatan broşürde siber sömürü; rıza olmadan kişisel fotoğraf ya da videoların internet ortamında dağıtılması ya da yayınlanması olarak tanımlanmıştır (OAG, 2017). Broşürde genel olarak tecavüz, kadınların fotoğraf ve video yayınlarında istismarı ve çocuk pornosu gibi konularda mücadeleye dikkat çekilmekte ve siber sömürü kavramı bu unsurlarla ilişkilendirilmektedir. Avrupa komisyonunun yayınladığı raporda da durum benzer bir nitelik göstermektedir (EUC, 2012: 2). Sömürünün siber ortamdan yapılması temelinde siber sömürü olarak isimlendirilmiş olan bu tanım, temsili bir niteliğe sahip olmakla birlikte çok

sınırlı bir tanım olarak nitelendirilebilecektir. Siber sömürü, sadece kişisel fotoğraf ya da videoların yayınlanmasından çok öte, sistemsel ve kitlesel sömürüleri de kapsamakta olan bir kavramdır.

Erickson (2008, 115-118), siber sömürüyü, onun sadece kişisel verilerin internette dağıtım ve yayının olması ötesinde, programlama odağından incelemiştir. Ona göre siber sömürünün en etkili yöntemlerinden biri de bilgisayar programlarının güvenlik açıklarından yararlanarak onların içerisine sızarak onu kullanan kişi ya da kurumun bilgisi dışında, programı farklı amaçlar doğrultusunda kullanmaktır. Bu yöntemle programın güvenlik açıklarından faydalanılarak program ya farklı işlevlerde ya da kendi programlandığı işlevler doğrultusunda ancak farklı amaçlarla kullanılabilecektir. Örneğin bir program, kendisinin bir işlevi gereği bilgisayardaki klavye hareketlerini (basılan tuşlar vb.) kayıt altında tutmaktadır ancak bir hacker bunu siber sömürü olarak bilgisayarda diğer internet siteleri ya da banka hesabı şifrelerini öğrenmek ve ele geçirmek adına kullanabilecektir.

Siber sömürüye farklı bir açıdan bakılacak olursa, “sömürgecilik” kavramının politik yönlü tanımına odaklanmakta fayda vardır. Sömürgecilik kelime anlamıyla, temele “yerleşmek” konulmaktadır. Bu doğrultuda “yeni bir ülkede bir yerleşke, yeni bir yere yerleşen, ancak anayurtlarına tabi halde ya da onunla bağlantısını koruyarak bir topluluk oluşturan bir grup insan; yerleşimi ilk olarak gerçekleştirenlerin soyu ve ardılları tarafından bu şekilde oluşturulan topluluk anayurtla bağlantıyı koruduğu sürece bu yerleşime “colonia” ismi verilmektedir (Loomba, 2000: 18-19’dan akt. Tatar, 2011: 198). Bu açıdan bakıldığında, siber uzayda yer alan, büyüklüğü ve nüfuzu küresel boyutta olan siber platform şirketlerinin ekonomik, kültürel ve siyasi sömürüleri de siber sömürü kapsamında ele alınabilecektir. Teknolojik açıdan gelişmiş ülkelerin uçak vb. malları diğer ülkelere satmalarının yanında siber teknoloji ile kontrollerini halen elde bulundurmaları, Google (Lindh ve Nolin, 2016: 4), facebook vb. dünya devi internet sitelerinin dünyanın neresindeyse her ülkesinde büyük kullanım oranlarına sahip olup, o ülkedeki firmaların internet

üzerinden iş yapabilmeleri için gereken reklam giderlerinden büyük kar elde etmeleri, bankacılık, finans, yönetim ve güvenlik gibi alanlarda yazılım üreten firmaların bu yazılımları, ülkelere pazarlayarak o ülkelerdeki kişi ve kurumlardan çeşitli bilgiler sızdırması gibi durumlar da siber sömürü sayılabilecektir.

Siber sömürünün iş dünyasındaki varlığı ve etkileri de önemli bir konudur. Kötü amaçlı kişilerce şirketlerin tüketicilerine yönelik sömürüler siber uzay yoluyla gerçekleştirilebilmektedir. Şirketlerin isimlerini kullanarak benzer ya da sahte domain uzantılarıyla müşterilere atılan mailler, onların çeşitli bilgilerini gizlice alarak farklı amaçlar için kullanılmasını sağlayabilmektedir. Facebook, Google ve Twitter gibi platformların kişisel bilgilerin gizliliğini ihmal ederek kişilerin cinsiyet, yaş, ürün arama bilgileri, e-mail adresleri ve cep telefonu numaralarını şirketlere sattıkları iddiaları[11] geride bırakılan yakın dönemde sıkça gündeme gelmiştir.

Siber sömürü bireysel boyutun dışında ülkeler arası boyutta da kendini göstermektedir. Shakarian ve arkadaşları (2013: 114-150) ülkeler arasındaki siber sömürü hükümetler tarafından politik olarak destekleniyor olmasına inanmanın akıl dışı olmadığını vurgulamaktadırlar. Onlara göre hükümetler istihbarat politikalarının bir uzantısı olarak diğer devletlerden bilgi çalmakta ve bunları istihbarat koleksiyonu ya da entelektüel varlık olarak kullanarak çeşitli amaçlar için (silah teknolojileri bilgilerinin öğrenilmesi gibi) kullanmaktadırlar. Yazarlar kitaplarının 7.nci bölümünde Çin'i odak alarak ülkenin siber doktrinini, ülkedeki hackerların bakış açılarının evrimini, Birleşmiş Milletlere karşı yaptıkları bilgi çalma operasyonlarını ve bu operasyonların neredeyse tüm anatomilerini incelemişler ve bunları siber sömürü çerçevesinde ele almışlardır. Örneğin Çin'in Birleşmiş

---

[11] Söz konusu iddiaları içeren örnek haberler için bkz. http://www.hurriyet.com.tr/facebook-kisisel-bilgileri-satacak-10944027 , http://www.haberturk.com/ekonomi/teknoloji/haber/781735-facebook-mahreminizi-satiyor

Milletlere yaptığı siber sömürülerden en önemlisi “Titan Yağmuru” (Titan Rain) olarak isimlendirilen operasyondur (Shakarian, v.d., 2013: 124, 126). Bu operasyon ve sömürü 2003’ten 2005’e kadar sürmüş, operasyon kapsamında ABD’de bulunan Savunma Bilgi Sistemleri Kurumundan, Sandia Ulusal Laboratuvarlarından, Dünya Bankasından, Lockheed Martin havacılık şirketinden ve NASA’dan çeşitli bilgiler düzenli olarak ele geçirilmiştir. Bu sömürülerde temel saldırı mantığı olarak, içine sızdığı sistemdeki bilgileri onu kullanan kaynağa ileten “Trojan Atı” kullanılmıştır.

Siber saldırıların bir uzantısı, bir amacı ve aynı zamanda bir sonucu olarak gerçekleşen siber sömürüler, kapitalist sömürü düzenindeki kolonyal sisteme mantık olarak benzemekle birlikte yapısal niteliği ve sömürülecek kaynaklara erişim sürekliliği konusunda daha dinamik ve aynı zamanda kırılgan bir yapıya sahiptir. Zira ülkelerin saldırı ya da savunma için somut askeri kaynakları bulunmasa da, bilgisayarlar ve nitelikli hacker ya da coder insan kaynağına sahip olduklarında, gelecek saldırılara karşı savunma, sömürüyü durdurma ve hedeflere karşı saldırı imkanları olabilecektir. Diğer yandan siber sömürü amaçlı olarak hedef kaynakların Çin-ABD örneğinde olduğu üzere trojan vb. çeşitli siber silahlarla işgal edilmesi ve bir ülkenin diğer ülkenin çeşitli kurumlarına istihbarat toplamak amaçlı ajanlar yerleştirmesi aynı işleve sahiptir. Bu yönde bir yaklaşımda, siber sömürünün ülkeler arası boyuttaki önemi de net bir şekilde kavranabilecektir. Siber sömürü konusunda genel açıklamalarda bulunulan bu bölümün akabinde siber güvenlik bağlamında, risk, tehdit ve güvenlik açığı kavramları ele alınacaktır.

2.3.4. Risk, Tehdit ve Güvenlik Açığı

Gelişen bilgisayar ve iletişim teknolojileri, sistemleri ve dolayısıyla büyüyen siber uzay, bu uzaya bağlı şekilde işleyen, bireysel, özel ve kamusal sistemler siber güvenliğin önemi gün geçtikçe artırmaktadır. Siber sistemlerin güvenliğinin temel

unsuru ise siber saldırılara karşı dayanıklılığıdır. Söz konusu sistemler içerdikleri bileşenler, sistemin büyüklüğü, fonksiyonu, altyapısı, programlaması, kullanım koşulları gibi birçok öğeye bağlı olarak güvenlik riskleri içerebilmektedir. Riskler, negatif olasılıklara, negatif olasılıklar ise istenmeyen gerçeklere dönüşerek sistemlere ve sistemlere bağlı olarak işleyen diğer sistemlere zarar verebilmektedir.

Collier ve arkadaşları (2013) çalışmalarında, siber sitemlerin var olduğu alanları sıralayarak bu alanlar üzerindeki siber güvenlik risklerini irdelemişlerdir. Bunlardan ilki fiziksel alandır. Fiziksel alan, siber sistemin donanımsal parçalarını ifade etmektedir. Söz konusu risk donanımsal zincirdeki parçaların ya da bileşenlerin zarar görmesinden kaynaklanmaktadır. Doğal afetler sebebiyle internet bağlanılan altyapıların (fiber kablolar, santraller ya da serverlar) zarar görerek sisteme bağlantının olanaksız hale gelmesi buna örnek olarak gösterilebilecektir. Buradaki risk faktörü ise doğal afetler olacaktır. Diğer bir alan, bilgi alanıdır. Bilgi alanı; izleme, bilgi depolama ve görselleştirme bileşenlerine sahiptir. Bilgilerin yer aldığı kısımlar tehlikelere karsı değiştirilip ulaşım engellenmek koşuluyla riskler en aza indirilebilir. Bilişsel alan ise sistemin sahip olduğu bilgilerin işlendiği ve analiz edildiği alandır. Aynı zamanda alanda, sistemsel karar verme fonksiyonu da gerçekleşir. Bu alanda çıkacak ikilemlerde karar yine insan zekası ile alınacaktır. Son alan, sosyal alandır. Siber güvenlik ve risk konularında alınacak kararların sosyal yönü de vardır. Söz konusu kararlar etik gibi sosyal boyutlar düşünülerek verilmelidir. Örgütlerin siber tehditlere karşı nasıl daha iyi hazırlanacağı, gelişim trendleri ve izlenecek yollar gibi sosyo-politik konular da bu alan içine girmektedir.

Siber güvenlik riskleri hem özel şirketleri (Shackelford, 2012) hem kamu kurumlarını (Herbolzheimer, 2016: 13) hem de global olarak tüm dünyayı (DTCC, 2014) ilgilendiren risklerdir. Öğüt ve arkadaşları (2011) siber güvenliğin bilgi güvenli ile eş anlamlı kullanıldığını belirtirlerken, özel sektör firmalarını odak aldıkları çalışmalarında firmaların siber güvenlik risklerine paralel olarak riskler karşısında meydana gelecek olan kayıpların hesaplanamadığını

vurgulamaktadırlar. Bunun yanında güvenlik açıklarından doğan bilgi kayıplarını dahi tam olarak belirlemek mümkün değildir. Yazarlar, yapılan bir araştırmada (Ponemon, 2006'dan akt. Öğüt, v.d., 2011: 498) şirket veri tabanlarında yer alan 10.000 ve üzeri kayıt sızdırılmasının belirlenebilme oranı %68, 100 ve daha az kayıt sızdırılmasının belirlenebilme oranı ise %51 olarak belirlenmiştir. Bu anket sonuçları algılanan oranları belirtmektedir. Pfleeger ve Caputo (2012) ise siber güvenlikte ortaya çıkacak olan riskleri hafifletmek adına ortaya koydukları modellerinde, siber güvenlik ve davranış bilimlerini birlikte düşünmeyi ve güvenlik sistemlerinin bu yönde kurulmasını önermişlerdir. Teknolojinin insan faktörü olmadan bir anlam ifade etmeyeceği savunusuyla yola çıkan araştırmacılar, insanların güvenliğin artmasına karşı (örneğin, dönemsel zorunlu şifre değiştirme gibi) verdiği tepkiler ve tutumları ölçmüşlerdir. Çeşitli ölçümler ile birlikte insan faktörüne daha uygun ancak aynı zamanda daha az risk içeren siber güvenlik sistemlerinin nasıl tasarlanabileceğine yönelik düşünceler geliştirilmiştir. Söz konusu sistemler sadece bilgi sızdırılmasına karşı değil aynı zamanda süreç kontrollerine ve işleyişlerine karşı riskleri de içerebilecektir. Siber güvenlik, aynı zamanda bilgisayar ve iletişim teknolojilerine bağlı olarak işleyen sistemlerin güvenliğini de içermektedir (Baybutt, 2004: 285). Dolayısıyla siber tehditler bu sistemlerin işleyişine karşı da tehlike oluşturmaktadır.

Siber ortamdaki tehditler ise fiziki ve bilgisel olarak ayrılabilecektir (Ulsch, 2014: 32). Fiziki tehditler, kişi ya da kurumların siber güçlerine dayanarak hedefleri donanımsal yönleriyle tahribata uğratma ihtimalleri (sistemin çalışmaz hale getirilmesi, işleyişine müdahale vb.) üzerine inşa olmuş tehditleri içerirken, bilgisel tehditler ise siber sistemde barındırılan bilgilerin sistemden rıza dışı alınmasını nitelemektedir. Fiziksel tehditlere en önemli örnek olarak siber güvenlik alan yazınında çok önemli bir yere sahip olan bir örnek olarak Stuxnet gösterilebilecektir. Stuxnet, genel bir anlatımla, Siemens SCADA endüstri kontrol sistemlerini hedef almak üzere üretilmiş, ABD ve İsrail'in, İran'ın yaptığı nükleer

çalışmaları sekteye uğratmak üzere kullandıkları bir solucan/trojandır (Mueller ve Yadegari, 2012). Ancak bunlar sadece bir iddia olarak kalmış devletler tarafından kabul edilmemiştir. Bu solucan söz konusu endüstri kontrol sistemlerine fiziki yaptırımlarda bulunabilmektedir (Matrosov, v.d., 2010). Stuxnet konusu çalışmanın ilerleyen bölümlerinde detaylı olarak ayrıca ele alınacaktır.

Siber tehditlerin siber sistemlere karşı olan potansiyelleri, bu sistemlere gerçekleştirilen saldırıların miktar ve boyutları ile de doğru orantılı olarak düşünülebilecektir. IBM'in Küresel Operasyonlar Merkezi yaptığı araştırmada 140 ülkeyi ve bu ülkelerde yürütülen siber sistemlere bağlı süreçleri gözlemlemiş ve gözlem sonucunda 5 ila 10 milyar arası siber güvenlik tahribi olayının gerçekleştiğini belirlemiştir (Radcliff, 2010: 31'den akt. Andreasson, 2012: 29). Söz konusu saldırılar daha önceden de değinildiği gibi ülke içerisinden ya da dışarısından olabilmektedir. Ülke dışarısından olan ve hedef aldığı ülkenin ulusal güvenliğini tehdit eden siber dış mihraklar, siber güvenlik alan yazınının önemli bir bölümünü oluşturmaktadır. Clarke ve Robert (2010), bu bağlamda, ülkelerin siber tehditlere karşı dayanıklılıklarını belirtmek üzere siber güvenlik konusunda süper güç kabul edilen ülkelerin siber tehditlere karşı gücünü puanlamıştır. Puanlama yaparken ülkelerdeki siber saldırılar karşısında tepki unsurlarını (tüm ülke bağlantısını bir anda kesme, internet ağı yayılımı, ağ sağlayıcılarına göre siber bağımlılık, serverlar vb.) hesaba katmıştır. Söz konusu ülkelerin güçlerine yönelik algının içinde bulunulan dönemlerde de değişmediği söylenebilecektir (Breene, 2016). Bu doğrultuda Clarke ve Robert'ın yapmış olduğu puanlama aşağıdaki tabloda sunulmuştur:

Tablo 3: Ülkelerin Siber Güvenlik Güç Puanlamaları

	ABD	Rusya	Çin	İran	Kuzey Kore
Siber Saldırı	8	7	5	4	2
Siber Bağımlılık[12]	2	5	4	5	9
Siber Savunma	1	4	6	3	7
Toplam	**11**	**16**	**15**	**12**	**18**

Kaynak: Clarke ve Robert, 2010.

Tabloda görüldüğü üzere, Kuzey Kore siber güvenlik ve siber tehditlere karşı dayanıklılık açısından en güçlü ülkedir. Kuzey Kore'yi sırasıyla Rusya, Çin, İran ve ABD takip etmektedir. Clarke ve Robert (2010), ABD'nin düşük puanının ülkenin siber savunmadaki başarısızlığına bağlamakta ve diğer ülkelerle toplam puanlamalarda olan farkın kapanması için saldırıdan daha fazla şekilde savunma alanına yapılacak yatırımlarla gerçekleştirilmesi gerektiğini aksi takdirde ulusal güvenliğin sağlanmış olmayacağını belirtmektedir.

Siber güvenlik açıkları ise siber tehdit ve siber güvenlik riski konularıyla bağlantılı bir konudur. Siber güvenlikte güvenlik açıkları siber güvenlik ve siber güvenlik dışı unsurlardan kaynaklanabilecektir. Chang ve arkadaşlarına (1999: 252) göre siber güvenlik unsurları bilgisayar güvenliği, iletişim güvenliği, uygulama programları

[12] Burada yer alan "siber bağımlılık" kavramı ilk bakışta olumsuzluk belirten bir kavram olarak algılanabilecek olsa da, destek mekanizmaları, elektrik sistemleri, hat borularının da siber sisteme bağlı olma durumunu ve bunların tek bir merkezden kontrol altında tutulabilmesine yarayan bir sistemi belirtmektedir.

güvenliği, operatör program güvenliği, bilgi sınıflandırma güvenliği ve şifrelemeden meydana gelmektedir. Siber güvenlik ile ilgili olmayan, diğer adıyla fiziksel güvenlik olarak adlandırılan güvenlik unsurları ise operasyon güvenliği, güvenlik politikası ve farkındalık, denetim, kişisel güvenlik ve iş devamlılığı planıdır. İlk kategoride sayılan unsurlar doğrudan güvenlik açığı barındırabilecek unsurlar iken, ikinci kategoride yer alan fiziksel unsurlar dolaylı olarak barındırabileceklerdir. Örneğin operasyon güvenliğinde var olan ya da sonradan oluşabilecek bir güvenlik açığı, operasyon sırasında siber sisteme taşınabilir bellek, harici bellek vb. araçlarla solucan ya da casus yazılım sokulmasına imkân verebilecektir.

Siber güvenliğin bireysel ve kurumsal boyutu olduğu gibi siber güvenlik açıklarının da bireyleri ve kurumları ilgilendirdiği söylenebilecektir (Kritzinger ve Solms, 2010). Bireysel siber güvenlik açıkları, kişileri kullandıkları siber unsurlarda kendilerine bağlı olarak aldıkları güvenlik önlemlerinden (anti-virüs programı kullanma, şifrelerini diğer kişi ve firmalarla paylaşma, kişisel verileri sanal ortamlarda paylaşma, şifrelendirme) meydana gelebileceği gibi kullanmayı tercih ettikleri program ya da dosyaların güvenlik açıklarından da meydana gelebilecektir. Kurumsal siber güvenlik açıkları ise bireyselde olan etmenlere artı olarak kurumun içinde yer alan insan faktörüne bağlı bir şekilde, bireylerin bilinçsiz ya da kasti olarak ortaya çıkardıkları güvenlik açıklarına da maruz kalmaktadır. Söz konusu siber güvenlik açıkları sebebiyle ortaya çıkacak olan olumsuz sonuçlar kurumu, bünyesindeki bireyleri ve (kamu kurumu ise) devleti etkileyecektir.

Siber güvenlik konusuna daha çok ulusal bir perspektiften yaklaşan Cavelty (2014), siber güvenlik açıklarının gün geçtikçe daha azalmaktan çok daha da fazlalaştığını, kişisel ve ulusal siber güvenliğin de aynı oranda azaldığını savunmaktadır. Büyük ve uluslararası firmaların tüketici odaklı yaklaşımlarının yanında, devletlerin de geçmişten bu yana düstur edindikleri “kritik altyapıları koruma” politikaları, siber güvenliği askeri bir unsur olarak ele alama tutumu, dünya genelinde çoğunlukla uygulanan liberal politikaların da etkisiyle siber güvenlik önlemlerini zayıf

tutmaktadır. Burada siber güvenlik açısından yaşanan büyük bir ikilemin altı çizilmekte ve siber güvenlik açıklarının bu ikilemden dolayı giderek kontrolsüz bir şekilde büyüdüğü vurgulanmaktadır. Bu ikilemde, birey ve ulus güveliği çatışmaktadır. Devletler kritik altyapıların korunmasına ve siber güvenliğin artırılarak güvenlik açıklarının azaltılmasına yönelik olarak daha merkezi ve katı kurallar koymak üzere adımlar atacak iken, bireyler ise kendi özgürlüklerine yönelik olarak siber uzaydaki hareket alanlarını en serbest şekilde muhafaza etmek istemektedir. İkilem bu çatışmadan doğmaktadır. Bu ikilemde, uluslararası şirketler de liberal görüşün etkisinde, bireylerin tutumundan yana taraf almaktadır. Devletler açısından, siber uzayda bireylere ve firmalara (özellikle yazılım firmalarına) sunulan serbesti, aynı zamanda ulusal siber güvenlik açısından genişleyen güvenlik açıklarını da beraberinde getirmektedir. Bu ikileme çözüm geniş kapsamlı tanımları ve birbirine bağımlı değişkenleri içeren, bireysel ve ulusal güvenlik önceliklerini belirleyerek bir uzlaşma temelinde oluşturulacak olan siber güvenlik politikası olarak düşünülmektedir.

Çalışmanın bu başlığı altında siber güvenlik kavramı ile birlikte kullanılan ve onu tamamlayan diğer kavramlar ve konulara genel hatlarıyla yer verilmiştir. Çalışmanın bir sonraki başlığında ise aynı şekilde siber uzayı oluşturan, güvenlikleri siber güvenlik altında incelemeye tabi ve siber güvenlik risk ve tehditlerinin hedefi olan teknoloji ve sistemlerden bilgisayar teknolojileri, internet, iletişim teknolojileri, bilgi sistemleri, endüstriyel yönetim ve otomasyon sistemlerine yer verilecektir.

2.3.5. Kritik Altyapılar

Kritik altyapılar konusunda, Türkiye'de de siber güvenliğin ilgili alt sistemlerine yönelik strateji çalışmaları yapılmaktadır. Bununla ilgili olarak güncel bir belge olan, Kalkınma Bakanlığının 2015-2018 yılları arası için yayınlamış olduğu Bilgi Strateji

ve Eylem Planı'na değinmekte yarar vardır. Planda bilgi sistemleri ve iletişim sistemleri üzerine oluşturulan güvenlik stratejilerine rastlanmaktadır. Plana göre (BTSEP, 2015-2018: 70); Ulusal bilgi güvenliğini sağlamak üzere yasal, teknik ve idari altyapı oluşturulacak ve bu çerçevede, hem kamu hem de özel sektöre ait bilgi sistemleri ve kritik bilgi altyapılarına ilişkin denetim, standardizasyon ve koordinasyon yetki ve sorumlulukları kanunla düzenlenecek ve alanlara özgü kurumsal yapılar oluşturulacaktır. Kritik bilgi altyapılarının olası siber saldırılara karşı korunması için gerekli tüm önlemler alınacaktır. Bilgi güvenliği kültürünün kurumsal ve bireysel düzeyde oluşmasını sağlayacak bilinçlendirme çalışmaları yapılacaktır. Söz konusu çalışmalar, bilgi güvenliğine dair farkındalığı artırıcı nitelikte olacaktır. Ulusal bilgi güvenliğinin korunmasında uluslararası işbirliği güçlendirilecektir. Geçmiş dönemlerde karar alınan politikalarla tutarlı olarak, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı etkin şekilde uygulanacak ve bu plan teknolojik eğilimler ve ihtiyaçları doğrultusunda güncelleneceği belirtilmiştir.

Siber güvenliğin ilişkili olduğu altyapılar sadece bilgi altyapıları değildir. Bir ülkede kritik altyapı sayılabilecek her unsur siber güvenlik açıkları doğrultusunda birer hedef haline gelebilecektir. Bu anlamda hangi unsurların birer kritik altyapı sayılacağına değinmekte yarar vardır. AB Komisyonunun hazırlamış olduğu 2004 tarihli, 702 sayılı ve "Terörizmle Mücadele Kapsamında Kritik Altyapıların Korunması" başlıklı tebliğde Kritik altyapı; "…insanların hayati sosyal fonksiyonlarının, sağlıklarının, emniyetlerinin, güvenliklerinin, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve aksama veya yok edilmesi bu fonksiyonları sürdürmede yetersiz kalma sonucunda bir üye ülkede belirgin etki gösterecek varlık, sistem veya ilgili parçaları" şeklinde tanımlanmıştır. Bu bağlamda ülkeden ülkeye değişebilecek olsa da en genel hatlarıyla; bankacılık ve finans, enerji, gıda, iletişim, nükleer, su, turizm, ulaşım ve uzay sistemlerine yönelik altyapıları kritik altyapı sayılabilecektir.

Ülkeler, özellikle ulusal güvenliklerinin sağlanması ve kritik altyapıların korunması noktasında geleneksel güvenlik yöntemlerinin yanı sıra gelişen teknolojiler ve bu teknolojiler beraberinde dönüşen kritik altyapılarla birlikte siber güvenlik konusunda farkındalık kazanmaktadırlar. Zira siber güvenlik, kritik altyapılar olan bilgisayar sistemleri, bilgi sistemleri, iletişim, enerji, su, finans sistemleri gibi sistemlerin yanında önceki dönemlerde fiziki olan ancak içinde bulunulan dönemde büyük oranda (özellikle yönetim mekanizmaları) siberleşmiş enerji ve endüstriyel kontrol sistemlerinin güvenliğini de içeren bir alan haline gelmiştir. Bu bağlamda ülkeler, ulusal anlamda kritik altyapıları ve kamusal bilgi ve belgeleri, bireysel anlamda ise vatandaşların bilgi güvenliğini sağlamak üzere çeşitli siber güvenlik stratejileri oluşturmakta ve siber güvenlik politikaları uygulamaktadır.

Türkiye'de kritik altyapıların korunmasına yönelik algı oluşmuştur. Bu bağlamda ilgili kurumlar da çeşitli çalışmalar yapmaktadır. Buna bir örnek olarak Bilgi Teknolojileri ve İletişimi Kurumunun kritik altyapıların korunmasına ilişkin çalışması verilebilecektir (BTK, 2010). Siber ortamdaki tehditlerin en önemli hedefi haline gelmekte olan kritik altyapılar konusuna dikkat çekmek amacıyla hazırlanan çalışmada kritik altyapıların tanımına ve kapsamına ilişkin bilgiler verilmesinin ardından ABD, AB ve Japonya'nın kritik altyapılarına ilişkin hukuki düzenlemeler ele alınmıştır. Yapılan literatür taramasında Türkiye'de kritik altyapı konusunun akademik araştırmalarda da iyiden iyiye yer bulduğu gözlemlenmiştir.

Çalışmanın diğer bölümünde siber güvenlik, ulusal güvenlik politikaları çerçevesinde ele alınacaktır. Bölümün ilerleyen kısımlarında ise daha önce tablo 3'te yer verilmiş olan ülkelerin siber güvenlik politika ve stratejileri incelenecektir.

2.4. SİBER GÜVENLİK İLE BAĞINTILI TEKNOLOJİ VE ALT SİSTEMLER

Siber güvenlik, çalışmanın önceki kısımlarında da ele alındığı üzere, siber uzayda yer alan, etkileri hem siber uzayda hem de fiziksel ortamda gözlemlenebilen sonuçlar doğuracak siber risk ve tehditlere karşı oluşturulmuş olan bir güvenliği nitelemektedir. Siber uzay çeşitli siber alt sistemlerin içinde yer aldığı bir evrendir. Siber uzayı meydana getiren söz konusu alt sistemlerin başında bilgisayar teknolojileri ve sistemleri gelmektedir. Ancak bu sistemlere değinmeden önce, genel anlatımlarda sıkça rastlanan "bilişim" kavramını açıklamakta yarar vardır. Türkçeye resmi olarak 1981 yılında, Türk Dil Kurumunun yayınladığı "Bilişim Terimleri Sözlüğü"nde, Köksal (1981: 126) tarafından kazandırılmıştır. Kaynakta, bilişim şu şekilde tanılanmıştır (Köksal, 1981: 126'dan akt. Bensghir, 2002: 82); "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi birimi. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözetilerek inceleyen uygulamalı bilim dalı. Disiplinler arası özellik taşıyan bir öğretim ve hizmet kesimi olan bilgisayarda ve içerde olmak üzere bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar. Bundan başka her türlü endüstri üretiminin özdevimli olarak düzenlenmesine ilişkin teknikleri kapsayan özdevin alanına giren birçok konu da, geniş anlamda, bilişimin kapsamı içerisinde yer alır". Buradan hareketle bilişim kavramının bilgisayar teknolojileri, iletişim teknolojileri, endüstri yönetim sistemleri gibi siber güvenliğin alt sistemlerinde yer alan tüm sistemler için kullanılmasının sakıncasının olmadığı kanısına varılabilecektir.

Bilişim sistemlerinden olan bilgisayar teknolojileri ve sistemleri günlük hayatın önemli yer tutan araçlarından biri haline gelmiştir. Doğrudan bilgisayar kullanımı ile

internetten bilgiye erişim, profesyonel ya da günlük işlerin bilgisayarlar yolu ile gerçekleştirilmesi ve dahi devlet hizmetlerinden bilgisayar ile yararlanma gibi durumlar, alışılmış hale gelen kullanım örnekleridir. Bilgi ve iletişim teknolojilerinin kamu yönetimindeki yansıması "e-devlet" çalışmaları olarak görülebilir. Merkezi yönetimde ve yerel yönetimlerde, yasama, yürütme ve yargı organlarında hızlı bir şekilde bu teknolojilerden yararlanmaya yönelik olan projeler sürmektedir. Gelişmiş ülkeler, kamu kesimince sunulan neredeyse tüm bilgi ve hizmetleri aynı zamanda bu teknolojiler aracılığıyla sunmaya hazırlanmaktadırlar. Türkiye'de de bugün hali hazırda birçok e-devlet projesi yerel ve merkezi yönetim ölçeğinde devam etmektedir (Sadioğlu ve Yıldız, 2007: 348). Devlet hizmetlerinin siber sistemlerce verilmesi, devlet ve vatandaş bilgilerinin ve belgelerinin bu sistemler haznesinde saklanması ve işlenmesi, siber risk ve tehditleri beraberinde getirerek, söz konusu bilgi ve belgelerin güvenliğinin sağlanabilmesi sorunsalını doğurmaktadır. Devlet ve vatandaş bilgi ve belgelerinin sistematik olarak saklanıp kullanıldığı bu sanal arşivler de belki bir "kritik altyapı" sayılabilecektir. Bu yönüyle söz konusu sistemler siber güvenlik dâhilinde düşünülerek korunmalıdır.

İnsanlar doğrudan olduğu gibi dolaylı olarak da bilgisayar sistem ve teknolojilerinden yararlanmaktadır. Yapılarında dolaylı olarak bilgisayar sistemlerini barındıran teknolojilere "bilgisayar destekli teknolojiler" ismi verilmektedir. 8-12 Eylül 1985 yılında Montreal Kanada'da, 600 delegenin bir araya geldiği I. Uluslararası Bilgisayar Destekli Teknolojiler Konferansı'nda, bilgisayar destekli sistemlerin kullanım alanlarına yönelik kategoriler ayrılmıştır Söz konusu kategoriler; Robotik ve Bilgisayar Destekli Üretim, Bilgisayar Destekli Endüstriyel Operasyonlar, Bilgisayar Destekli Tasarım, Bilgisayar Destekli Karar Verme, Gelişmiş Yazılımlar, İnsan-Makine Ara Yüzleri, Bilgisayar Destekli Eğitim, Bilgisayar İletişimi, Bilgisayar Grafikleri, Yapay Zeka, Bilgisayar Destekli Ulaşım olarak belirlenmiştir (CII, 1986: 461). Konferansta kategorilere ayrılan konular içinde bulunulan dönemde de bu teknolojilerin en yoğun olarak kullanıldığı ve insan

hayatında yer aldığı alanları oluşturmaktadır. Fabrikalardaki üretimde ve otomasyon sistemlerinde, önceden değinildiği üzere nükleer çalışmalarda, tekstilden otomotive kadar endüstriyel ürünlerin tasarımında, yönetim organlarında bilgi temelli karar vermede, görsellerin oluşturulmasında ve son yıllardaki en popüler haliyle kendi kendine karar verebilen ve aldığı karar doğrultusunda iş yapan yapay zekâlar (Jones, 1991), hem bilgisayar teknoloji ve sistemlerini oluşturmakta hem de siber güvenliğin sınırları içinde yer almaktadır.

Siber güvenliğin sınırları içerisinde yer alan bilgi ve iletişim teknolojilerine yönelik olabilecek risklerin kontrol edilmesi ve bu altyapıların siber saldırılara karşı dirençlerinin geliştirilmesi, ülkelerin siber güvenlik stratejilerinin ana hedefleri arasında yer almaktadır (Klimburg, 2012: 56). İçinde bulunulan dönemde olduğu üzere, gelecekte de artan bir biçimde toplum, ağırlıklı olarak bilgisayar ve ağlara bağlı sistemlere bağımlı olan kritik altyapılarla iş gören endüstriyel kontrol sistemlerine sahip olacaktır. Söz konusu endüstriyel kontrol sistemleri kimya endüstrisi, akıllı sistemler, enerji ağları, şehirler, ev sistemleri, tarım, tıp, otomotiv vb. alanlarda yaygın olarak kullanılmaktadır (Kobara, 2016: 787). Diğer yandan elektrik santralleri, bitki sulama sistemleri, akıllı şebekeler de bilgi ve iletişim sistemlerini taban alan diğer kritik altyapılar arasındadır (Genge v.d., 2012: 1146). Bu kritik altyapılar geleneksel harp yöntemlerinde, ülkeleri zayıf kılmak için ilk hedef alınan ilk bölgeler içinde yer almaktadır. Siber saldırılar ve siber tehditler de söz konusu kritik altyapıları hedef almaktadır. Bunun ötesinde siber saldırılar, hedef aldıkları bu kritik altyapılara verdikleri zararlar dolayısıyla önceki dönemlerde olduğu gibi sadece siber sorunlara (programların çökmesi, bilgisayarların kapanması vb.) değil aynı zamanda fiziksel sorunlara da yol açabilmektedir. Ulaşımın kilitlenmesi, gaz ve su şebekesinin durması ve bunun akabinde insanların bunlardan mahrum kalarak hastalık ya da ölümlere kadar varan sonuçlar doğabilmektedir (Genge v.d., 2015: 1). Bunlardan daha ciddi ve kritik olarak da nükleer program altyapıları da endüstriyel kontrol sistemleri ile işleyen altyapılar

olarak siber saldırıların hedefi olabilmektedir. İlgili alan yazınında da bunun en somut örneği olarak sıklıkla Stuxnet solucanı gösterilmektedir.

Çalışmanın önceki bölümlerinde görüldüğü üzere tüm alt sistemleri ile birlikte siber sistemlerin güvenliği için pek çok akademik çalışma yapılmıştır. Diğer yandan şaşırtıcı olabilecek bir durum olarak, endüstriyel kontrol sistemlerinin güvenliğinin yanında bu sistemlere yapılacak saldırılara karşı üretilmiş akademik makaleler de alan yazınında yer almaktadır. Söz konusu sistemler de gelişerek farklı şekiller almıştır. Örneğin, Zhang ve arkadaşları (2016: 99) kablosuz internet tabanlı endüstriyel kontrol sistemleri için daha iyi bir savunma mekanizmasının kurulabilmesine olanak sağlamak için, saldırganın gözünden “en iyi saldırma takvimi” çalışması yapmışlar ve bu sistemlere yapılacak saldırıların etkilerini optimal seviyeye getirmek için hangi aralıklarda ve ne şekilde saldırı yapılması gerektiğini araştırmışlardır. Buradan yola çıkacak olan yetkililer, en iyi saldırı tekniklerini öğrenerek bu saldırılara yönelik daha kapsamlı önlemler alabileceklerdir. Alınacak önlemler sadece mikro ölçekte enstitü ya da özel firmaların endüstriyel kontrol sistemleri için değil, aynı zamanda ulusal kritik altyapıların güvenliğini sağlamak ve korumak için de önem arz etmektedir. Bu bağlamda ABD’de Standartlar ve Teknolojiler Ulusal Enstitüsü (National Institute of Standards and Technology) güvenlik standartlarını sağlamak, artırmak ve söz konusu sistemleri kullanan kullanıcılara rehber niteliğinde olabilecek yayınlar yapan kurumlar arasından örnek gösterilebilecektir.

2.5. ÜLKELERİN ULUSAL GÜVENLİK POLİTİKALARI TEMELİNDE SİBER GÜVENLİK: STUXNET ÖRNEĞİ

Önceki başlıklarda ulusal güvenliğin içinde bulunulan dönemde sadece fiziki-askeri saldırı ve tehditlere karşı oluşturulan bir güvenlik çeşidi ve uygulanan bir güvenlik politikası olmadığı vurgusu yapılmış ve ortaya çıkan yeni ulusal güvenlik tehditleri sıralanmıştır. Siber güvenlik de son dönemlerde ulusal güvenliği yakından ilgilendiren ve ulusal güvenlik politikaları oluşturulurken hesaba katılması gereken konuların başında gelmektedir. Siber güvenliğin önemine ilişkin olarak PEW Araştırma Merkezi'nin (PEW Research Center) raporuna (2014) göre, araştırmaya katılan 1600 teknoloji uzmanının 3'te 2'sine göre 2025 yılında büyük maddi kayıp ile can kaybının olacağı bir siber savaş beklenmektedir (Rainie, v.d., 2014'ten akt. Kshetri, 2016: 54). Siber güvenliğin ulusal güvenlik bağlamında böylesi bir risk potansiyeli, ona yönelik politikalar almayı da gerekli kılmaktadır.

Siber güvenlik farklı boyutlarda ele alınması gereken bir konudur. Siber güvenlik, bireysel, bölgesel, ulusal ve uluslararası boyutta bir kapsama sahiptir. Bireyler, siber ortamdaki kişisel bilgilerini güveli tutmak için anti virüs programları ve şifreleme sistemleriyle çeşitli önemler alırken, bölgesel yönetimler siber güvenlikleri adına farklı politikalar, daha büyük bir boyut olan ulusal boyutta devletler ulusal politikalar ve en geniş anlamıyla uluslararası boyutta çeşitli kuruluşlar da topluluk politikaları üretmektedir. Siber güvenliği ulusal boyutta ele alan bu çalışmanın ilerleyen kısımlarında belirlenmiş bazı devletlerin ulusal ve varsa bölgesel siber güvenlik politikaları daha detaylı ele alınacaktır. Uluslararası boyutta yürütülen siber güvenlik politikalarına kısa örneklerle değinilecek olursa, iki örnek olarak AB Komisyonu ve North Atlantic Treaty Organization (NATO) ele alınabilecektir. AB Komisyonu tarafından sunulan strateji belgesinde (European Comission, 2013'den akt. Stitilis, v.d., 2016; Pernik, 2014), AB'nin siber güvenlik politikası şu şekilde belirtilmektedir:

-Siber manevra esnekliğini sağlamak,

-siber suçları olabildiğince geniş ölçüde önlemek,

-genel güvenlik ve savunma politikasına uygun olarak siber savunma politikalarını geliştirmek,

-siber güvenlik için endüstriyel ve teknolojik altyapılar geliştirmek,

-AB'yi ve AB değerlerini desteklemek üzere tutarlı uluslararası siber uzay politikası üretmek.

Aynı kaynaklarda belirtildiği üzere ve NATO'nun siber savunma politikasına göre ise kuruluşun siber güvenlik politikasındaki öncelikler; koordinasyon temelli bir yaklaşımla siber saldırılara karşılık verecek mekanizmalar geliştirmek için plan ve kapasite gelişimi sağlamak, tüm üye devletler bazında bir politika oluşturmak adına devletlerin siber savunma politikalarını uyumlu hale getirmektir. Bu bağlamda NATO, kendince merkezileştirilmiş ancak üye devletlerinin her birinin asgari siber savunma gerekliliklerinin karşılandığı bir politika ortaya koymaktadır.

Ülkelerin tasarladıkları siber güvenlik politikalarında, kamu-özel işbirliklerinin rolü de göz ardı edilmemesi gereken bir konudur. Hare (2009), ABD üzerine odaklandığı çalışmasında, kamu kurumlarının özel sektöre, kendi değimiyle siber fırtına(siber dünya) içerisinde rol biçerek onlara ulusal siber güvenlik politikalarının oluşturulmasında katılım şansı verilmesi gerektiğini vurgulamaktadır. Bunun için Savunma Bakanlığının özel sektöre bilgi aktarma ve işbirliği kurma kapasitesinin geliştirilmesi gerektiğinin altını çizmektedir. Diğer yandan, devlet kurumları olmayan özel şirket ya da STK gibi kurumlara yapılacak olan siber saldırılarda da yine devletin sağlayacağı bir güvenlik beklentisi söz konusudur (Lin, 2012: 41). Diğer yandan devlet sadece özel sektörü koruyucu bir rolde değil aynı zamanda siber savaşlarda iş birliği ve ortağı olarak özel sektörden yardım da alabilecektir.

Borah (2015: 458), devletin sahip olduğu siber uzay ile özel sektörün sahip olduğu siber uzayı birbirinden ayırarak, bir devletin başka bir devletin siber sistemine girmek üzere özel sektörün siber uzayını ve kodlama sistematiğini kullanabileceğini belirtmektedir. Örneğin, aralarında iş birliği olup olmaması bir kenara bırakıldığında Çin, ABD'ye saldırmak için Microsoft ve CISCO'nun kodlamalarını kullanmıştır. Söz konusu saldırılar, ülkelere sadece siber sistemler üzerinden zarar vermenin yanında, fiziki kritik altyapıları izleyen ya da kontrol eden siber sistemlere zarar vererek dolaylı olarak fiziki zararlar da meydana getirebilmektedir (Karabacak, v.d., 2016: 1). Söz konusu risklere karşı alınacak önlemlerde; devlet kurumları, özel sektör, endüstri, uluslararası partnerler ve kamuoyuyla bilgi aktarımı ve koordinasyon en optimal seviyeye çıkarılmalı bu koordinasyonlu iletişim sayesinde oluşan risklere ve saldırılara karşı olabilecek en çabuk zamanda pozisyon alacak ve cevap verebilecek yapılar oluşturulmalıdır (Stoddart, 2016: 1087).

Stuxnet, siber dünyanın savaşçı yönünü ve bu savaşın ortaya çıkaracağı tahribatın aynı zamanda fiziki bir tahribat olabileceğini açık bir şekilde gözler önüne sermiş örnek bir olaydır. Stuxnet, genel bir anlatımla, Siemens SCADA endüstri kontrol sistemlerini hedef almak üzere üretilmiş, devletler tarafından resmi olarak kabul edilmemekle birlikte ABD ve İsrail'in, İran'ın yaptığı nükleer çalışmaları sekteye uğratmak üzere kullandıkları bir solucan/trojan olarak alan yazınında yer almaktadır (Mueller ve Yadegari, 2012). Başlığın bu kısmından itibaren, devletler tarafından resmi olarak kabul edilmese de Stuxnet, alan yazınında genel kabul gördüğü düşünüldüğü şekliyle, İran Nükleer Programını sekteye uğratmak üzere geliştirilmiş bir solucan olarak ele alınacaktır.

Stuxnet, son derece usta bir kodlama tekniğiyle hazırlanmıştır ve hedef aldığı sistemlere saldırıyı üç aşamada gerçekleştirmektedir. Solucan öncelikle Microsoft Windows sistem ve makinaları hedef almaktadır ve kendini bu ortamlarda tekrarlı bir şekilde kopyalamaktadır. Daha sonraki aşamada söz konusu ortamlar üzerinden onlara bağlı bulunan ve yine Windows tabanlı çalışan Siemens Step7

yazılımlarına bulaşmaktadır. Üçüncü aşama olan son aşamada ise bu yazılımlarla kontrol edilen endüstriyel sistemlere etki etmektedir (Kushner, 2013: 50). Sutxnet'in diğer bilgisayar solucan ya da virüslerinden ayrılan en büyük özelliği, ortaya çıkardı zararların sadece sanal ortamda değil gerçek dünyada da meydana gelmesidir (Collins ve McCombie, 2012: 80). Önceki dönemlerde bazı virüsler bilgisayarların, hard disk, güç kaynakları ya da ekran kartları gibi donanımlarına zarar verebilseler de bunlar bilgisayarların içleriyle sınırlı kalmaktaydı. Ancak bu durum Stuxnet'de daha önce hiç görülmemiş bir şekilde değişmiştir.

Biraz daha teknik bir anlatımla Stuxnet, İran nükleer programında, "supervisory control and data acquisition (SCADA)" olarak isimlendirilen ve Türkçeye "merkezi denetim ve veri toplama" sistemi olarak çevrilebilecek sistemlerce kullanılan santrifüjlere zarar vermek, patlatmalarına yol açmak üzere bir silah olarak kullanılmıştır. Merkezi denetim ve veri toplama sistemleri birçok fiziki sistemin operasyon işlevini yürütmektedir. Elektrik şebekeleri, su dağıtım ve toplama sistemleri, iletişim sistemleri, akaryakıt boruları ve demir yolları bu sistemlere örnektir. Stuxnet'in spesifik saldırı noktası ise merkezi denetim ve veri toplama sistemi içerisinden programlanabilir mantık denetleyicileri, İngilizce programmable logic controllers (PLC)'dir. PLC'ler, anahtarlar, röleler ve zamanlayıcı/sayıcılar gibi elektrik donanımlarının fonksiyonlarını kontrol eden küçük bilgisayarlardır (Tsang, 2010'dan akt. Collins ve McCombie, 2012: 84). Böylesine ince detaylarda yazılmış bir solucan, akla hedef alınacak olan donanılar hakkında önemli ölçüde bilgi sahibi olunması gerekliliğini akla getirmektedir. Bu yönde bir yaklaşım, solucanı yazan ve geliştirenlerin arkasında bir devlet gücünün (donanımları geliştiren devletler) ve politik bir motivasyonun olduğu düşüncesini (Chen ve Abu-Nimeh, 2011: 91) desteklemektedir.

Stuxnet, taşınabilir flash disk ile sisteme bulaşan bir solucandır. Bulaştığı endüstriyel kontrol sistemlerin veri ve sinyallerini değiştirdiği halde, bunu izleyen kontrol mekanizmalarına sahte sinyaller göndererek her şeyin yolunda gittiği

izlenimini uyandırmaktadır (Karnouskos, 2011). Solucanın flash bellek ile bulaştırılması önemli ölçüde, hedef alınan sistemlere odaklanılması ve solucanın yayılımının kontrol altında tutulmasına yöneliktir. Gibney ve Shmuger'in (2016) Stuxnet'i konu aldığı filmlerinde işlendiği kadarıyla, solucan öncelikli olarak İran nükleer programının ilişkide olduğu ve tesisin içerisine bir şekilde girerek oradaki bilgisayarlara çeşitli nedenlerle flash bellek takabilecek firmalara bulaştırılmıştır. Zira bu firmalar ulaşılması daha kolay ve sayıca daha fazla olan, birer aracı hedef niteliğinde görülmüştür. Asıl hedef olan nükleer tesise ulaşmak üzere bu hedefler birer basamak olarak kullanılmıştır.

Stuxnet, girdiği endüstriyel kontrol sistemlerine birçok fiziki etkiyi onları gözlemleyen sistemlerin haberi olmadan yaptırabilecek bir güçteydi. Bu solucan, bir şehrin tüm elektriğini kesebilir, doğalgaz akışını durdurabilir, ulaşım sistemini kilitleyebilir, nükleer santrallerini patlatabilirdi. Stuxnet, antivirüs taramalarına yakalanmamak adına çalıntı dijital sertifikalar kullanmış ve sonucunda hedefe ulaşmıştır. Yine de Stuxnet, İran nükleer programını yıkım noktasında bir tahribata uğratmamıştır. Tesisteki yaklaşık 1000 adet (Fidler, 2011: 56) hızını bozarak fiziksel tahribata uğratmak suretiyle patlatarak asıl işlevi uranyum zenginleştirmek olan (Baylon, 2017: 215) programın gelişimini yavaşlatmıştır. İsrailliler, ABD'den Stuxnetin daha saldırgan ve agresif bir yapıya kavuşması için baskıda bulunmuş, ancak özellikle ABD tarafının böyle bir değişiklikte solucanın yayılımının da kontrolden çıkacağını düşünerek tereddütlü davranmıştır. Belgesel filme göre (Gibney ve Shmuger, 2016) Stuxnet'in açığa çıkması da İsraillilerin onun kodlarıyla oynaması ve kontrolsüz kullanması dolayısıyla olmuştur. Solucan, ilk olarak Belarus'ta bir yazılımcının bilgisayarında kendisi tarafından bulunmuş, internetteki bir virüs ifşa platformunda diğer yazılımcılarla tartışıldıktan sonra Symantec ve Kaspersky şirketlerindeki ilgililer tarafından araştırma altına alınmıştır. Filmde de tartışmalar, varsayımlar ve mülakatlar bu firmaların ilgilileri ile ABD, İsrail ve İran devletleri tarafından ilgilileri arasında geçmektedir.

Stuxnet, siber yazılımların sadece siber dünyada internet siteleri ve bilgisayarlarda (Kenney, 2015: 115) karmaşa ve bozukluklara yol açan yazılımlar olmanın ötesine geçerek, fiziksel tahribata yol açan birer silah olarak kullanılabileceğini dünyaya göstermiş bir örnektir. Bu örnekle birlikte önceden sadece siber olarak ele alınan ve savaş hukukunda fiziki tahribata yol açan silahlara göre daha masum görülen siber saldırı araçlarının bu yönleriyle fiziki tahribata yol açan silahlarla bir tutulması gerektiği tartışmaları doğmuştur (Jenkins, 2013). Üstelik bu silah geleneksel savaş taktiklerinden ziyade, mühimmat, kaynak ve politik güç dengelerini altüst edebilecek ve yeni, asimetrik savaş-güç dengeleri kurabilecek bir silahtır (Lindsay, 2013: 370). Böyle bir silahın yayılımı, geliştirilmesi ile birlikte kontrol edilemeyecek kötü amaçlı kişi ya da örgütlerin eline geçmesi ile birlikte, tüm ülkeler ve dahi ABD, risk altında olacaktır (Farwell ve Rohozinski, 2011: 35-36). Buna benzer bir iddia da belgesel filmde (Gibney ve Shmuger, 2016) geçmektedir. İddiaya göre Stuxnet İsrailliler tarafından kodları değiştirilerek daha agresif ve saldırgan bir hale getirilmiş, kontrolsüz bir şekilde kullanılarak yayılması önlenemez bir hale gelmiştir Bu yönüyle tüm devletler ve hatta ABD de risk altındadır.

Stuxnet'in ortaya çıkması ve gündeme bomba gibi düşmesiyle birlikte endüstriyel kontrol sistemlerinin ve kritik altyapıların güvenliklerine karşı bakış açısı değişmiş ve yeni tedbirler alınmaya başlamıştır. Solucanın saldırı esnasında, sistemlerin kontrol merkezlerine her şey yolundaymış gibi bir izlenim vermesi göz önüne alınarak, işleyen mekanizmalara ait parametrelerin farklı açılardan farklı şekillerde birden fazla boyutta kontrol edilmesi ve kontrol altında tutulması gibi önlemler bunlardan bazılarıdır. Bir habere göre (NS, 2011: 6) endüstriyel sistemlerin güvenliklerinden sorumlu olan mühendis ya da ilgililer, Stuxnet'in ortaya çıkması ve buna benzer başka saldırılara karşı kendilerine tedbir alma şansı doğmasından dolayı çok şanslılardı.

Devletler Stuxnet olayında sessiz kalmayı tercih etmişlerdir. İran tarafı bu saldırıyı detaylı bir şekilde açıklamazken, ABD ya da İsrail de saldırıyı resmi olarak kabul

etmemiş ve sessiz kalmıştır. Böyle bir olayın kabul edilerek tarafların belirlenmesi, dünya açısından hem diğer gelişmiş ülkeler hem de bu teknolojilere karşı eğilim gösterebilecek gelişmekte olan ülkeler açısından da bir kamuoyu baskısı doğurabilecektir. Bunun yanında olayın mahiyetinin aynı zamanda fiziki bir nitelik taşıması, uluslararası savaş hukuku içerisinde ele alınarak taraflar için farklı yaptırımlar doğurabilecektir (Fidler, 2011: 56-57). Tüm bu konular ve detaylarla birlikte Stuxnet, siber güvenlik ve siber savaş alanına yeni bir boyut kazandırmış, siber güvenlik ile ulusal güvenliğin, siber savaş ile fiziki savaşın arasındaki siber olguların daha tehlikesiz ve önemsiz olarak algılanmasına neden olan sınırları kaldırmış, siber güvenliğin önemini özellikle devletler açısından kalıcı bir şekilde gün yüzüne çıkarmıştır.

3. BÖLÜM: ULUSAL GÜVENLİK POLİTİKALARI ÇERÇEVESİNDE SİBER GÜVENLİK: BAZI ÜLKE İNCELEMELERİ

Çalışmanın bu bölümünde, daha önce de siber güç bağlamında ele alınan ABD, Rusya, Çin, İran ve Kuzey Kore; bunlara ek olarak da Almanya ve İsrail ülkelerinin siber güvenlik politikaları ülkelerin siber güvenlik anlamında yaptığı hukuki düzenlemeler, strateji belgeleri, raporlar vb. ulaşılabilir dokümanlar temelinde ele alınarak incelenmiştir.

3.1. ABD'NİN SİBER GÜVENLİK POLİTİKASI

ABD'nin siber güvenlik politikasını anlamak için öncelikle bu politikanın hangi bileşenlerden ve aktörlerden ileri gelerek oluşturulduğunu ve bu politikayı bütüncül şekilde anlamak için nasıl bir yol izlenebileceğini belirlemekte yarar vardır. Bu bağlamda ABD'nin siber güvenlik politikası üzerine yönelimlerinin Ulusal Güvenlik Politikası ve Stratejisi, diğer stratejik belgeler, kanunlar, direktifler ve önerilen düzenlemeler, siber güvenlik ile ilgili kurumlar (9/11 komisyonu da dâhil olmak üzere) ve son olarak üçüncü parti kuruluşlar; yani think-tankler (düşünce üretim kuruluşları) etkileriyle (Tirrell, 2012: 7) gerçekleştiği söylenebilecektir. Çizilen bu çerçeve, ele alınacak olan diğer ülkeler içinde eksiği ya da fazlası olabilmesi ihtimali saklı tutularak, ana çerçeve olarak kullanılabilecektir.

ABD'de, Başkanlığa ait Ulusal Güvenlik Stratejisi'nde ve Güvenlik Ofisinin (Department of Defense; kısaca DOD) ulusal güvenliğe ilişkin politikalarının belirtildiği belgelerde "siber" terimi ve ofisin çıkardığı "Askerî Terimler Sözlüğü"nde, bu terimle türetilmiş birçok siber disiplin yer almasına karşın, belgelerde siber güvenliğin açık bir vurgusu son dönemlere kadar yapılmamıştır (Tirrell, 2012: 9).

Son dönemde ise siber güvenliğin önemi kabul edilmiş görünmektedir. Bu minvalde, ABD'de siber güvenlik ile ilgili konular içeren belgeler kronolojik bir şekilde eskiden yenide doğru incelenecek ve bu belgeler üzerinden ABD siber güvenlik politikasının temel sınırları çizilmeye çalışılacaktır.

ABD'de siber güvenlik ile ilgili olarak yayınladığı ilk kapsamlı belge Beyaz Saray tarafından yayınlanan 2003 yılında "Secure Cyberspace" (Güvenli Siber Uzay) belgesidir (WH, 2003). Bu belge incelendiğinde, belgede "siber güvenlik" terimin yalnızca üç kez geçtiği görülmekte ve bunun yerine genel olarak güvenli siber alan/uzay teriminin kullanıldığı görülmektedir. Belgede siber alan, "kritik altyapıların işleyişini sağlayan ve birbirine bağlı yüzbinlerce bilgisayarın, serverların, modemlerin, anahtarların, fiber optik kabloların oluşturduğu alan" olarak nitelendirilmiştir (WH, 2003: vii). Siber alanın korunması, ulusal güvenliğin sağlanmasında önemli bir bileşen olarak görülmüş ve belge, Ulusal Güvenliğin Sağlanmasına Yönelik Ulusal Strateji (National Strategy for Homeland Security) ile Kritik Altyapıların ve Değerli Varlıkların Fiziki Korunmasına Yönelik Ulusal Strateji (National Strategy for the Physical Protection of Critical Infrastructures and Key Assets) belgesinin bir uygulama bölümü olarak hazırlanmıştır. Belge, siber güvenlik konusuyla ilgili olan ulusal ve federal kurumların direktiflerini içermekte ve devlet ile yerel yönetim kurumlarının, özel sektör firmalarının, sivil toplum kuruluşlarının ve vatandaşların kolektif siber güvenliği geliştirmek üzere atacağı adımları belirlemektedir .

Secure Cyberspace belgesine göre, ulusal güvenliğin sağlanmasında beş adet ulusal öncelik bulunmaktadır. Bu öncelikler:

-Ulusal bir siber uzay güvenliği karşılık sistemi,

-ulusal bir siber uzay güvenliği tehdit ve güvenlik açığı savunma programı,

-ulusal bir siber uzay güvenliği farkındalık ve geliştirme programı,

-hükümetin siber uzayını güvenlik altında tutma,

-ulusal güvenlik ve uluslararası siber uzay güvenliği işbirliğidir.

Yukarıda adı geçen Secure Cyberspace belgesini, uygulama alanı olarak alt kategorisinde şekillendiren Siber Uzay Güvenliği Ulusal Stratejisi belgesi ise, ulusal siber güvenliğin sağlanması ardından karşı cevap verilmesine yönelik sekiz önemli eylem ve gelebilecek olan siber tehditlere karşı önlem niteliğinde sekiz önemli öncelik tanımlamaktadır (WH, 2003: x). Bunlar aşağıdaki tabloda gösterilmiştir:

Tablo 4: Siber Güvenlikte Sekiz Önemli Öncelik

Tehditlere Karşı Eylem	**Tehditlere Karşı Önlem**
Ulusal boyuttaki siber güvenlik tehditlerine karşılık vermek üzere bir kamu-özel işbirliği yapısı kurmak.	Siber ataklarda önleyiciliği ve caydırıcılığı sağlamak üzere hukuki düzenlemeler yapmak.
Siber saldırı ve güvenlik açıklarının değerlendirilmesi için taktiksel ve stratejik analizler geliştirmek.	Ulusal siber tehdit ve güvenlik açıklarının potansiyel sonuçlarını değerlendirmek üzere bir süreç oluşturmak.
Siber uzayın sağlığına yönelik sinoptik bir bakış açısı geliştirmek üzere özel sektörün kapasitesinin geliştirilmesi üzerine teşvikte bulunmak.	Protokol ve bağlantılar geliştirerek internet mekanizmalarının güvenliğini sağlamak.
Siber uzayın güvenliğini sağlamak ve Siber Güvenlik Departmanının siber güvenlik ile ilgili kriz yönetimindeki rolünü desteklemek üzere siber uyarı ve bilgilendirme ağını genişletmek.	Güvenilir dijital kontrol ve veri güvenliği sistemlerinin kullanımını yaygınlaştırmak.
Ulusal olaylar yönetimini geliştirmek.	Yazılım açıklarını önlemek.
Ulusal boyuttaki kamu-özel işbirliğinin devamlılığını sağlamak üzere gönüllü katılımını koordine etmek.	Altyapı bağımlılıklarını kavrayarak siber ağlar ve iletişim sistemlerinin fiziksel güvenliklerini sağlamak.
Siber güvenliğin devamlılığına yönelik federal planları yürütmek.	Federal siber güvenlik araştırma ve geliştirme kurumlarını önceliklendirmek.
Siber saldırı, tehdit ve güvenlik açıklarına yönelik kamu-özel sektör arasındaki bilgi akışı ve paylaşımını geliştirmek ve zenginleştirmek.	Aciliyet sistemlerini değerlendirmek ve güvenliklerini sağlamak.

Kaynak: WH, 2003: x.

Belge, siber uzayın güvenliğine ilişkin algıyı geliştirerek uluslararası işbirliğinin sağlanması ve güçlendirilmesi için çeşitli eylem ve öncelikleri de sıralamıştır. Algıyı güçlendirmek adına çeşitli programlar önerirken, uluslararası işbirliğinin güçlendirilmesi adına da, küresel siber güvenlik kültürünün oluşmasına yönelik çalışmaların hem özel hem de kamusal firmalarla birlikte geliştirilmesine yönelik vurgular içermektedir (WH, 2003: xii-xiii). Diğer bir önemli nokta ise belgede kamusal siber uzayın korunmasına yönelik maddelerin sıralanmasıdır. Belgeye göre devletin siber uzayının korunmasına yönelik beş önemli eylem ve öncelik bulunmaktadır. Bunlar şu şekilde sıralanmıştır (WH, 2003: xii):

1. Federal siber alanların risk ve güvenlik açıklarının sürekli bir şekilde değerlendirilmesi.

2. Federal siber sistem onaylı kullanıcılarını yetkilendirmek.

3. Federal yerel kablosuz ağların güvenliğinin sağlanması.

4. Devletin dış kaynak ve ihale yoluyla girdi sağladığı sistemlerin güvenliğinin sağlanması.

5. Merkezi ve yerel yönetim kuruluşlarını, diğer benzer ülkelerdeki kurumlarla geliştirebilecekleri bilgi teknolojileri güvenliği programlarını müzakere etmek üzere teşvik etmek.

Belge genel olarak yukarıda ele alınan öncelik ve eylem maddelerinin açılımları ve detayları üzerinden şekillenmektedir. Genel olarak ulusal boyutta öne çıkan vurgu, kamu-özel sektör ve vatandaşların bireysel siber alanlarına yönelik koordineli güvenliğin sağlanması, işbirliği ve katılım, kritik altyapıların korunması, ortak işbirliği ve farkındalık programlarının geliştirilmesidir. Uluslararası boyutta ise Kuzey Amerika Güvenli Siber Uzayını oluşturmak üzere Kanada ve Meksika ile yapılacak olan, siber tehdit ve risklere karşı ulaşım, enerji dağıtımı, iletişim,

bankacılık gibi ortak kritik altyapıların korunmasına yönelik işbirliği örneği göze çarpmaktadır.

2003 yılında yayınlanan Secure Cyberspace belgesinin dışında ABD siber güvenlik politikası üzerine ulaşılabilir diğer belgeler 2011, 2013 ve 2015 yıllarında yayınlanmıştır. 2011 yılında yayınlanan siber güvenlik strateji belgesi beş adet stratejik öncelikten oluşmaktadır. Bu öncelikler şu şekilde sıralanmıştır (DOD, 2011):

1. Savunma Departmanının (DOD) siber uzayın tüm potansiyeline hakim olabilmesi için onu organize etmek, geliştirmek ve donatmak üzere operasyonel bir bağlam olarak ele alması.

2. DOD sistem ve ağlarını korumak üzere yeni operasyonel savunma içerikleri temin etmek.

3. Bütünsel bir siber güvenlik stratejisi oluşturmak üzere diğer devlet ve özel sektör kurumlarıyla işbirliği yapmak.

4. Kolektif siber güvenliği sağlamak üzere ABD müttefikleri ve uluslararası ortaklarla güçlü ilişkiler kurmak.

5. Daha iyi bir siber güç ve teknolojik inovasyon kabiliyeti için ulusun yaratıcılığını artırmak.

2013 yılında DOD, “Savunma Departmanının Ağları, Sistemleri ve Bilgiyi Savunma Stratejisi” (DoD Strategy for Defending Networks, Systems, and Data) isminde bir belge yayınlamıştır (DOD, 2013). Belgede stratejinin ana hedefleri şu şekilde sıralanmaktadır:

1. Esnek bir siber savunma yapısı oluşturmak (savunulabilir bir bilgi çevresi oluşturmak, siber hijyen ve en iyi uygulama örnekleriyle siber güvenliği geliştirmek, bilgi savunmalarını güçlendirmek, endüstriyel kontrol sistemleri üzerine olan ilgiyi artırmak, tehdit odaklı mühendisliği kurumsallaştırmak),

2. Siber savunma operasyonlarını dönüştürmek (aktif bir siber savunma kapasitesi geliştirmek, siber saldırganlığı azaltmak, manevraya hazır kuvvetler oluşturmak, öngörülemez savunma stratejileri geliştirmek),

3. Siber olaylar farkındalığını geliştirmek (siber sezgi altyapısını geliştirmek, büyük veri analizinin gücünden yararlanmak, çok boyutlu bir siber-operasyonel resim çizmek, bilgi paylaşımı ve işbirliğini artırmak),

4. Çok büyük ve kapsamlı siber saldırılara karşı dahi ayakta kalabilir sistemler geliştirmek (yüksek öncelikli görev alalarının belirlenmesi, geniş kapsamlı siber ataklara karşı başarı, yenilenebilir siber kapasite oluşturmak).

2014 yılında ise Beyaz Saray Basın Ofisi ABD ile AB arasında yapılan siber güvenlik işbirliğine dair bir yazılı açıklama yapmıştır (WHOPS, 2014). Söz konusu işbirliği internet yönetişimi, internet özgürlüğü, siber uzayda insan haklarının korunması gibi konular üzerinedir. İşbirliğinde yer alan konu başlıkları ise şu şekildedir:

-Uluslararası siber uzay gelişmeleri,

-online insan hakları tanıtımı ve korunması,

-yürürlükteki uluslararası hukukun uygulanışı, siber güvenlik ölçütleri geliştirme, siber ortamdaki davranış normları gibi uluslararası güvenlik konuları,

-üçüncü taraf ülkelerde siber güvenlik kapasitesi geliştirme.

Aynı ofis 2015 yılında Birleşik Krallık (United Kingdom, kısaca; UK) ile yaptıkları siber güvenlik işbirliğine dair bir açıklama yayınlamıştır (WHOPS, 2015). Buna göre, ABD ve Birleşik Krallık, kritik altyapıların siber güvenliğinin geliştirilmesi, siber savunmadaki işbirliğinin güçlendirilmesi, siber güvenlik üzerine yapılacak akademik çalışmaların desteklenmesi konularında uzlaşmışlardır.

DOD'un son olarak 2015 yılında yayınladığı diğer bir belge ise "Siber Strateji" (Cyber Strategy) ismini taşımaktadır. Belgeye verilen isim daha önceki isimlendirmeler olan "siber uzay güvenliği" ya da "siber güvenlik" isimlendirmelerine bakarak daha genel bir stratejiyi ifade eder niteliktedir. Belgenin içeriği incelendiğinde ise (DOD, 2015) belgenin, yeni bir siber stratejiyi ön görmekle birlikte stratejiye yönelik atılan somut adımların da altını çizer nitelikte olduğu görülmektedir. Belge yeni bir siber stratejinin gerekliliği olarak üç durumdan bahsetmektedir. Birincisi ABD çıkarlarına, DOD ağlarına ve bilgi sistemlerine karşı artarak devam eden kapsamlı saldırılar; ikincisi, dönemin başkanı Obama'nın DOD'a diğer Birleşmiş Milletler (BM) ülkeleriyle birlikte hareket ederek bir savunma planı oluşturma direktifi ve son olarak da 2012 yılından itibaren DOD'un oluşturmaya başladığı ve kurumun görevlerini yerine getirmek üzere operasyonları yürütecek olan, sivil, askeri yaklaşık 6.200 personelden oluşan Siber Görev Güçleri (Cyber Mission Force; kısaca, CMF) yeni stratejinin nedenleridir. Bu gelişmeler ve oluşan yeni bileşenler yeni bir stratejiyi gerekli hale getirmiştir.

2015 yılında yayınlanan strateji belgesi önceden de değinildiği üzere, somut adımlara önem vermiş gözükmektedir. Bu doğrultuda diğer belgelerde belirtilen stratejik hedeflerin dışında bu belgede, stratejik hedeflere ulaşılması için gerçekleştirilen uygulamalara da yer verilmektedir. Bu doğrultuda belgede yer alan beş adet stratejik hedef ve bu hedefler doğrultusunda yapılan uygulamalar aşağıda kısaca ele alınacaktır.

1. Siber uzay operasyonlarını gerçekleştirmek ve yürütmek üzere hazır güçler ve diğer unsurlar oluşturulacaktır. Bu hedefe yönelik olarak yukarıda da belirtildiği üzere CMF oluşturulmuş ve bu oluşuma yatırımlar yapılmış ve yapılmaktadır. Söz konusu gücün eğitimi ve her daim hazır bulunması için ona bir antrenman alanı oluşturulacaktır. Bu alan diğer devlet kurumları, özel sektör ve sivil toplum kuruluşları işbirliği ile gerçekleştirilecektir. Söz konusu oluşumda yer alan personele işlerinde yükselebilecekleri bir kariyer sistemi getirilecektir. Siber güvenlik konusunda sivillerin ve toplumun eğitilmesi için programlar oluşturulacaktır. Operasyonlar için teknik bir altyapı oluşturulacak; bu doğrultuda bütünleşik bir platform meydana getirilecek, ar-ge çalışmaları yürütülecek, emir komuta mekanizması oluşturulacak (oluşturulmuş; United States Cyber Command; kısaca, USCYBERCOM), kurumsal kapasite gözden geçirilecektir.

2. DOD'un bilgi ağını savunmak, verilerini korumak ve DOD hedeflerine yönelik riskleri azaltmak adına çok aktörlü fakat tek bir güvenlik çatısı kurulacaktır. Bu çatıda yönlendirici mekanizma USCYBERCOM olacaktır. Sürekli gözden geçirmeler ve güncellemelerle bilinen ve bulunan güvenlik açıkları kapatılacaktır. DOD bilgi ağlarının, sistemlerinin ve verilerinin korunmasından sorumlu olarak Siber Koruma Takımı (Cyber Protection Team; kısaca CPT) kurulacaktır.

3. Ülkeyi ve ülkenin çıkarlarını yıkıcı siber saldırılardan korumak için hazır durumda bulunulacaktır. Acil uyarı ve tehditleri önceden haber almaya yönelik istihbarat yapısı kurulacaktır. Bunun için hem insan kaynağı, hem de siber olanaklar seferber edilecektir. Oluşturulan CPT ve CMF birimleri, saldırılara karşı her zaman ve her koşulda hazır ve antrenmanlı olacaklardır. Birimler ülkedeki güvenlikten sorumlu diğer birimlerle (FBI, açılımı Federal Bureau of Investigation ve CIA, açılımı Central Intelligence Agency) sürekli işbirliği içerisinde bulunacaklardır. Kritik altyapıların koruması için siber güvenlik ilgili kurumları devamlı bir şekilde kendi kapasitelerini ve olanaklarını değerlendirip gelişime doğru ilerleyeceklerdir.

4. Uluslararası güvenlik ve istikrarı sağlamak üzere artan ortak tehditlere karşı güçlü uluslararası ittifaklar ve ortaklıklar geliştirilecektir. Özellikle Orta-Doğu, Asya-Pasifik ve Avrupa bölgeleri gibi stratejik bakımdan öncelikli bölgelerdeki ilgili kurumlarla ortaklıklar kurulacak ve bunun için kapasite geliştirilecektir. ABD'nin, bu bölgelerdeki siber sistemlerin güvenliklerine belgede özel olarak ilgi gösterdiği ve onların siber sistemlerinin güvenliklerini kendi siber sistem güvenlikleri kadar önemsediği göze çarpmaktadır. Diğer bir vurgulanan nokta ise siber güvenliğin sağlanmasına yönelik uzlaşmacı adımlar atılması ve karşı taktiğin (savaş doktrini vb.) daha iyi anlaşılabilmesi için Çin ile siber güvenliğe ilişkin bir diyaloğun geliştirilmesidir.

5. Stratejinin yönetilmesi. Stratejinin belirlendiği gibi ilerlemesine ve süreçte çıkacak sorunların çözülmesine ilişkin olarak DOD'a bağlı bir Temel Siber Danışma Birimi (Principal Cyber Advisor Office) kurulacaktır. Bunun yanında Siber Yatırım ve Yönetim Platformu (Cyber Investment and Management Board) ve Üst Düzey Yönetici Forumu (A Senior Executive Forum) kurulacak, kurulan bu birimler oluşumun bütçe, strateji, kapasite, hedefler, uygulamalar, sonuçlar gibi fonksiyonlarına yönelik yönetim ve denetimi güçlendirilecektir.

Tüm bu incelenen hususların doğrultusunda ABD'nin siber güvenlik politikası geliştirmede öncü bir ülke olduğu gözlemlenmektedir. Oluşturduğu siber altyapıların milli olması ülkenin siber bağımlılığını asgari düzeyde tutarken, kritik altyapıların büyük çoğunlukla siber altyapılara bağlı olması ülkenin siber savunma fonksiyonunu zayıflatmaktadır. Bu durum Clarke ve Robert'ın (2010) ülkenin siber güvenlik güç puanlamasını doğrulamaktadır.

Yukarıda incelenen belgeler ve noktalar düşünüldüğünde, ABD'nin siber güvenliğe yönelik farkındalığının henüz 2000'li yılların başlangıcına kadar geriye götürülebiliyor olması dikkat çekicidir. 2003 yılında yayınlanan Siber Uzay Güvenliği belgesi bu farkındalığın bir göstergesidir. Diğer yandan siber güvenlik ile

ilgili olarak 2015 yılında yayınlanan strateji belgesinde gelinen noktaya bakıldığında, bu zaman aralığında çıkarılan diğer belgelere karşın somut adımların daha çok son dönemde atıldığı ve halen gelişmekte olduğu gözlemlenmektedir. Bu durum Türkiye açısından ele alındığında, siber güvenlik konusuna yönelik olarak yapılan çalışmalar ve gelişmeler için henüz çok geç kalınmadığı, hızlı yapısal reformlar ve yerinde politikalarla siber güvenlik konusundaki altyapı oluşumlarında kalkan treni yakalamanın mümkün olabileceği düşüncesi ortaya çıkmaktadır. Bu düşünce diğer ülkelerin incelenmesiyle yeniden test edilecektir.

3.2. RUSYA'NIN SİBER GÜVENLİK POLİTİKASI

Bu başlık altında, Rusya'nın siber güvenlik politikası, ulaşılan İngilizce ve Türkçe belgeler, akademik çalışmalar temelinde ele alınacaktır. Konuya öncelikle internetten ulaşılabilen 2015 yılında yayınlanmış Rusya'nın ulusal güvenlik stratejisinin incelenmesi ve bu belgede siber güvenliğe dair izler aranarak başlanacaktır.

Yayınlanan belgede (RNS, 2015), öne çıkan ana konular, Rusya'nın toprak güvenliği, birey ve toplumun güvenliği, iç ve dış tehditlerin önlenmesi, temel hak ve hürriyetlerin korunması, yaşam standartlarının iyileştirilmesi, bağımsızlık, bütünlük, sürdürülebilir ekonomik gelişme şeklinde sıralanmaktadır. Güvenlik konusunda ise bireysel, kamusal, bilgisel (informational), çevresel, ekonomik güvenlik, ulaştırma ve enerji güvenliği konularının özellikle altı çizilmiştir. Ulusal güvenliğe tehdit tanımı, "ulusal çıkarlara doğrudan ya da dolaylı olarak zarar potansiyeline sahip tüm durumlar ve faktörler" şeklinde yapılmıştır.

Belgede "siber güvenlik" terimi geçmemektedir. Bunun yanında belgedeki çok sınırlı bir miktarda olsa da çeşitli noktalarda siber güvenliğe dolaylı olarak işaret eden açıklamalar ve maddeler yer almaktadır. Belgede geçen 21. maddede (RNS, 2015: md.21) "küresel bilgi arenası" kavramından bahsedilmektedir. Ülkelerin

jeopolitik amaçlarına ulaşmak üzere özellikle bilgi ve iletişim teknolojilerini geliştirmeye çabaladıkları vurgulanmaktadır. Madde 33'te ise (RNS, 2015: md.33) Rusya'nın ulusal savunma hedeflerinin ülkenin huzurlu ve dinamik sosyo-ekonomik gelişimini sürdürmek üzere yürütüleceği belirtilmektedir. Dolayısıyla ülkeye yönelik olacak siber tehdit ve saldırılar da bu savunma anlayışı içerisinde değerlendirilebilecektir. Madde 43'te (RNS, 2015: md.43) ise bilginin daha çok ideolojik çarpıtmalar ve manipülasyonlar için kullanılabilecek bir araç olarak kullanıldığı vurgulanırken, siber güvenlik, bilgi ve iletişim teknolojileri kavramındaki anlamından uzaklaşmaktadır. Madde 22'de (RNS, 2015: md.22) bilgi ve iletişim teknolojilerinin gelişimine bağlı olarak illegal göç, insan ticareti, uyuşturucu ticareti, uluslararası suçların da arttığı belirtilmektedir, ancak bu suç çeşitleri arasında siber güvenlik ya da ona yakın çağrışım yapan bir bakış açısı sezilmemiştir. Bunun yanında bilgi ve iletişim teknolojilerinin faşizmi, aşırıcılığı, terörizmi, ayrımcılığı destekler ve tırmandırır şekilde kullanıldığı, toplumsal huzur, politik ve sosyal istikrarı tehdit eder bir hale geldiğinin de altı çizilmektedir. Görüldüğü üzere 2015 yılı gibi yakın bir tarihte yayınlanmasına karşın Rusya'nın Ulusal Güvenlik Stratejisinde siber güvenlik terimi ve kavramının yer almamasının yanında, siber güvenliğin bileşenleri olan bilgi ve iletişim teknolojileri de sadece diğer suç ve olumsuzlanan gelişmeleri daha da besleyecek birer araç olarak vurgulanmışlardır.

Bunun yanında son dönemde yayınlanan Ulusal Güvenlik Strateji Belgesinde yeterince yer almamasına karşın, Rusya'nın siber güvenlik ile ilgili spesifik stratejiler oluşturarak belgeler yayınladığı ve dahi bu konuda ABD'den daha erken işe başladığı söylenebilecektir. Uluslararası İletişim Birliği (International Telecommunications Union, kısaca; ITU) Rusya'nın siber güvenlikle ilgili politikalarını belirleyen belgelerin 2000 yılından bu yana geliştirildiğini belirtmektedir. Bu belgeler (ITU, 2015), Rusya Federasyonu Bilgi Güvenliği Doktrini (RFBGD, 2000), Uluslararası Bilgi Güvenliğinde Rusya Federasyonu Devlet Politikası Temel Prensipler Belgesi (2013 ve 2020 yılları için çıkarılan iki adet)

(Basic Principles for State Policy of the Russian Federation in the field of International Information Security) ve henüz taslak halinde bulunan Rusya Siber Güvenlik Strateji (RSG, t.y.) belgeleridir.

2000 yılında yayınlanan ilk belge (RFBGD, 2000), bilginin toplanması, tesis edilmesi, bilgi sistemleri ile bilgi ve iletişim teknolojileri, web siteleri, iletişim ağları, bilgi işlem süreçleri, bu teknolojilerin geliştirilmesi ve güvenliklerinin sağlanmasını konu almaktadır. Temel amaç ülke çıkarlarını iç ve dış bilgi konulu tehditlere karşı korumak ve sürekli gelişimi muhafaza etmektir. Bilgi güvenliğinin; istihbarat, karşı istihbarat, bilim ve teknoloji, bilgi analizi gibi fonksiyonlarla insani ve ekonomik kaynakların bilgiye karşı olan tehdidin öngörülmesi, belirlenmesi, önlenmesi ve zararlı sonuçlarının yok esilmesi amacıyla kullanılması esastır. Söz konusu bilgi güvenliği konusu, devlet kurumları, araştırma kurumları ve askeri-endüstriyel kurumların koordineli ve planı bir şekilde uygulayacakları aktiviteler ile sağlanacaktır (RFBGD, 2000: md.8,11). Bu aktivitelere ek olarak, siber uzaydaki artan karmaşıklık ve kritik altyapılara yönelik büyüyen tehdit, yabancı devletlerin Rusya Federasyonuna karşı gerçekleştirecekleri saldırılara yönelik oluşturulacak istihbarat ağının güçlendirilmesini gerekli kılmıştır. 2000 yılında yayınlanan belgede dikkat çeken önemli bir nokta da o dönemki yerli bilgi sistem ve teknolojileri ile bilgi güvenliği konusunda yapılan akademik çalışmalar ve oluşturulan insan kaynağının yeterli düzeyde görülmemesidir (RFBGD, 2000: md.18). Ülkelerin bilgi teknolojileri alanında kaydettikleri gelişmelerle siber uzaydaki hâkimiyetlerini artırarak, bu alanda domine olma hedefleri göz önüne alınarak Rusya'da çalışmalar hız kazanmalı ve yerli üretim sistem ve ağlara yönelinmesi gerekmektedir. Ülkelerarası bilgi güvenliğinin sağlanması ve ülkelerin stratejik istikrarlarının, eşitsizliklerin korunmasına yönelik uluslararası düzenlemelerin eksikliğinin altı çizilmektedir (RFBGD, 2000: md.19).

Belgede (RFBGD, 2000: md.20-29), Rusya'nın bilgi güvenliğini sağlanması için ulaşılması öngörülen hedefler şu şekilde sıralanmaktadır:

1. Bilgi güvenliğindeki stratejik hedefler, bireysel, toplumsal ve ulusal çıkarların bilgi güvenliği alanında gelecek iç ve dış tehditlerden korunmasına yöneliktir.

2. Rusya'nın askeri-politik stratejisine uyumlu olarak bilgi güvenliği konusunda gerçekleştireceği savunma fonksiyonları; bilgi teknolojileri kullanımıyla ortaya çıkacak askeri tehditlerin önlenmesi, askeri ve diğer savunma unsurlarının bilgi sistemlerinin güçlendirilmesi, bilgi sistemlerine yönelik tehditlerin öngörülmesi ve belirlenmesi, Rusya'nın müttefiklerinin bilgi güvenliklerinin sağlanmasıdır.

3. Bilgi güvenliğinin sağlanması aynı zamanda kamusal düzen ve güvenliğin sağlanması, bütünlüğün ve egemenliğin korunması, vatandaşların temel hak ve hürriyetlerinin korunması, kritik bilgi sistemleri altyapısının korunması konularını kapsamaktadır.

4.Bilgi güvenliğinin, dolayısıyla kamu düzeninin sağlanmasında temel yönelimler; bilgi teknolojilerinin aşırılık ve karşıt ideolojik fikir propagandalarının yapılması amacıyla kullanımının önlenmesi, bilgi ve iletişim teknolojilerinin diğer devletlerce Rusya'ya tehdit olarak kullanılmasına karşı savunma mekanizması geliştirilmesi, kritik altyapıların korunmasına yönelik yeni siber sistemlerin geliştirilmesi, askeri silahların yönetimini barındıran ve bilgisel ağlarla kontrol edilen askeri yönetim mekanizmalarının güvenliklerinin sağlanması, Rusya'nın toplumsal değerlerine zarar verecek bilgi yayılımının etkisizleştirilmesi ve atılan adımlarla daha optimal planların geliştirilmesidir.

5. Bilgi güvenliğinin sağlanması, bilgi teknolojilerine yönelik yeni gelişimler sağlamak ve nitelikli insan kaynağı yetiştirmekle mümkün olacaktır.

6. Öncelikli amaç siber uzayda güçlü ittifaklar kurmaktır.

7. Tüm bu hedeflere ulaşarak, Rusya'nın bilgi güvenliğinin sağlanması ve geliştirilmesi adına yasal mekanizmaların ve kurumların oluşturması, planlamanın ilk sıralarında yer alacaktır.

Ulaşılabilen kaynaklardan Uluslararası Bilgi Güvenliğinde Rusya Federasyonu Devlet Politikası Temel Prensipler Belgesi, 2020 (ISS, 2017) ele alındığında, belgenin başlığının spesifik olarak "bilgi güvenliği" kavramını içeriyor olması, siber güvenlik konusunun kapsamına daha yakın bir belge olduğunu göstermekle birlikte bu belgede de "siber güvenlik" terimi geçmemektedir. Belge, ulusal stratejik hedeflerden ziyade, uluslararası hedefleri belirtmeye yöneliktir. Buna rağmen bu strateji belgesinin hukuki altyapısını, yapılan uluslararası anlaşmaların yanında, federal kanunlar ve ulusal anlamda gerçekleştirilen diğer hukuki düzenlemeler oluşturmaktadır (ISS, 2017: md.3). Belgedeki temel prensiplere bakıldığında; federe hükümetler ile Rusya'nın uluslararası bilgi güvenliğini sağlamak üzere, hükümetler arası hedef planlarını, konuyla ilgili hukuki ve örgütsel fonksiyonları da dahil ederek, daha iyi bir uluslararası bilgi güvenliği sistemi oluşturmaya yönelik hazırladığı göze çarpmaktadır. Bununla birlikte, stratejik belgelerin etkili uygulanabilmesi amacıyla kurumlar arası iş birliğinin sağlanması ve reel ekonomide, bilgi iletişim teknolojilerini ileri düzeyde kullanan diğer güçlü devletlerle Rusya'nın gelişmişlik eşitliğinin sağlanması ve korunması temel hedefler arasında yer almaktadır.

Belgede, 2000 yılında yayınlanan belgeye göre bilgi güvenliği açısından daha kapsamlı tanımlara yer verilmiştir. Buna göre uluslararası bilgi güvenliği kavramı (ISS, 2017: md.6), "bireysel hakların gaspı olasılığını, bireysel, toplumsal ve ülkesel bilgi alanına karşı tehditleri, kritik bilgi altyapıları üzerindeki yıkıcı ve kanuni olmayan etkileri önlemek adına küresel bilgi alanında sağlanan durum" olarak tanımlanmaktadır. Uluslararası bilgi güvenliği sistemi ise "bilgi alanında farklı aktörlerin aktivitelerini düzenleyen ulusal ve uluslararası kurumlar seti" şeklinde tanımlanmış olup, bilgi güvenliği sistemi bu kurumların özneleştirilmiş hali olarak

ele alınmıştır (ISS, 2017: 2). Belgede tehdit olarak görülen durumların, bilgi ve iletişim teknolojilerinin şu şekillerde kullanılması ile ortaya çıktığı belirtilmiştir:

-Devletlerin bütünlüğünü, huzur ve düzenini bozan, şiddet ve karışıklıkları destekleyen, uluslararası hukuka uymayan, askeri ve politik amaçlarla kullanılan bir silah,

-terörist eylem ve aktiviteler ve kritik bilgi altyapılarını zarara uğratmak üzere kullanılan bir araç,

-faşizm, ayrımcılık ve aşırıcılık gibi ideolojileri besleyerek özellikle devletlerin iç huzur ve düzenlerini bozan bir silah,

-bilgisayarlara erişmek, oradaki bilgileri çalmak, manipüle etmek, oluşturmak, kullanmak, programlara zarar vermek ya da amaçları dışında kullanmak üzere etki eden bir araç.

Uluslararası bilgi güvenliğini sağlamak üzere, uluslararası hukuki bir rejim sürdürmeyi temel politikası olarak belirleyen devletin görevleri ve siber güvenlikle ilgili izleyeceği politikalar, genel hatlarıyla şöyle açıklanabilmektedir; (ISS, 2017: 3-4):

-İkili, çoklu, bölgesel ve küresel boyutlarda uluslararası bilgi güvenliği sistemi sağlamak,

-ülke bütünlüğü ve istikrarına zarar vermeye, stratejik istikrarı ve uluslararası huzuru bozmaya yönelik bilgi ve iletişim teknolojileri kullanımına bağlı olarak meydana gelecek risk ve tehditleri önlemek,

-bilgi ve iletişim teknolojilerinin terörist amaçlar doğrultusunda kullanılmasını önlemek adına uluslararası mekanizmalar oluşturmak,

-bilgi ve iletişim teknolojilerinin ülkelerin dış ilişkilerine müdahale etmek amacıyla aşırıcı amaçlar doğrultusunda kullanımını engellemek,

-bilgi ve iletişim teknolojilerinin kullanımıyla işlenen suçlarla mücadelede, uluslararası işbirliğinin önleyici ektisini artırmak,

-gelişmiş ve gelişmekte olan ülkelerin bilgi ve iletişim teknolojilerindeki gelişmişlik düzeyleri arasındaki eşitsizliği gidermek üzere geliştirici programların düzenlemesine olanak sağlamak.

Belgede, hedeflere ulaşmak üzere araç olarak kullanılacak olan kurumlarda başat aktör federal yönetim organları gösterilirken, bu organların yapacakları kamu-özel sektör işbirliğinin de altı çizilmiştir. Federasyonun güvenlik konseyi ise yönetim organları arasındaki koordinasyonu sağlayacak yönlendirici birim olarak görülmüştür. Rusya'nın siber güç anlayışını yukarıda olduğu gibi resmi belgelerin dışında, aynı zamanda Rusça alan yazınından incelemiş ve Rusya'nın siber güvenlik politikasını Jervis'in saldırı-savunma kuramı üzerinden değerlendiren Medvedev (2015: 3), ülkenin siber görevler üstlenen kurumlarını; Federal Güvenlik Servisi (Federal Security Service, kısaca; FSB), Dış İstihbarat Servisi (Foreign Intelligence Service, kısaca; SVR) ve ordunun Ana İstihbarat Direktörlüğü (Main Intelligence Directorate, kısaca; GRU) olarak belirtmiştir. Diğer yandan araştırmanın önemli bir sonucu olarak Rusya'nın siber güvenlik anlayışı savunmadan daha ziyade saldırı anlayışıyla şekillenmektedir. Savunma anlayışı sadece yapılacak yatırımların daha dikkatli bir şekilde şekillendirilmesine yön verirken, alan yazınında devletin siber güvenlik anlayışının rakipleri düşman olarak görmek ve saldırılara saldırı ile karşılık vermek üzere strateji geliştirmek olduğu görüşü ağır basmıştır.

Giles'in (2013) çalışmasında ise yukarıda incelenen strateji belgelerini destekler biçimde Rusya'nın vatandaşların internet ve sosyal medya kullanımında aktivist

hareketlerin önüne geçmek adına bir takım sansür ve sınırlamalara gittiği vurgulanmaktadır. Bu sınırlamaların federal hukuki altyapıları da bulunmaktadır. Diğer ülkelerde olduğu gibi internet ve siber alan, Rusya'da da politik olmaktan çok ekonomik ve sosyal bir oluşum olarak görülse de 2011-2012 yıllarında yapılan seçimlere yönelik protestoların sosyal medya ve internette geniş bir eyleme dönüşmesi bu görüşü maskelemiştir (Giles, 2013: 2). Söz konusu farkındalık artırıcı olayın sonrasında Rusya'da strateji belgelerinde de yer aldığı gibi ülke içi huzur ve istikrarı bozacak olan her türlü siber olaya karşı önlem alınması görevine karşılık, internet üzerinde devlet kontrolü de artmıştır. Yazar, internet ve dolayısıyla ifade özgürlüğü temelinde Rusya siber güvenlik politikasının böyle bir ortamda aldığı karışık halin, taslak aşamasında olan Siber Güvenlik Politikası belgesiyle açığa kavuşacağını beklemektedir. Bu anlayışa paralel olarak başka bir çalışmasında Giles (2012: 65), Londra Siber Konferansında Birleşik Krallık Dışişleri sekreteri ve arkadaşlarının sunumlarında siber uzayı "gelişim, yenilik, yeni fikir ve açıklamalara açık bir alan" olarak nitelerken, Rusya Bakanı Shchegolev'in bunu "ulusal hukuki düzenlemelere uygunluk, ve özgürlüğün ülkenin güvenlik önceliklerini sağlamak kaydıyla" ifadeleriyle tamamladığının altını çizmektedir. Aslında bu bakış açısı, Rusya'nın siber güvenlik ve siber uzaya bakış açısını batı konsensüsünden en temel şekilde ayıran farklılığı da temsil etmektedir. Bu noktada Rusya'nın siber güvenliğe karşı tutumunu özetleyen iki anahtar kavram "ulusal internet" ve "ülke egemenliğine karşı siber uzaydan gelecek herhangi bir tehdit potansiyeline karşı katı koruma" olarak nitelendirilebilecektir.

Rusya'nın siber güvenlik politikalarına dair devlet söylemleri, ülke içinde ulusal ve uluslararası bilgi güvenliğini sağlamak adına yapılan çalışmalar doğrultusunda hazırlanan belgeler ve ülkelerin siber güvenlik politikalarını ve süreçlerini analiz eden Clarke ve Robert'ın (2010) puanlama çalışması da göz önüne alındığında; Rusya'nın siber güvenlik politikası oluşturma sürecinin savunmacı anlayışla temellendiği, fakat gelişim sürecinde saldırıya saldırı politikasıyla güvenlik

anlayışını geliştirerek farklılaştırdığı gözlemlenmektedir. Bu gözlem, bahsi geçen tablodaki saldırı puanının 7, savunma puanının ise 4 olarak belirlenmesi ile de örtüşmektedir.

3.3. ÇİN'İN SİBER GÜVENLİK POLİTİKASI

Çin Halk Cumhuriyeti'nin kuruluşundan sonraki ilk 30 yıllık dönemdeki (1949-1978) dış politikası genel olarak ülkenin egemenliğini sürdürmek ve ülkeye karşı gelmesi muhtemel işgal niteliğindeki tehditlerin önlemek üzerinde gelişmiştir. Bilgi toplumuna geçişle birlikte gelişen yeni teknolojiler ve kaynak bağımlılıkları Çin açısından yeni handikapları da beraberinde getirmiştir. Her yıl önemli oranda artan bir ivmeyle 2010 yılında internet kullanıcı sayısı 457 milyona, 2017 yılında 731 milyona ulaşmış (Techinasia, 2017), ülkede internet olmadan iş yapmak olanaksız hale gelmiştir (Fei, 2011: 185). Artan internet, bilgi ve iletişim teknolojilerinin doğrultusunda ülkede, siber suçlar artmış, uluslararası boyutta ise ülke dışından Çin internet ağına yapılan siber saldırılar artmış ve siber güvenlik konusu Çin'in de öncelik verdiği bir konu haline gelmiştir.

Siber güvenliğin önemine, Çin'in algısı da diğer ülkelere benzer şekilde gelişmiştir. Devlet açısından siber güvenliği önemli kılan konular; siber eylemlerle ülkedeki kritik altyapı fonksiyonlarının zarara uğratılması, internetin, bilginin ve her türlü sanal dosyanın toplum düzenine, ekonomik gelişim sürecine, bireysel mülkiyet hakkına, askeri kapasitenin gelişimine zarar vermek amacıyla kullanılması gibi etmenlerdir (Swaine, 2013: 3). Bu tehditlere karşı Çin'in uyguladığı siber güvenlik politikası daha ulusal ve uluslararası platforma kısmen kapalı olması suretiyle batı ülkelerinden ayrılmaktadır. Gierow (2015) yaptığı çalışmada, Çin'in bir takım yönleriyle batı ülkelerinden ayrılan siber güvenlik politikasının ana hatlarını belirtmiştir. Buna göre, Çin kendi bilişim teknolojisini üreterek sektördeki lider ülkelerin hegemonyasından uzak durmakta ve ulusal egemenliğini bu alanda da

sürdürmek hedefindedir. Politikanın ana yaklaşımı bağımsız internet teknolojisi olmadan siber güvenliğin sağlanamayacağı yönündedir. Devlet yönetimi, uluslararası alanda ihracat yapan yerli teknoloji firmalarına kayda değer desteklerde bulunmaktadır. Söz konusu firmalar, küresel olarak kabul görmüş internet yazılımlarına ve teknoloji donanımlarına alternatif üretimlerde bulunmaktadır. Çin'in ürettiği akıllı telefonlar ve en önemlisi alternatif akıllı telefonlar için uygulama indirme mağazaları buna somut birer örnektir. Ülkede bu örneklerin küresel boyutta dış ülkeler tarafından üretilenleri için kullanım yasakları ve sansürler uygulanmaktadır. Bu engellemelerin nedeni ise ülke içi ve dışı bilgi sızdırılması ve espiyonajdır. Diğer yandan Çin'de korsan yazılımların kullanılma oranın yüksekliği ve bu nedenle yazılımların düzenli güncellemelerle daha güvenlikli hale getirilmemesinden dolayı hackerlik ve siber suç girişimleri artmakta, oluşan durum siber güvenliğe zarar vermektedir.

Çin'in siber güvenlik ile bilgi ve iletişim teknolojilerine verdiği önemin geçmişi 20. Yüzyılın sonlarına yani bu teknolojilerin ilk ortaya çıktığı zamanlara kadar dayanmaktadır. İlk olarak 1986 yılında ekonomik bilgilerin yönetimine dair küçük bir grup kurulmuştur ve 2001 yılına kadar aktif görevlerde bulunmuştur. 2003 yılında ise siber güvenliğe dair ilk sivil belge olan Belge 27 yayınlanmıştır. Belge, kritik altyapıların korunmasına yönelik aktif bir savunma politikası oluşturmayı amaçlarken, dinamik gözlemleme, gelişimi destekleme, devlet organları ve kurulan ekonomik bilgilerin yönetimi grubuyla iş birliği yaparak siber güvenlik politikalarını yönlendirmeyi amaçlamıştır (Raud, 2016: 11). Çin'in siber güvenlik alanında yaptığı kurumsal ve hukuki düzenlemelerin geçmişi 2014 yılının biraz öncesine dayanmaktadır. KMPG'nin yayınladığı raporda (KMPG, 2016: 5) bu düzenleme ve gelişmeler kronolojik olarak sıralanmıştır. 2014 yılından önce yapılan düzenlemeler siber güvenliğe ve sistemsel altyapıların önemine odaklanılmış, devlet tarafından oluşturulan konsey bilgisayar bilgi güvenliği prosedürleri oluşturulmuş, Kamu Güvenliği Bakanlığı (Ministry of Public Security) bilgisayar virüslerine karşı

savunma ve internet için birtakım standartlar geliştirmiştir. 2014 yılında, Çin devlet başkanı Xi Jinping başkanlığında siber güvenlik grubu kurulmuş ve yapılan çalışmalar o yılki hükümet raporunda yer almıştır. 2015 yılında Çin'in ulusal kongresi olan NPC'de (Standing Committee of the National People's Congress) kamuoyu yoklaması yapmak suretiyle halkın da görüşlerini göz önüne alarak Siber Güvenlik Kanunu tasarısını oluşturmuştur. Tasarı, Haziran 2016'da kongre tarafından ikinci kez tartışmaya açılırken, aynı yılın Temmuz ayında tasarının son halini kuruluş resmi internet sitesinde yayınlanmış ve kamuoyunun ilgisine sunuluştur.

NPC'nin oluşturduğu kanun taslağı 1 Ocak 2017'de uygulanmak üzere yürürlüğe girmiş ve uygulanmaya başlamıştır. Kanun (COV, 2017) 7 bölüm ve 79 maddeden oluşmaktadır. 1. ve 2. bölümde genel prensipler ve hükümetin genel siber güvenlik stratejisi hakkında bilgi verilmektedir. 3. bölümde servis sağlayıcı ve ilgili kuruluşlarının sağlaması gereken siber güvenlik standartları Çok Boyutlu Ağ Güvenliği Koruması Şematiği altında verilmiştir. 4. bölümde bilgi güvenliği konuları; özel hayatın gizliliği, siber suçlar, zararlı yazılımlar, kanunsuz bilgi yayılımı gibi odak noktalar üzerinden ele alınmıştır. 5. bölümde ağların izlenmesi ve acil durumlarda tehlikelere karşı yapılacak hamleler açıklanmıştır. 6. bölümde ağ güvenliği kurallarının ihlal edilmesi durumunda uygulanacak yaptırımlar belirtilirken, son bölümde tanımlar ve diğer ek bilgiler yer almıştır. Kanunda özellikle altı çizilen konular şu şekilde sıralanmaktadır:

1. Siber Uzay Güvenliği Prensibi: Bu prensibe göre devlet kendi sınırları içerisinde, her türlü siber düzenlemeyi yapmaya yetkilidir. Bu prensibin temelini devlet başkanı Xi Jinping'in siber strateji üzerine son dönemde verdiği talimatlar etkili olmuştur.

2. Ağ Ürün ve Servis Sağlayıcılarının Güvenlik Standartları Zorunlulukları: Yukarıda bahsedilen Çok Boyutlu Ağ Güvenliği Koruması Şematiği altında sınıflandırılan güvenlik standartları, söz konusu sağlayıcılar için zorunlu hale

getirilmiş ve bu sağlayıcıların kendi güvenliklerini sağlayabilmeleri hedeflenmiştir. Bu sağlayıcıların ürettiği servis ve hizmetler pazara çıkmadan önce akredite edilmiş test merkezleri tarafından kontrol edilip kanunda belirlenen ulusal standartlara uygun olup olmadığı belirlenecektir.

3. Kişisel Bilgilerin Korunması: Kişiler bilgilerin koruması ile ilgili gerekli zorunluluklar da servis sağlayıcı ve operatörlere yüklenmiştir. Buna göre firmalar, elde ettikleri ve kullandıkları, kişilere ait bilgileri izin olmadan paylaşamayacaklardır.

4. Kritik Bilgi Altyapılarının Korunması: Kritik bilgi altyapılarında meydana gelecek bilgi sızması, altyapının hasara uğraması, fonksiyonunu yitirmesi ulusal boyutta bir güvenlik sorunu olarak ele alınmıştır. Söz konusu altyapılar özellikle iletişim, finansal servisler, ulaştırma ve e-devlet alanlarında son derece önemli fonksiyonlar üstlenmektedir. Altyapıların korunmasına yönelik önlemler hem operatörler hem de bunların alt yüklenici firmaları tarafından alınacaktır.

5. Sınır Ötesi Veri Transferi: Ülke dışına veri transferi gerektiren durumlarda, siber güvenliğe yönelik tüm değerlendirmelerin yapılarak adım atılmasının altı özellikle çizilmektedir.

6. Yabancı Saldırganlar İçin Uygulanacak Yaptırımlar: Standartlara uygunsuzluğa karşı verilecek uyarı, lisans iptali, para cezası gibi yaptırımların dışında yeni kanunda, dış ülke firmalarının Cin'in siber güvenliği tehdit edecek saldırılarına karşı faaliyetlerini durdurma, ülke içindeki mal varlıklarına el koyma gibi yaptırımlar uygulayabilecektir.

7. Ağ Bütününde Birlikte İşlerlik ve Standartlaşma: Siber güvenliğe karşı bilgi altyapılarının birlikte işlerliğinin altı çizilmiştir. Buna göre ulusal siber güvenlik standartlarının oluşturulmasında Çin'in milli, devlet kurumları, özel sektör firmaları ve üniversiteleri işbirliği içerisinde olacaklardır. Burada belirtmekte yarar vardır ki,

Çin'in oluşturduğu ulusal güvenlik standartları ile uluslararası standartların uyuşmaması durumunda nasıl bir yol izleneceği belirgin değildir.

8. Reşit Olmayanların Korunması: Siber uzayda, reşit olmayan bireylerin gelişimlerine zararlı olabilecek durum ve etmenlerden korunması üzerine tasarılar oluşturulacaktır.

Çin Halk Cumhuriyeti'nin siber güvenlik konusunda geliştirdiği politikalar güçlü ulusal güvenlik standartlarının oluşturulması dışında, diğer ülkelerin siber güvenliklerine risk ve tehdit oluşturan bir çizgi de izlemektedir. Bu saldırılardan mustarip olan ülkeler ABD, Tayvan ve Almanya olarak örnek gösterilebilecek olsa da bu saldırılardan dolaylı olarak etkilenen ülke sayısı 2009 yılında 103'ü bulmuştur (Spade, 2012: 3-4). Özellikle ABD kongresinde dile getirilen konulardan birisi olarak, Çin'in siber devlet güçlerinin kendi milli firmalarına rekabet üstünlüğü sağlamak üzere ABD firmalarının teknoloji bilgilerini çalmaya yönelik birçok saldırıda bulunduğu vurgulanırken, Çin tarafı bunu "hırsızlığın durdurulması için ağlayan bir hırsız" olarak nitelemektedir (Lindsay, 2015: 7-8). ABD ve Çin arasındaki söz konusu atışma ve suçlamaların yanında, alan yazınında iki ülke arasında yapılan siber güvenlik anlaşması önemli bir yer tutmaktadır.

Çin ile ABD arasındaki dış ilişkiler Çin Halk Cumhuriyeti'nin kurulmasından bu yana çeşitli alanlarda fikir ayrılığı, çatışma ve stratejik güvensizlik çizgisinde ilerlemiştir. Son yıllarda bu iki ülkenin en fazla çatışma yaşadığı alanlardan biri de siber uzay konusu olmuştur. Çatışma ve fikir ayrılıklarını yumuşatmak üzere iki ülke arasında görüşmeler 2013 yılında başlamış olsa da 2014 yılında ABD'nin Çinli bazı askeri görevlilerin espiyonaj faaliyetlerinde bulunduğunu tespit etmesiyle aniden kesilmiştir (Harold, v.d., 2016, iii). 2015 yılında ise Çin devlet başkanı Xi Jinping'in Beyaz Saraya yaptığı ziyarette, ABD başkanı Obama ve Jinping arasında bir siber mutabakat gerçekleştirilmiştir. Buna göre iki ülke zararlı siber eylemlere karşı bilgi ve yardım ihtiyacında işbirliğinde bulunma, siber hırsızlık ve entelektüel sermayeye

zarar verecek siber kaçakçılıklardan kaçınma, ülkelerin siber politikalarında uluslararası standartlara uyum gösterme, siber suçlarla mücadelede iki ülke arasında çok gelişmiş bir diyalog mekanizması kurulması konularında fikir birliğine varılmıştır (Rollins, 2015).

Lieberthal ve Singer (2012: vi-x) çalışmalarında, ABD ve Çin arasında siber politikalardaki uyuşmazlıkları çeşitli konu başlıkları halinde sıralamışlardır. Yazarlara göre uyuşmazlıklar; farklılaşan siber terminolojiye bağlı olarak iki ülkenin kullandığı kavramların içlerinin farklı doldurulması (siber saldırı, bilgi saldırı gibi), siber eylemlerin asıl amaçlarının belirsizliği, savunma odaklı bekleyiştense önce saldıran olmanın avantajlı olması algısı, siber olaylardaki zaman planlaması karmaşıklığı (saldırı ya da savunma için harcanan ve beklenen doğru zaman), eylemlerin yerelleşmesi (tek bir merkezden yönetilmemesi) gibi konuların doğurduğu istikrarsız ve güvensiz ortamdan kaynaklanmaktadır. Diğer yandan ABD ve diğer ülkelerin Çin'i siber güvenlik konusunda güçlü bir risk oluşturan bir ülke olarak görmesine karşın, Çin de dünya genelindeki internet ve bilgisayar teknolojisinin büyük Pazar payının ABD'nin olması dolayısıyla siber güvenlik konusunda ABD lehine büyük bir eşitsizliğin söz konusu olduğunu savunmaktadır.

Çin'in siber güvenlik stratejisini daha çok saldırı odaklı olarak tanımlandığı yapılan alan yazını taramasında göz çarpmaktadır. Fakat bu yönde genel geçer bir tanımın yanlış olacağı düşünülmektedir. Çin, diğer ülkelerden ayrı olarak kendi milli siber ağlarını kullanarak ve uluslararası platformlarda aygın bir şekilde kullanılan birçok ağı kullanmayı yasaklayarak ya da kullanımına sınırlar getirerek aslında en güçlü savunma mekanizmasını geliştirmiştir. Bu yönde izlenen bir politika ülkeyi somut savunma mekanizmaları kurmasa da, ülkeyi siber güvenlik konusunda batı ülkelerine nazaran daha güvenlikli bir hale getirmektedir. Sahip olunan görüşe paralel olarak, çalışmanın önceki kısımlarında ele alınan Clarke ve Robert'in (2010) ülkelerin siber güçlerini puanlandırdıkları çalışmalarında Çin'in savunma puanı, saldırı puanından daha yüksek olarak belirlenmiştir. Bunun sebebinin ise bu

başlıktaki değinilen konular göz önüne alındığında, devletin uyguladığı uluslararası boyutta sıkılıkla kullanılan siber yazılım ve donanımların Çin tarafından engellenmesi ve yerlerine milli alternatiflerin üretilmesi ve kullanılması, ayrıca hukuki düzenlemelerle servis sağlayıcı ve operatörlere yüklenen yaptırımlı güvenlik zorunlulukları ve kritik altyapılara yönelik güvenlik politikaları olarak kabul edilebilecektir.

3.4. İRAN'IN SİBER GÜVENLİK POLİTİKASI

BM yetkililerin ve özel araştırma şirketlerinin altını çizdiği üzere İran, siber güvenlik konusuna önem veren ve siber kapasitesi en gelişmiş ülkelerden biridir. İran'ın siber uzay konusunda böyle bir noktaya geldiği fikrini destekleyen 4 kritik konu ve gelişme vardır. Birincisi, devlet yönetimi özellikle nükleer enerji programları doğrultusunda, siber yeteneklerini artırmaya ve siber kapasitelerini geliştirmeye son derece kararlı bir şekilde yönelmişlerdir. İkinci olarak; İran'ın diğer ülkelere benzer bir şekilde tüm siber kapasitesini ortaya koyan belirli bir siber güvenlik strateji ve politikası yayınlanmamıştır. Yine de bu durum, ülkenin sahip olduğu siber kapasite öngörüsünü olumsuz etkilememektedir. Üçüncü ve bir önceki konuya destek olarak, İslam Devrim Muhafızları Birlikleri (IRGC) komutanlarından Tuğgeneral Behrouz Esbati'nin verdiği röportajlarından bu kapasitenin kayda değer bir boyuta ulaştığı anlaşılmaktadır. Son olarak bu yorumlar, İran'ın siber güvenlik konusunu kavrayışının son derece detaylı olduğunu ve gelecekteki hedeflere ulaşılması açısından siber güvenliğe hat safhada önem verdiği anlaşılmaktadır (Bucala, 2015).

Lewis'e (2014: 2-3) göre İran'ın siber güvenliğe verdiği önem özellikle rejimin devamlılığını sağlamak üzere internet destekli olası muhalif ayaklanmaları bastırmak temelinde gelişmeye başlamıştır. Özellikle 2009 yılında ülkede meydana gelen Yeşil Hareketi, İran rejim yönetimini interneti gözlemleme ve internette

meydana gelecek organize hareketleri önlemek üzere siber kapasitesini artırmaya itmiştir. Diğer yandan dünyada gelişen Arap Baharı gibi internet üzerinden pekişmiş diğer toplumsal olaylar da İran için siber güvenliğin toplumsal hareketleri izleme ve önleme fonksiyonunun bir göstergesi olmuştur. Bu doğrultuda İran internet erişim altyapısını detaylı bir şekilde oluşturmuş, istihbarat birimleriyle iş birliği içinde çalışarak siber güvenliğini zenginleştirmiştir. Gelinen noktada İran, ayaklanma, kargaşa, ya da dış tehdit durumlarında ülkenin ve vatandaşlarının büyük bölümünün küresel internet erişimini durdurabilecek mekanizmalar geliştirmiştir. Söz konusu durumlarda kararlar almak ve stratejilere yön vermek adına Siber Güvenlik Yüksek Kurulu oluşturulmuştur. Kurul, güvenlik ve istihbarat birimlerinden önde gelen yetkililer ile kültür ve iletişim bakanlarından oluşmaktadır. Operasyonel olarak ise abartı olarak görülebilecek olsa da 120.000 gönüllü hackerdan oluşan “Siber Ordu” kurulmuştur. Bu ordunun ilk icraatı ise İran‘ın en önemli yakıt tesisine yapılan siber saldırıdan sonra karşı bir cevap ve gövde gösterisi olarak nitelendirilebilecek ve İran’ın en büyük şüpheli faili olarak görüldüğü, Sudi Aramco and BM RasGas şirketlerine yapılan saldırılardır. Bu saldırılar sonucunda yaklaşık 30.000 bilgisayardaki bilgiler silinmiş ve şirketlerin rafineri kontrol sistemleri zarar görmüştür. Yazara göre bu saldırı, çalışmanın önceki kısımlarında detaylı olarak yer verilen ve İran’a ABD ve İsrail tarafından gerçekleştirilen Stuxnet saldırısı kadar nitelikli olmasa da, başarılı bir operasyondur. Diğer yandan Eisenstadt (2016: 11-12) İran’ın siber kapasitesinin biraz abartıldığı görüşüyle birlikte Ortadoğu ülkelerinin internet altyapısı geçmişlerinin ve deneyimlerinin henüz çok yeni olduğunun altını çizmektedir. İran’ın siber güvenlik anlayışı genel olarak yazılım saldırılarına karşı koymak, istihbarat toplamak, siber ve fiziksel alanlardaki saldırıları tespit etmek, siber saldırılara hedef olma konusunda risk altında bulunan kritik altyapılarını korumaktır. İran’ın siber saldırılara karşı verdiği tepki ya da cevaplar ise daha çok yine hedef alındığı şekilde siber ortamda, devlet destekli siber uzay insan kaynaklarını kullanarak karşılık mahiyetinde siber saldırıda bulunması şeklinde gerçekleşmiştir.

Ülkede küresel internet üzerindeki geniş kapsamlı sansürler ve engellemeler ise yönetim tarafından, ülkede yaşayan halkın değerlerini yozlaştırmaya yönelik bir batı tehdidi şeklinde algılanmakta ve yansıtılmaktadır. Bu anlamda internet ve sosyal medya, batı ülkelerinin İran'ın aleyhine fikir empozesi, iç karışıklık ve ayaklanmaları tetikleme potansiyeline sahiptir ve dahi bu anlayış neticesinde 2012 yılında yabancı uzantılı e-mail domainleri kullanılması yasaklanmıştır (Hagestad, 2013). Siber saldırılara yanıt verme ve siber güvenliğin sağlanması adına bu ülkede de kamu ve kamu dışı aktörleri işbirliği desteklenmektedir.

İran'ın elektronik ticarete dair yaptığı hukuki düzenlemelerde de siber güvenliğin çeşitli boyutlarda sağlanmasına yönelik izlere rastlamak mümkündür. Yayınlanan İran İslam Cumhuriyeti Elektronik Ticaret Kanunu'nda (ETK, 2004) elektronik bilgilerde güvenliğe yönelik kimlik doğrulaması, müşterinin korumasına yönelik olarak ürün ve hizmet sağlayıcılarının bilgilerinin mevcudiyeti, müşteriye ait özel bilgilerin ürün ve hizmet sağlayıcıları tarafından korunması konuları siber güvenlik açısından ele alınabilecek konulardır.

İran'ın siber kapasitesini diğer ülkelere nazaran daha güçlü konuma getiren politikalarından birisi de kendi yerli proxy kanallarını kurmasıdır. Kurulan bu altyapıları destekler nitelikle Cyber Hizbullah ve devlet tarafından desteklenerek geliştirilmeye devam eden Ashiyane hacker grubu ile işbirlikleri gerçekleştirilmektedir (Cilluffo, 2013: 11-12). Söz konusu iş birlikleri ve gerekli donanımsal altyapının geliştirilmesi için devlet finansal kaynaklarını cömert bir şekilde siber sistemler için seferber etmektedir (Eisenstadt, 2016: 5). Diğer yandan tüm bu geliştirmeler uluslararası standartların dışında gerçekleştirilmektedir. Bunun anlamı, İran'ın ne bireysel geliştirmelerde ne de kurumsal geliştirmelerde uluslararası oluşturulan standartlara akredite olmuş bir sertifikasyon sistemi yoktur (ITU, 2015: 2). Diğer yandan yukarıda bahsedilen devlet destekleri, teşvikler, kamu-özel sektör işbirliği gibi atılan adımların, resmi belge ya da stratejilere dayanmıyor olması da altı çizilmesi gereken başka bir noktadır. Ülkede, siber

güvenlik ile ilgili olan ve sorumluluk paylaşan kurum ve kuruluşlar ise BASIJ , -IRGC (Islamic Revolutionary Guard Corps), Bilgi ve İletişim Teknolojileri Bakanlığı, İran Pasif Savunma Kurumu, İran Bilgi Teknolojileri Kurumudur (ITU, 2015: 1). İran'ın siber güvenlik politikası, özellikle ülkenin kendi Proxy ağlarını kurması yönünden Çin'in milli siber altyapı politikasına benzer bir özellik taşımaktadır. Bu girişim ve teşviklerin Çin'de olduğu gibi kendi operatör ve servis sağlayıcılarını oluşturma, kendi yazılımlarını geliştirme ve kendi siber donanımlarını üretme safhasından çok geride olduğu gözlemlenmiştir. Bir diğer politika olarak devletin siber insan kaynağını hem kamu hem de kamu dışı sektörden oluşturması ve bunlara destek vermesine dayanan politika da yine Çin'in politikası ile benzerlik gösterirken, Çin'de bu politikanın; ülkenin kendi yazılım ve donanım firmalarını sektörde gelişmek ve bağımsızlaşmak adına yaptığı hamlelerle, daha sistematik ve kurumsal bir şekilde geliştiği söylenebilecektir.

3.5. KUZEY KORE'NİN SİBER GÜVENLİK POLİTİKASI

Kuzey Kore'nin ulusal güvenlik anlayışı yakın tarihte tarihinde yaşadığı bir takım olaylar etkisinde şekillenen bir yapıya sahiptir. Bu olayları iç ve dış tehdit olarak ayırmak mümkündür. İç tehdidi genel olarak yönetime gelecek kişilerin kendi aralarında yaşadıkları taht kavgaları olarak nitelemek mümkündür Bu çekişmeler Kim Jong-Un başa geçmesi ile istikrara kavuşmuş gözükmektedir. En büyük dış tehdit ise Güney Kore ile olan çatışma ve bunun dolayısıyla diğer dünya ülkeleri ile gerilen ilişkiler, ülkenin nükleer denemelerine karşı yine dünya ülkelerinden gelen dış tehditler olarak ayırmak mümkündür (Dissanayake, 2014: 2016). Tüm bu tehditlerin arasında Kuzey Kore'nin güvenlik politikasını diğer ülkelerden ayrı olarak boyutlandırmak gerekmektedir. Çalışmanın önceki bölümlerinde ulusal güvenliğin bireysel, bölgesel, ulusal ve uluslararası boyutlarından bahsedilmiştir. Kuzey Kore'ye bakıldığında bu boyutlar değişime uğramaktadır. Bireysel güvenlik, aynı zamanda rejimin ve devletin güvenliği olabilmektedir. Buna göre bireysel güvenlik

Öncelikle devlet başkanı Kim ve en yakınındaki yardımcılarının güvenliği, ikincil olarak ordunun güvenliği ve son olarak da İşçi Partisinin güvenliği olarak, devletin güvenliği ise bu bireysel boyutların toplamı olarak ele alınabilecektir (Yoon ve Lim, 2013: 146). Buna göre ulusal güvenlik, dikta rejiminin güvenliğine ve egemenliğine dayanmaktadır.

Kuzey Kore'nin ulusal güvenliğini etkileyen dış olaylardan en büyüğü içinde bulunulan dönemde Trump'ın başkanlığındaki ABD ile yaşadığı zıtlaşmalardır. ABD ve Kore arasında iki ülkenin karşılıklı tehditkâr politik açıklamaları, yapılan gövde gösterisi niteliğindeki askeri tatbikatlar, Kore'nin nükleer silahlarını ön plana çıkardığı savaş potansiyeli açıklamaları sadece Kore ulusal güvenliğini değil küresel güvenliği de endişelendiren etmenlerdir. Kore tarafından gösterilen bu tutum, ulusal güvenliğe karşı dış ülkelerden gelecek tehditlere karşı birer gözdağı niteliğindedir. Söz konusu gerilim ortamında, hesaba katılması gereken bir diğer önemli faktör ise Çin'dir. Çin ve Kore arasında 1961 yılında imzalanan, 1981 ve 2001 yılında yenilenerek 2021 yılına kadar geçerli olan "Batı Güçlerine Karşı Birleşik Cephe" amaçlı yardım ve işbirliği anlaşması bulunmaktadır (Sputnik, 2017). Yine'de Çin'in, son dönemde Kore'yi frenleyen ve ABD ile Kore arasındaki gerginliği azaltmaya çalışan bir arabulucu rolü üstlendiği izlenmektedir (BBC, 2017). Çin'in yanında Rusya'da batı ülkelerine karşı Kuzey Kore'nin güvendiği bir diğer yardımcı güç olarak göze çarpmaktadır (DOD, 2012b: 5).

Kuzey Kore'nin siber güvenlik konusuna gelindiğinde, diğer ülkelerden farklı olarak belki de siber kapasite bakımından en belirsiz ülke olarak konumlandırılabilecektir. Ülkenin dışa kapalı olan ve değim yerindeyse su sızdırmayan yapısından kaynaklı olarak siber kapasitesinin sınırları da belirsiz bir çizgi izlemektedir. Bunun yanında, ülkede bulunan ve bu konu ile ilgili yetkililerin açıklamalarına göre Kuzey Kore, dünya üzerinde ABD ve Rusya'dan sonra en geniş siber kapasiteye sahip ülkedir. 2004 yılında Kuzey Kore Savunma Güvenliği komutanı Song Yeong-geun ülkenin siber saldırı ve hackleme kapasitesinin CIA'den sonra en güçlüsü olduğunu

vurgularken, 2012 yılında aynı görevdeki Bae Deuk-shik Kuzey Kore'nin ABD ve Rusya'dan sonra siber alanda en güçlü ülke olduğu görüşüne katıldığını belirtmiştir. Bu söylemlere rağmen Mansourov (2014: 3), ülkenin siber kapasitesinin daha çok yerli üretim siber altyapılara dayandığını ancak bu gücün dünya ülkeleriyle karşılaştırılma bağlamında abartıldığı görüşündedir.

CRS (2017) raporuna göre; Kuzey Kore'nin siber geçmişi 1980'li yıllara dayanmaktadır. Ülke bu yıllarda siber alanlarda görev alabilecek uzmanlar yetiştirmeye başlamıştır. ABD ise Kuzey Kore'nin siber kapasitesinin farkına 1990'lı yıllarda varmaya başlamıştır. Tanımlanış belirli bir siber doktrini olmayan ülkede, askeri güç egemenlik adına büyük bir öneme sahipken, siber kapasite de sivil toplumdan çok ordunun eli altında toplanmıştır. Ülkenin dışa kapalı olmasından dolayı bu kapasite diğer ülkelerce çok açık bir şekilde belirlenemese de ülkenin yaptığı istihbarat toplamaya yönelik olan siber saldırılar kayda değer görülmektedir. Kurumsal boyutta, Halkın Silahlı Kuvvetleri Bakanlığı bünyesinde kurulan, ulusal güvenlik komisyonuna bağlı olarak direkt olarak Kim Jong-un'a bilgi veren Genel Keşif Bürosu siber konulardaki yetkili merkezdir. Bu merkez iki önemli operasyonel birime sahiptir bunlar Ofis 91 ve Unite 121'dir. Bu birimler siber operasyonlarda önemli rol oynamaktadır. Bunlara ek olarak siber espiyonaj ve savaşta Ünite 110, 204 ve 35 destek birimleri bulunmaktadır. Bu birimlerin görevlerini kısaca şu şekilde özetlemek mümkündür (CRS, 2017):

Ofis 91: Pyongyang'ın Mangkyungdae bölgesinde bulunan birim, siber operasyonlarda ana kumanda merkezi olarak görev yapmaktadır.

Ünite 121: Çin'in Kuzeydoğusunda, Shenyang'daki Chilbosan Hotel'de bulunan birim Ünite 110 ile birlikte siber operasyonlarda istihbarat toplama hücuma dayalı hamlelerde bünyesinde bulundurduğu 600'den fazla hacker ile görev almaktadır.

Ünite 204: Araştırma ve psikolojik siber operasyonlarda görev almaktadır.

Ünite 35: Bu birim İşçi Partisi Soruşturma Grubunun direktörlüğünde bulunup, siber operasyonlara yönelik eğitim ve tatbikat merkezidir.

Bu birimlerle birlikte Kuzey Kore'nin siber operasyonları daha çok ABD ve Güney Kore başta olmak üzere, ülkelere finansal kuruluşlarına espiyonaj ve uyarı amacıyla gerçekleştirilmiştir. Buna örnek olarak, Kuzey Kore lideri Kim Jong Un'i öldürmek üzere bir komplo kurgusuna sahip bir filimin yayınlanmasını önlemek üzere SONY'e yapılan siber saldırı olarak gösterilebilecektir (DSB, 2017: 1; Whyte, 2016). Kuzey Kore'nin yaptığı bu saldırı ülkenin siber operasyonları stratejik olarak kullanma kapasitesinin geliştiğinin de bir göstergesi sayılabilecektir.

Siber operasyonlar üzerine Kuzey Kore'nin bu sistematik kurumsallaşması daha çok askeri gücü pekiştirmek adına asimetrik savaş taktiklerinin, konvansiyonel savaş taktiklerine tercih edilmesinden kaynaklanmaktadır. Bu anlamda siber kapasite bir ülkenin askeri gücünü asimetrik bir şekilde geliştirebilecek önemli bir faktör haline gelmiştir. Diğer yandan siber kapasiteyi artırmak üzere yapılacak olan yatırımların fiziki silah yatırımlarından daha az maliyetli olması (HP, 2014: 16) ve asimetrik savaş arenasında ülkeye önemli avantajlar sağlaması da Kuzey Kore'nin ilgisini çekmektedir. Koreli bir bilgisayar bilimleri profesörü olan Heung-kwang'ın altını çizdiği üzere, ülkede bu amaçla programlamanın da temelini oluşturan matematik eğitimine önem verilmektedir ve ülke kurduğu altyapısı dolayısıyla artık emin olduğu siber savunma mekanizmasından ziyade saldırı mekanizmalarına yoğunlaşmaktadır (HP, 2014: 17).

Ülkenin siber savunma mekanizmasını güçlü kılan internet altyapısına değinilecek olursa, HP Araştırma Merkezinin ülke üzerinde yaptığı detaylı araştırmaya değinmekte yarar vardır (Park, 2015: 10-12). Araştırmanın bulgularına göre ülkede iki ayrı internet ağı bulunmaktadır. Birincisi her ülkede kullanılan internet ağı olmakla birlikte bu ağ devlet yönetimi tarafından sıkı denetimde tutulmakta ve ülke vatandaşlarının erişimleri önemli ölçüde kısıtlanmaktadır. Diğer ağ ise Bulguenbyol

(Kızıl Yıldız) olarak isimlendirilen operatör yazılımla çalışan, temelleri Linux üzerinden olan ve 2002 yılında geliştirilmeye başlanan ağdır. Bu ağ ülkenin kendi geliştirdiği operatör yazılımı içermektedir. Bu ağda kısıtlamalar söz konusu değildir ancak bu ağı kullanacak olan bilgisayarların tahsisi de devlet yönetimi tarafından gerçekleştirilmektedir. Ülkenin siber altyapısı genel olarak özetlenecek olursa; internet Çin proxyleri üzerinden kısıtlamalı, yerel internet ise küresel internetten ayrı olarak sadece ülke içinde kullanılmaktadır. Operatör yazılım olarak (Windows yerine) ülkenin kendi geliştirdiği Bulguenbyol kullanılmaktadır. Yardımcı yazılılar ve paket programlar yine milli olarak geliştirilmektedir. Donanımlar ise Çin'den ithal edilmekte ve sınırlı sayıda alınmaktadır. Ülkede internete bağlanmayan ancak yerel nete bağlana 3g servisi kullanılmakta ve vatandaşlar akıllı telefonlar aracılığıyla sadece yerel internete bağlanabilmektedirler (HP, 2014: 10-15). Söz konusu uygulamalar paragrafın başında vurgulandığı üzere, ülkenin genel profilinde olduğu gibi siber sistem konusunda da dışa kapalı olduğunu göstermektedir. Bu kapalılık ülkenin siber güvenliğini ise hat safhada güvenilir bir pozisyona getirmektedir. Zira çalışmanın önceki kısımlarında, siber güvenlik politikaları ele alınan bu ülkelerin siber kapasite puanlandırmasının gösterildiği tabloda (Clarke ve Robert, 2010), Kuzey Kore'nin siber saldırı kapasitesi "2" olarak puanlanırken siber savunma kapasitesi "7" olarak puanlanmıştır. Bu puanlama, Kuzey Kore'nin siber politikasına yönelik yapılan bu alan araştırmasına tutarlı şekilde, ülkenin güvenliğe dayalı altyapısının siber kapasitesinin önemli bir bölümünü oluşturduğunu göstermektedir. Diğer yandan söz konusu puanlamada ülkenin siber bağımlılığı "9" gibi yüksek bir rakamla puanlanmıştır. Yapılan araştırmanın sonucunda ise bu yüksek bağımlılığın, donanımsal ve internet ip yapılanması olarak Çin'den taban alınması durumunun bir yansıması olarak ortaya çıktığı kanısına ulaşılmıştır.

Başlığın geneline bakıldığında, Kuzey Kore'nin siber güvenlik politikasının ele alınan ülkelerden daha çok Çin ile benzerlik gösterdiği ve dahi bu konuda Çin'i

taban aldığı söylenebilecektir. Yine de ülkenin küresel arenada, her yönüyle dışarı kapalı bir ülke olması dolayısıyla her türlü kurumsal kapasitesinin olduğu gibi siber kapasitesinin de durumu diğer ülkeler açısından gizemini korumaktadır. Dolayısıyla, ülkenin siber potansiyelini en az bu başlık altında değinilen noktalar ve atıfta bulunulan çalışmalarda yer alan konular boyutunda değerlendirmenin yine okuyucuyu fikir sahibi yapacağı düşünülmektedir.

3.6. İSRAİL'İN SİBER GÜVENLİK POLİTİKASI

İsrail'in ulusal güvenliği diğer ülkelerinkinden farklı olan bazı unsurların üzerinde temellenmektedir. Ülkenin henüz yakın bir tarihte (1948) kurulmuş olması, her ne kadar demokratik vurgular yapılsa da, ülkenin dini düşüncesinin devlet politikalarını etkilemesi ve bunların yanında da ülkenin Arap-Müslüman Ortadoğu coğrafyasında bulunması bu unsurların başlıcalarıdır (Tabansky ve Israel, 2015: 9). Devletin bugün bulunduğu konuma ve dengeye ulaşana kadar Arap Dünyasıyla yaşadığı çatışmalar (özellikle 1920-1947 arası ayaklanmalar ve çatışmalar), ulusal güvenlik anlayışının temellerini oluşturmaktadır. Zira İsrail'e tehdit oluşturabilecek en yakın ülkelerle durumunu belirleyen barış anlaşmaları da bu yıllarda yapılmıştır.

Yadak (2014: 167-169), İsrail'in ulusal güvenliğini etkileyen unsurları iç unsurlar, bölgesel unsurlar ve uluslararası unsurlar olmak üzere üçe ayırmaktadır. Yazara göre, iç unsurlardan biri ülkenin coğrafi konumudur. İsrail'in etrafının Arap devletleriyle sarılı olması ya da tersten okununca; devletin Arap devletlerin ortasına kurulması, onun güvenlik politikalarını birincil olarak etkilemektedir. Bu durum onun güçlü ülkelerle müttefik olmasını zorunlu kılmıştır. Diğer yandan çeşitli ülkelerden göç ederek gelen ve etnik, kültürel çeşitlilik gösteren halkı, devletin politik amaçlarını şekillendiren dini boyutu, askeri gücünün ülkenin sınırlarına göre yetersiz olması, sınırlı ekonomi ve insan kaynakları iç unsurlar arasındadır. Bölgesel unsurlar, Arap devletlerinin birbiri arasında işbirliklerine gitmeleri,

yakınlaşmaları, bölgedeki ülkelerin teknoloji alanında gelişme çabaları, Filistin'in direnişinin başka ülkelerce de haklı bulunmaya başlanması ve Filistin'e gelen yardımlar olarak belirtilmiştir. Son olarak, başat güç olan Amerika'nın İsrail'in her türlü politikasında onun yanında yer alması ve Filistin'e karşı uygulanan şiddetin "terörle mücadele" başlığı altında meşrulaştırılma çabası ise uluslararası unsurlar arasında sıralanmaktadır.

Yukarıda ele alınan, ulusal güvenliğine etki eden unsurların yanında İsrail, siber güvenlik konusuna son derece büyük bir ilgi göstermektedir. Ulusal güvenliğin temel yatırımlarından ayrı olarak ülke, 82 milyar dolarlık bir siber güvenlik endüstri hacmine sahiptir. Ülke siber güvenlik ürünleri ile ilgili dışarıdan da yatırımlar almaktadır (Forbes, 2017). Israil'de 2017 itibarı ile siber güvenlik alanında faaliyet gösteren 150 aktif firma bulunmaktadır (BVP, 2017). İsrail'in siber güvenliğe ilişkin en büyük pratiği, 2014 Gazze Şeridine yaptığı harekatta dünyadan Filistin'i destekleyen çeşitli ülkelerin İsrail'e karşı başlattığı siber savaş olmuştur. Bu saldırılar hem devletlerin kurumlarından hem de sivil kurumlardan gelmiş ve İsrail'in devlet kurumları ile iletişim altyapılarını hedef almıştır (Raska, 2015: 5). #OpSaveGaza hashtagi altında hem Türkiye'den hem dünyadan birçok hacker grubu Gazze'yi vuran İsrail'e misilleme olarak çok sayıda internet sitesine siber saldırı düzenlemiştir. Saldırılarda İsrail Adalet Bakanlığı, devlet arşiv portalı ve ulusal reklam ajansı dâhil çok sayıda bakanlık ve kurumun internet siteleri hedef alınmıştır (Aljazeera, 2014).

Ülkenin siber güvenliğinden sorumlu 4 ana kuruluş bulunmaktadır. Bunlar, İsrail Savunma Kuvvetlerine Bağlı olarak, askeri personelden oluşan ve askeri sinyalizasyon, şifreleme alanlarından sorumlu olan ve 1952'de kurulan Birim 8200; görevi ülke içindeki bilgisayarların güvenliğini sağlamak, ulusal altyapı ve hükümet sistemlerinin savunmasını sağlamak olan iç istihbarat birimi Shin Bet; sistemler

bütünü, kolordu iletişim ve siber savunma faaliyetlerinden sorumlu olan C4I[13] ve dış ülkelerden gelecek siber saldırılara karşı güvenlik sistemi, iş dünyası ve akademi dünyasını bir araya getirerek bir savunma politikası geliştiren İsrail Ulusal Siber Bürosu[14] (INCB)'dur (Kara, 2013: 64). 2015 yılında yapılan düzenlemeler ve siber güvenliğin operasyonel koordinasyonunu güçlendirmek adına Ulusal Siber Güvenlik Otoritesi[15] (NCSA) kurulmuştur. Ulusal Siber Bürosu ve Ulusal Siber Güvenlik Otoritesi'nin üzerinde bir yapı olarak da Ulusal Siber Direktörlük[16] (Ma'arach) kurulmuştur. Siber güvenlik ile doğrudan ilişkili olan İsrail Ulusal Siber Bürosunun siber güvenlik ile ilgili temel görev ve amaçları şu şekilde sıralanabilecektir (RN3611, 2011):

- Yılda bir kez ulusal siber güvenlik tehditlerini yenilemek ve tanımlamak.

- Siberuzay ve bilgisayar sistemlerine ilişkin araştırma ve geliştirme faaliyetlerine destek olmak.

- İsrail'deki siber endüstriyi teşvik etmek için çalışmalarda bulunmak.

- Siberuzayda meydana gelecek acil durumlardaki kontrolü sağlamak için ulusal bir konsept belirlemek.

- Ülkede siber güvenlikle alakalı olan tüm topluluklardan, siber güvenlik istihbaratı toplamak.

- İlgili tüm birimlerden siber güvenlikle alakalı durum bilgisi almak.

---

[13] Uzun yazılımı, Command, Control, Commonications, Computers, Intelligence, Türkçesi, Komuta, Kontrol, Haberleşme, Bilgisayar ve İstihbarat.
[14] Israel National Cyber Bureau.
[15] National Cyber Security Authority.
[16] National Cyber Directorate.

- Yurt dışındaki alternatif kurumlarla siber güvenlik işbirliği için gereken zemini sağlamak.

- Devlet kurumlarında, akademide, endüstride, özel sektörde yer alan, siber güvenlikle ilgili tüm kurum ve kuruluşlar arasında koordinasyon ve işbirliği sağlamak.

- Ulusal bir siber güvenlik kalkanı oluşturmak.

- Siber savunmada ortaya çıkacak aksaklıklara karşı çözüm mekanizmaları oluşturmak.

Görüldüğü üzere İsrail Ulusal Siber Bürosunun ülke siber güvenliği için rolü bir hayli kapsamlıdır. Siber güvenliğe ait bilgi toplama, düzenlemeler yapma, kurumlar arası işbirliği ve koordinasyona bütünleştirici katkı sağlama gibi kritik görevler bu büronun görev tanımı içerisinde yer almıştır. Diğer yandan 2015 yılında Siber Güvenlikte Devletin Lider Rolünün Artırılması ve Ulusal Düzenlemenin Sağlanması (RN2443, 2015) kararıyla devletin siber güvenlik konusundaki düzenlemelerin uygulanmasında hem sektöre hem de sivil topluma örnek olması amaçlanmıştır. Bu karar daha önce 2011 yılında alınan ve yukarıda Ulusal Siber Büronun görevlerinin içerisinden sıralandığı 3611 numaralı “Siberuzayda Ulusal Kapasiteyi Geliştirme” kararına ek olarak alınmıştır. Kararda altı çizilmesi gereken noktalar şu şekilde sıralanabilecektir:

- Ekonomiye daha fazla düzenleme getirmeden ancak eldeki düzenlemelerin esnekleştirilmesi güçlendirilmesiyle birlikte özel sektörü ve sivil toplumun da siber saldırılara karşı hazırlıklı hale getirilmesi ve bu yönde tatbikatlar yapılması.

- Ulusal Siber Büro bünyesinde siber güvenlikle ilgili tüm sektörü düzenlemek üzere bir birim kurulması, bu birimin Başbakanlığın bir birimi olan Ulusal Siber Güvenlik Otoritesine bağlı olması.

- Devletin siber güvenlik konusundaki liderliği için, diğer devlet kurumları, yardımcı kurum ve kuruluşlara bir rehber niteliğinde birimin kurulması (YAHAV) ve siber tehditlere karşı merkezi bir kumanda ve kontrol biriminin kurulması (the Governmental SOC).

- Devlet birimlerinde siber güvenlik alanında uzmanlaşılması için direktörlerin görevlendirilmesi, birimlerde siber güvenlik yöneticilerinin seçilerek bu yöneticilerin siber güvenlikle ilgili tehditlerde liderlik yapması.

- Siber güvenlikte devletin liderliğini sağlamak üzere Ulusal Siber Büro direktörüne "Yönlendirici Komite" kurması görevi verilmesi ve bu komite ile devletin, siber güvenlikte diğer aktörlere yönlendirici bir rehber/lider olması.

İsrail, siber güvenliğini sadece devlet içerisinde yaptığı düzenlemeler, uyguladığı politikalarla değil aynı zamanda yaptığı uluslararası anlaşmalarla da sağlamaya çalışmaktadır. İsrail devleti, siber güvenlikte çeşitli atılımlar yaptığı gibi uluslararası işbirlikleri de sağlamaktadır. Bu konuda en büyük müttefiki Amerika olsa da diğer ülkelerle de işbirliği içerisindedir. İsrail tarafından 2013 yılında İtalya ile siber güvenlik konusunda deklarasyon imzalanmış, 2014 Mayıs ayında Japonya ile anlaşma yapılmış, 2014 yılının şubat ayında İsrail AeroSpaces Industries (IAI), Singapur'da Siber Erken Uyarı Sistemleri Araştırma ve Geliştirme merkezi kurulması kararını imzalanmıştır. Söz konusu merkezin, siber erken uyarı sistemleri prototipi üretimi yaparak, ürünlerin Singapur ve dışında pazarlaması planlanmaktadır. Merkezdeki araştırmaların kritik ve acil alanlar olan, siber saldırganların gerçek zamanlı olarak tespit edilmesi, siber geo-location18 çözümleri ile siber saldırganların fiziksel lokasyonunun belirlenmesi, ileri düzey tespit sistemleri, gibi projeler üzerinde yoğunlaşması öngörülmektedir (Sanalp, 2016: 17).

Kritik altyapılar konusu da İsrail'in siber güvenliğin bir unsuru olarak önem verdiği konulardan biridir. Devletin 2000'li yılların başındaki siber güvenlik politikasında, kritik altyapılara ilişkin "merkeziyetçi" bir tutum izlenmektedir. Daha sonraki yıllarda ise bu sorumluluk siber güvenlik konusunda uzman kurumlara paylaştırılmış ve bu paylaşımlı sorumluluğun izleyici ve denetleyicisi olarak yukarıda bahsi geçen Yönlendirici Komite belirlenmiştir. Bu komite politikanın genel perspektifini belirlemektedir. Bu komitenin yanında, politikaların uygulanmasında bir rehber olacak ve aynı zamanda kritik altyapıları "kullanıcı" olarak işleten ya da dolaylı olarak kritik altyapılar üzerinden iş yürüten taraflara sorumluluklar yükleyen "ulusal birim" kurulmuştur (Tabansky ve Israel, 2015: 35). Kritik altyapıların güvenliğini sağlamak üzere kurulan birimlerden birisi de Ulusal Bilgi Güvenliği Kurumu[17] (NISA)'dur (Housen-Couriel, 2017: 11). Bu kurum özellikle bilgisayar tabanlı bilgi sistemleri ile yine bilgisayar tabanlı kritik altyapı yönetim sistemlerinin güvenliğini sağlamaya yönelik bir fonksiyona sahip olarak düşünülmüştür.

İsrail'in siber güvenlik politikasına genel olarak bakıldığında ülkenin politikasının, askeri ve sivil savunma unsurlarının siber güvenlik etrafında birleşmesi, ülke çapında siber güvenlik tehditlerine karşı her daim hazırlıklı olunması, siber saldırılara cevap verilmesinde operasyonel gücün beslenmesi, akademik kuruluşların siber güvenlik konusunda araştırmalar yaparak devlete katkıda bulunmaları ve özellikle de siber güvenliğin sağlanmasında kamu-özel işbirliğinin sağlanması (Raska, 2015: 11) ilkeleri etrafında şekillendiğini söylemek mümkündür. Çalışmada ele alınan diğer ülkelerle kıyaslandığında, İsrail'in tüm ülkelerden daha önce siber güvenlikle ilgili çalışmalara önem vermeye başladığı görülmektedir (2000'li yılların başları). Diğer yandan ülkede siber güvenliğin sağlanması, kritik altyapıların korunması konularında kurulan birimler diğer

[17] National Information Security Agency.

ülkelerdeki denk birimlerine göre daha ayrıntılı yapılanmışlardır. Siber güvenlik için yukarıda ele alınan Ulusal Siber Güvenlik Bürosu, Ulusal Siber Güvenlik otoritesi ve Direktörlüğü altında yer alarak farklı görevler yüklenmiş, kritik altyapılar için hali hazırda var olan Ulusal Bilgi Güvenliği Kurumu ve Yönlendirici Komite görevler üstlenmiştir. Diğer yandan ülke, siber güvenlik ile ilgili birçok özel şirketi desteklemiş, bu alanda dışarıdan yatırımlar alarak siber güvenlik özel sektörünü bir hayli geliştirmiştir. Böylesine gelişen özel sektörün ürettiği siber güvenlik bilgi kaynağının, kamu-özel sektör ortaklıklarıyla, devletin siber güvenliğine ve siber güvenlik politikalarına olumlu etki ettiği düşünülmektedir. Diğer yandan, yabancı yatırımın ülkeye bu firmalar aracılığıyla girmesi ve siber güvenlik gibi önemli bir konu üzerine çalışan bu firmaların ülke dışı yatırımcılarının bulunması ise bir risk olarak değerlendirilebilecektir.

Başlık altında ele alınan pratik deneyimleri sonucu ve siber güvenlik alanına yaptığı büyük yatırımlar dolayısıyla İsrail, siber tehditlere karşı en hazır ülkelerden biri konumundadır. Ülkede siber güvenlik hükümet ve vatandaşların ortak bir faaliyeti ve sorumluluğu olarak görülmektedir. İnter ağını büyük oranda izleme yetisine sahip olan ülke, kendi kritik işlemlerini yaptığı ağı ise internet ağından ayrı olan bir Ethernet ağında yürütmekte ve sistemlerini dışa karşı korunaklı hale getirmektedir. İnternet üzerinden gelebilecek siber tehditlere karşı kendini kapamış ve kritik ulusal sistemlerinin güvenliğini sağlamıştır (Yılmaz ve Sağıroğlu, 2013: 327-328). Tüm bu yönleriyle İsrail'in siber güvenliğe gösterdiği ilgi ve önem siber güvenlik çalışma alanı açısından dikkat çekici niteliktedir.

3.7. ALMANYA'NIN SİBER GÜVENLİK POLİTİKASI

Almanya'nın ulusal güvenlik anlayışı özellikle son 10 yılda dönüşüme uğramıştır. Bu dönüşümde, ülkenin dış politika anlayışındaki değişim etkili olmuştur. Ülke, özellikle Soğuk Savaşın sona ermesinden bu son 10 yıla kadar daha durağan, kendi vatandaşlarının güvenliğini ve iç huzurunu sağlamaya yönelik bir güvenlik politikası uygulama anlayışına sahip olmuştur. Dünya siyaset arenasında liderliğe yönelen bir ülke olmamıştır (Kıratlı, 2016: 213). Son yıllarda ise Almanya, dış politikada uluslararası barışa katkıda bulunmak üzere daha müdahaleci ve dışa açık bir rol üstlenmiş (Schockenhoff, t.y.: 1; Şahin, 2017: 13) böylece kendi ulusal güvenliğine gelebilecek tehditleri (terör, siber terör vb.) de artırmıştır. Edindiği bu misyon ve dünya arenasında yer aldığı bu konum itibarı ile Almanya'nın ulusal güvenlik anlayışı şu 7 ilke etrafında özetlenebilecektir (WP, 2016: 24-25):

- Vatandaşların güvenliğini sağlamak, ülkenin egemenliğinin ve toprak bütünlüğünün korunması.

- Müttefik ülkelerin vatandaşlarının güvenliğinin, toprak bütünlüğünün ve ulusal egemenliklerinin sağlanması.

- Kurallara dayalı olan ulusal düzeni, uluslararası hukuka uygun olarak korumak.

- Özgür ve engelsiz bir dünya ticaretinin yanında, güçlü bir Alman ekonomisi temelinde vatandaşların refahının sağlanması.

- Dünya genelindeki sınırlı kaynakların adil ve sorumluca kullanımını teşvik etmek.

- Avrupa Birliği entegrasyonunu derinleştirmek ve Transatlantik ortaklığını güçlendirmek.

Görüldüğü gibi Almanya'nın siber güvenlik anlayışı da son yıllarda değişen dış politika anlayışının etkisinde ülke sınırlarını aşarak, müttefiklere ve hatta tüm dünyaya yayılan bir seyir izlemiştir. Bundan önceki dönemlerde Dünya Savaşları ve Soğuk Savaş döneminde daha sınırları içinde ve kendi ulusal güvenliğini odak alan bu anlayış değişmiştir. Konuya siber güvenlik açısından bakıldığında ise Almanya'nın bu dışa açık ulusal güvenlik politikasının, siber güvenliğe ne şekilde yansıdığı da alanda yapılacak başka çalışmalar için iyi bir araştırma sorusu sayılabilecektir.

Ülkenin siber güvenlik stratejisi büyük oranda Alman ordusu tarafından belirlenmektedir. Fakat siber güvenliğin geniş kapsamı ve siber tehditlerin yönün ve büyüklüğünün belirsizliği nedeniyle birçok uluslararası kuruluşla da işbirliği içerisindedir. Bunlara örnek olarak AB, Avrupa Konseyi, BM, NATO, G8 ve AGİT verilebilecektir (SGR, 2012: 33).

Almanya'da bilgi güvenliği adına yapılan çalışmalar siber güvenlik kavramının ortaya çıkmasından çok daha öncelere dayanmaktadır. İkinci Dünya Savaşı sırasında Nazi Almanyası tarafından kullanılan ve Enigma adı verilen aygıt, Alman askerlerinin birbirleri ile haberleşmelerini şifreleyen, bunun yanında diğer ülkelerin birbirlerine gönderdikleri bilgileri de deşifre etmeye yarayan bir şifre makinesi olarak tarihe geçmiştir. Aygıtın zamanının şartlarına göre kırılması oldukça zor bir şifreleme algoritmasının olması ve bu algoritmanın karşı devletlerce kırılması savaşın seyrini değiştirir nitelikte olmuştur (Güngör, 2015: 26).

Teknolojinin hızla gelişmesi ve fiziki savaşın yavaş yavaş yerini siber savaşa bırakması nedeniyle ülkeler, gelişmişlik seviyeleriyle doğru orantılı olarak artan siber saldırılara ve siber saldırı girişimlerine maruz kalmaktadır (Kasapoğlu, 2017). Örneğin, Almanya Silahlı Kuvvetleri'nin bilgisayar sistemlerine 2017 yılının yalnızca ilk iki ayında 284,000 siber saldırı gerçekleştirildiği ilgili birimlerce belirtilmiştir (Politico, 2017). Siber ataklara oldukça fazla maruz kalan Almanya, saldırılara karşı

almakta olduğu ve alacağı önlemleri Federal İçişleri Bakanlığı tarafından hazırlanan” Enformasyon Altyapı Savunması İçin Ulusal Plan" başlıklı belgede bir araya getirmiştir ve belirlenen bu ulusal plan "Enformasyon Üyeliğinden Sorumlu Federal Ofis" (BSI) (Bundesamt für Sicherheit in der Informationstechnik) tarafından yürütülmektedir. 13 Haziran 2005 tarihinde Federal Kabine tarafından kabul edilen ve siber ataklara karşı koyabilmek adına oluşturulan ulusal planın 3 stratejik hedefi bulunmaktadır. Bu hedefler şu şekilde sıralanmaktadır (TBMM, t.y.: 761):

- *Önleme:* Kullanılan teknolojilerin ve enformatik altyapının korunması adına gerekli tedbirlerin alınması.

- *Hazırlıklı Olma:* Gelebilecek saldırılara daha etkili cevap verebilmek adına ulusal planın yürütüldüğü birim tarafından Enformasyon Teknolojisi Kriz Müdahale Merkezi’nin kurulması ve bu merkezin ulusal bir kontrol ve analiz birimi haline gelmesi.

- *Sürdürülebilirlik:* Devlet içerisinde alınan önlemlerin yeterli olmaması sebebiyle halkın ve özel sektörün de bilgilendirilmesi ve ülke genelinde siber güvenliğin önemine dair bir bilinç oluşturularak bireysel önlemlerin alınmasına halkın teşvik edilmesi.

Almanya, siber güvenlik konusunda daha çok yeni kurumsal yapılar oluşturma ve yasal düzenlemeler gerçekleştirmeye ağırlık veren bir politika izlemektedir. Kritik altyapıların korunmasına yönelik olarak bilişim teknolojileri güvenliğinin güçlendirilmesi, ulusal siber müdahale merkezinin kurulması ve ulusal siber güvelik konseyinin oluşturulması, federal kurumlardaki personelin eğitim ve gelişiminin sağlanmasını ulusal siber güvenlik strateji belgesine dâhil etmiştir. Ayrıca siber olaylara karşı kullanacakları müdahale araçlarının yerli olması da politikasının bir parçasıdır (Küçüksille, vd, 2013: 3). Almanya’nın siber güvenlik konusunda

oluşturduğu söz konusu belgeler ve kurumlar kronolojik olarak ele alınacak olursa, bunlardan ilki 1989 yılında bilgi güvenliği alanında yayınlanan Ulusal Politika belgesidir. Bunun ardından 2005 yılında Bilgi Güvenliği ve Kritik Altyapıların Korunmasına İlişkin Ulusal Strateji Belgesi yürürlüğe girmiştir. 2011 yılında yürürlüğe giren Alman Ulusal Siber Güvenlik Stratejisi ise özellikle siber uzaydan kaynaklanan risk ve tehditler ile mücadele amacına yoğunlaşmıştır. Almanya'nın siber güvenliğinin sağlanmasında rol oynayan temel yapı olan Alman Federal Bilgi Güvenliği Örgütünün birimleri, ülkenin siber güvenlik konusunda uzmanlaşmacı bir politika izlediğini göstermektedir. Söz konusu örgütte, Siber Güvenlik Dairesi, Kriptoloji Dairesi, Güvenli Elektronik İşlemler Sertifikasyon ve Standardizasyon Dairesi, Profesyonel Ağ Savunma Birimi gibi birimler bulunmaktadır (Tuluk ve Seferoğlu, 2016). Bilgi Güvenliği Federal Ofisi (BSI), ülkedeki siber güvenlik ve kritik altyapıların korunması çalışmalarının koordinasyonundan sorumlu olan kurumdur. İlgili diğer kurumlar ise, Siber Güvenlik Müdahale Merkezi ve Siber Güvenlik Konseyidir.

Almanya Siber Güvenlik Strateji Belgesi ve Siber Güvenlik Yasası ile kritik altyapıları işleten kuruluşlara bir takım uyulması gereken bilgi teknolojileri güvenlik zorunlulukları getirmiştir. Bu zorunluluklar şu şekilde özetlenebilir (TBD, 2015: 26):

- Kritik altyapıların işlevselliği için gerekli olan bilgi teknolojileri sistemi bileşen ve süreçlerinin korunması için gereken tedbir ve önlemlerin iki yıl içerisinde uygulanması.

- Güvenlik denetimlerinin en az iki senede bir olmak üzere düzenli bir şekilde yapılması ve bu denetimler sonucu oluşturulacak raporların Bilgi Güvenliği Federal Ofisine iletilmesi.

- Kritik altyapılar üzerinde gözlenen güvenlik olaylarının Bilgi Güvenliği Federal Ofisine bildirilmesi.

Almanya'nın siber güvenliğine ilişkin İngilizce ya da Türkçe alan yazınında fazlaca kaynak bulunmamaktadır. Ancak İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsünün Türkçe olarak hazırladığı "Siber Güvenlik Raporu" (SGR, 2012). Almanya'nın siber güvenlik politikasının üzerine odaklandığı 10 stratejik alanı kapsamlı bir şekilde ele almıştır. Bu alanlar, kısaca şu şekilde özetlenebilecektir:

- *Kritik Bilgi Altyapılarının Korunması:* Siber güvenlik, neredeyse tüm kritik altyapıların en önemli bileşeni haline gelmiştir. Bilgi teknolojilerinde yaşanacak olası krizlerde belirli uyum kurallarının gerekliliğini incelemek, bilgi paylaşımında kamu ve özel sektör arasında daha iyi bir koordinasyon oluşturulması hedeflenmiştir.

- *Ülkede Güvenli Bilgi Teknolojileri Sistemleri:* Vatandaşlar ve KOBİ'ler tarafından kullanılan iç sistemler için de daha güvenli bir altyapı oluşturulmalıdır. Kullanıcılar bilgi teknolojilerindeki riskler ve güvenlik konusunda bilgilendirilmelidir. Devlet, internet sağlayıcılarının kullanıcılara sunduğu hizmetlerin güvenlik denetimlerini de gerçekleştirmelidir. Bu güvenliğin desteklenmesi için Ekonomi ve Teknoloji Federal Bakanlığı ve sanayinin katılımı ile bir görev gücü kurulmuştur.

- *Kamu Yönetiminde Bilgi Teknolojileri Güvenlik Güçlendirilmesi:* Kamu Yönetimi bilgi teknoloji sistemlerinin korunması artırılacak, devlet yetkilileri bu konuda rol model olarak hizmet edecektir. Federal yönetimin de kendi güvenli ağ altyapısını oluşturması gerekmektedir. Bilgi teknolojileri ile ilgili kaynakların merkezi ve yerel düzeyde uygun olarak dağıtılması gerekmektedir.

- *Ulusal Siber Müdahale Merkezi:* Tüm devlet kurumları arasında operasyonel iş birliğinin oluşturulması ve siber güvenliğin sağlanması için Ulusal Siber Müdahale Merkezi kurulacaktır. Bilgi teknolojilerinin SWOT analizleri ile hızlı ve yakın bilgi

paylaşımı için bu merkez etkin tavsiyeler verecektir. Ayrıca merkez, düzenli olarak ve belirli olaylar için Ulusal Siber Güvenlik Konseyine öneriler sunacaktır.

- *Ulusal Siber Güvenlik Konseyi:* Bu konsey, önleyici araçları ve kamu ve özel sektör arası siber güvenlik yaklaşımlarını koordine etmek için tasarlanmıştır. Konseyin amacı stratejik düzeyde, siber güvenlik alanında bilgi teknolojileri planlama kurulu iş yönetimini tamamlamak olacaktır.

- *Siberuzayda Etkili Suç Kontrolü:* Siber suçların kontrolünde, kolluk kuvvetleri ile Federal Dairenin yeteneklerinin güçlendirilmesi gerekmektedir. Yapısal zayıflıkları olan ortak ülkelere de bu konuda destek sağlanması planlanmaktadır.

- *Avrupa'da ve Tüm Dünyada Siber Güvenlik Sağlamak İçin Etkili Koordine Eylemleri:* Bu hedef, başlıkta daha önce de ifade edilen, Almanya'nın güvenlik anlayışının uluslararasılaşmasının bir sonucu olarak göz çarpmaktadır. BM, OSCE, OECD ve NATO gibi uluslararası örgütler ile siber güvenlik politikalarının uyumlu hale getirilmesi amaçlanmaktadır.

- *Güvenilir ve Sağlam Bilgi Teknolojileri Kullanımı:* Güvenilir bilişim sistemlerinin ulaşılabilirliği sürekli olarak sağlanmalıdır. Güvenlik için yenilikçi koruma planlarının sosyal ve ekonomik açıları da dikkate alınarak ele alınması desteklenmelidir.

- *Federal Makam ve Mercilerde Personel Gelişimi:* Devlet kurumlarında siber güvenlik için ek bir kadroya ihtiyaç olup olmadığı saptanmalıdır. Mevcut personele gereken eğitimler verilmelidir.

- *Siber Saldırılara Cevap Vermek İçin Araçlar:* Siber saldırılara karşı cevap verebilmek için koordineli ve kapsamlı araçlar bütünü yetkili devlet makamlarının iş birliği ile kullanılmalıdır. Gerekli hallerde ek kanuni yetkilerin oluşturulması gerekip gerekmediği şimdiden incelenmelidir.

Görüldüğü üzere Almanya siber güvenlik konusuna bir hayli titiz yaklaşmakta ve politikalarını hem siber güvenlik hem de kritik altyapılar üzerinde ayrı ayrı şekillendirerek, hukuki düzenlemeler ve kurumsal altyapı zeminini sağlam tutarak oluşturmaktadır. Süreç olarak ülkenin siber güvenlik çalışmalarının çok eski dönemlere dayandığı söylenemez ancak, oluşturulmaya çalışılan kurumsal altyapı ile siber güvenlik ve kritik altyapıların korunması konularında belirlenen strateji ve hedeflerin çok detaylı ve sistematik bir şekilde ele alındığı göz çarpmaktadır. Bu durum, özellikle siber güvenlik konusunda çalışmalara daha yakın dönemlerde başlayan ülkeler açısından siber güvenliğe ilişkin kurumsal altyapının oluşturulması ve siber güvenlik politika üretiminde göz önünde bulundurulacak stratejik konuların belirlenmesi konusunda ilham verici nitelikte olabilecektir.

4. BÖLÜM: TÜRKİYE'DE SİBER GÜVENLİĞİN HUKUKİ VE KURUMSAL DAYANAKLARI

Türkiye'de, hem siber güvenlik konusundaki farkındalığın yukarı yönlü ivme kazandığı yıllarda gerçekleştirilen ilk devlet tabanlı girişimler olmaları, hem de süregiden dönemde üretilen siber güvenlik politikalarına yön vermeleri dolayısıyla, siber güvenlikle doğrudan ya da dolaylı olarak ilgili olan hukuki düzenlemeler, çalışma açısından son derece önemlidir. Bu yüzden söz konusu belgeleri incelemek ve siber güvenlik politikalarına verdikleri yönü anlamaya çalışmak, genel anlamda Türkiye'nin siber güvenlik politikalarını analiz etmek için iyi bir başlangıç noktası olacaktır.

Türkiye'de siber güvenlik konusunda yasal düzenlemeler, özellikle siber güvenliğe odaklı olan bir düzenleme olarak Bakanlar Kurulu'nun 11/06/2012 tarihli, 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"ın 20/10/2012 tarihli, 28447 sayılı Resmi Gazete'de yayınlanarak yürürlüğe girmesi ile başlamıştır. Bu kararın yürürlüğe girmesinden önce Türkiye'de siber güvenlikten sorumlu olan kurum TUBİTAK iken, bu kararın yürürlüğe girmesi ile birlikte siber güvenlikten sorumlu olan kurum Ulaştırma, Denizcilik ve Haberleşme Bakanlığı olmuştur (Bıçakçı, vd., 2016: 35). Söz konusu Karar ile Siber Güvenlik Kurulu kurulmuş olup, Siber Güvenlik Kurulu ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığının görev ve yetkileri belirlenmiştir. Dönemin Ulaştırma, Denizcilik ve Haberleşme Bakanı Binali Yıldırım, Siber güvenlik Kurulunun amacını "ülkenin kritik altyapıları başta olmak üzere kişilere ve kurumlara yönelik olası saldırılara karşı tedbir almak, farkındalık oluşturmak. Buna rağmen herhangi bir saldırı sonucu hasar meydana gelirse bunun zararlarını asgariye indirmek" olarak belirtmiştir. Diğer yasal düzenleme ise Siber Olaylara Müdahale Ekiplerinin Kuruluş Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ'dir. Diğer yandan, 2008 yılında yürürlüğe giren 5809

Sayılı Elektronik Haberleşme Kanunu da bu konudaki yasal düzenlemeler arasında gösterilebilecektir.

4.1. ULUSAL SİBER GÜVENLİK ÇALIŞMALARININ YÜRÜTÜLMESİ, YÖNETİLMESİ VE KOORDİNASYONUNA İLİŞKİN KARAR

Siber güvenliğe odaklı olan bir düzenleme olarak Bakanlar Kurulu'nun 11/06/2012 tarihli, 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"ın 20/10/2012 tarihli, 28447 sayılı Resmi Gazete'de yayınlanarak yürürlüğe girmesi, Türkiye'deki elektronik haberleşmeye yönelik temel kanun olan 5809 Sayılı Elektronik Haberleşme Kanunu'nun siber güvenlik odağında güncellenmesi anlamına gelmektedir. Kararın önemli getirilerinden birisi de siber güvenlik ile ilgili alınacak önlemlerin belirlenmesi, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını, koordinasyonunu sağlamak amacıyla (Karar3842, md.4) kurulan Siber Güvenlik Kuruludur.

Siber Güvenlik Kurulu, üyelerin konum ve yetkileri gereği de üst düzey temsil bakımından önemli bir kuruldur. Kurul, Ulaştırma, Denizcilik ve Haberleşme bakanı başkanlığında, Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genel Kurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme bakanının belirleyeceği bakanlıkların ve kamu kurumlarının üst düzey yöneticilerinden oluşmaktadır.

2012/3842 sayılı Bakanlar Kurulu Kararı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na siber güvenliğe ilişkin olarak aşağıdaki görevler verilmiştir (Karar3842, md.5):

. Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak.

· Kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasları hazırlamak.

· Ulusal Siber Güvenliğin sağlanmasında kamu kurum ve kuruluşlarında teknik altyapının oluşturulmasını takip etmek, uygulamaların etkinliğinin doğrulanmasını ve test edilmesini sağlamak.

· Ulusal bilgi teknolojileri ve iletişim altyapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik altyapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik çalışmalar yapmak.

· Ulusal Siber Güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretilmesini teşvik etmek, kullanımını sağlamak.

· Ulusal Siber Güvenlik açısından kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini, eğitimi ve gelişimini Türkiye'de Siber Güvenlik ve Nükleer Enerji / 38 planlamak, koordine etmek ve yürütmek.

· Bu Karar çerçevesinde diğer ülkeler ve uluslararası kuruluşlarla işbirliği yapmak.

· Ulusal Siber Güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek.

· Bilgi güvenliği alanında eğitim, test ve çözüm üretme alanında çalışan gerçek ve tüzel kişilere usul ve esaslarını belirleyerek güvenlik belgesi vermek.

· Siber Güvenlik Kurulunun sekretarya hizmetini yürütmek.

Görüldüğü üzere çıkarılan kararname, siber güvenlik adına somut çalışmaların yürütüleceği bir kurulu oluşturduğu gibi aynı zamanda ilgili bakanlığa da siber güvenlik konusunda spesifik görevler yüklemektedir. Bu açıdan kararname, Türkiye açısından siber güvenlik algısının politika düzleminde oluştuğunun bir göstergesi sayılabilecektir. Aslında söz konusu algı, siber güvenlik oluşumunu bütünüyle içermese de, "bilgi güvenliği" konusunda henüz 1990'lı yılların sonu ve 2000'li yılların başından itibaren oluşmaya başlamıştır. Bunun en büyük göstergesi ise Milli Savunma Bakanlığı'nın koordinasyonluğunda, Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı ile kurulması amaçlanan ancak hayata geçirilemeyen Ulusal Bilgi Güvenliği Teşkilatı girişimidir. Bıçakcı ve arkadaşlarının (2016: 32) belirttiği üzere, ilgili kanun taslağı Başbakanlık altında, ülkenin bilgi güvenliği politikalarını yönetmekle sorumlu Başbakan, Adalet, Milli Savunma, İçişleri, Dışişleri, Ulaştırma, Sanayi ve Ticaret Bakanları ile Milli Güvenlik Kurulu Genel Sekreteri, Genel Kurmay Muharebe Elektronik ve Bilgi Sistemleri Başkanı, Milli İstihbarat Teşkilatı (MİT) Müsteşarı ve TÜBİTAK'ın oluşturacağı bir Ulusal Bilgi Güvenliği Üst Kurulu'nun kurulmasını öngörmüştür. Tasarı aynı zamanda Ulusal Bilgi Güvenliği Kurumu Başkanlığı'nın kurulmasını da tasarlamıştır. Bu başkanlık taslak olarak Plan Program ve Koordinasyon, Bilgi Güvenliği, Kriptoloji, Bilgi Destek ile Denetleme ve Bilgilendirme Daire Başkanlıkları şeklinde bir organizasyon yapısında oluşturulmuştur. Söz konusu öngörüleri somutlaştıracak yasa tasarısının 2003 yılı ortalarında onanması öngörülmüş ancak söz konusu tasarının son halinde uzlaşılamaması üzerine tasarı rafa kaldırılmıştır. Kurulun

öngörülen üyeleri ele alındığında, dönemin mevcut bakanlıkları ve devlet kurumları da düşünüldüğünde, Siber Güvenlik Kurulu ile büyük oranda benzeştiği göze çarpmaktadır. Siber güvenlik kurulunda farklı olarak, 2006 yılında kurulup 2016 yılında kapatılan Telekomünikasyon İletişim Başkanlığı ile 2000 yılında kurulan Bilgi Teknolojileri ve İletişim Kurumu tasarlanan Ulusal Bilgi Güvenliği Teşkilatında yer almamaktadır. Diğer yandan, teşkilatın Milli Savunma Bakanlığının koordinasyonu altında ve Başbakanın başkanlığında düşünülmesi, bilgi güvenliğinin direkt olarak genel savunma fonksiyonunun içinde algılandığına işaret etmektedir. 2012 yılında kurulan Siber Güvenlik Kurulu ise Ulaştırma, Denizcilik ve Haberleşme Bakanlığı koordinasyonunda kurulmuştur ve başkan olarak ise bu bakanlığın bakanı belirlenmiştir. Bu yönüyle Siber Güvenlik Kurulunda siber güvenlik algısının daha özel bir platformda konumlandırılıp, yetkinin daha spesifik bir uzmanlık alanına (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı) bırakıldığını söylemek mümkündür.

4.2. 5809 SAYILI ELEKTRONİK HABERLEŞME KANUNUNA SİBER GÜVENLİK EKLERİ

Bir önceki başlıkta detaylı olarak incelenen Bakanlar Kurulu Kararı'nın içeriği, 06/02/2014 tarihinde yayımlanan 6518 sayılı kanun ile 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'na ilave edilen Ek Madde 1 ile kanunlaştırılmış, 5809 sayılı Elektronik Haberleşme Kanunu'na ilave edilen ek fıkralar ile Bilgi Teknolojileri ve İletişim Kurumu'na siber güvenlik ile ilgili yeni görevler verilmiştir (BTK, 2017).

Şüphesiz ki kanuna eklenen en somut düzenlemelerden birisi Siber Güvenlik Kuruluna ilişkin maddedir. Ek madde 1'de yer alan düzenlemeye göre Siber Güvenlik Kurulunun görevleri şu şekildedir (kurulma amacı kanunda geçtiği şekliyle bir önceki başlıkta verilmiştir):

a) Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak.

b) Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak.

c) Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek.

ç) Kanunlarla verilen diğer görevleri yapmak.

Kurulun görevlerinden anlaşılacağı üzere, siber güvenlik politikalarındaki önemi büyüktür. Alınacak kararlar, izlenecek strateji ve politikalar bu kurumun onayından geçmekte ve karara bağlanmaktadır. Diğer yandan araştırmanın önceki bölümlerinde bahsi geçen ve siber güvenliğin önemli unsurlarından biri olan kritik altyapıların belirlenmesine ilişkin kararlar da bu kurul tarafından alınmaktadır. Öyleyse Siber Güvenlik Kurulu, gelinen noktada Türkiye için siber güvenlik politikaları belirleme açısından merkezi bir aktör olarak gösterilebilecektir.

Kanuna yapılan bir önemli ekleme ise Bilgi Teknolojileri ve İletişim Kurumunun görev ve yetkileri arasına siber güvenlikle ilgili olarak “Siber güvenlik ve internet alan adları konularında Bakanlar Kurulu, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek” İbaresi (v bendi olarak) eklenmiştir. Eklenen düzenlemeden anlaşılacağı üzere siber güvenlik politikası üretim sürecinde alınacak olan politika kararlarının yürütme mekanizması olarak Bilgi Teknolojileri ve İletişim Kurumu belirlenmiştir. Söz konusu düzenlemeye benzer bir şekilde fakat daha kapsamlı olarak yapılan bir diğer önemli düzenleme ise sayılı Elektronik Haberleşme Kanununun 5. maddesinin birinci fıkrasına eklenen “h” bendidir. Bu düzenleme ile Ulaştırma Denizcilik ve Haberleşme Bakanlığına, bir önceki başlıkta yer verilen siber güvenlik ile ilgili görevler verilmiştir. Verilen b görevler ile bakanlığın görevleri arasına ilk kez siber güvenlik kavramına ilişkin fonksiyonlar

eklenmiş, geçmiş yıllarda Milli Savunma Bakanlığı üzerinde düşünülen siber güvenlik fonksiyonları da bu bakanlığa devredilmiştir. Böylece Türkiye'nin siber güvenlik politikalarında yetkili en üst merkezi aktörü de Ulaştırma Denizcilik ve Haberleşme Bakanlığı olmuştur.

Görüldüğü üzere Türkiye'nin siber güvenlik konusundaki hukuki altyapısı henüz 2000'li yılların başında kurulmaya çalışılsa da, bu çaba somut bir sonuç ortaya koymamış, ülke siber güvenlik alanındaki hukuki düzenlemeleri ancak 2012 yılından itibaren hayata geçirebilmiştir. Düzenlemeler sonrası var olan kurumlara siber güvenlik ile ilgili yeni görev tanımları getirilmiş ve siber güvenlik konusunda yeni görevler üstlenecek yeni kurumlar oluşturulmuştur. Bu durumda, siber güvenliğin dünya arenasında yakaladığı gündem, gerçekleşen siber saldırılar ve siber olaylar sonrasında dünya devletlerinin konuya olan ilgisinin artması etkili olmuştur. Çalışmanın bir sonraki başlığında ise yapılan bu düzenlemelerle birlikte kurulan Siber Güvenlik Kurulunun yaptığı toplantılar, Ulusal Siber Güvenlik Stratejisi ve Eylem Planları ile kurulun verdiği kararlarla oluşturulan Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Siber Olaylara Müdahale Ekibi (SOME) incelenecektir.

4.3. ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ (USOM)

Türkiye'nin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerini azaltılması ya da ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur (USOM, 2017). Bu oluşum, kamu kurum ve kuruluşları ile özel sektör kuruluşlarında kurulacak olan Siber Olaylara Müdahale Ekiplerinin (SOME) koordinasyon ve merkez birimi olarak düşünülebilir. Bu başlık altında USOM hakkında genel bilgi verilecektir.

Çalışmanın ilerleyen bölümlerinde, merkezin Türkiye'nin siber güvenlik politikalarındaki yeri daha detaylı ele alınacaktır.

Sektörel SOME'ler söz konusu sektörü düzenleyip denetleyen kurumların bünyesinde bahse konu sektörde yer alan kurum, kuruluş ve işletmeleri içine alacak biçimde oluşturulur. Gerek duyulması halinde, ilgili bakanlık bünyesinde farklı sektörlerde sektörel SOME kurmak mümkündür. Stratejik önemi haiz işkolları ile kritik önem taşıyan sektörlerde, sektörel SOME kurulması ise zorunludur. Söz konusu sektörlerin hangileri olduğu Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından belirlenir ve belirlenen bu sektörler yine kurum tarafından güncellenir. Diğer yandan Kurumsal SOME'ler, kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber hücumlara karşı gereken tedbirleri almak ya da aldırmak, bu olaylara müdahale geliştirebilecek mekanizmayı ve olay kayıt sistemlerini kurmak veya kurdurmak ve kurumların bilgi güvenliğini sağlamaya dönük çalışmaları yapmak ya da yaptırmakla sorulu olan ekiplerdir (Türker, 2015: 62). Ülkede bu birimlerin hangi gerekçelerle ne şekilde oluşturulduğunu görmek adına Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Sivil Havacılık Genel Müdürlüğünün SOME'lerin kurulması ile ilgili yayınladığı genelgenin ilgili kısmını ele almakta yarar vardır. Genelgede SOME'lerin kurulmasına dair gerekçe ve süreçler şu şekilde anlatılmıştır:

> *"Kurum ve kuruluşların bilgi ve iletişim sistemlerinde bulunan güvenlik zafiyetleri, bu sistemlerin hizmet dışı kalmasına veya kötüye kullanılmasına, kişisel bilgilerin ifşasına, can kaybına, büyük ölçekli ekonomik zarara, kamu düzeninin bozulmasına ve/veya ulusal güvenliğin ihlaline neden olabileceğinden sektör kuruluşlarının siber güvenlik açıklarının azaltılması amacıyla; - 01/06/2016 tarihine kadar ekli listede yer alan işletmelerde "Kurumsal SOME Kurulum ve Yönetim Rehberi" temel alınarak Kurumsal SOME'lerin kurulumları tamamlanacak ve ekteki "Kurumsal SOME İletişim Bilgileri Formu" eksiksiz doldurularak gereği için Genel Müdürlüğümüze bildirilecektir, - Kurumsal SOME'lerin faaliyetleri (sızma testleri, detaylı ve gerçekçi durum analizi, bilinçlendirme, iletişim, eğitim vb.) "Kurumsal SOME Kurulum ve Yönetim Rehberi" ne ve Ulusal Siber Güvenlik Stratejisi ve*

Eylem Planlarına uygun şekilde yerine getirilecektir, - Siber güvenlik konusundaki ilgili mevzuat, rehberler ve ulusal stratejilere http://udhb.gov.tr/h-12-siber-guvenlik.html adresinden ulaşılabilmektedir. - Kurumsal SOME'lerin "Kurumsal SOME Kurulum ve Yönetim Rehberi" nde belirtilen siber olay öncesi, siber olay esnası ve siber olay sonrası süreçleri titizlikle uygulanacaktır, - 31.12.2016 tarihine kadar kuruluşlar bilişim sistemlerini ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardına uygun hale getirerek ve belgelendirecektir, - Siber güvenliğe ilişkin Genel Müdürlüğümüz Sektörel SOME'si ve USOM tarafından yapılan duyuru ve ihbarlar takip edilerek gerekli önlemlerin alınacaktır, - Kurulacak Kurumsal SOME'lerde Kurumsal SOME Rehberinde yer alan fonksiyonları yerine getirmek üzere kurum/kuruluş içerisinden bir yönetici görevlendirilecek ve: o Mevcut personel içerisinden yeterli sayıda personel görevlendirilecek veya, o Kurumsal SOME hizmetleri hizmet alımı yöntemiyle gerçekleştirilecektir. - Kurum/Kuruluşlardaki Kurumsal SOME birimi raporlarını Kurum/Kuruluşun idari yöneticisine sunar. - Bu genelge kapsamına giren kurum/kuruluş Genelge'ye ilaveten Milli Sivil Havacılık Güvenlik Programı Ek'i olan "Siber Tehditlere Karşı Yapılacak İşlemler Talimatı" 'nda yer alan önlemleri de alır. - Genel Müdürlük Siber Güvenlik tedbirlerini haberli/habersiz denetler/denetletir ve test eder/ettirir. Bu kapsamda, ilgili kurum ve kuruluşlarda Kurumsal SOME birimlerinin ivedilikle kurulması ve Genelge içeriğinde yer alan açıklamalara titizlikle riayet edilmesi, uyulmaması halinde işletmelere Genel Müdürlüğümüzce 2920 sayılı Türk Sivil Havacılık Kanununun 143 üncü maddesi gereğince idari işlem yapılacağı konusunda bilgi edinilmesi hususunda bilgilerinizi ve gereğini önemle rica ederim."

USOM, kurumsal ve sektörel SOME'lere ulusal ve uluslararası seviyede siber ortamda ortaya çıkan tehditler ile ilgili kendisine ulaştırılan ihbarları da değerlendirerek, söz konusu tehditlerin tespit ve bertaraf edilmesi için yönlendirmelerde ve yardımda bulunur, siber güvenlik olayları ile ilgili eğitim ve tatbikatlar düzenler. Merkez bu yönüyle kurumsal ve sektörel SOME'lerin bağlı olduğu ve bu ekiplerin üzerinde yer alan bir birim olarak düşünülebilir.

USOM, 2014 yılında kurulmuş bir yapı olarak günden güne kendisini gerek siber olaylara müdahale fonksiyonlarını geliştirmek suretiyle gerekse SOME'lerini artırarak geliştirmektedir. Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM)'nin yaptığı çalışmada ise 2015 yılında Türkiye'ye Anonymus ve Redhack grupları

tarafından yapılan saldırıya karşı yapılan savunmada USOM'un kriz yönetiminin olmamasından kaynaklana müdahale yetersizliği (Bıçakçı, v.d, 2016) eleştirilmiştir.

5. BÖLÜM: TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARININ KAMU POLİTİKASI ANALİZİ YAKLAŞIMLARI ÇERÇEVESİNDEKİ YÖNELİMLERİ

Çalışmanın bu bölümünde, yapılan araştırmanın sistematiğine, örneklemine, veri toplama tekniği ve süreci ile elde edilen verilerin analiz edilmesi, bulguların elde edilmesi ve değerlendirilmesine ilişkin bilgiler verilmiştir.

5.1. ARAŞTIRMANIN AMACI VE KAPSAMI

Bu çalışmada, Türkiye'nin siber güvenlik politikalarını belirleyen ve belirten resmi belgeler (kalkınma planları, strateji ve eylem belgeleri, hukuki belgeler ve raporlar) incelenerek ve belirli bir yöntem temelinde kodlanarak analiz edilmiştir. Analiz sonucunda Türkiye'nin siber güvenlik politikalarına dair bulgular yorumlanarak söz konusu politikalar, kamu politikası analizi ve karar verme yaklaşımları bağlamında değerlendirilmiştir. Yorumsamalar sonucunda resmi belgelerde belirlenen ve belirtilen, Türkiye'nin siber güvenlik politikalarının hangi yaklaşımlar çerçevesinde şekillendiği belirlenmiştir. İleride üretilecek ve uygulanacak olan siber güvenlik politikalarının, kamu politikası analizi yaklaşımları ve karar verme modelleri kapsamındaki yönelimleri öngörülmeye çabalanmıştır. Bu yönüyle çalışma, Türkiye'nin siber güvenlik politikalarının hangi kamu politikası analizi yaklaşımları çerçevesinde, hangi karar verme modelleri temel alınarak, hangi yönelimlerde (altyapısal, teknolojik, statükocu vb.) olduğunu belirlemeyi amaçlamaktadır. Türkiye'de, yeni bir akademik çalışma alanı olan kamu politikasının kuramsal kısmını yine Türkiye açısından yeni bir kavram olan siber güvenlik ve onun politikalarıyla ilişkilendirerek analiz eden bu multidisipliner çalışmanın, kamu yönetimi alan yazınına katkı sağlayacak bir nitelikte olduğu düşünülmektedir. Araştır

5.2. ARAŞTIRMANIN KISITLARI

Araştırma, veri toplama tekniklerinden doküman analizi tekniği kullanılarak yapılan bir araştırmadır. Araştırmanın ana konusu olan siber güvenlik, ulusal güvenlik açısından ülke için stratejik bir öneme sahiptir. Bu doğrultuda, ülkenin siber güvenlik politikalarına ilişkin kamuoyu ile paylaşılmayan ya da varlığına ilişkin bilgiler verilmeyen belgeler (devlet sırrı niteliğinde belgeler) var ise bu belgeler araştırma kapsamına alınamamaktadır. Dolayısıyla araştırma sonucunda yapılacak olan çıkarsamaların geneli yansıttığı önermesi bu varsayım da hesaba katılarak algılanmalıdır.

5.3. KONU ÜZERİNE TÜRKİYE'DE YAZILAN DİĞER LİSANSÜSTÜ TEZLER

Siber güvenlik, bilim alan yazınında henüz yeni bir çalışma alanı olarak araştırmacıların ilgisini çekmektedir. Çalışmanın önceki bölümlerinde, alan yazını taramasından elde edilerek atıf verilen kitap, makale, araştırma raporu, strateji belgesi, politika belgesi gibi çeşitli kaynaklar olduğu gibi aynı zamanda bu konu üzerine yazılmış yüksek lisans ve doktora tezleri de bulunmaktadır. Bu başlık altında, siber güvenlik üzerine Türkiye'de yazılmış lisansüstü tezleri incelenerek, konunun daha çok hangi disiplinler çerçevesinde ele alındığı saptanacak ve bu çalışmaların içerikleri ele kısaca ele alınacaktır.

Yukarıda belirtildiği üzere siber güvenlik, bilimde yeni bir çalışma alanı olmakla birlikte, Türkiye'de dünya geneline göre çok daha yeni sayılabilecek bir çalışma alanıdır. Yükseköğretim Kurulu (YÖK) Başkanlığının internet sitesinde yer alan tez

veri tabanında yapılan taramaya göre an itibari ile[18] 18 adet lisansüstü teze rastlanmıştır. Yazılan tezlerden biri dışında tümünün yüksek lisans tezi olduğu belirlenmiştir. Tezlerin büyük çoğunluğu Bilgisayar Mühendisliği bölümünde, kayda değer bir kısmı da Uluslararası İlişkiler bölümünde bulunan lisansüstü öğrencileri tarafından yazılmıştır. Kuruma başvuruda bulunan ancak henüz sistemde yer almayan tezlerin sayısı belirlenememekle birlikte, sistemde an itibari ile yer alan ve siber güvenlik terimini başlıklarında içeren tezlerin sayısı oldukça azdır. Aşağıda tezlerin yazıldığı bölüm, tarih, konu ve türünü belirten tablo verilmiştir.

Tablo 5: Türkiye'de Siber Güvenlik Terimlerini Başlığında İçeren Lisansüstü Tezler

Tezin Yazılığı Bölüm	Yıl Aralığı	Sayı/Tür
Bilgisayar Müh.	2012-2106	8 Yüksel Lisans Tezi
Uluslararası İlişkiler	2016	4 Yüksek Lisans/1 Doktora Tezi
Avrupa Birliği Siyaseti	2016	1 Yüksek Lisans Tezi
Strateji Bilimi	2015	1 Yüksek Lisans Tezi
Savunma Kaynakları Yönetimi	2015	1 Yüksek Lisans Tezi
Sosyoloji	2016	1 Yüksek Lisans Tezi
Hukuk	2013	1 Yüksek Lisans Tezi

Kaynak: YÖK Tez Veri Tabanı

Yukarıdaki tabloya göre yazılan tezlerin 7'si bilgisayar mühendisliği, 1'i yine bilgisayar mühendisliğine yakın olan ve bu çalışmada birlikte ele alınacak olan bilgi güvenliği mühendisliği gibi fen bilimleri alanından bir disiplinden yazılırken, geriye kalan 10'u sosyal bilimler alanındaki farklı disiplinlerden yazılmıştır. Siber güvenlik

[18] Tarama 17.07.2017 tarihinde gerçekleştirilmiştir (https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp). Taramada anahtar sözcükler olarak "siber güvenlik" kullanılmıştır. Bu sözcükler dışında başka sözcüğe yer verilmemiş olup, siber güvenlik terimini direkt olarak içeren tezlere ulaşılması amaçlanmıştır.

terimini içeren ilk tez 2013 yılında hukuk disiplini içerisinde yazılmış olup, söz konusu tarih de siber güvenliğin lisansüstü tezlerinde çok yakın bir tarihte yer almaya başladığını göstermekte ve çalışma alanının Türkiye'de çok yeni olduğu fikrini desteklemektedir. Diğer yandan, tezlerin biri dışında tümünün yüksek lisans tezi olması, konunun daha geniş bir araştırma olarak nitelendirilebilecek doktora tezi araştırması kapsamına alınacak nitelikte görülmediğine işaret etmektedir. Yazılan tek doktora tezi ise siber güvenlik tezlerinin daha fazla yapıldığı Uluslararası İlişkiler bölümünde ve 2016 yılında yazılmıştır. Bu tarihten önceki yapılan çalışmaların türü yüksek lisans tezi olup, gelecek yıllarda doktora tezi sayılarının artacağı düşünülmektedir.

Siber Güvenlik terimini başlığında içeren tezlerin, yukarıda yer alan sayısal verilerinin yanında bu tezlerin içeriklerinin de önemli olduğunun altı çizilmelidir. Bu başlığın sonunda yapılacak politika-etki değerlendirmesi için de bu çalışmaların içerikleri önem taşımaktadır. Bu bağlamda, tezlerin içeriklerine kısaca değinmekte yarar vardır.

Bilgisayar mühendisliği alanında yazılan tezlerin daha çok siber güvenliğin teknik boyutlarını irdeleyen bir çizgi izlemesi beklenmesine karşın durum bu şekilde gözlemlenmemiştir. Bu alanda yazılan 8 yüksek lisans tezinden yalnızca üçü teknik boyutları ele alan konular üzerine yazılmıştır. Bunlardan birisi Hoşsucu'nun (2015) yazdığı, siber güvenlikte metinlerin anlamsal olarak yorumlanması ve güvenlik boyutunda kullanımını konu alan tezdir. Diğer bir tezde Filiz'in yazdığı (2013), biyometrik yöntemler ve yüz tanıma problemi üzerinde araştırma yaparak, kullanılan temel yöntemleri inceleyen tezdir. Teknik boyutta yazılan son tez ise Akyıldız'ın (2013) yazdığı ve dijital ortamda depolanan bilgilerin üçüncü şahıslar tarafından ele geçirilmesini önlemek için kullanılan sızma testlerini, bu testlerin başarısı için gereken teknik altyapıyı araştıran tezdir. Bu tezler dışında bölümde yazılan tezler, beklenenin aksine, sosyal bilimler alanında yazılan tezlere benzer olarak sosyal konuları da odak alan tezlerdir. Örneğin Tosun (2015), tezinde siber

saldırıların hedeflerinin yalnızca donanımsal olmadığının, bunun yanında insan zafiyetlerine yönelik saldırılar da olabileceğinin altını çizmiştir. Hackerlar, siber donanım ve yazılımlardan ziyade insan faktörünü ve zaaflarını sistemdeki en kırılgan nokta olarak görerek saldırıları bu noktada yoğunlaştırabilmektedirler. Yazar, teknik konuların yanı sıra insan unsurunun ve onun çeşitli sosyal özelliklerinin siber saldırıların ve saldırı tekniklerinin niteliklerini belirlediğini vurgulamaktadır. Bilgisayar mühendisliği bölümünde, siber güveliği sosyal bilimler çerçevesinde ele alan bir tez olarak sayılabilecek bir tez de Kademi'nin (2014) yazdığı ve Nijerya için bir milli güvenlik stratejisi öneren tezdir. Çalışmada siber güvenliğin sosyal tanımlarına, milli güvenlik stratejisindeki konumuna yer verildikten sonra Nijerya'nın mevcut siber güvenlik durumu hukuki, yönetsel, ekonomik ve stratejik olarak ele alınmıştır. Çalışmanın sonucunda ise ülkenin siber güvenlik stratejileri için çeşitli önerilerde bulunulmuştur. Tez, siber güvenliğin sosyal bilimler alanına giren boyutlarını ele almakla birlikte, aşağıda yer alan ve uluslararası ilişkiler bölümündeki lisansüstü öğrencilerinin yazdığı tezlerin konularıyla çok büyük benzerlikler göstermektedir.

Türkiye'de siber güvenlik terimini başlığında içeren ve YÖK tez veri tabanında bulunan, tarihsel olarak yazılmış ilk tez Aydın'ın (2012) tezidir. Matematik ve bilgisayar sistemleri anabilim dalı altında yazılmıştır. Tezin araştırma sorusu "Ulusal güvenlik stratejisinde devlet etkili bir rol almalı mıdır? Eğer almalıysa bu nasıl bir rol olmalıdır?" olarak belirlenmiştir. "Türkiye'nin ulusal korunmasında siber güvenlik" başlıklı bu tezin hem başlığı hem de araştırma sorusu siber güvenlik, strateji, devlet, devletin rolü, ulusal güvenlik gibi anahtar kelimeleri içermektedir. Söz konusu anahtar kelimeler başlı başına uluslararası ilişkiler, siyaset bilimi ve kamu yönetimi gibi disiplinlerin öncelikli çalışma alanları arasındadır. Çalışma, kavramsal çerçevede bir takım teknik terimleri içerse de bu başlıklar siber güvenliğin sosyal bilimler alanında ele alınışında da olması gereken miktarlarda ve ölçütlerde kalmıştır. Çalışmanın özet kısmında ise siber güvenliğin Türkiye'nin

9.uncu kalkınma planındaki mevcut yeri, gelecek kalkınma planındaki olması gereken yeri gibi konulara vurgu yapılmış, devletin siber güvenlik konusunda, kamu kuruluşlarını, özel şirketleri ve vatandaşlarını koruma, eğitme ve yol göstermede daha etkin rol alması gerektiği belirtilmiştir. Tüm bu yönleriyle söz konusu tez de fen bilimleri alanında yazılmış sosyal bilimler odaklı bir tez olarak değerlendirilebilecektir.

Yine bilgisayar mühendisliği disiplini ile ilişkilendirilebilecek olan bilişim sistemleri anabilim dalında, Aytekin (2015) tarafından yazılan, “Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi” isimli tez de sosyal bilimler ağırlıklı bir içeriğe sahiptir. Çalışmanın içeriğinde ulusal güvenlik stratejisi hazırlama yöntemlerine Uluslararası Telekomünikasyon Birliğinin çıkardığı rehber temelinde yer verilmiş, ABD, İngiltere ve Türkiye’nin siber güvenlikle ilgili strateji belgeleri incelenerek karşılaştırma yapılmıştır. Sonuç ve önerilerde ise kamu-özel işbirliği, amaç, misyon, vizyon vb. hususların belirsizliği, siber güvenlik yasal altyapısı, ürün geliştirme standartları, bütçe ve kurumlar arası koordinasyon meselelerine değinilmiştir. Nihayetinde bu çalışma da belirgin karakteristiği bakımından sosyal bilimler alanında üretilebilecek bir tez niteliği taşımaktadır. Son olarak Erol’un (2016) yazdığı tez ise bilgi güvenliğini sağlamak üzere bilgi güveliğinde farkındalık yeterlilik seviyesinin ölçülmesine yönelik bir model geliştirilmesini konu almaktadır. Bilgi güvenliği mühendisliği alanında yazılan bu tez konusu itibarı ile alana uygun gözükmekte olsa da tezin içeriği, bilgi güvenliğinin sağlanmasında yazılımsal ya da donanımsal teknik konulardan ziyade farkındalık konusunu ana odak olarak almıştır.

Tez veri tabanında taranan diğer tezlere dönülecek olursa, sayıca ikinci en çok siber güvenlik terimini içeren tezlerin yazıldığı alan uluslararası ilişkiler alanıdır. Konu ile ilgili tek doktora tezi de bu alanda yazılmıştır. Yüksek lisans tezlerinde; ABD’nin ulusal ve uluslararası siber güvenlik stratejileri (Küçükaydın, 2016) incelenmiş, siber güvenlik kavramının gelişimi ve bu kavramın içerdiği bileşenler

ele alınmıştır (Çeliktaş, 2016). Siber güvenlik ile birlikte ortaya çıkan asimetrik savaş unsurlar ve fonksiyonlarına paralel olarak geleneksel güvenlik anlayışının değişim ve dönüşüme uğraması (Kurnaz, 2016) irdelenmiştir. Diğer bir yüksek lisans tezinde ise siber güvenlik; devletlerin birbiri arasındaki ilişkilerin bir nesnesi olarak ele alınmış ve buna bağlı olarak ulus devletlerin değişen güvenlik algıları ve dolayısıyla güvenlik stratejilerini tartışılmıştır (Koik, 2015). Uluslararası ilişkiler alanında yazılan doktora tezi (Güntay, 2016), siber güvenliği öncelikle değişim ve dönüşüme uğrayan güç olgusu içerisinde ele alırken, devletlerin siber güvenlik alanındaki işbirliklerinin ekonomik boyutu üzerinde durmakta ve çeşitli kök kuramlar ışığında analiz etmektedir.

Siber güvenlik terimini içeren ve yine bir sosyal bilimler disiplini olan sosyoloji alanında yazılmış yüksek lisans tezi (Zerin, 2016), Türkiye'de internet yönetiminde siber güvenlik etkilerini özellikle son on yıllık dönemde incelerken, siber güvenliğin yönetim için bir iktidar stratejisi haline gelişini ele almaktadır. Hukuk alanında yazılan yüksek lisans tezinde (Sarı, 2013), internet ve siber ortamın yapısının karmaşıklığı, sınırsızlığı ve muğlaklığı ile birlikte bu alanda işlenecek suçların da sonuçları sorgulanmaktadır. Buna göre siber suçlar, ortamları gereği sadece tek bir ülkede değil aynı anda birçok ülkede işlenerek birçok farklı hukuk sistemi içerisinde vuku bulabilmektedir. Bu bağlamda, siber suçlar için oluşturulacak hukuki düzenlemelerde ülkeler arası işbirliği önemlidir. Strateji bilimleri alanında yazılmış olan yüksek lisans tezi (Ercan, 2015), siber saldırılarda kullanılan yöntemleri, kritik altyapıları ve kritik altyapılara yapılan saldırı çeşitlerini ele almaktadır.

Siber güvenlik üzerine Türkiye'de bilgisayar bilimleri alanında yazılan lisansüstü tezlerden teknik konular odağında yazılanları, ülkenin siber güvenlik altyapısının güçlendirilmesi adına önemli çalışmalardır. Bu çalışmalar Türkiye'nin siber güvenliği adına doğrudan bir politika üretmeseler de üretilecek politikaların envanterini sağlayacaklardır. Diğer yandan bilgisayar bilimleri alanından siber güvenlik ile ilgili yazılmış fakat temellerinde sosyal bilimler odaklı olan tezlerden biri

(Kademi, 2014) siber güvenliği bir strateji olarak ele almış, bunun akabinde Nijerya için bir model önerisi geliştirmiştir. Diğer yandan Aytekin'in (2015) çalışması da Tükiye'nin Siber Güvenlik Stratejisi ve Eylem Planını incelemiş, ABD ve İngiltere'de oluşturulan belgeler ile kıyaslayarak belgelerde yapılan politika önermeleri üzerinden Türkiye'nin eksikliklerini belirlemeyi amaçlamıştır. Zira tezlerde amaçlanan sosyal bilimler bakış açısı, kavramsal, kuramsal ve metodolojik yeterliliği yakalayamamıştır. Siber güvenlik alanında ülkenin bu alanlardan ihtiyaç duyduğu bilimsel desteğin daha çok teknik boyutta olduğu düşünülmektedir. Bu yüzden özellikle siber güvenlik konulu, pozitif bilimler alanında yapılacak akademik çalışmaların sosyal bilimler alanına giren konularla meşgul olmasından ziyade kendi entelektüel kapasitelerini teknik boyutta, yeni sistemlerin üretilmesine, var olanların geliştirilmesine yönelik yansıtmalarının daha faydalı olacağı düşünülmektedir. Tezlere yapılan eleştiri, bu tezlerin ilgili oldukları konular bakımından kendi alanlarının dışına çıkması hususunda değildir. Bunun bir adım ötesi olarak fen bilimleri ve sosyal bilimler arasında yapılacak multidisipliner çalışmaların yararlı olacağı aşikardır. Zira bilgi güvenliği mühendisliği alanında yayın yapan bir derginin (UBGMD, 2017) ilgilendiği konulara bakıldığında, sosyal bilimler alanına da giren birçok konuya yer verdiği görülebilecektir. Ancak incelenen çalışmalardaki durumun multidisipliner olmaktan ziyade, fen bilimleri tabanlı olarak sosyal bilimler alanında yazılmış olmalarıdır. Yapılan eleştiri, söz konusu çalışmaların sayıca kısıtlı olmalarına karşın, bünyesinde yazıldığı alanların çeşitliliğinin aynı şekilde tezlere yansımaması noktasındadır. Lisansüstü çalışmalarında, ilgili alanlardaki öğrencilerin yaptıkları çalışmaların onların uzmanlıklarını belirtir çalışmalar olduğu düşünüldüğünde, bilgisayar mühendisliği gibi bir bölümde, siber güvenlik alanında yazılacak tezlerin daha çok teknik yönde olması beklemek yanlış olmayacaktır. Siber güvenlik stratejilerinin değerlendirilmesi, kalkınma planlarında siber güvenliğin aranması, siber güvenliğin ulusal bir güvenlik politikası olarak ele alınması ve yine siber güvenliği bir iktidar stratejisi olarak ele alınması, sosyal bilimlerin odak konuları daha çok devlet

yönetimi, uluslararası ilişkiler olan bölümlerinde çalışılması beklenen konular olduğu düşünülmektedir.

Sosyal bilimler alanında yapılan çalışmalara bakıldığında ise bu çalışmalar daha çok kendi alan sınırları içerisinde kalmış gözükmektedirler. Çalışmalar, siber güvenliğin önemini kavramsal açıdan vurgulayan, siber güvenlik ile birlikte değişen ve dönüşen güvenlik anlayışını ve hukuki yaptırımlar sorgulayan, siber güvenliğin yönetimlere etkisini inceleyen tezlerdir. Şaşırtıcı olan nokta, bilgisayar mühendisliği alanından yazılan tezlerde siber güvenlik strateji ve politikalarına doğrudan odaklanılan öreklere rastlanırken sosyal bilimler alanından yazılan tezlerde, bunun daha sınırlı bir şekilde kalmasıdır. Çalışmaların siber güvenliğin ilgili konu, kavram ve unsurlarını farklı açılardan ele almalarının Türkiye açısından siber güvenlik anlayışının gelişmesine katkı sunacağı düşünülmektedir.

5.4. ARAŞTIRMA SORULARI

Bu araştırma, “Türkiye’nin siber güvenlik politikalarının kamu politikası analizi yaklaşımları çerçevesindeki yönelimleri nelerdir?” temel sorusuna cevap aramaktadır. Bu temel soruyu destekleyecek şekilde ve araştırmanın önceki bölümlerinde işlenen konularla karşılaştırmalı olarak değerlendirmek üzere aşağıdaki sorulara da cevap aranmaktadır.

-Türkiye’nin siber güvenlik politikaları kamu politikası analizi yaklaşımlarından hangisi üzerinde yoğunlaşmaktadır?

-Türkiye’nin siber güvenlik politikalarının oluşturulmasında hangi karar verme yaklaşımlarının etkileri ne şekilde gözlemlenmektedir?

-Ülke dinamikleri göz önüne alındığında, Türkiye'nin siber güvenlik politikalarının üretilmesinde hangi kamu politikası analizi yaklaşım ve karar verme modelleri öncelik alınmalıdır?

-Türkiye'nin siber güvenlik politikaları ile kritik altyapı politikaları arasında bir etkileşim var mıdır?

-Kamu politikası analizi açısından Türkiye'nin siber güvenlik politikalarının diğer ülkelerin siber güvenlik politikaları ile kesişen yönleri var mıdır, nelerdir?

-Türkiye'nin siber güvenlik politikaları hangi konular üzerinde yoğunlaşmaktadır?

5.5. ARAŞTIRMA EVRENİ VE ÖRNEKLEM

Araştırma, Türkiye'nin siber güvenlik politikalarını kamu politikası analizi çerçevesinde değerlendirmeyi amaçlamaktadır. Bu çerçevede, araştırma evrenini Türkiye'nin siber güvenlik politikalarını belirleyen ve belirten resmi belgeler oluşturmaktadır. Araştırma örnekleminde kullanılacak olan belgelerin seçiminde, derinlemesine araştırma yapabilmek amacıyla, çalışmanın amacı bağlamında bilgi açısından zengin durumların seçildiği "amaçlı örnekleme" (Balcı, 2001) yöntemi kullanılmıştır. Buna göre, araştırmacı örneklem için hangi birimlerin seçileceğine kendisi karar verir. Araştırmacının araştırma için uygun gördüğü kümeler, gruplar, birimler araştırmanın amacına da uygun olarak belirlenmektedir (Koçak ve Arun, 2006: 26). Bu bağlamda araştırmada, belirlenen evrenin de doğrultusunda, Türkiye'nin siber güvenlik politikaları ile alakalı olabilecek resmi belgeler ele alınmaktadır. Söz konusu belgelerin belirlenmesinde, Türkiye'nin merkezi yönetim kurum ve kuruluşlarında siber güvenlik ile ilgili konularda çalışan ve yetkili bulunan uzmanlarla görüşmeler yapılarak fikirleri alınmıştır. Uzmanların fikirleri doğrultusunda belirlenen belgelerden (strateji belgeleri, eylem planları, kalkınma planları) 1'i dışında (2016-2019 Siber Güvenlik Eylem Planı) tümüne ulaşılmıştır.

Uzmanlar tarafından önerilen belgelerin dışında, araştırmacı kendi araştırmaları sonucu, araştırma ile ilgili olarak belirlediği (strateji belgeleri, raporlar, hükümet programları, ve hukuki belgeler) dokümanları da araştırmaya dâhil etmiştir. Çalışmanın evreni olarak belirlenen "Türkiye'nin siber güvenlik politikalarını belirleyen ve belirten belgeler"in biri dışında tümüne ulaşılmıştır. Dolayısıyla araştırmanın sonucunda ortaya konulacak olan çıkarsamalar genellemeyi verecektir.

Araştırmada kullanılarak analiz edilen dokümanlara ait genel bilgiler aşağıdaki tabloda verilmiştir.

Tablo 6: Araştırmada Kullanılan Dokümanlar

Tür	Belge İsimleri	Adet
Strateji Belgeleri	-2006-2010 Bilgi Toplumu Stratejisi, -Ulusal Siber Güvenlik Stratejisi (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile Bilgi Güvenliği Derneği), -2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, -2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi, -2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı -2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, -2016-2019 Ulusal Siber Güvenlik Stratejisi, -BTK (Türkiye'deki Mevcut Durum Ve Alinmasi Gereken Tedbirler)	8
Kalkınma Planları	-1. Kalkınma Planı -2. Kalkınma Planı -3. Kalkınma Planı -4. Kalkınma Planı -5. Kalkınma Planı -6. Kalkınma Planı -7. Kalkınma Planı -8. Kalkınma Planı -9. Kalkınma Planı -10. Kalkınma Planı	10
Raporlar	-Emniyet Genel Müdürlüğü 2016 Raporu -Meclis Araştırma Komisyonu Raporu-1 -Meclis Araştırma Komisyonu Raporu-2	3
Hukuki Belgeler	-Elektronik Haberleşme Kanunu -Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı -Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi -Yönetilmesi ve Koordinasyonuna İlişkin Karar	3
Hükümet Programları	-58. Hükmet Programı -59. Hükmet Programı -60. Hükümet Programı -61. Hükmet Programı	4
Toplam		**28**

5.6. ARAŞTIRMANIN YÖNTEMİ

Bu çalışmada, nitel araştırma yöntemi kullanılmıştır. Nitel araştırmalar, insanlar, davranışlar, resimler, videolar, ses kayıtları, yazılı belgeler gibi veri kaynaklarından gözlem, anket ve mülakat gibi yöntemlerle elde edilen verilerin sistematik bir biçimde kodlanarak, gruplandırılarak yapılan analizler sonucu elde edilen sonuçların sunulmasını sağlar. Bazı durumlarda söz konusu sonuçlar, nitel verilerin belirli bir sistematik ile sayısallaştırılması (nicel hale getirilmesi) şeklinde de sunulabileceği (Strauss ve Corbin, 1998: 11) gibi genel olarak nitel verilerin yorumsamacı yaklaşımla çözümlenmesi ve analiz edilmesine dayamaktadır

Çalışmada, nitel araştırmalarda kullanılan veri toplama tekniklerinden olan doküman analizi tekniği (Snape ve Spencer, 2003: 3) kullanılmıştır. En genel tanımıyla doküman analizi; çeşitli materyalin araştırma konusu veriyi içermesinden dolayı, söz konusu materyalin çözümlenmesi işlemidir (Gürbüz ve Şahin, 2014: 182). Araştırmacı, konusunda göre hangi dokümanları ya da materyalleri kullanacağına kendisi karar vermektedir. Araştırmanın konusunda ve amacına göre incelenecek materyallerin türü de değişiklik göstermektedir. Berg'in (2001: 189-192) tanımına göre ise doküman analizi; arşiv araştırmalarına dayanan örtülü (unobtrusive) bir veri toplama yöntemidir. Doküman analizi veri toplama tekniği, araştırmanın sorularına cevap ortaya koyacak olan verileri araştırmacıya kendi içinde bir bütün halinde sunmaktadır. Araştırmacı kendi araştırma sorusu çerçevesinde, bu bütün veriyi çeşitli kodlama yöntemleriyle belirli bir sistematik dâhilinde parçalara bölerek, sınıflandırarak, veriler arasında bağlantılar kurarak analiz edilmiştir. Çalışmada temelde nitel veriler olan politika önermeleri, yorumsamacı bir yaklaşımla analiz edilmiş ve analiz edilen politika önermeleri, sınırları çizilen kategoriler içerisinde gruplandırılarak sayılmış (dolayısıyla nicelleştirilmiş) ve yoğunlukları belirlenmiştir. Parçaların birleştirilmesi ile belirlenen yoğunluklar üzerinden tüme varımlar yapılmıştır.

Söz konusu verilerin analizinde veri kaybının yaşanmaması, kodlar, kategoriler ve temalar arasındaki ilişkilerin ve farklı boyutların daha açık belirlenmesi için nitel çalışmalarda yaygın olarak kullanılmakta olan nitel veri analizi programı Nvivo 11 nitel veri analiz yazılımı kullanılmıştır. Bu yazılım ile nitel araştırmada kritik olan verilerin zenginliğini kaybetmeksizin tüm nitel verileri derinlemesine inceleyerek analiz etmek ve yönetmek mümkün olabilmektedir (Bazeley & Richards, 2000; Lynne, 2006; Lakeman, 2008; Sepulveda, v.d., 2012). Bu bağlamda analiz sürecinde, araştırmacı tarafından elde edilen belgeler Nvivo programına aktarılmıştır. Belgelerde kullanılan kodlar direkt olarak araştırma sorusunun cevap aradığı konular temelinde isimlendirilmiştir. Kodlamalar yapılırken belgelerin şekil ve içeriklerinin farklılıkları göz önünde bulundurularak her belge türü için ayrı bir proje oluşturulmuş ve kodlamalar aynen ya da belge türüne uygun küçük değişikliklerle yeniden oluşturulmuştur. Oluşturulan kodlar ardından analizlere ve yorumsamalara ilişkin mantık çerçevesi Ek-1'de yer alan örnek tabloda tasvir edilmiştir. Bu mantık çerçevesinde kodlanan her bir ilgili politika önermesi, hem oluşturulan üst kategori kodlamaları hem de alt kategori kodlamaları çerçevesinde yorumlanmıştır. Yorumlanacak politika önermelerinin belirlenmesinde, öncelikle araştırma sorusu temelinde ilgili olabilecek kavramlar olan Ulusal Güvenlik, Siber Güvenlik, Kritik Altyapılar, Politika kavramları yakın anlamlı, sesteş, eş anlamlı sözcükler ile taratılmış, bulunan noktalardaki belge bölümleri okunmuş ve analiz edilmiştir. Odaklanılmış bu okumalardan sonra gözden kaçan ya da programın olası hatalarına karşın göz ardı edilebilecek politika önermelerini saptamak üzere belgeler tekrardan bir bütün olarak okunmuştur. Dokümanlardan kategorilerin geliştirilmesi için, nitel içerik analizi çerçevesinde tümevarımcı kategori geliştirmeye dayalı sistematik indirgeme süreci ile yönetilen ve Mayring (2002'den akt. Taşçı, vd., 2008) tarafından önerilen bir sistematik esas alınmıştır. Çalışmanın kodlama sürecinde; paragraf veya cümlelerden hareketle kavramlar oluşturulmuştur. Kavramsallaştırma aşamasından sonra, çalışma, analiz edilecek birim sayısını azaltabilmek için birbirleriyle ilişkili kavramları her bir doküman kendi içerisinde

analiz edilip, gruplandırarak kategoriler (temalar) oluşturulmuştur. Kategorileştirme sürecinde; veriler önce açık kodlama sistemi ile kodlanmış; ardından seçici ve eksen kodlar kullanılmıştır. Açık kodlama sırasında; elde edilen dokümanların her biri parçalara ayrılarak dar kapsamda incelenmiştir. Bu incelemede, parçalar arasındaki farklılık ve benzerlikler değerlendirilmiştir. Eksen kodlama[19] bu noktada, açık kodlamada oluşan kategoriler arasında bir korelasyon kurarken Strauss ve Corbin'in (1998) paradigma modeli çerçevesinde gerçekleştirilmiştir. Paradigma modeli, bir olgunun oluşumunu gelişimini etkileyen durum ve olaylar, sonrasında bu olgunun niteliklerini, olguyu etkileyen koşulları ve olguyu yönlendiren etkileşim çıktılarını ifade etmektedir. Seçici kodlamada; kamu politikası analizi yaklaşımları (rasyonel, yorumsamacı ve karma yaklaşımlar) merkez kategori olarak kullanılmıştır. Tümdengelimci olarak kazanılmış ana kategorilerin araştırma analizlerine sistematik olarak yerleştirilmesi ile nitel analiz basamakları tekrar oluşturulmuştur. Diğer bütün kategoriler (karar verme yaklaşımları); bu merkezi kategori ile ilişkilendirilerek, merkez kategoriler kavramsallaştırılmış ve bunun sonucunda merkez kategoriye bağlanmıştır. Kodlamalar sırasında, karar verilemeyen durumlarda tez danışmanı ile görüşülerek, fikir birliğine ulaşıldıktan sonra kodlamalar tamamlanmıştır.

5.6.1. Politikaların Analizinde Uygulanan Yöntem

Bu başlık altında çalışmanın yöntemini oluşturan sistematiğin kuruluşuna dair izlenen yollar hakkında bilgiler sırası ile verilecektir.

---

[19] Eksen kodlama, açık kodlamada oluşturulan kategoriler arasında bağ kurulmasını sağlar.

5.6.1.1. Politika Analizi ve Karar Verme Yaklaşımlarının Sınıflandırılması

Verileri parçalara ayırma, tek tek anlamlı birimlere göre kategorileştirme araştırmanın analizini, yorumlanmasını ve sonucunu direkt olarak etkilemektedir. Araştırma amacı ve hipotezimize uygun olarak araştırmada çeşitli kategorilendirme ve kodlamalara yer verilmiştir. Belgelerden elde edilecek olan politika önermeleri, çalışmanın ilk bölümünde yapılan kamu politikası analizi ve karar verme yaklaşımları sınıflandırması çerçevesinde gruplandırılacak ve yorumlanacaktır. Araştırma sistematiğinin genel çerçevesine bakıldığında da, doküman analizinden elde edilecek veriler kodlanarak verilerin altında yatan politika boyutları ve boyutlar arasındaki ilişki yorumsamacı yaklaşımla ortaya koyulacaktır. Bu bağlamda, ilk bölümde yapılan kamu politikası analizi ve karar verme yaklaşımlarının sınıflandırılmasına ait tablo aşağıda tekrar verilmiştir.

Tablo 7: Kamu Politikası Analizi Yaklaşımlarının Sınıflandırılması

	Kamu Politikası Analizi (KPA) Yaklaşımları		
	Rasyonel KPA	**Karma KPA**	**Yorumlamacı KPA (Post-Pozitivist KPA)**
Analiz Yöntemi	Nicel Analiz	Nicel-Nitel Analiz	Nitel Analiz
Temel Alınan Kuramlar	-İşlem Maliyeti -Kamu Tercihi -Sibernetik -Yön-Eylem	-Sınırlı Rasyonalite	-Post-Modernist Kuramlar -Karmaşıklık Kuramı
Karar Verme Modelleri	-Basamaklar Modeli -Çöp Kutusu Karar Verme Modeli -Çoklu Akımlar Modeli -Politika Formülasyonu Modeli -Lowi'nin Sınıflandırma Modeli	-Normatif Optimum Karar verme Modeli -Karma-Tarama Karar Verme Modeli	-Savunma Koalisyonu Modeli -Artırımcı Karar Verme Modeli

Analize tabi tutulacak olan belgelerden elde edilecek olan politika önermeleri, yukarıdaki verilen tablo temelinde sınıflandırılmıştır. Söz konusu sınıflandırmanın yapılması için politika önermelerinin tabloda belirtilen analiz yöntemleri, kuramsal kökenleri ve araştırmanın ilk bölümünde yer alan kamu politikası analizi yaklaşımlarının kuramsal açıklamalarında yer alan çeşitli özelliklerden (değer

ayrımları, radikal ya da artırımcı politikalar, katılımcılık vb.) oluşturulan kodlar birer **bağımsız değişken** olarak belirlenmiştir. Bu kodlar, doküman analizinden elde edilecek ve aynı zamanda araştırmanın **bağımlı değişkenlerini** oluşturan politika önermelerini analiz etmekte kullanılmıştır. Politika önermelerinin belirlenmesinde ise bir nitel veri analizi programından yararlanılmış olup, bu belirlemelerin yapılmasında kullanılan sistematik, ilerleyen başlıklarda açıklanmıştır. Aşağıdaki tabloda bağımsız değişken olarak belirlenen kodlar gösterilmektedir.

Tablo 8: Kodlanan KPA Yaklaşımları ve Karar Verme Modelleri (Bağımsız Değişkenler) Tablosu

Rasyonel KPA Yaklaşımı	**Karma KPA Yaklaşımı**	**Yorumsamacı KPA Yaklaşımı**
Karar Verme Modelleri		
Basamaklar Modeli (Lasswell) -Süreçler -Rasyonel Kararlar -Kamu Tercihi -Ampirik Veriler	**Normatif Optimum Model (Dror)** -Oluşan Yeni Durumlar -Yenilikçilik -Yaratıcılık -Beklentiler -Sezgisel Yargı -Uzmanlaşma -Gelişmekte Olan Ülkelerde	**Savunma Koalisyonu Modeli (Sabatier)** -Çıkarlar -Güç Mücadelesi -İttifak -İnanç Sistemi -İdeoloji -Değerler -Sosyal Yapı
Çöp Kutusu Karar Verme Modeli (Cohen, March, Olsen) -Problematik Tercih -Tam Anlaşılmamış Teknoloji -Problemler – Çözümler -Daha Ayrıntılı Rasyonalite	**Karma Tarama Model (Etzioni)** -Değişen şartlar -Geniş Açı Tarama -Artırımcı ve Rasyonel Karışık	**Artırımcı Karar Verme (Lindblom)** -Marjinal Fayda -Kök Problem -Basite İndirgeme -Artırımcı Karar -Gelişmiş Ülkelerde
Çoklu Akımlar Modeli (Kingdon) -Çöp Kutusu Model Revize -Gündeme Gelme -Problem-Politika Alternatifi-Siyaset Akımı -Organize Baskı Grupları	**Sınırlı Rasyonalite (Simon)** -Tatmin Edici Seçim -Belirsizlik -Öngörülemezlik	
Politika Formülasyonu (Peter) -Analitik Duruş -Problemlerde Çözülebilirlik-Karmaşıklık-Ölçek-Bölünebilirlik-Parasallaştırılabilirlik		

Yukarıdaki tabloda yer alan ve başlıklar altında sıralanan kodlar (bağımsız değişkenler) NVivo 11 programında yapılan kodlamalar ve okumalar sonucunda ortaya çıkarılan politika önermeleri içerisinde, içerik analizi yöntemi ile aranmış, söz konusu politikalar uygun başlıklara eşleştirilerek analiz edilmiştir.

5.6.1.2. Kodlamalara İlişkin Tablolar ve Kodlama Sayıları

Araştırma çerçevesinde yapılan kodlamalara ilişkin tablolar aşağıda sıralanmıştır. Yapılan kodlamalar, güvenlik, içerisinde siber güvenlik ve kritik altyapılar olarak belirlenmiştir. Kritik altyapılar kategorisi içerisinde yer alan kodlar (kritik altyapı çeşitleri) AB Konseyi tarafından kritik olarak belirlenen altyapılar çerçevesinde (BTK, 2010: 5-6) oluşturulmuştur. Çalışmanın önceki başlıklarında belirtildiği üzere, kodlamalar belge türlerine göre ayrı ayrı projeler halinde düzenlenmiştir. Belge türleri ve içeriklerine göre, yapılan kodlamalarda ufak farklılıklar gözlemlenmektedir. Belgelerde yer alan kodlamalar ilgili kavramların eş ve yakın anlamlı sözcükler de dâhil edilerek taratılması ile belirlenmiştir. Kodlamaların birer "politika önermesi" olarak ayrıştırılarak tablolaştırılmış hali, araştırmanın "bulgular" başlığı altında verilecektir. Tablolarda "sources" sütunu altındaki sayılar kodlamaların yapıldığı belge sayısını, "references" sütunu altındaki sayılar ise yapılan kodlama sayısını göstermektedir.

Tablo 9: Strateji Belgelerine Ait Kodlamalar

Nodes

Name	Sources	References
Güvenlik	8	662
Siber Güvenlik	8	654
Ulusal Güvenlik	3	8
Kritik Altyapılar	8	1011
Bankacılık ve Finans	7	42
Enerji	7	78
Gıda	6	41
İletişim	8	565
Nükleer	3	6
Su	7	38
Turizm	4	27
Ulaşım	8	183
Uzay	3	13
Politika Analizleri	0	0

Ele alınan strateji belgelerinde 662 adet güvenlik temalı kodlama yapılırken, bunların 654'ü siber güvenlik, 8'i ise ulusal güvenlik şeklinde belirlenmiştir. Kritik altyapılara ilişkin toplam 1011 adet kodlama yapılmıştır.

Tablo 10: Kalkınma Planlarına Ait Kodlamalar

Nodes

Name	Sources	References
Güvenlik	10	738
Siber Güvenlik	1	1
Sosyal Güvenlik	10	367
Ulusal Güvenlik	9	64
Kritik Altyapılar	10	3535
Bankacılık ve Finans	10	301
Enerji	10	959
Gıda	9	317
İletişim	10	388
Nükleer	9	61
Su	10	637
Turizm	10	506
Ulaşım	8	355
Uzay	4	11
Politika Analizi	0	0

Kalkınma planlarına ait yapılan kodlamada güvenlik temalı toplam 738 adet kod belirlenirken bunların 367'si sosyal güvenlik, 64'ü ulusal güvenlik ve sadece 1 adedi ise siber güvenlik ile ilgilidir. Kritik altyapılar için belirlenen kod adedi 3535'tir.

Tablo 11: Raporlara Ait Kodlamalar

Nodes

Name	Sources	References
Güvenlik	3	390
Siber Güvenlik	3	358
Ulusal Güvenlik	2	32
Kritik Altyapılar	3	1378
Bankacılık ve Finans	2	39
Enerji	2	60
Gıda	1	7
İletişim	3	1198
Nükleer	2	3
Su	2	22
Turizm	1	16
Ulaşım	2	21
Uzay	2	12
Politika Analizi	0	0

Ele alınan raporlara ait yapılan kodlamada güvenlik temalı toplam 390 adet kod belirlenirken bunların 358'ü siber güvenlik, 32'ü ise ulusal güvenlik ile ilgilidir. Kritik altyapılar için belirlenen kod adedi 1378'dır.

Tablo 12: Hukuki Belgelere Ait Kodlamalar

Nodes

Name	Sources	References
Güvenlik	3	73
Siber Güvenlik	3	64
Ulusal Güvenlik	2	9
Kritik Altyapılar	3	268
Bankacılık ve Finans	1	1
Enerji	0	0
Gıda	0	0
İletişim	3	230
Nükleer	0	0
Su	1	1
Turizm	1	4
Ulaşım	3	30
Uzay	1	2
Politika Analizi	0	0

Ele alınan ilgili hukuki belgelere ait yapılan kodlamada güvenlik temalı toplam 73 adet kod belirlenirken bunların 64'ü siber güvenlik, 9'u ise ulusal güvenlik ile ilgilidir. Kritik altyapılar için belirlenen kod adedi 268'dir.

Tablo 13: Hükümet Raporlarına Ait Kodlamalar

Nodes

Name	Sources	References
Güvenlik	4	67
Kritik Altyapılar	4	230
Bankacılık ve Finans	4	53
Enerji	4	39
Gıda	3	6
İletişim	4	25
Nükleer	3	4
Su	3	15
Turizm ve Kültür	4	57
Ulaşım	4	29
Uzay	1	2
Politika Analizleri	0	0

Hükümet raporların ait yapılan kodlamalarda sadece genel güvenlik ve kritik altyapılar kavramlarına ilişkin kodlamalar saptanmıştır. Genel güvenliğe ilişkin belirlenen kodların sayısı 67, kritik altyapılara ilişkin kodlama sayısı ise 230'dur.

Kodlamaların geneline bakıldığında, güvenlik temalı toplam 1930 kodlama yapılmıştır. Bu kodlamalardan 1077'si siber güvenlik ile ilgilidir. Kritik altyapılar ile ilgili olarak ise toplamda 6422 kodlama yapılmıştır. Genel toplamda ise 8352 adet kodlama yapılmıştır.

5.6.1.3. Bulguların Analiz Edilmesi

Araştırmada elde edilen bulguların analizi, araştırmanın kamu politikası kuramlarına ilişkin olarak hazırlanan ilk bölümü temel alınarak gerçekleştirilmiştir. Bu bağlamda, araştırmanın yöntemi bölümünde anlatılan şekilde yapılan kodlamalar sonrası elde edilecek olan politika önermelerinin, alt kodlamalar olarak belirlenen karar verme yaklaşımlarından hangilerine yakın ya da içerisinde olduğu saptanmıştır. Bu saptama yapılırken, bağımsız değişken olarak belirlenen karar verme yaklaşımları (normatif optimum, çoklu akımlar, politika formülasyonu vb.) sınıflandırılması için oluşturulan kodlar kullanılacak ve politika önermelerinde bu

kodlara ait izler aranarak önermeler sınıflandırılmıştır. Yapılan sınıflandırma sonucunda belirli bir karar verme yaklaşımı içine ayrılan politika önermeleri, aynı zamanda üst kodlamalarda (rasyonel, yorumsamacı ve karma kamu politikası analizi) belirlenen ve alt kodlamalarda karar verme yaklaşımlarını barındıran kamu politikası analizi yaklaşımları (rasyonel, yorumsamascı ve karma) içerisinde gruplandırılmıştır. Politika önermelerinin sayısı çok fazla olduğu için bu sınıflandırmaların tümünün seçilme sürecine ve adımlarına çalışmada yer verilmemiştir. Söz konusu uygulama ve uygulama mantığına bir örnek olarak oluşturulan tablo Ek 1'de sunulmaktadır.

Politika önermeleri alt ve üst kodlamalarda gruplandırıldıktan sonra Türkiye'nin siber güvenlik politikalarını yansıtan politika bulguları rasyonel, yorumsamacı ve karma politikalar olarak üç başlık altında analiz edilmiş ve yorumlanmıştır. Çalışmanın Türkiye'nin siber güvenlik politikalarını kamu politikası analizi kapsamında değerlendirmeyi amaçlamasından dolayı yapılan analizler politika-politika analizi (karşılaştırmalı politika analizi) olmaktan çok politika-kuram analizi şeklinde gerçekleştirilmiştir. Bu bağlamda, siber güvenlik ve kritik altyapılarda ortaya çıkan genel politika eğilimlerinin hangi kamu politikası analizi yaklaşımları çerçevesinde, hangi karar verme modelleri baz alınarak, hangi yönelimlerde (altyapısal, teknolojik, statükocu vb.) olduğu ayrı ayrı analiz edilmiş ve araştırma sorularına cevap aranmıştır.

5.7. ARAŞTIRMANIN BULGULARI

Araştırmada yapılan kodlamalardan sonra ortaya çıkan siber güvenlik ve bağlantılı olarak kritik altyapı politika önermelerinin sayıları ve bu önermelerin kamu politikası analiz yaklaşımları ile karar verme modelleri içerisinde sınıflandırılmasıyla meydana gelen bulgular aşağıda sıralanmıştır. Bulgular sunulurken her bir belge türü için elde edilen bulgular ayrı alt başlıklar halinde gösterilmiştir. Bulgular,

tablolar ve grafikler halinde tüm bulguları yansıtır bir biçimde sunulurken, elde edilen politika önermelerinin metin halleri, politika önermelerinin fazlalığı nedeniyle tamamıyla gösterilmemiştir. Bunun yerine politika önermelerinin metinleri, sınıflandırıldıkları kamu politikası analizi yaklaşımları ve karar verme modelleri altında, sırasıyla 1'inci, 2'nci ve 3'üncüönermeler olmak üzere rastgele seçilen 3'er adet (politika önerme sayısı yetersiz olması takdirde daha az) örnekler şeklinde verilmiştir. Yine araştırma bulguları bölümünün makul uzunlukta tutulması için, bulgular verilirken, elde edilen bulgular belge türlerinin içinde yer alan her bir belge için ayrı ayrı verilmemiş, belge türlerine ait olarak genel bir tablo halinde sunulmuştur. Belge türleri içerisinde tekil olarak yer alan ve bulguların analizi açısından kayda değer farklılaşmalar gösteren belgelerin bulgu sonuçlarına analiz bölümünde ayrıca yer verilecektir.

5.7.1. Siber Güvenlik Strateji Belgelerinden Elde Edilen Bulgular

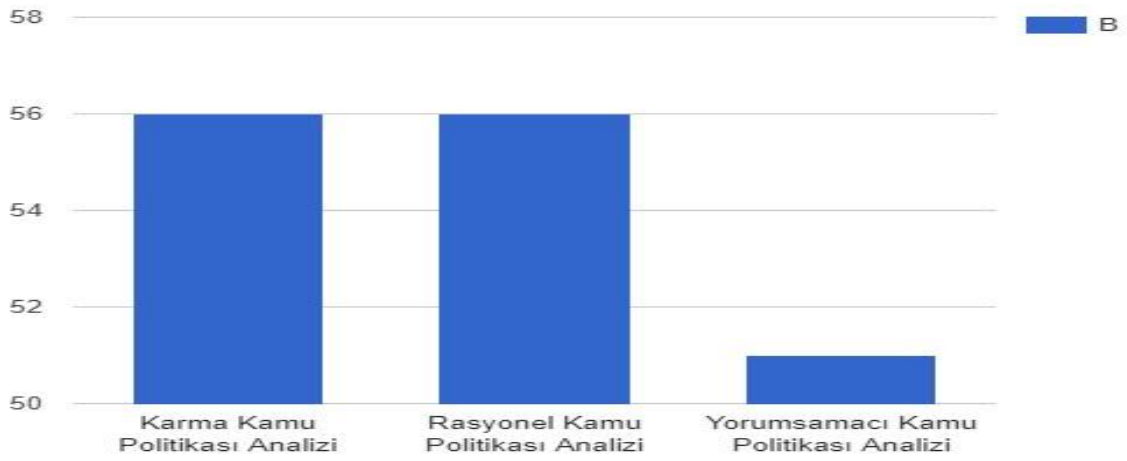
Bu başlık altında, Türkiye'nin siber güvenlikle ilgili strateji belgelerinden elde edilen bulgular, siber güvenlik ve kritik altyapılar olmak üzere iki grup halinde sunulmuştur.

5.7.1.1. Kritik Altyapılara İlişkin Bulgular

5.7.1.1.1. Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı

Araştırmada ortaya çıkan bulgulara göre, strateji belgelerinde kritik altyapılar ile ilgili toplamda 163 adet politika önermesi yer almaktadır. Söz konusu politika önermelerinin 56'sı Rasyonel, 51'i Yorumsamacı, 56'sı ise Karma Kamu Politikası analiz yaklaşımı içerisinde yer almıştır.

Tablo 14: Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı (Strateji Belgeleri)



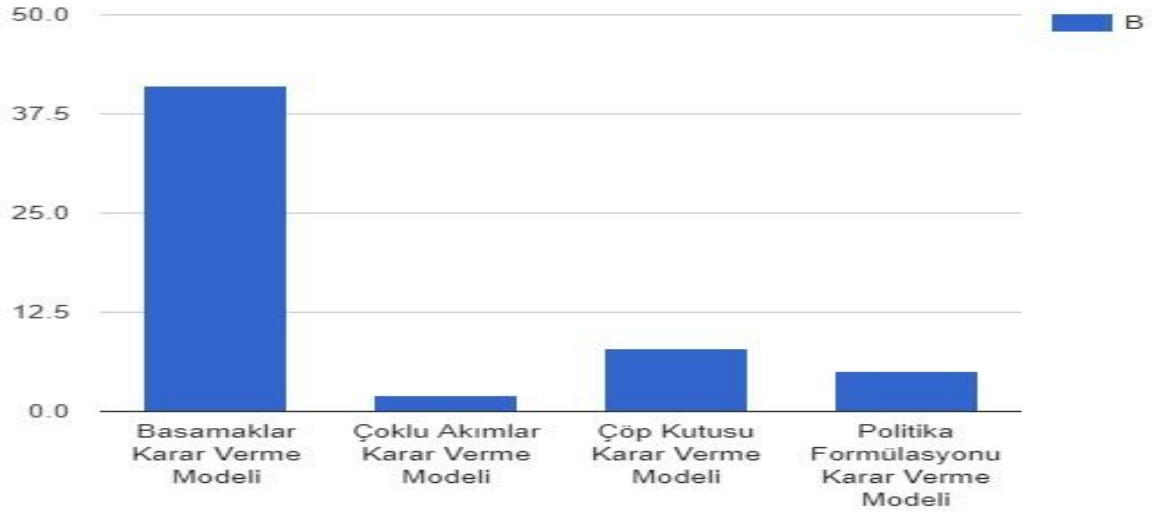
Bu politika önermelerinin hangi karar verme modelleri içerisinde yer aldığı ise aşağıdaki tablolarda, her bir kamu politikası analizi yaklaşımı için ayrı ayrı gösterilmiştir.

5.7.1.1.2. Karar Verme Modellerine Göre Politika Önerme Dağılımı

5.7.1.1.2.1. Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Siber Güvenlik Strateji Belgeleri)

Politika önermelerinin Rasyonel Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Basamaklar Karar Verme Modelinde 41, Çoklu Akımlar Karar Verme Modelinde 2, Çöp Kutusu Karar Verme Modelinde 8 ve Politika Formülasyonu Karar Verme Modelinde 5 politika önermesi belirlenmiştir.

Tablo 15: Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Strateji Belgeleri)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Basamaklar Karar Verme Modeli

> *"modellerinin hayata geçirilmesine yönelik politikalar belirlenecektir. Metropol bölgelerinde ve kentsel dönüşüm kapsamındaki bölgelerde akıllı kent uygulamalarına öncelik verilecek ve buna ilişkin bir yol haritası oluşturulacaktır"*

> *"Bölgesel bazda düzenleme yaklaşımının oluşturduğu etki düzenli olarak takip edilecek ve bu kapsamda oluşturulacak raporlar kamuoyuyla paylaşılacaktır"*

> *"Alınacak düzenleyici kararların öncesinde uzun vadeli etki analizi yapılması genel prensip olarak benimsenecektir. Analizin yapılacağı düzenleyici kararların kapsamı tespit edilecek; belirlenen kapsamdaki düzenlemelere ilişkin öncül etki analizi yapılması, bağlayıcılığı sağlamak için mevzuata derecelendirilecektir. Elektronik haberleşme sektöründe faaliyet gösteren işletmeciler ve ilgili diğer tarafların mevcut etki analizlerine katılım sağlaması için bir mekanizma geliştirilecektir. İlgili tüm paydaşların görüşlerini alarak ve bilimsel yöntemlerden istifade edilerek her bir düzenlemenin etkileri öncül olarak analiz edilecektir".*

Çoklu Akımlar Karar Verme Modeli

“Elektronik kamu hizmeti sunumunda, iş süreçlerinin imkân verdiği her koşulda, başvurudan hizmetin tamamlanmasına kadar tüm süreçler elektronik ortamda yürütülecektir. Kimlik belirleme, elektronik ödeme ve benzeri ortak işlemler tek kapıdan yürütülerek, hizmetlere erişim kolaylaştırılacak ve iş süreçleri hızlandırılacaktır”

“Elektronik haberleşme altyapısı kurmak isteyen işletmecilerin yerel yönetimler ve kamu kurumlarıyla yaşadıkları geçiş hakkı sorunlarının ortadan kaldırılması sağlanacak, bu alandaki düzenleme etkin biçimde uygulanacaktır”.

Çöp Kutusu Karar Verme Modeli

“Ulaşımda trafik yoğunluğunun engellenmesi ve mevcut altyapının etkin kullanılabilmesi için yeni teknolojilerden faydalanılarak ulaşım talebinin etkin yönetimine yönelik uygulamalar gerçekleştirilecektir”

“İletişim Hizmetlerinde Vergi Düzenlemesi: İletişim hizmetleri üzerindeki vergiler, hizmet sunum maliyetlerinin önemli bir bölümünü oluşturmaktadır. Katma Değer Vergisine ek olarak alınan Özel İletişim Vergisi (ÖİV), vergi yükünü artırdığı gibi mobil ve sabit iletişim hizmetlerine uygulanan farklı ÖİV oranları, benzer hizmetler arasında adil olmayan bir vergi yükü yaratmaktadır. Bu nedenle, ÖİV, hizmetler arası farklılıkları ve hizmet sunum maliyetlerini azaltacak şekilde yeniden düzenlenecektir. Böylece, iletişim hizmetlerine olan talep ve kullanım artırılacak, benzer mobil ve sabit hizmetler arasında eşit rekabet ortamı oluşturulacaktır”

“Spektrum politikası adil paylaşım, etkin rekabet, erişim maliyetleri, teknolojik gelişmeler, hız ve kalite unsurları değerlendirilerek gözden geçirilecektir. Bu kapsamda kullanılmayan kaynakların teknoloji tarafsız olarak işletmecilere tahsisi sağlanacaktır”.

Politika Formülasyonu Karar Verme Modeli

“Yeni nesil erişim şebekelerinde yaygınlığı artırmak üzere işletmeciler tarafından üstlenilen yatırım kısmi devlet yardımlarıyla desteklenecektir. Genişbant altyapısının götürülmesinin işletmeciler açısından kârlı olmadığı bölgelere yatırım yapılması evrensel hizmet gelirleri ile teşvik

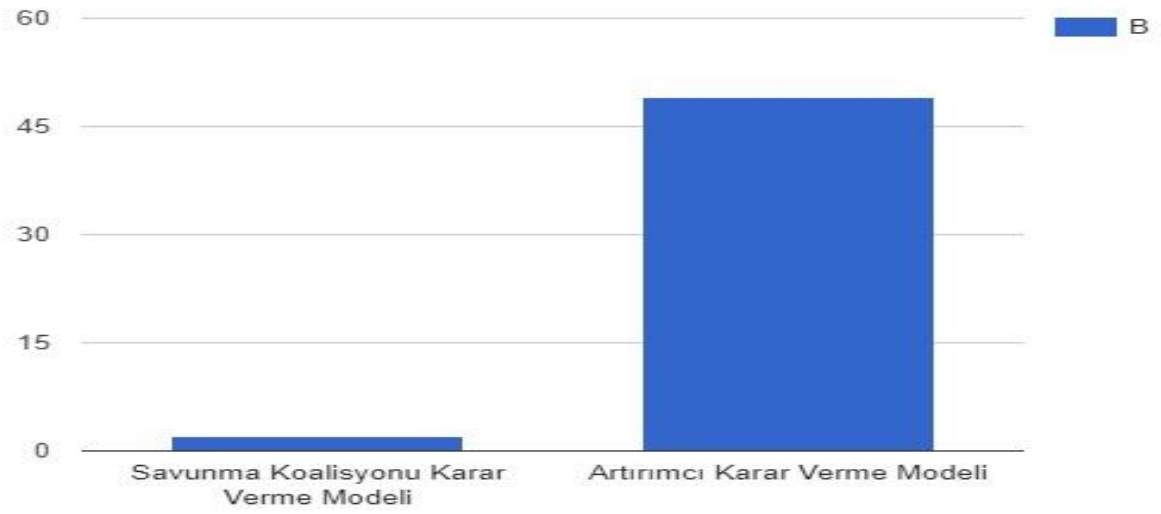
edilecektir. Söz konusu gelirlerin amacına uygun ve etkin kullanımı temin edilecektir".

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Rasyonel KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.1.1.2.2. Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Yorumsamacı Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Artırımcı Karar ver Modelinde 49, Savunma Koalisyonu Karar Verme Modelinde 2 politika önermesi belirlenmiştir.

Tablo 16: Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Strateji Belgeleri)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Artırımcı Karar Verme Modeli,

> *"Bilgi toplumuna dönüşüm, ekonominin geleneksel mekanizmalarının yanı sıra sosyal ve kültürel değişimi de bünyesinde barındıran bütüncül bir süreçtir. Vatandaşların gündelik yaşamlarında ve çalışma hayatlarında bilgi ve iletişim teknolojilerini etkin ve yoğun kullanımı, bilgiye erişim imkânlarının geliştirilmesi suretiyle kendi potansiyellerini gerçekleştirmelerini ve yaşam kalitelerini artırmalarını sağlayacaktır"*
>
> *"Yüksek Motivasyon ve Zengin İçerik: Vatandaşların bilgi ve iletişim teknolojilerini kullanma motivasyonlarını artırmak üzere; bu teknolojilerin günlük hayatta sağlayacağı faydalar konusunda bilinçlendirme çalışmaları yapılacak, kamu ve özel kesimin elektronik ortamda sunduğu hizmetler yaygınlaştırılacaktır"*
>
> *"Yerel yönetimlerce elektronik ortamda sunulan hizmetler geliştirilecek, veri paylaşımı sağlanacak ve bunlara ilişkin esaslar belirlenecektir. Yerel hizmetlerin çevrimiçi sunumunda başarılı uygulamalar yaygınlaştırılacaktır. e-Demokrasi uygulamalarıyla halkın yönetime etkin katılımı sağlanacaktır. Ayrıca, yerel yönetimlerde bilgiye dayalı performans değerlendirme mekanizmaları yaygınlaştırılacaktır".*

Savunma Koalisyonu Modeli

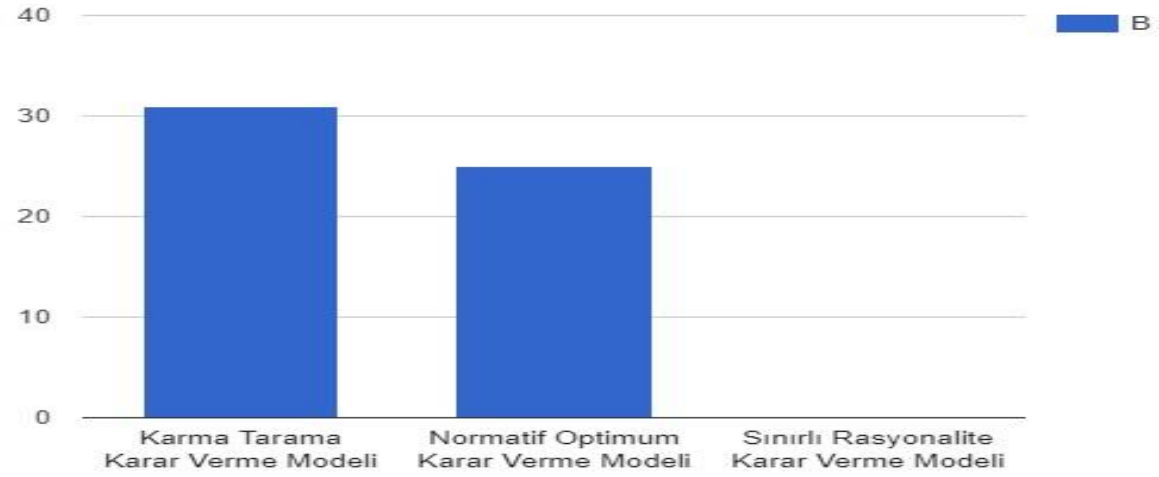
> *"Engellilerin BİT'e erişim imkânları geliştirilecektir. Bu kapsamda, BİT'e erişebilmek için özel yazılım ve donanıma ihtiyaç duyan engellilerin bu ürün ve hizmetleri edinebilmeleri teşvik edilecektir"*
>
> *"Bireylerin BİT erişim ve kullanım durumları ile becerileri daha sağlıklı ölçülecektir. Dezavantajlı olarak nitelendirilebilecek orta yaş ve üstü, gelir düzeyi düşük, kadın, engelli, kırsal kesimde veya az gelişmiş bölgelerde yaşayan bireylerin BİT erişim ve kullanım durumları ile becerileri ölçülerek her bir gruba yönelik odaklı politikalar geliştirilmesini mümkün kılacak bir sayısal bölünme endeksi geliştirilecektir".*

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Yorumsamacı KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.1.1.2.3. Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Karma Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Karma Tarama Karar Verme Modelinde 31, Normatif Optimum Karar Verme Modelinde 25 politika önermesi belirlenirken, Karar Vermede Sınırlı Rasyonalite grubunda hiçbir politika önermesi belirlenmemiştir.

Tablo 17: Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Strateji Belgeleri)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Karma Tarama Karar Verme Modeli

"Tarım bilgi sisteminin kurulumu tamamlanacak, tarım politikaları ve tarımsal destek mekanizmaları, bilgi teknolojileri yardımı ile bilimsel analizlere dayalı şekilde oluşturulacaktır"

"Ortak Teknoloji Hizmetleri ve Altyapı: Kamu hizmetlerinin elektronik sunumunda; ödeme, kimlik belirleme ve onaylama gibi ortak hizmetlerin merkezi bir altyapı üzerinden sunulması, e-devlet kapısı, mobil hizmetler platformu, güvenli kamu ağı, bilgi sistemleri olağanüstü durum yönetim merkezi, çağrı merkezi ve coğrafi bilgi sunum platformu gibi ortak altyapıların

kurulması, bazı ortak yazılımların geliştirilerek kurumlara yaygınlaştırılması sağlanacaktır”

“Meslek içi eğitimler etkinleştirilecek ve yaygınlaştırılacaktır. Bu doğrultuda, BİT alanında belirlenecek konularda özel sektörün meslek içi eğitim amacıyla yapacağı harcamalara yönelik destek mekanizması oluşturulacak, buna ilişkin mevzuat hazırlanacaktır”.

Normatif Optimum Karar Verme Modeli

> *“Eğitim ve Kültür Hizmetleri: Yükseköğretimde kayıt, yurt ve burs başvuru işlemleri elektronik ortama taşınacaktır”*
>
> *“Elektronik imza uygulamasının yaygınlaştırılması ve elektronik belge yönetimi standardizasyonu ile kurumiçi ve kurumlararası tüm yazışmalar, kademeli olarak, belirli güvenlik standartları dâhilinde elektronik kanallara taşınacaktır. Yasal sınırlamalar dışında, 2010 yılında kamuda tüm iç ve dış yazışmaların elektronik ortamda yapılması sağlanacaktır”*
>
> *“Bilgi toplumuna geçişte devlet, vatandaş ve işletmeler arasındaki ilişkilerin etkin şekilde yürütülmesine imkân veren iletişim altyapı ve hizmetlerinin geliştirilebilmesi ve yaygın kullanımının sağlanması için telekomünikasyon sektöründe hizmet ve altyapılarda etkin rekabet ortamı tesis edilecektir. Bu yolla hızlı, güvenli, sürekli ve kaliteli iletişim hizmetlerinin uygun maliyetlerle sunulmasının yanı sıra yeni teknolojilere dayalı telekomünikasyon altyapılarının kurulması için uygun ortam yaratılacaktır”.*

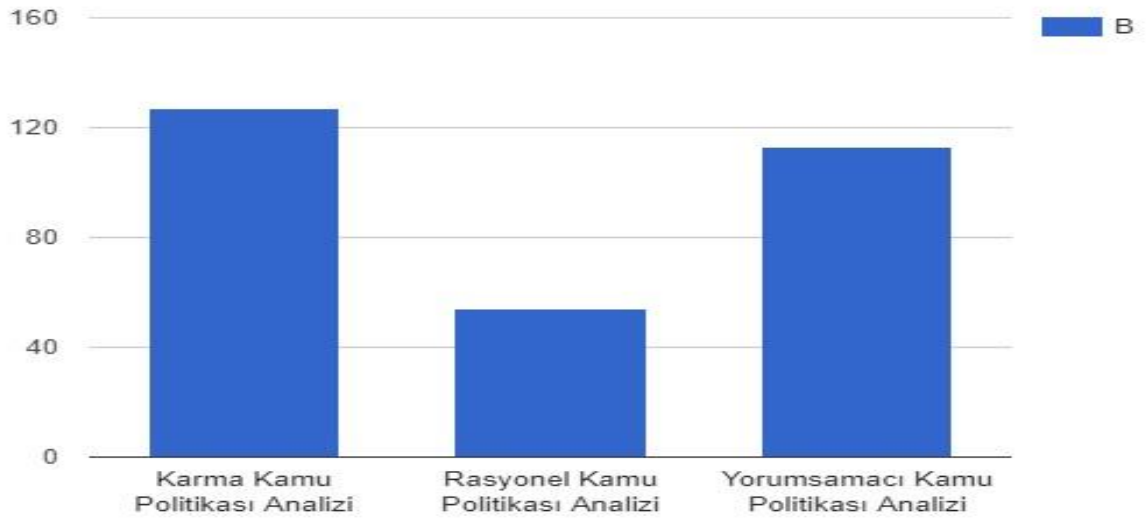
Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Karma KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.1.2. Siber Güvenliğe Ait Bulgular

5.7.1.2.1. Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı

Araştırmada ortaya çıkan bulgulara göre, strateji belgelerinde siber güvenlik ile ilgili toplamda 294 adet politika önermesi yer almaktadır. Söz konusu politika önermelerinin 54'ü Rasyonel, 113'ü Yorumsamacı, 127'si ise Karma Kamu Politikası analiz yaklaşımı içerisinde yer almıştır.

Tablo 18: *Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı (Strateji Belgeleri)*



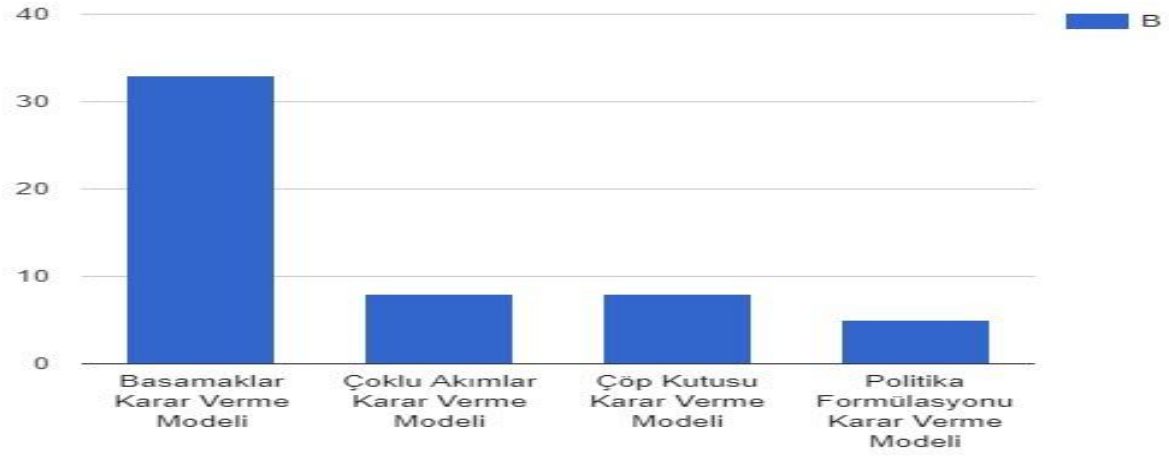
Bu politika önermelerinin hangi karar verme modelleri içerisinde yer aldığı ise aşağıdaki tablolarda, her bir kamu politikası analizi yaklaşımı için ayrı ayrı gösterilmiştir.

5.7.1.2.1. Karar Verme Modellerine Göre Politika Önerme Dağılımı

5.7.1.2.1.1. Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Rasyonel Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Basamaklar Karar Verme Modelinde 33, Çoklu Akımlar Karar Verme Modelinde 8, Çöp Kutusu Karar Verme Modelinde 8 ve Politika Formülasyonu Karar Verme Modelinde 5 politika önermesi belirlenmiştir.

Tablo 19: Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Strateji Belgeleri)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Basamaklar Karar Verme Yöntemi

> *"Yetkinliklerin artırılmasında ve sektörün dışa açılımında sürekliliği ve etkinliği sağlamaya yönelik yönetişim yapıları kurulacak ve ilgili süreçler tasarlanacaktır. Bilgi teknolojileri sektöründe mesleki tanım ve standartlar oluşturulacaktır"*

“Stratejinin genel koordinasyonu, politika belirlemede İcra Kuruluna müşavirlik, gerekli kaynakların tahsisi, bütünleşik e-devlet yapısının oluşumu için standartların ve uyum mekanizmalarının belirlenmesi, uygulamaların strateji hedeflerine uyumunun takibi, uygulama projelerinin yürütülmesinde kurumlara rehberlik, iletişim, ölçme, değerlendirme ve raporlama işlevlerini yerine getirecektir”

“Kamu politikalarının oluşturulmasında yapılacak bütün çalışmaların çerçevesini çizecek BİT Destekli Katılımcılık Programı hazırlanacak ve ilan edilecektir. Katılımcı yönetim konusunda mevzuat taraması yapılacak; mevzuattaki eksiklikler giderilecek; katılımcılık ilke, usul ve esasları belirlenecektir. Türk kamu yönetiminde katılımcı uygulamalar envanteri çıkarılacak; dinamik bir yapıda güncelliği sağlanacak ve en iyi uygulamalar paylaşılacaktır. Katılımcılığa yönelik kuram ve pratik bilginin zenginleştirilmesi ve uygulamaya aktarılması amacıyla katılımcılığa yönelik araştırmalar desteklenecektir. Başbakanlık BİMER, Türk kamu yönetiminde katılımcı yönetim mekanizmasının bir unsuru olacak şekilde geliştirilecektir. Bakanlıklar ve merkezi kamu kurumları tarafından, Başbakanlıkça hazırlanacak Katılımcılık Programı ve güncellenecek BİMER uygulaması çerçevesinde kurumsal Katılımcılık Eylem Planları hazırlanacak ve uygulamaya geçirilecektir”.

Çoklu Akımlar Karar Verme Modeli

“Ulusal farkındalığın arttırılmasına katkı sağlamak amacıyla Mayıs ayının “Siber Güvenlik Farkındalık Ayı” olarak kabul edilmesi ve tüm kamu ve özel sektör kurumlarının bu ayda konuyla ilgili olarak belirli bir plan dâhilinde çalışmalar yürütmesi”.

Çöp Kutusu Karar Verme Modeli

“Bireylerin bu teknolojileri kullanmalarına önemli bir engel teşkil eden güvenlik endişesinin giderilmesi ve güvenli bir İnternet ortamının yaratılması için gerekli tedbirler alınarak kullanımın artırılması yönünde motivasyon sağlanacaktır”

“Siber ortamda çeşitli siber güvenlik olayları meydana geldiğinde kurumların sorumluluklarının ve ulusal düzeyde koordinasyonun nasıl sağlanacağının belirlenmesi”

“Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) "1511 Öncelikli Alanlar Araştırma Teknoloji Geliştirme ve Yenilik Projeleri Destekleme Programı" kapsamında belirlenen öncelikli alanlara “siber

güvenliğin” eklenmesi”.

Politika Formülasyonu Karar Verme Modeli

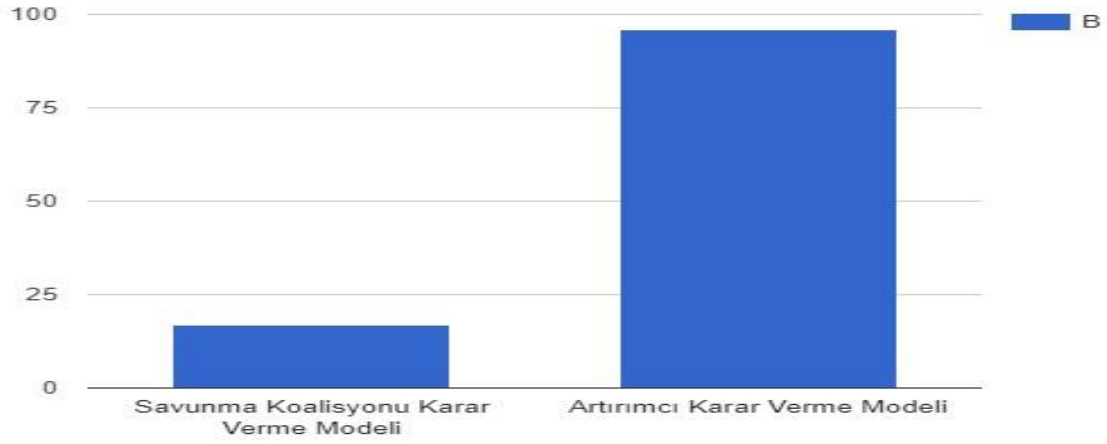
> *“Bilişim sistemlerinin kritik noktalarında kullanılan, yerli veya yabancı donanım ve yazılım ürünlerinin içerdiği açıklıkların kötüye kullanılmasına engel olmak üzere açıklık analizi ve sertifikasyon çalışmalarının yapılması”*
>
> *“Siber Güvenliğin Milli Güvenliğe Entegrasyonu Bu stratejik eylem kapsamında devleti ve ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek, iyi organize olmuş tehdit unsurları tarafından gerçekleştirilecek kasıtlı saldırıların verebileceği zararı azaltmaya dönük eylemlerin gerçekleştirilmesi planlanmaktadır”*
>
> *“Alınan siber güvenlik önlemlerinin ilgili risklerle orantılı olması, olumlu ve olumsuz etkilerinin değerlendirilmesi ve dengelenmesi sağlanır”.*

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Rasyonel KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.1.2.1.2. Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Yorumsamacı Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Artırımcı Karar Verme Modelinde 96, Savunma Koalisyonu Karar Verme Modelinde 17 politika önermesi belirlenmiştir.

Tablo 20: Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Strateji Belgeleri)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Savunma Koalisyonu Karar Verme Modeli

> *"e-Devlet hizmetlerinin sunumunda, kişisel bilgilerin mahremiyetine saygı gösterilecek, kişisel bilgilere erişime ilişkin yetki sınırları belirlenecektir. Bu amaçla, kişisel verilerin korunmasına ilişkin yasal düzenleme yapılacaktır"*
>
> *"Siber ortamda şeffaflık, hesap verilebilirlik, etik değerler ve ifade özgürlüğü desteklenir"*
>
> *"Siber uzay güvenliğinin sağlanması ve sürdürülmesinde; kamu, özel sektör, üniversiteler, sivil toplum kuruluşları ve bireyler dâhil tüm paydaşlar arasında işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımı esas kabul edilir ve güven inşa edilir".*
>
> Artırımcı Karar Verme Modeli
>
> "*Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi Orta ve uzun vadede; siber güvenlik konusunda ülkemizin sahip olduğu teknik birikim, olanak ve kabiliyetler artırılacaktır. Kamu ve özel sektörün Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı 20/47 araştırma ve geliştirme gereksinimlerinin karşılanmasına yönelik tüm eylemlerde işbirliği içerisinde çalışması sağlanacaktır"*

“Mevcut proje teşvik sistemleri içerisine siber güvenliğin öncelikli konu olarak dâhil edilmesi”

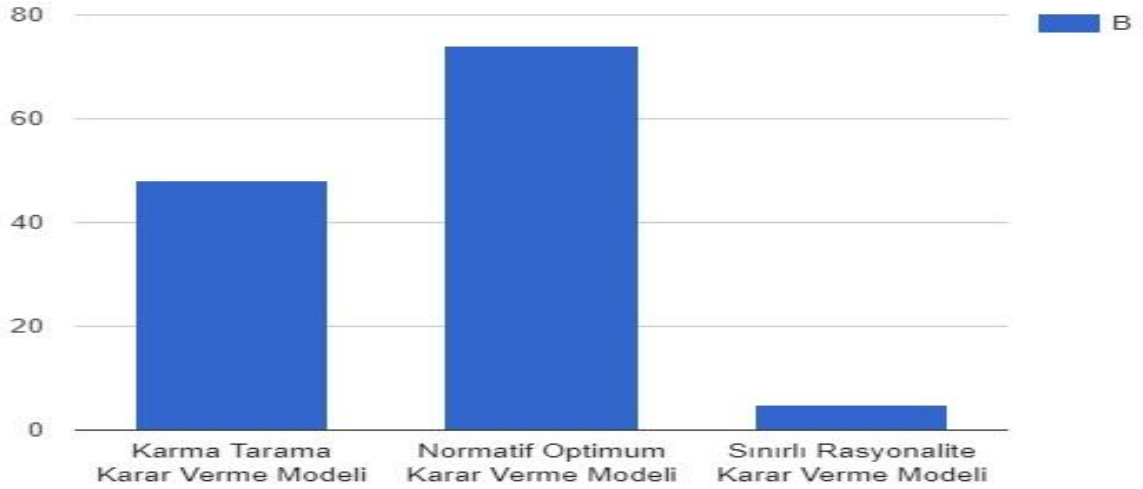
“Toplumun her kesiminde siber güvenlik bilincinin oluşturulması, eğitim kurumlarının çalışmalarına ilave olarak yazılı ve görsel medyada farkındalık çalışmalarının yapılması”.

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Yorumsamacı KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.1.2.1.3. Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Karma Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Karma Tarama Karar Verme Modelinde 48, Normatif Optimum Karar Verme Modelinde 74, Karar Vermede Sınırlı Rasyonalitede 5 politika önermesi belirlenmiştir.

Tablo 21: Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Strateji Belgeleri)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Karma Tarama Karar Verme Modeli

> *“Bilgi toplumuna dönüşüm sürecinde belirlenen stratejilerin ve eylemlerin çeşitli düzeylerde koordinasyonu, hayata geçirilmesi ve izlenmesi için kurumiçi, kurumlararası ve kurumlarüstü örgütsel yapılar oluşturulacak veya mevcut yapılar geliştirilecektir”*
>
> *“Yasal Düzenlemelerin Yapılması 2013-2014 döneminde, ulusal siber güvenliğin sağlanması konusunda gerek kurum ve kuruluşların görev, yetki ve sorumluluklarını tanımlayan, gerekse ihtiyaç duyulan alanlarda mevcut eksiklikleri gidermeyi amaçlayan mevzuatın oluşturulması çalışmalarına başlanacaktır. Söz konusu çalışmalar, ceza hukuku, medeni hukuk, idari yargı ve bunlara ilişkin tüm usul hükümlerinin düzenlenmesine destek olacak bir nitelik arz edecektir. Ayrıca, kavram kargaşasının önüne geçmek amacıyla siber güvenlik terminolojisi ve sözlüğü oluşturulacaktır”*
>
> *“İT vasıtasıyla kültürel miras niteliğinde eserlere ve bilimsel bilgiye erişim imkânları artırılacaktır. Kütüphane, arşiv ve müze gibi bilgi merkezlerinde sürdürülen ve planlanan sayısallaştırma çalışmalarında koordinasyon mekanizması ve standardizasyon süreci ortaya konacak, söz konusu bilgi merkezlerinde bulunan kültürel varlıkların ve eserlerin dijitalleştirilmesine yönelik çalışmalar yürütülecek ve bunlara farklı ortamlardan kolay erişimi mümkün kılacak araçlar hayata geçirilecektir. Ayrıca, bilimsel nitelikteki* bilginin açık bir şekilde sunumu için ulusal politikalar geliştirilecektir”.

Normatif Optimum Karar Verme Modeli

> *“Ehliyet başvurusu, emniyet raporları ve araç ruhsat işlemleri gibi hizmetler elektronik kanallar üzerinden sunulacaktır”*
>
> *“Veri sahipliği belirlenerek veri ve bilgilerin sayısal ortamda tutulması teşvik edilecek ve kamu kurumlarının iş süreçlerinde ihtiyaç duydukları veri ve bilgilere erişimlerini sağlamak üzere, belirlenmiş yetki sınırları dahilinde, güvenli ve etkin bilgi paylaşımını mümkün kılacak temel yapılar hayata geçirilecektir”*
>
> *“Zararlı yazılımları ve bu yazılımların bilişim sistemlerinde yaptığı etkileri belirleyebilecek laboratuvar altyapısının kurulması”.*

Sınırlı Rasyonalite

“Siber güvenliğin sağlanması için tüm paydaşların siber güvenlik risklerini bilmeleri, bu risklerin yönetilmesine ilişkin yaklaşımlarının kendileri kadar başkalarını da etkileyebileceğinin bilincinde olmaları gerekir. Bu farkındalık ve yetkinliğin sağlanması için tüm paydaşların gerekli eğitim ve deneyimi kazanmaları sağlanır. Teknik boyutun yanı sıra; hukuki, idari, ekonomik, politik ve sosyal boyutları da içeren bütüncül bir yaklaşım benimsenir”

“Siber güvenlik, risk yönetimini esas alan etkin ve sürekli değerlendirmeye ve iyileştirmeye dayalı yöntemler aracılığıyla sağlanır. Oluşturulan risk yönetimi metotlarının tehdit ve açıklıkları ele alarak bunlardan dolayı ortaya çıkacak riskleri belirlemesi, bu riskleri kabul edilebilir düzeye indirmek için yöntemler sunması hedeflenir”

“Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması Bu stratejik eylem kapsamında devleti ve ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek riskleri azaltmaya dönük eylemlerin gerçekleştirilmesi planlanmaktadır”.

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Karma KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.2. Kalkınma Planlarından Elde Edilen Bulgular

Bu başlık altında, Türkiye’nin siber güvenlikle ilgili kalkınma planlarından elde edilen bulgular, siber güvenlik ve kritik altyapılar olmak üzere iki grup halinde sunulmuştur.

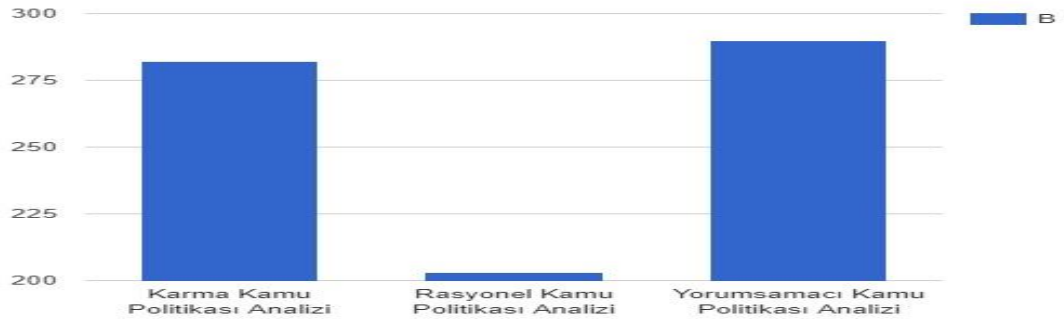
5.7.2.1. Kritik Altyapılara İlişkin Bulgular

5.7.2.1.1. Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı

Araştırmada ortaya çıkan bulgulara göre, kalkınma planlarında kritik altyapılar ile ilgili toplamda 775 adet politika önermesi yer almaktadır. Söz konusu politika

önermelerinin 203'ü Rasyonel, 290'ı Yorumsamacı, 282'si ise Karma Kamu Politikası analiz yaklaşımı içerisinde yer almıştır.

Tablo 22: Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı (Kalkınma Planları)



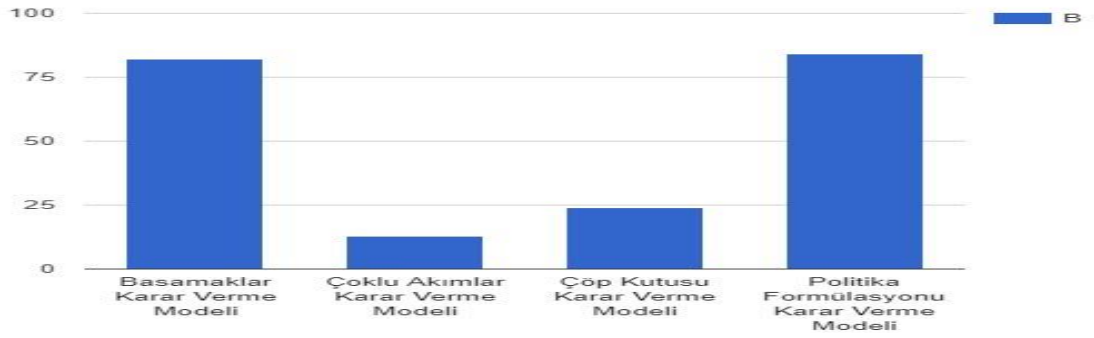
Bu politika önermelerinin hangi karar verme modelleri içerisinde yer aldığı ise aşağıdaki tablolarda, her bir kamu politikası analizi yaklaşımı için ayrı ayrı gösterilmiştir.

5.7.2.1.2. Karar Verme Modellerine Göre Politika Önerme Dağılımı

5.7.2.1.2.1. Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Rasyonel Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Basamaklar Karar Verme Modelinde 82, Çoklu Akımlar Karar Verme Modelinde 13, Çöp Kutusu Karar Verme Modelinde 24 ve Politika Formülasyonu Karar Verme Modelinde 84 politika önermesi belirlenmiştir.

Tablo 23: Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Kalkınma Planları)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Basamaklar Karar Verme Modeli

> *"Ulaştırma türleri ve koridorları, lojistik merkezler ve diğer lojistik faaliyetleriyle bütünleşik Lojistik Master Planı hazırlanarak hayata geçirilecektir. Bu çerçevede, lojistik merkezler için yer seçiminde rehber niteliği taşıyacak şekilde ülkemizin ulaştırma alternatiflerini gösteren ulaştırma koridor haritalarının çıkarılması sağlanacaktır"*

> *"Kırsal yerleşimlerin farklı sektörlerdeki ihtiyaçlarının bir arada programlanmasından oluşacak ilçe bazlı yerel kalkınma programı hazırlanacaktır. Programın tasarımı şehirlere yakınlık durumuna göre, orta ve uzak kırsal yörelerin şartları dikkate alınarak farklılaştırılacaktır"*

> *"Yeraltı ve yerüstü su kalitesinin ve miktarının belirlenmesi, izlenmesi, bilgi sistemlerinin oluşturulması; su kaynaklarının korunması, iyileştirilmesi ile kirliliğinin önlenmesi ve kontrolü sağlanacaktır".*

Çoklu Akımlar Karar Verme Modeli

> *"Tarımsal üretim maliyetlerinin düşürülmesi ve verimliliğin artırılması durumunda ülkemizde dünya fiyatlarının üzerinde seyreden gıda fiyatları düşebilecektir. Bu durum, yerli fiyatların dünyada artan gıda fiyatlarına yaklaşması yoluyla ülkemiz açısından bir fırsat oluşturabilecektir. Öte yandan, artan nüfusu ve gelirinin yanı sıra kültürel yakınlığıyla da önemli bir potansiyel taşıyan Ortadoğu, Kuzey Afrika ve Yakın Doğu'nun*

Türkiye için gıda ürünlerinde daha büyük bir dış pazar haline gelmesi beklenmektedir"

"Gelişmekte olan ülkelerde kömür tüketiminin ve nükleer enerji kullanımının artmaya devam edeceği, dünya genelinde hem hidrolik santrallerin hem de diğer yenilenebilir enerji santrallerinin üretim düzeylerinde ciddi artışlar olacağı; elektrik için yapılacak yatırımların tutarının fosil yakıtların aranması, çıkarılması ve dağıtılması için harcanan tutarlar ile aynı seviyede olacağı tahmin edilmektedir. Enerji verimliliğini artırmaya yönelik kapsamlı programlar yürütülmesinin de gündeme geleceği öngörülmektedir"

"Onuncu Kalkınma Planı döneminde kamu kaynaklarıyla gerçekleştirilecek yatırımlar içinde, tarım sektörünün payının başta GAP Bölgesi olmak üzere sulama yatırımlarının hızlandırılması sonucunda artması; yerli kaynaklara dayalı enerji politikası çerçevesinde enerji hammaddesi aramalarına ağırlık verileceğinden madencilik sektörünün payının artması; kamu tarafından yürütülen hidroelektrik santrallerinin (HES) tamamlanma aşamasına gelmiş olması ve özelleştirmeler sonucu enerji sektörünün payının azalması; en yüksek paya sahip olmakla birlikte ulaştırma sektörünün payının bazı otoyollar, büyük limanlar, havalimanları, gar kompleksleri gibi projelerin KÖİ yöntemiyle gerçekleştirilecek olması nedeniyle azalması; yeni kurulan üniversitelerin ihtiyaçları ve okulların sınıf mevcudunun azaltılması hedefi doğrultusunda eğitim sektörünün payının artması; şehir hastaneleri ve sağlık kampüsleri projelerinde KÖİ yönteminin yaygın olarak uygulanacağı sağlık sektörünün payının azalması; adalet, güvenlik, içme suyu, kanalizasyon ve teknolojik araştırma sektörlerinin paylarının verilen öncelikler çerçevesinde artması öngörülmektedir".

Çöp Kutusu Karar Verme Modeli

"Nüfus artışı, hızlı şehirleşme ve iklim değişikliğinin yağış rejiminde ortaya çıkardığı istikrarsızlık nedeniyle, güvenilir su kaynaklarına erişim ve tarıma elverişli alanların korunması daha fazla önem kazanmıştır. Ekilebilir arazilerin giderek azalması, gıda güvenliği konusunda kritik riskler barındırmaktadır. Dünya genelinde tarım arazileri ve su kaynakları ile ilgili olarak oluşan kısıtlar ve artan talep baskısı, küresel ve bölgesel düzeyde yeni politika ve önlemler geliştirilmesini gerektirmektedir. Ormansızlaşma ve ormanların bozulması konusu ise dünya için giderek artan bir tehdit oluşturmaktadır"

“Dördüncü kesimde değinildiği gibi sektör ve alt sektör Ana planları (i) gelişmelerinde aksama veya tutarsızlık olması halinde öngörülen kalkınma hız ve biçimini olumsuz yönde etkileyebilecek olan ve kamunun hâkim olduğu ya da yönlendirebileceği kritik sektörler için (demir çelik gibi temel imalât sanayileri, enerji, ulaştırma, haberleşme, savunma, madencilik, tarımda sulama, ormancılık), (ii) Eğitini ve sağlık gibi fizik üretimle ve yaşama düzeyi ile yakından ilgili olan kamu hizmetleri için, (iii) üretimle ilişkisi bulunmayan, fakat üretken sektörlerle ayrılan kaynakları sınırlayıcı nitelikteki diğer kamu hizmetleri (genel idare, adalet, asayiş, güvenlik) için yapılacaktır”

“Plan döneminde taşımalarda can ve mal güvenliğinin ve ulaşılabilirliğin artması; taşıma taleplerinin karşılanması; taşıma maliyetlerinin, enerji tüketiminin ve tek enerji türüne bağımlılığın azaltılması; denizyolu, demiryolu ve boru hattı taşımacılığına ağırlık verilmesi; daha verimli bir işletmecilik yapılması, uluslararası taşımalarda döviz kazancının artması sağlanacaktır”.

Politika Formülasyonu Karar Verme Modeli

“Uzun vadeli kalkınma amacımız, yeniden şekillenmekte olan dünyada milletimizin temel değerlerini ve beklentilerini esas alarak gerçekleştirilecek yapısal dönüşümlerle ülkemizin uluslararası konumunu yükseltmek ve halkımızın refahını artırmaktır. Bu çerçevede, 2023 yılında GSYH’nın 2 trilyon dolara, kişi başına gelirin 25 bin dolara yükseltilmesi; ihracatın 500 milyar dolara çıkarılması; işsizlik oranının yüzde 5’e düşürülmesi; enflasyon oranlarının kalıcı bir biçimde düşük ve tek haneli rakamlara indirilmesi hedeflenmektedir”

“Onuncu Kalkınma Planı döneminde uygulanacak politikalar sonucunda reel GSYH’nın yıllık ortalama yüzde 5,5 oranında artması öngörülmektedir. Plan dönemi sonunda, ülkemizin 2023 hedefleriyle de uyumlu olarak, cari GSYH’nın 1,3 trilyon dolara, kişi başına gelirin ise 16 bin dolara ulaşması hedeflenmektedir”

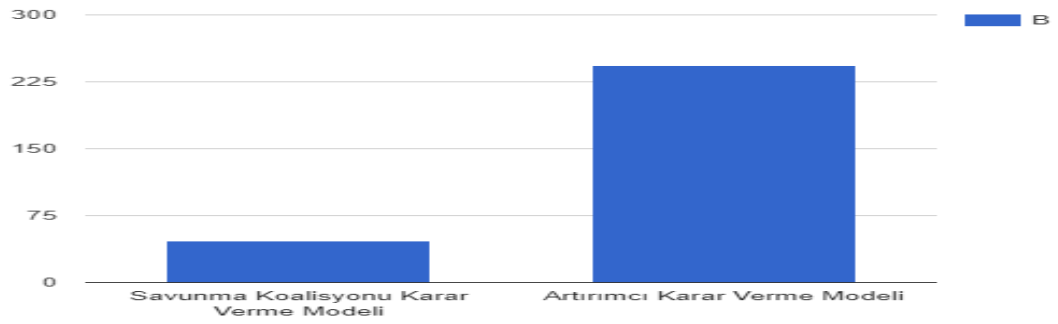
“Plan döneminde yılda ortalama yüzde 17,0 oranında artması öngörülen birincil enerji kaynaklarında en hızlı üretim gerçekleşmesi linyitte görülecektir. Üretim değeri 1978'de 12,5 milyar liradan (15 milyon Ton) 1983'te 31,8 milyar Linyit liraya (51,6 Milyon Ton) çıkarılacaktır. Birinci enerji kaynakları açısından en büyük açığın oluştuğu ham petrolde üretimin IV. Plan döneminde yılda ortalama yüzde 17,4 oranında artarak 1983'te 6 milyon tona ulaşması hedef alınmıştır”.

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Rasyonel KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.2.1.2.2. Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Yorumsamacı Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Artırımcı Karar Verme Modelinde 243, Savunma Koalisyonu Karar Verme Modelinde 47 politika önermesi belirlenmiştir.

Tablo 24: Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Kalkınma Planları)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Savunma Koalisyonu Karar Verme Modeli

> *"Yerli kömür kaynakları özel sektör eliyle yüksek verimli ve çevre dostu teknolojiler kullanılarak elektrik enerjisine dönüştürülecektir. Afşin-Elbistan havzası linyit rezervleri elektrik üretimi için değerlendirilecektir. Küçük rezervli kömür yataklarının bölgesel enerji üretim tesislerinde değerlendirilmesi sağlanacaktır"*

“Madencilik işletmeciliğinin milli kalması temel ilkedir. Özel kesimin sorumluluğunda yürütülecek maden işletmeciliğinin plan ilke ve politikaları doğrultusunda gelişebilmesi özendirilecektir”

“Yatırım kararlarında çevresel etki değerlendirmesi konusuna önem verilecek, ulaştırma sistemlerinin çevreye olumsuz etkileri en aza indirilecektir”.

Artırımcı Karar Verme Modeli

“Fiyat istikrarı ve finansal istikrar amaçları doğrultusunda, krediler ve döviz kuru kanallarının daha etkin çalışması için geleneksel ve geliştirilen yeni araçlarla birlikte, destekleyici bir araç olarak iletişimin de kullanılmasına devam edilecektir”

“Finansal piyasaların sağlıklı işlemesine, finansal ürün çeşitliliği karşısında bireylerin bilinçli kararlar almasına ve yurtiçi tasarrufların artmasına katkı sağlayan finansal eğitim yaygınlaştırılacaktır”

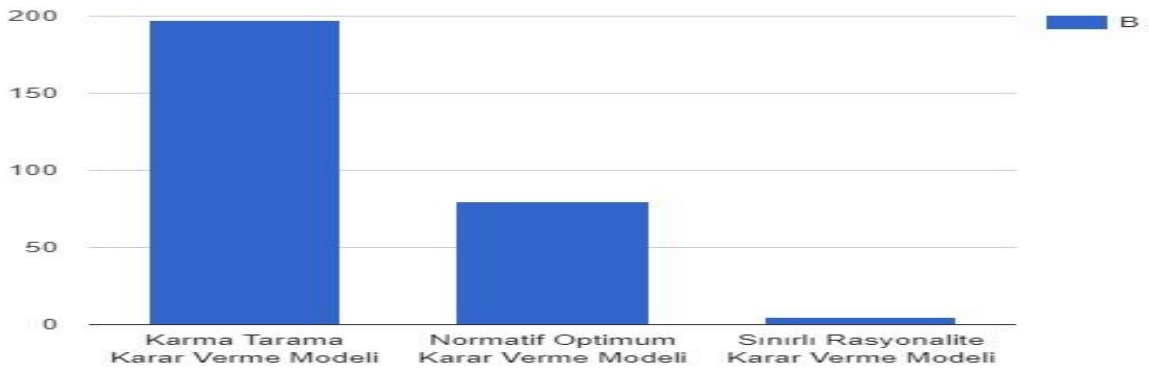
“Su kaynakları dışındaki yenilenebilir kaynaklardan elektrik üretiminin artırılması için yatırım gerçekleşmelerine yönelik izleme ve değerlendirme yapılması”.

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Yorumsamacı KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.2.1.2.3. Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Karma Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Karma Tarama Karar Verme Modelinde 197, Normatif Optimum Karar Verme Modelinde 80 politika önermesi belirlenirken, Karar Vermede Sınırlı Rasyonalite grubunda 5 politika önermesi belirlenmemiştir.

Tablo 25: Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Kalkınma Planları)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Karma Tarama Karar Verme Modeli

> *"Devlet sulama şebekelerinde sulamadan yararlanabilmek için çiftçilerin sulama birlikleri kurmaları bir ön şart haline getirilecektir. Bunun sağlanması, gerek bugünkü, gerekse yani yapılacak şebekelerde dikkate alınacaktır. Kendiliklerinden birlik kurarak sulama tesisleri yapmak isteyen çiftçilerin bu projeleri ekonomik görüldüğü takdirde, devlet yatırımlara katılmayı ve kredi yoluyla yardım yapmayı öncelikle ele alacaktır"*
>
> *"Gıda güvenliğini teminen ürün piyasalarında ve çiftçi gelirlerinde istikrar gözetilerek etkin stok yönetimi, üretim, pazarlama ve tüketim zincirinde kayıpların azaltılması, piyasaların düzenlenmesine ilişkin idari ve teknik kapasitenin güçlendirilmesi ve dış ticaret araçlarının etkin kullanılması sağlanacaktır. Üretici örgütlerinin pazara erişimi kolaylaştırılacaktır"*
>
> *"Katma değeri yüksek ürünlerin geliştirilmesine, gen kaynaklarının korunmasına, ıslah çalışmalarına, nano-teknoloji ve biyo-teknolojiye yönelik araştırmalara öncelik verilecek, tarım ve gıda odaklı teknoparklar ile sektörel teknoloji platformlarının tesis edilmesi sağlanacaktır".*

Normatif Optimum Karar Verme Modeli

"…Bu dönüşüm sürecinde, Türkiye'de bilim ve teknoloji alanındaki gelişmelerin yakından takip edilerek yenilik üretme kapasitesinin yükseltilmesi, yeniliklerin mevcut üretim yapısıyla bütünleştirilerek üretim yapısında dönüşümün sağlanması hedeflenmektedir"

"Akıllı uygulamaların sağlık, ulaştırma, bina, enerji ile afet ve su yönetimi gibi alanlar başta olmak üzere kullanımı yaygınlaştırılacaktır. Şehirlerin bilgi ve iletişim teknolojileri alanındaki altyapı, kapasite ve beceri düzeyleri artırılarak akıllı kentlere dönüşmesi desteklenecektir"

"Soğuk-donmuş zincirin geliştirilmesi ve teknolojisinin iyileştirilmesi ilgili araştırma, eğitim ve yatırım çalışmaları TÜBİTAK yapısında kurulacak Türk Soğuk Tekniği Enstitüsü'nce yönlendirilecektir".

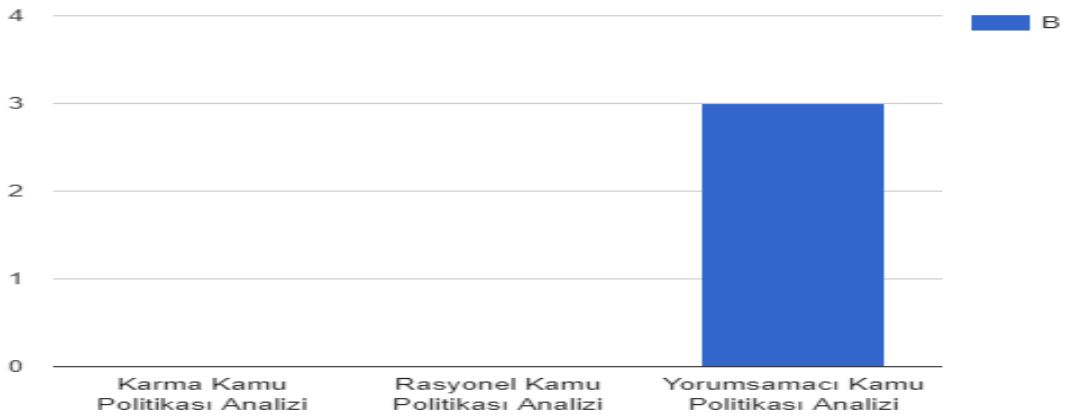
Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Karma KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.2.2. Siber Güvenliğe Ait Bulgular

5.7.2.2.1. Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı

Araştırmada ortaya çıkan bulgulara göre, kalkınma planlarında siber güvenlik ile ilgili toplamda sadece 3 adet politika önermesi yer almaktadır. Söz konusu politika önermelerinin tümü Yorumsamacı, Kamu Politikası analiz yaklaşımı içerisinde yer almıştır.

Tablo 26: Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı (Kalkınma Planları)



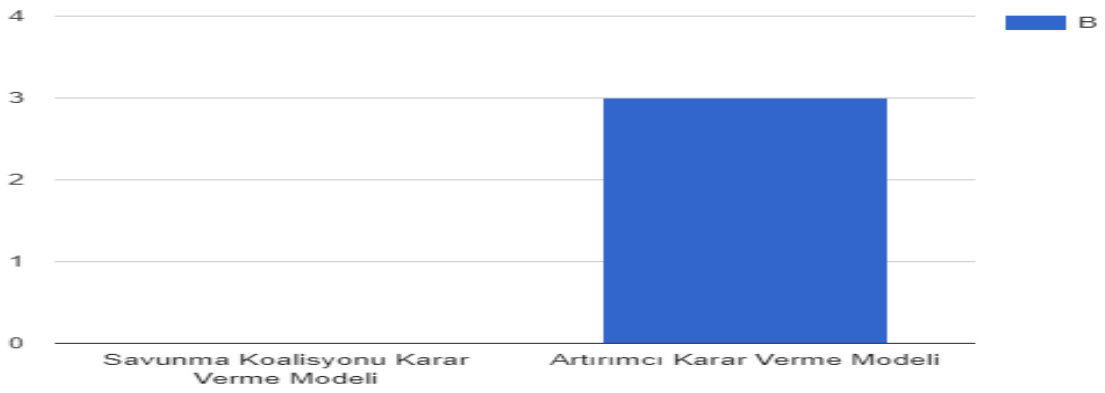
Bu politika önermelerinin hangi karar verme modelleri içerisinde yer aldığı ise aşağıdaki tablolarda, her bir kamu politikası analizi yaklaşımı için ayrı ayrı gösterilmiştir.

5.7.2.2.2. Karar Verme Modellerine Göre Politika Önerme Dağılımı

5.7.2.2.2.1. Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Yorumsamacı Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, sadece Artırımcı Karar Verme Modelinde 3 politika önermesi belirlenmiştir.

Tablo 27: Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Kalkınma Planları)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Artırımcı Karar Verme Modeli

> *"Ulusal ve uluslararası güvenlik stratejilerine paralel olarak, birey, kurum ve devleti tehdit eden siber suçlarla etkin bir şekilde mücadele edilecektir"*
>
> *"Kamu hizmetlerinin sunumunda bilgi güvenliği ve kişisel bilgilerin korunmasına ilişkin hukuki, idari ve teknik düzenlemeler gerçekleştirilecektir"*
>
> *"Kişisel verilerin korunması ve ulusal bilgi güvenliği alanlarında hukuki altyapı tamamlanacaktır".*

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Yorumsamacı KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.3. Hükümet Programlarından Elde Edilen Bulgular

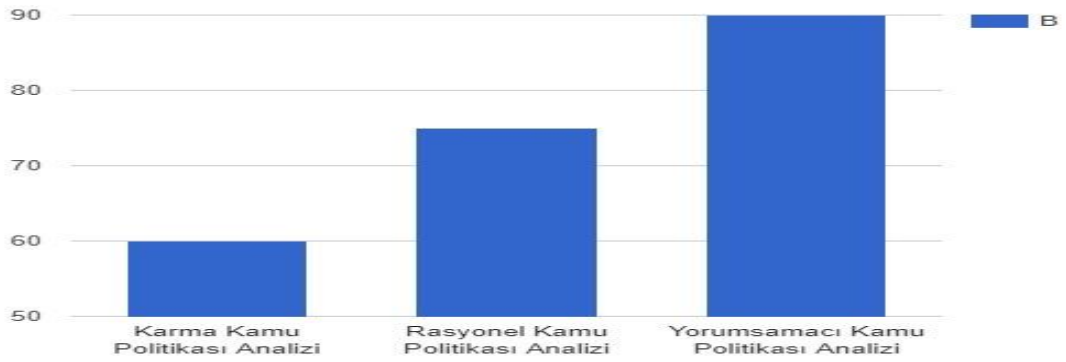
Bu başlık altında, Türkiye'nin siber güvenlikle ilgili hükümet programlarından elde edilen bulgular, siber güvenlik ve kritik altyapılar olmak üzere iki grup halinde sunulmuştur.

5.7.3.1. Kritik Altyapılara İlişkin Bulgular

5.7.3.1.1. Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı

Araştırmada ortaya çıkan bulgulara göre, hükümet belgelerinde kritik altyapılar ile ilgili toplamda 225 adet politika önermesi yer almaktadır. Söz konusu politika önermelerinin 75'i Rasyonel, 90'ı Yorumsamacı, 60'ı ise Karma Kamu Politikası analiz yaklaşımı içerisinde yer almıştır.

Tablo 28: Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı (Hükümet Programları)



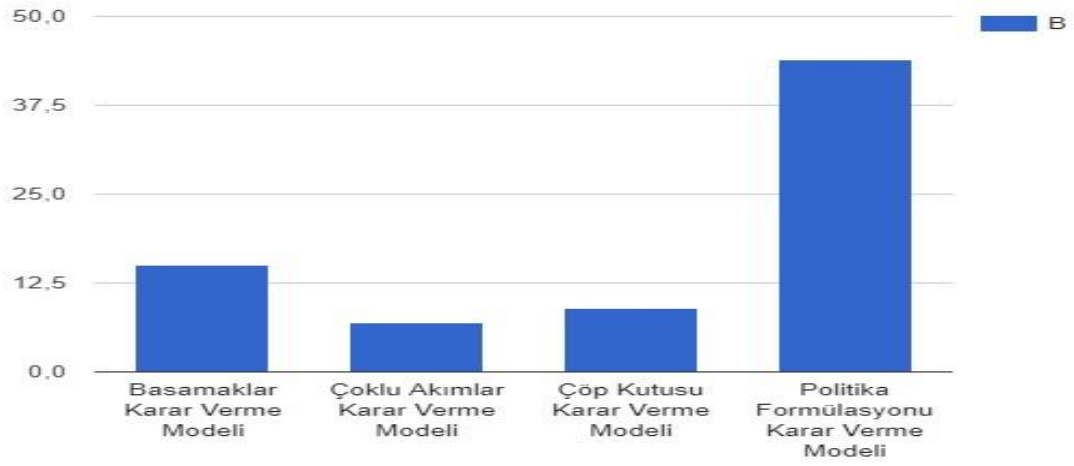
Bu politika önermelerinin hangi karar verme modelleri içerisinde yer aldığı ise aşağıdaki tablolarda, her bir kamu politikası analizi yaklaşımı için ayrı ayrı gösterilmiştir.

5.7.3.1.2. Karar Verme Modellerine Göre Politika Önerme Dağılımı

5.7.3.1.2.1. Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Rasyonel Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Basamaklar Karar Verme Modelinde 15, Çoklu Akımlar Karar Verme Modelinde 7, Çöp Kutusu Karar Verme Modelinde 9 ve Politika Formülasyonu Karar Verme Modelinde 44 politika önermesi belirlenmiştir.

Tablo 29: Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Hükümet Programları)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Basamaklar Karar Verme Modeli

> *"Tarım sektöründe verimliliğin ve üretimin artırılması, üretici gelirlerinin istikrara kavuşturulması, bu kesime yönelik teşviklerin rasyonel kullanılması, hayvancılık potansiyelinin yeniden canlandırılması ve en üst düzeye çıkarılması, ulusal ormancılık politikası doğrultusunda uzun*

vadeli bir ana plan hazırlanarak, gerekli destek ve teşviklerin sağlanması temel amacımızdır. Alternatif ürün projesi ile üretimin iç ve dış pazar talebine göre yönlendirilmesi sağlanacaktır"

"Enerji piyasasının rekabete açılması hızlandırılacaktır. Bu kapsamda, Enerji Piyasası Düzenleme Kurulu ile Enerji ve Tabii Kaynaklar Bakanlığı arasındaki yetki ve sorumluluk alanları netleştirilerek, Bakanlığın politika belirleme yönü güçlendirilecek, uygulamaya ilişkin hususlar Enerji Piyasası Düzenleme Kurulu'na bırakılacaktır. Bu kapsamda, elektrik enerjisi üretim ve dağıtım tesislerinin özelleştirilmesi hızlandırılacaktır"

"Ulaştırma sektöründe Hükümetimizin birinci önceliği, ulaşımın alt sektörleri arasındaki bütünleşmenin temini, ekonomik büyüme amacına en fazla katkının sağlanması ve çevreyi tahrip etmeyen bir ulaştırma altyapısının oluşturulmasıdır. Bu amaçla, ülke ekonomisinin ve sosyal hayatın beklentilerine uygun ulaştırma altyapısını oluşturmak üzere, taşıma türleri arasında dengeyi sağlayacak bir ulaştırma ana planı hazırlanacaktır".

Çoklu Akımlar Karar Verme Modeli

"Hükümetimizin finans sektörü vizyonu, Türkiye'nin bölgesel finans merkezi olarak tercih edilebilirliğini artırıcı ortamı güçlendirmektir. Finans sektöründe rekabetin ve etkinliğin iyileştirilmesi, bölgenin finansal ürün ve hizmet talebini karşılamada önemli avantaj sağlayacak, Türk ekonomisinin uluslararası rekabetinin artmasına önemli destek sunacaktır"

"Hazar Bölgesi ve Orta Doğu gaz rezervlerini Avrupa pazarlarına ulaştırmayı öngören Türkiye-Bulgaristan-Romanya-Macaristan-Avusturya, yani kısa adıyla NABUCCO Doğal Gaz Boru Hattı Projesi'nin gerçekleşmesi için çabamız sürdürülecektir"

"Ayrıca, Türkiye, Yunanistan ve İtalya, yani Güney Avrupa hattı arasında, yılda 12 milyar metreküp kapasiteli doğal gaz boru hattı ile elektrik iletim hattı devreye yakında alınacaktır".

Çöp Kutusu Karar Verme Modeli

"Dalgalı kur politikasına devam edilecektir. Ancak, Merkez Bankası, döviz piyasalarındaki makro ekonomik temellerle bağlantısı olmayan ve

spekülatif nitelikli dalgalanmalara daha duyarlı bir biçimde müdahale edecektir. Döviz kurunda sağlanacak istikrarın, açık pozisyon oluşturarak kâr elde etme şeklinde istismarını önlemek için, bankaların açık pozisyonlarının Bankacılık Düzenleme ve Denetleme Kurumu ile Merkez Bankası tarafından sıkı bir biçimde kontrol edilmesi sağlanacaktır"

"Elektrik enerjisi satış fiyatının ucuzlatılması ve özellikle sanayi sektörüne ucuz enerji temin etmek üzere; elektrik üretim maliyetlerinin, kayıp-kaçak oranlarının, verimsiz kullanımların ve satış fiyatlarının içindeki fon ve payların düşürülmesine yönelik çalışmalar sürdürülecektir"

"Hükümetimiz, ülkemizde yıllardır adeta kaderine terk edilen demir yollarımızın, özel sektörle birlikte ve çağdaş işletmecilik anlayışı çerçevesinde geliştirilmesine özel öncelik verecektir. TCDD Genel Müdürlüğü, bu amaçla yeniden yapılandırılacaktır".

Politika Formülasyonu Karar Verme Modeli

"Ayrıca, hükümetimiz, bölgesel kalkınmaya önem verecek, bunun için sosyal altyapılar güçlendirilecektir. Doğal afetlere karşın uygun tedbirler alınacaktır. Kamu çalışma alanında, fayda-maliyet analizi ve diğer yöntemlerle etkinlik ve şeffaflık artırılacaktır. Bu çerçevede hayatı kolaylaştıran altyapı hizmetlerinin sağlanması ve kalitesinin artırılmasına, elektronik ve bilişim altyapı sistemlerinin yenilenmesine, enformasyon teknolojisinin adaptasyonuna, çevre dosta sosyo-ekonomik yapıların oluşturulmasına, kamu güven ve huzurunun sağlanmasına, bölgesel işbirliğinin güçlendirilmesine özel önem verilecektir"

"Parasal ve mali disiplinin sağlanmasının yanında, yapısal reformların uygulanması, ülkemizde güven ortamını oluşturacak ve belirsizlikleri azaltacaktır. Buna bağlı olarak enflasyonda ve reel faizlerde kalıcı bir düşüş sağlanacaktır. Makro ekonomik istikrarı sağlamaya yönelik para ve maliye politikalarına ilaveten, reel sektörün canlanması için gerekli destek verilecek, üretim, yatırım, ihracat ve istihdamın artırılmasıyla birlikte arzulanan büyüme seviyesine ulaşılacaktır"

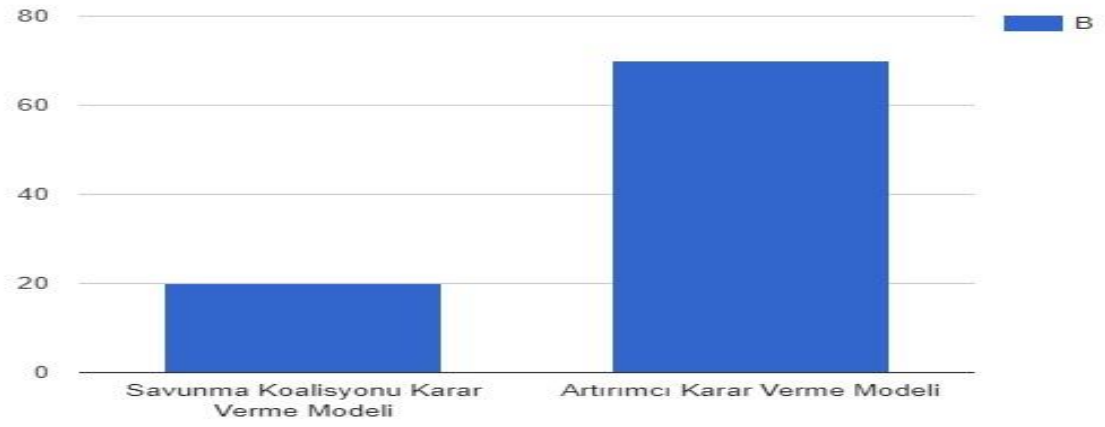
"Özellikle hidroelektrik santraller kapsamında, 2015 yılı sonuna kadar kamu ve özel sektör eliyle yürütülen toplam 5.500 MW'lık ilave gücü devreye alacağız".

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Rasyonel KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.3.1.2.2. Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Yorumsamacı Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Artırımcı Karar ver Modelinde 70, Savunma Koalisyonu Karar Verme Modelinde 20 politika önermesi belirlenmiştir.

Tablo 30: Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Hükümet Programları)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Artırımcı Karar Verme Modeli,

> *"Değerli milletvekilleri, enerji politikamızın temel amacı, rekabetin oluştuğu şeffaf bir piyasa ekonomisi ile artan nüfusumuzun ve hızla*

gelişen ekonomimizin enerji ihtiyacının sürekli, kaliteli, güvenli ve uygun maliyetlerle temin edilmesidir”

“İstanbul Uluslararası Finans Merkezi Projesini hayata geçiriyoruz. Burada vizyonumuzu, İstanbul'un öncelikle bölgesel nihai olarak da küresel bir finans merkezi olması şeklinde belirledik. Bu amaca yönelik olarak ilan ettiğimiz strateji ve eylem planını titizlikle uygulamaktayız. Bu faaliyetlerimizle, İstanbul'un 2023 yılında dünyadaki en önemli 10 finans merkezi içinde yer almasını hedeflemekteyiz”

“Nükleer santral kurulmasına ilişkin çalışmalarımızı hızlandıracağız”.

Savunma Koalisyonu Modeli

“Hükümetimizin enerji politikasının temelinde, ulusal çıkarlarımızı koruyarak, enerji arzının güvenliğini ve devamlılığını sağlamak, serbest rekabete dayalı bir enerji piyasası oluşturmak ve duyarlı olduğumuz çevreyi ve insan sağlığını korumak bulunmaktadır. Aynı zamanda, Türkiye’yi bir enerji köprüsü haline getirebilmek için hükümetimiz azami çaba içinde olacaktır”

“Tarım politikalarımızın temel hedefleri; ülkemizin temel gıda ürünleri üretimi bakımından sadece kendi kendine yeterli olmakla yetinmemesi, uluslararası piyasalarda rekabet edebilmesi, verimli tarım arazilerinin sürekli işlenir halde tutulması ve tarımsal üretimde verimliliğin artırılmasıdır”

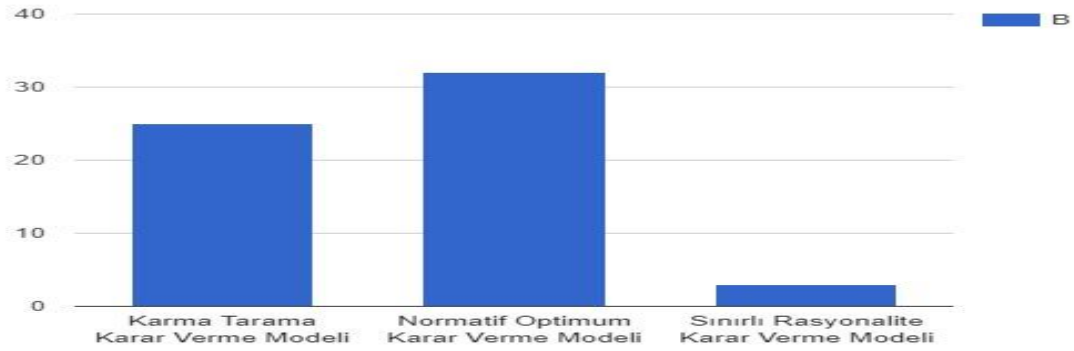
“Başta komşularımız, Türk Cumhuriyetleri, akraba topluluklar olmak üzere, ortak tarih ve kültürü paylaştığımız bütün ülkelerle kültürel ilişkilerimizi derinleştirecek ve bütün uluslararası kuruluşlarda ortak hareket etmemizi sağlayacak mekanizmalar geliştirilecektir. Bu doğrultuda UNESCO Türkiye Milli Komisyonu öncülüğünde bütün Türk Cumhuriyetlerinin, UNESCO Milli Komisyonlarını bir araya getiren düzenli bir işbirliği mekanizmasını hayata geçirdik. Önümüzdeki dönemde bu işbirliğini komşularımız ve bölge ülkelerini de kapsayacak biçimde geliştireceğiz”.

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Yorumsamacı KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.3.1.2.3. Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Karma Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Karma Tarama Karar Verme Modelinde 25, Normatif Optimum Karar Verme Modelinde 32, Karar Vermede Sınırlı Rasyonalite grubunda 3 politika önermesi belirlenmemiştir.

Tablo 31: Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Hükümet Programları)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Karma Tarama Karar Verme Modeli

> *"Temel parasal ve finansal göstergelerin, iç ve dış piyasa koşullarını yansıtacak şekilde oluşmasına imkân verecek para ve finans politikası geliştirilecektir. Merkez Bankası ve finans sektörünün düzenleme ve denetiminden sorumlu üst kurulların üstlendikleri rol ve fonksiyonu yerine getirecek bağımsızlığa sahip olması ön planda tutulacaktır"*

> *"Tarım, ormancılık ve hayvancılık ürünlerinin dünya piyasalarına arzı teşvik edilecek, sektörün kendi kendine yeterliliğine destek verilerek yoksulluğun ortadan kaldırılmasına ağırlık verilecek, karma ve alternatif tarımsal üretim ve metotları teşvik edilerek, tarım sektöründe çeşitlenme ve farklılaşma sağlanacak, tarım sektörüne daha rekabetçi yapı kazandırmak amacıyla, piyasa fiyatlarına duyarlı üretim sistemlerinin oluşmasına imkân sağlanacaktır. Sektörün piyasa yapısının güçlendirilmesi için gerekli yasal ve kurumsal düzenlemeler yapılacaktır"*

“Enerji politikamızda ana unsur, enerji arz güvenliğidir. Elektrik üretim ve dağıtımında özel sektör katılımının sağlanması, rekabetin oluştuğu işleyen bir piyasanın oluşturulması, tedarikçi ülkelerin çeşitlendirilmesi ve enerji üretiminde azami oranda iç kaynak kullanarak ithalata bağımlılığın azaltılması temel önceliklerimizdir”.

Normatif Optimum Karar Verme Modeli

“Yatırım ortamının iyileştirilmesi, etkin ve amaca uygun yapısal reformlar, sanayi ve enerji sektörünün yeniden yapılandırılması ve modernize edilmesi, tarım sektörünün yeniden canlandırılması, gıda sektörünün modernizasyonu, ormancılığın geliştirilmesi, kamusal işler ve konut sektörünün geliştirilmesi, altyapının rehabilitasyonu ve ulaşımın modernizasyonu, iletişim ve enformasyon teknolojisinin geliştirilmesi, turizmin güçlendirilmesi ve turizm sektöründe ürün ve hizmetlerin farklılaştırılması, su kaynaklarının etkin yönetimi, çevrenin korunması, KOBİ’lerin ve kooperatiflerin desteklenmesi, özelleştirme sürecinin şeffaf ve etkin gerçekleştirilmesi, finansal hizmetler sektörünün yeniden yapılandırılması, yabancı sermayenin teşvik edilmesi ve ihracatın artırılması yoluyla sağlanacaktır”

“Komşularımızdaki petrol ve doğal gazın dünya pazarlarına açılmasında ülkemizin dağıtım terminali olma imkanları iyi değerlendirilerek Ülkemiz enerjide bölgesel güç haline getirilecektir. Bu kapsamda, elektrik enerjisi alanında Avrupa ve bölge ülkeleri ile elektrik alış verişine imkan sağlayacak iletim altyapısının ve piyasa düzeninin geliştirilmesine önem verilecektir. Özellikle, Hazar Bölgesi doğal gaz ve petrolünün ülkemiz üzerinden dünya pazarlarına nakline yönelik politikalar sürdürülecektir”

“Önümüzdeki dönemde su kaynağı sorunu yaşanan alanlardaki rehabilitasyona ihtiyaç duyulan sulama tesislerinin modernizasyonunu gerçekleştireceğiz”.

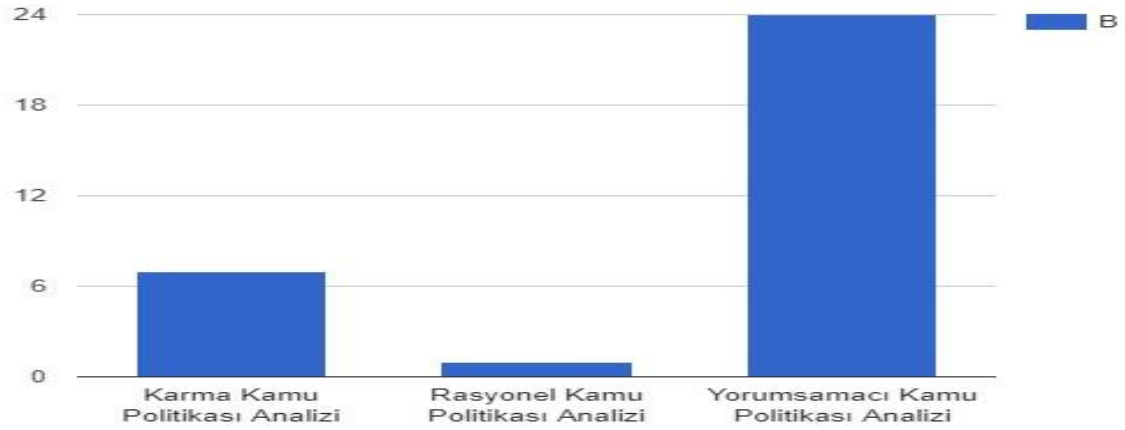
Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Karma KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.3.2. Siber Güvenliğe Ait Bulgular

5.7.3.2.1. Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı

Araştırmada ortaya çıkan bulgulara göre, hükümet programlarında siber güvenlik ile ilgili toplamda 32 adet politika önermesi yer almaktadır. Söz konusu politika önermelerinin 1'i Rasyonel, 24'ü Yorumsamacı, 7'si ise Karma Kamu Politikası analiz yaklaşımı içerisinde yer almıştır.

Tablo 32: Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı (Hükümet Programları)



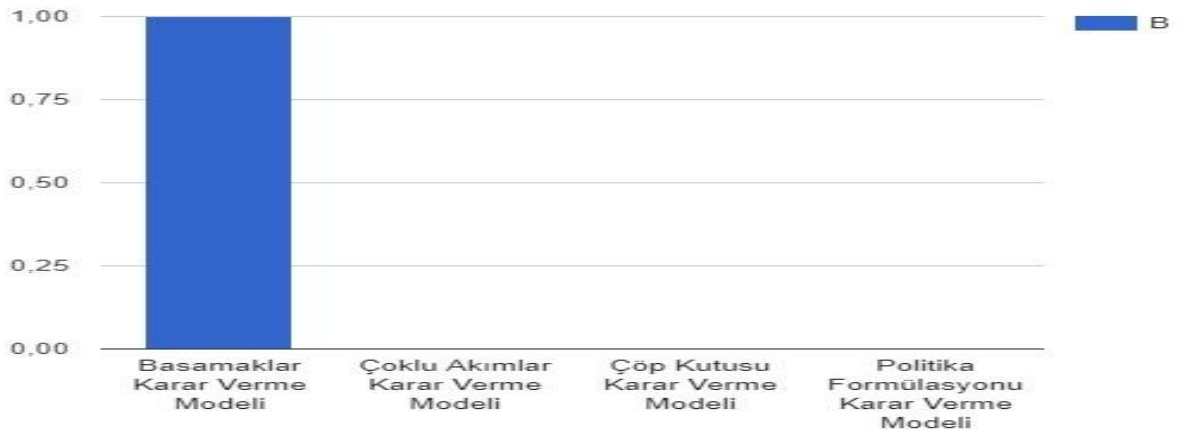
Bu politika önermelerinin hangi karar verme modelleri içerisinde yer aldığı ise aşağıdaki tablolarda, her bir kamu politikası analizi yaklaşımı için ayrı ayrı gösterilmiştir.

5.7.3.2.2. Karar Verme Modellerine Göre Politika Önerme Dağılımı

5.7.3.2.2.1. Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Rasyonel Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Basamaklar Karar Verme Modelinde 1, Çoklu Akımlar Karar Verme Modelinde 0, Çöp Kutusu Karar Verme Modelinde 0 ve Politika Formülasyonu Karar Verme Modelinde 0 politika önermesi belirlenmiştir.

Tablo 33: Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Hükümet Programları)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Basamaklar Karar Verme Yöntemi

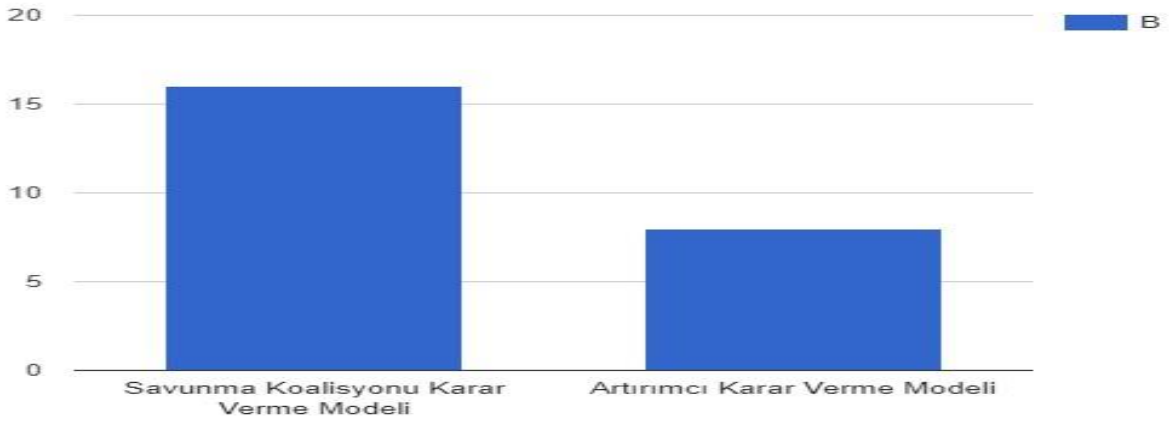
> *"Mobil iletişim teknolojisi kullanılarak kentlerimizin cadde, sokak ve meydanları görüntülü güvenlik denetimine alınmıştır"*

Yukarıda örnek olarak gösterilen politika önermesi yorumlanarak Rasyonel KPA içerisinde konumlandırılan ilgili karar verme yaklaşımı içerisinde gruplandırılmıştır.

5.7.3.2.2.2. Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Yorumsamacı Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Artırımcı Karar Verme Modelinde 8, Savunma Koalisyonu Karar Verme Modelinde 16 politika önermesi belirlenmiştir.

Tablo 34: Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Hükümet Programları)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Savunma Koalisyonu Karar Verme Modeli

> *"Hükümetimiz, bölgesel güvenlik ortamının, ekonomik kalkınmaya önemli katkıda bulunduğu görüşündedir. Bu nedenle, Türkiye, yakın çevresinde güven ve istikrarın tesisi için daha fazla çaba sarf edecek, komşularıyla diyaloga dayalı ilişkiler sürdürme çabasını artıracak,*

böylelikle bölgesel işbirliğinin gelişmesine daha fazla katkıda bulunacaktır"

"Türkiye'nin gücünü her türlü şart ve coğrafyada hissettirecek, hem konvansiyonel hem de asimetrik muharebeleri icra edebilecek, caydırıcılığı, beka kabiliyeti ve muharebe gücü yüksek bir savunma sistemi ve gücünün oluşturulması ana hedefimiz olmuştur, olmaya devam edecektir"

"Bundan önce olduğu gibi, bundan sonra da bireylerin, kurumların ve mülkiyetin güvenliğini, özgürlük ve güvenlik arasındaki hassas dengeyi dikkate alarak, insan haklarını ve evrensel değerleri esas alan bir asayiş ve güvenlik ortamının sağlanması temel amacımızdır".

Artırımcı Karar Verme Modeli

"Savunma sanayimizin uluslararası etkinliği de artırılmış, askerî hücümbot ve gemiler, silah, diğer savunma araç gereçleri ile komuta kontrol ve elektronik harp sistemleri ihracatımız 350 milyon dolara çıkarılmıştır"

"Hükûmetimiz, ekonomi politikalarında "şeffaflık", "süreklilik", "tutarlılık" ve "öngörülebilirlik" ilkelerini esas almaya devam edecektir"

"Hükümetimiz, teröre karşı uluslararası zeminler oluşturulması ve Türkiye'nin bu zeminlerde teröre karşı işbirliği yaparak mücadele edilmesine önem verecektir. Bu çerçevede 11 Eylül sonrası tırmanma eğilimi gösteren dinler ve kültürler arası gerilimlerin azaltılması ve küresel bir barış ortamının sağlanabilmesi için aktif çaba sarf edecektir".

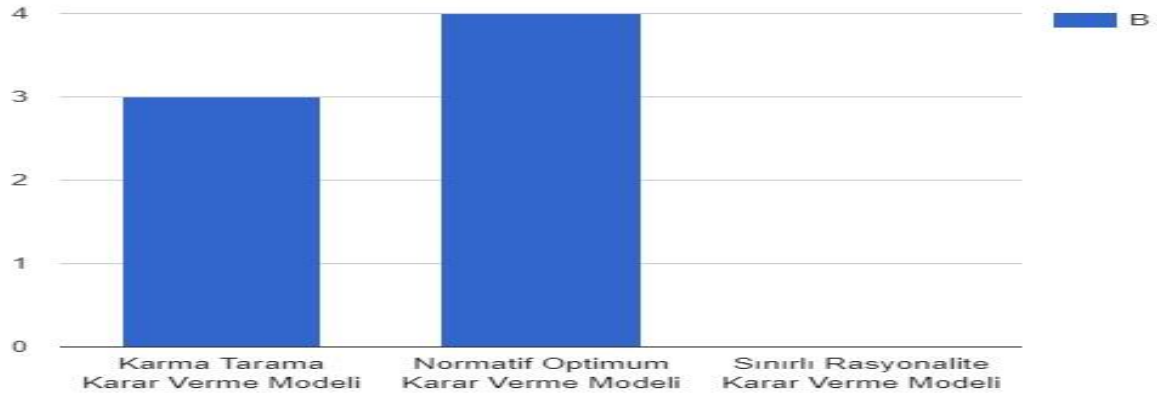
Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Yorumsamacı KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.3.2.2.3. Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Karma Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Karma Tarama Karar Verme

Modelinde 3, Normatif Optimum Karar Verme Modelinde 4, Karar Vermede Sınırlı Rasyonalitede 0 politika önermesi belirlenmiştir.

Tablo 35: Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Hükümet Programları)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Karma Tarama Karar Verme Modeli

> *"Türkiye'nin her bir köşesinde sosyal ve ekonomik kalkınmayı hızlandırmak, hiçbir bölgemizin geride kalmamasını sağlamak amacıyla çalışmalarımız yoğunlaşarak devam edecektir"*
>
> *"Millî güvenliğimizi güçlendirmek, ulusal birliğimizi muhafaza etmek için verdiğimiz bu mücadeleyi, 60'ıncı Hükûmet döneminde de her türlü meşru aracı kullanarak devam ettireceğiz"*
>
> *"Türkiye, özellikle yakın coğrafyasında bir istikrar, güvenlik ve özgürlük kuşağının yanı sıra, geniş ve ölçek ekonomilerini kullanan iktisadi refah havzaları oluşturacaktır. Türkiye'nin uzun dönemli refahı, ulusal ölçeği aşan bir ekonomik perspektifle mümkündür. Yakın komşularımızla yürüttüğümüz İkili Yüksek Düzeyli Stratejik İşbirliği Konseyi uygulamaları bu açıdan büyük öneme sahip olduğu gibi, uluslararası diplomasiye özgün bir katkı getirmiştir. Ayrıca, bölgesel işbirliği programları ile KEİ, İSEDAK ve EİT gibi çok taraflı örgütlerin sunduğu imkânlar bu çerçevede değerlendirilecektir. İlgili bakanlık ve kuruluşlarımız kendi*

görev alanlarında dışa dönük, bölgesel ve uluslararası perspektifi iş planlaması ve süreçlerine hâkim kılacaklardır".

Normatif Optimum Karar Verme Modeli

"Ankara savunma sanayimizin başkenti. İnşallah, yeni projelerle Ankara'nın bu vasfını daha da güçlendiriyor, dünyanın en büyük savunma sanayii merkezlerinden biri haline getiriyoruz"

"ASELSAN tarafından 100 milyon doların üzerinde bir yatırımla Gölbaşı'nda radar ve elektronik harp tasarım ve üretim merkezi kurulacak"

"Türkiye, Irak'ın güvenlik, barış ve demokrasiye kavuşması için en fazla çaba sarf eden ülkelerin başında oldu. Irak ile köklü tarihi, kültürel, coğrafi ve ekonomik bağlarımız bu çabaların gösterilmesini stratejik bir zaruret haline getirmektedir".

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermesi yorumlanarak Karma KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.4. Raporlardan Elde Edilen Bulgular

Bu başlık altında, Türkiye'nin siber güvenlikle ilgili meclis ve Emniyet Genel Müdürlüğü raporlarından elde edilen bulgular, siber güvenlik ve kritik altyapılar olmak üzere iki grup halinde sunulmuştur.

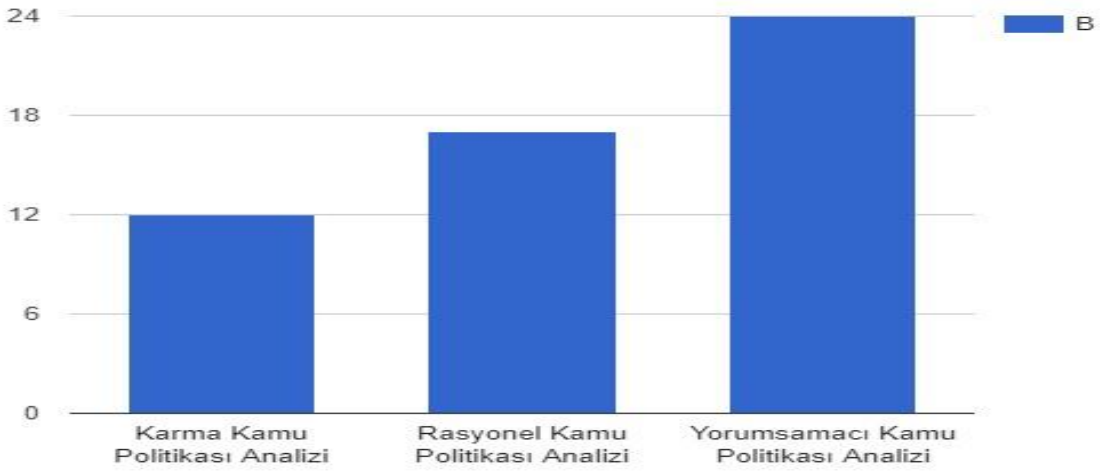
5.7.4.1. Kritik Altyapılara İlişkin Bulgular

5.7.4.1.1. Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı

Araştırmada ortaya çıkan bulgulara göre, raporlarda kritik altyapılar ile ilgili toplamda 53 adet politika önermesi yer almaktadır. Söz konusu politika

önermelerinin 17'si Rasyonel, 24'ü Yorumsamacı, 12'si ise Karma Kamu Politikası analiz yaklaşımı içerisinde yer almıştır.

Tablo 36: Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı (Raporlar)



Bu politika önermelerinin hangi karar verme modelleri içerisinde yer aldığı ise aşağıdaki tablolarda, her bir kamu politikası analizi yaklaşımı için ayrı ayrı gösterilmiştir.

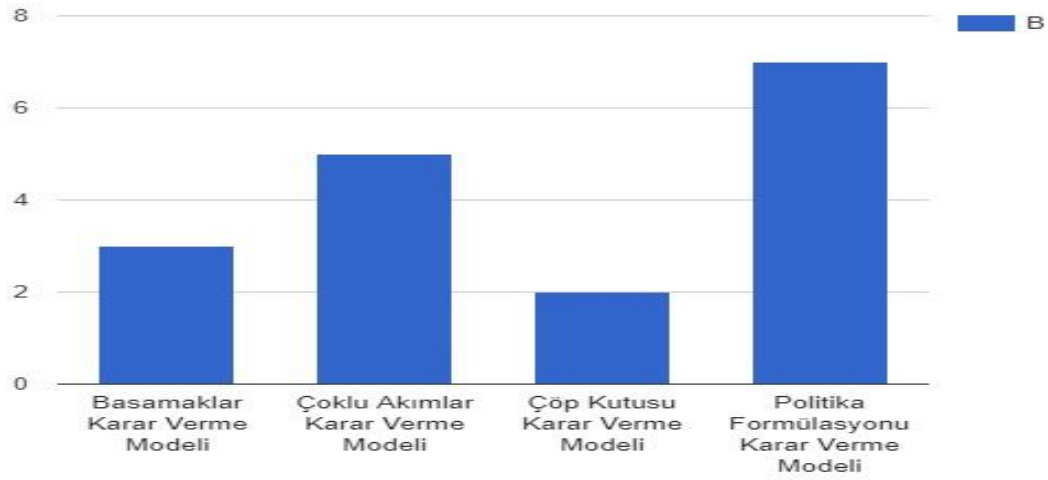
5.7.4.1.2. Karar Verme Modellerine Göre Politika Önerme Dağılımı

5.7.4.1.2.1. Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Rasyonel Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Basamaklar Karar Verme Modelinde 3, Çoklu Akımlar Karar Verme Modelinde 5, Çöp Kutusu Karar Verme

Modelinde 2 ve Politika Formülasyonu Karar Verme Modelinde 7 politika önermesi belirlenmiştir.

Tablo 37: Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Raporlar)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Basamaklar Karar Verme Modeli

> *"Bilgi İletişim Teknolojilerinin gündelik yaşamın vazgeçilmez bir öğesi olduğu günümüzde tartışılmaz bir hâl almıştır. Bilgi İletişim Teknolojilerinin getirdiği imkânlar beraberinde bir takım da riskleri barındırmaktadır. Bilgi İletişim Teknolojilerinin getirdiği imkânlar ve risklerin tespiti ve bu tespit sonucunda imkânların ve risklerin araştırılması, risklerin belirlenerek sorunların giderilmesi ve çözüm yollarının araştırılması amacıyla anayasamızın 98'inci maddesi, iç tüzüğün 104 ve 105'inci maddeleri gereğince ekte sunulan gerekçe çerçevesinde Meclis Araştırması açılmasını arz ve teklif ederiz"*

> *"Dünya örnekleri incelendiğinde, yazılım sektörüne devlet tarafından sağlanan katkıların doğrudan destek, teşvik ve dolaylı destekler olarak üç ana başlıkta gruplandığı görülmektedir. Bu tür destek ve teşvikleri İrlanda, İsrail, Hindistan, Çin, Malezya, Tayvan ve Brezilya gibi ülkeler uygulamaktadırlar. Ülkemizde de yazılım sektörünün, bahsedilen ülke*

örneklerinde olduğu gibi kritik sektör olarak değerlendirilmesi ve bu bağlamda bu sektörün ihtiyaçlarına ve yapısına özel destek ve teşvik enstrümanlarının geliştirilmesi gerekmektedir"

"İlaveten, bilgi ve iletişim sektörünün ulusal ve uluslararası patent veri tabanlarından daha etkin faydalanmasını sağlayacak eğitim vb. programların hazırlanması ve uygulanması gerekmektedir".

Çoklu Akımlar Karar Verme Modeli

"Bu konuda, 5809 sayılı Kanun'un 5'inci maddesinin birinci fıkrasının (ğ) bendi ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 40'ıncı maddesi ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilen yetkiler, yazılım sektöründe beklenen sıçramayı sağlamaya yönelik bir fırsat olarak görülmektedir. Bu nedenle, belirlenen mevzuat uyarınca toplanacak araştırma - geliştirme gelirlerinden yazılım sektörüne gereken kaynağın ayrılması beklenilmektedir"

"Gelişen telekomünikasyon imkânları ve bilgi teknolojileri hizmetleri, bilgi çağına geçişi hızlandırmış ve ülkeler kalkınma planlarını belirlerken bu teknolojilere yatırım yapmayı ihmal etmemişlerdir. Hemen hemen her sektörde etkin bir şekilde kullanılan bilişim teknolojileri ve uygulamaları, ülkelerin gerek yönetimlerinde gerek gelişimlerinde önemli rol oynamaktadır. Bilişim teknolojileri her geçen gün yenilenmekte, günlük hayata yeni yeni ürünler girmektedir. Bu kadar dinamik ve finansal kapasitesi yüksek, hemen hemen her sektörün gelişimine önayak olan bu sektörün, ülkemizde de gelişmesi için gerekli yatırımların yapılması, Ar-Ge faaliyetlerinin özendirilmesi ve bilişim kültürü ve önemi farkındalığının arttırılması, gelişmiş ülke olma şartlarından biri olarak değerlendirilmektedir"

"Türkiye'nin büyüme ve gelişmesine en büyük katkıları sağlayan sektörlerden biri olan elektronik haberleşme sektöründe, vergi ve mali yükümlülüklerin hafifletilmesinin, yeni teknolojik gelişmeler ve uygulamaları teşvik edeceği ve bu suretle, mobil genişbant ve telemetri uygulamalarında ciddi bir pazarın oluşacağı değerlendirilmektedir. Bu sayede, oluşan değer zincirinden, bilgi toplumuna dönüşümün yanında, işletmeciler dışında cihaz üreticileri ve yazılım sektöründeki çözüm ortakları da kazanç sağlayacaktır".

Çöp Kutusu Karar Verme Modeli

“Ayrıca yetkilendirme ücretinin Bilgi Teknolojileri ve İletişim Kurumu’nun göstereceği süre içerisinde ödenmemesi halinde yetkilendirmenin iptal edileceği hususunun, anılan Kanun’un yaptırımları genel olarak düzenleyen maddesi yerine, yetkilendirme bedellerini düzenleyen maddesinde, kanunen belirlenmiş bir süreyi de içerecek şekilde düzenlenmesinin kanunilik ilkesinin etkinliği açısından daha uygun bir tercih olacağı düşünülmektedir”

“Şehirlerarası iletişim altyapısı çalışmalarında kamulaştırma ve altyapı güvenliği gibi sıkıntılar yaşanabilmektedir. Bu sıkıntıların etkin bir şekilde çözülebilmesi için şehirlerarası karasal şebekelerin, TCDD’nin demiryolu ağları ve BOTAŞ’ın petrol ve doğal gaz boru hatlarının geçtiği güzergâhlara konuşlandırılmasında büyük yarar bulunmaktadır”.

Politika Formülasyonu Karar Verme Modeli

“Ülkemizin bilgi ve iletişim sektöründeki 2023 yılı vizyonu ve hedefleri arasında yer alan bilişim sektörünün 160 milyar dolara ulaşması ve bunun GSYH’deki payının %8’e çıkarılması, yazılım sektörünün öncelikli alan olarak belirlenmesi ve toplam ihracatta yazılım sektörü payının %2’ye çıkarılması hedeflerinin gerçekleştirilebilmesi için bilişim sektörü stratejik sektör olmalı, siyasi sorumluluk ve sahiplenme gerçekleştirilmeli, devlet destekleri ve teşvikleri arttırılmalı, yerli üretim ve girişimcilik desteklenmeli ve talepler arttırılmalı, rekabetçi piyasa oluşturulmalıdır”

“Dolaylı vergilerin yüksek olması, dolaylı ve dolaysız vergiler arasındaki dengesizliği artırmaktadır. Dolaylı vergiler tüketicilerin gelir düzeyine bakılmaksızın tahsil edilmektedir. Elektronik haberleşme sektöründe uygulanan vergiler Avrupa Birliği’ne uyum sürecinde yürütülen müzakerelerde ve ilerleme raporlarında eleştirilmektedir. Bu açıdan, elektronik haberleşme sektöründeki dolaylı vergi yükünün Avrupa Birliği ortalamasına çekilmek suretiyle hafifletilmesi ve Avrupa Birliği müktesebatıyla uyumun sağlanması hedefine ulaşılmalıdır”

“Ülkemizin jeopolitik özellikleri de dikkate alındığında, soğutma maliyetlerinin düşük olduğu, iklimlendirmede avantajlı bölgelerine, genişbant internet altyapısı başta olmak üzere yapılacak yatırımlar ve hizmeti cazip kılacak vergilendirme ve fiyatlandırma politikaları ile hem

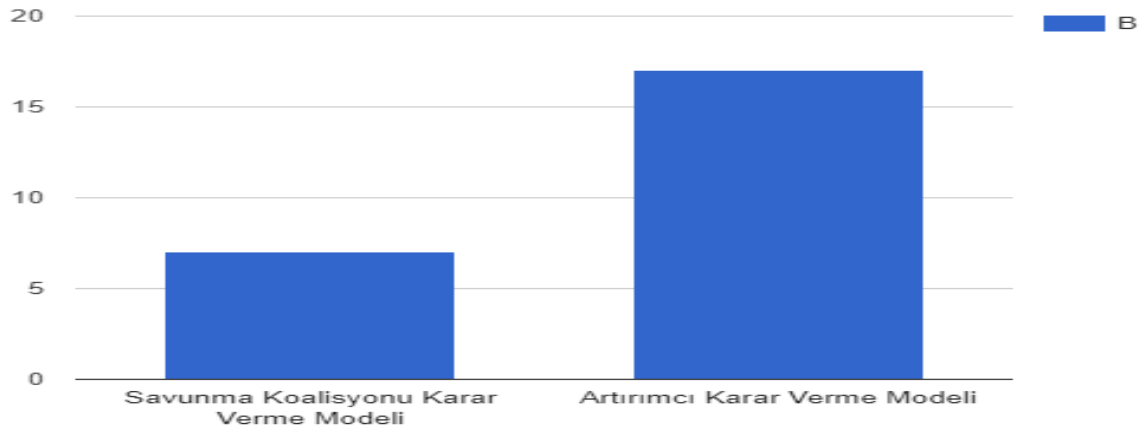
yerli içeriğin yurt içinde barındırılması sağlanarak bu alanda dışa bağımlılık azalacak, hem de bölge ülkelerine de bu hizmetin sunulması fırsatı doğacaktır. Ayrıca, barındırma maliyetlerinin ve dolayısıyla barındırma ücretlerinin düşmesi, içerik üreticilerini de cesaretlendirecek ve yerli içerik üretimini artıracak bir hususdur".

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Rasyonel KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.4.1.2.2. Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Yorumsamacı Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Artırımcı Karar ver Modelinde 17, Savunma Koalisyonu Karar Verme Modelinde 7 politika önermesi belirlenmiştir.

Tablo 38: Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Raporlar)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Artırımcı Karar Verme Modeli,

“İşletmelerin uygun koşullarda finansman kaynaklarına erişimi kolaylaştırılacak ve bu kaynaklarda çeşitlilik sağlanacaktır. Başta KOBİ’ler olmak üzere girişim sermayesi, başlangıç sermayesi ve kredi garanti sistemi geliştirilerek işletmelerin kredi temini kolaylaştırılacaktır”

“Bilişim sektöründe istihdamı artırmak amacıyla yazılım sektörü stratejik bir alan olarak değerlendirilmelidir. Bilişim sektörü istihdamı için uluslararası düzeyde veri tabanı ve yazılım uzmanı, ağ teknolojileri uzmanı, bilgi güvenliği uzmanı, web programcısı yetiştirilmeli ve bilgi teknolojileri proje yönetimi eğitimi verilmelidir. Meslek lisesindeki bilişim bölümlerinin kalite ve nitelikleri artırılmalıdır. Fen edebiyat fakültelerinde isteğe bağlı yazılım dersleri verilmeli ve öğrenciler bu derslere yönlendirilmelidir“

“İlk tesis özel iletişim vergisinin kaldırılması, İnternet hizmetlerine uygulanan mali yükümlülük çeşitliliğinin azaltılması”.

Savunma Koalisyonu Modeli

“Yerli içeriğin yaygınlaştırılmasını teminen, işletmecilerin özel iletişim vergisi, idari ücret ve evrensel hizmet gibi mali yükümlülüklerinin elektronik haberleşme hizmetlerinden elde ettikleri gelirleriyle sınırlandırılması, içerik, ürün satışı, e-ticaret, mobil ödeme ve katma değerli servis gelirlerinin ise söz konusu mali yükümlülüklerin ve idari para cezalarının matrahına dâhil edilmemesi”

“Türkiye kaynaklı arama motoru, sosyal paylaşım siteleri, e-posta sağlayıcıların yaygınlaştırılmasının sağlanmasını teminen, söz konusu faaliyetlerin teşvik edilmesi ve vergisel kolaylıklar da dâhil gereken kamusal desteğin sağlanması”

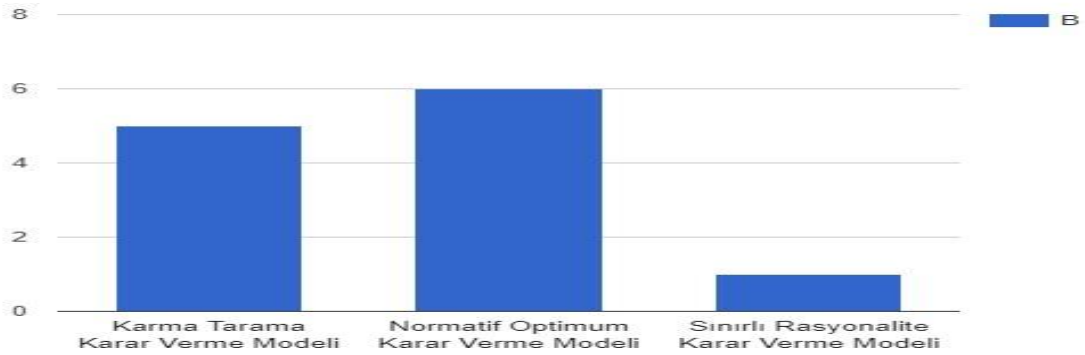
“Bilişim sektöründe donanım ve yazılım alanında yatırımcılara pazar alanlarının oluşturulması, üretilen ürünlere devlet tarafından belli miktarlarda alım garantisi verilmesi ve bu konuda üreticiyi destekleme esnasında koşullar konularak kuralların belirlenmesi, Türkiye’de tüketimi artan iletişim araçlarının üretiminin yerelleştirilmesinin sağlanması”.

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Yorumsamacı KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.4.1.2.3. Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Karma Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Karma Tarama Karar Verme Modelinde 5, Normatif Optimum Karar Verme Modelinde 6, Karar Vermede Sınırlı Rasyonalite grubunda 1 politika önermesi belirlenmemiştir.

Tablo 39: Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Raporlar)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Karma Tarama Karar Verme Modeli

> *"Bilişim ve haberleşme teknolojileri ürünleri ile internet kullanımı, bir yandan da toplumun en temel ihtiyaçlarından birisi olan ve Anayasa ile teminat altına alınmış bulunan haberleşme hak ve hürriyetinin kullanımına, özel hayatın gizliliğine ve kişisel verilerin korunmasına ilişkin bulunmaktadır. Kişisel bilgilerin korunmasını, özel hayatın ve haberleşmenin mahremiyetini de ilgilendiren bilişim sektörünün*

fırsatlarından azami ölçüde istifade edilmesini ve öngörülen hedeflere ulaşılmasını teminen; öncelikle hizmet sunumunu özgürlük olarak algılayan, gerekli olmadıkça idarenin müdahalesini en aza indirmeyi amaçlayan, teknolojinin gelişimi önündeki engelleri azaltmayı hedefleyen, işletmecileri sektöre özgü sınırlı ve belirli yükümlülüklere tabi kılan, mali yükümlülük ve idari yaptırımlar ile kişi özgürlüklerini kısıtlayan hukuki olayları sıkı koşullara bağlayan, çağdaş hizmet sunumu anlayışının benimsenmesi gerekmektedir. Dünyanın en önemli sektörlerinden birisi olan bilişim sektörüne bu anlayışı hakim kılmak, dünyaya entegre ve bilgi toplumu olma yolunda hızla ilerleyen ülkemiz için bir zorunluluk olarak değerlendirilmektedir"

"Bilişim teknolojilerinin yaygınlığını artırmak amacıyla, e-devlet uygulamalarının tüm kamu kurum ve kuruluşlarında vatandaşın ve çalışanların işlerini kolaylaştıracak şekilde kullanılması, geliştirilmesi ve ulaşılabilir hale getirilmesi"

"Bilişim yatırımları için fayda-maliyet, fizibilite, etki analizi gibi çalışmalar genel kabul görmüş standartlara uygun gerçekleştirilmelidir".

Normatif Optimum Karar Verme Modeli

"KOBİ'lerin ve girişimcilerin rekabet güçlerini artırmak ve yeni pazarlara açılmalarını sağlamak için, iş kurma ve iş geliştirme aşamalarında eğitim ve danışmanlık hizmeti sağlanacaktır. Bu amaçla, İŞGEM ve benzeri yapılanmalar yaygınlaştırılacak ve etkinliklerini artırmak üzere gerekli düzenlemeler yapılacaktır"

"bilişim sektörünün gelişimi ve bilgi toplumuna dönüşme hedef ve stratejilerinin gerçekleştirilmesini ve sayısal uçurumun giderilmesini teminen; hem sabit fiber altyapının hem de mobil altyapının kurulmasında işletmecilerin karşılaştığı idari ve mali güçlüklerin giderilmesi, bürokrasinin minimize edilmesi, işletmecilerin kamu mülkiyetindeki arazilerden, doğalgaz, petrol, elektrik ve enerji nakil hatlarından, karayolu, demiryolu ağlarından ve bunların haberleşme atıl altyapı ve kapasitelerinden uygun koşullarla sağlanmasının gerekli olduğu değerlendirilmektedir"

"İşsizlikle mücadelede, bilişim ve teknoloji kanalları ile bilgisayar eğitimi önemli olup, bilgi akış kanallarını doğru kullanan, en önemli bilgi kanalı haline gelen internetten doğru ve hızlı yararlanabilen, teknoloji ve bilimsel gelişmelere ayak uyduran ve bu konularda aldığı eğitimlerle öne

> *çıkan kişilerin, iş bulma olanağı yüksektir. Buna karşın, bilgi ve iletişim teknolojileri alanında gereken beceriyi sağlayamayan ve gelişmelere ayak uyduramayan bireylerin iş bulma imkânı da zorlaşmaktadır. Bilişim teknolojilerinin kullanımı, mevcut iş alanlarında talebi şekillendirerek, yeni iş alanları yarattığı gibi, işsizlik sorunun çözümünün de anahtarıdır. Bu nedenle teknoloji kullanım kültürünü anahtar yetkinlik kabul eden bir eğitim reformu, Türkiye'nin atılım stratejisinin en önemli parçalarından birisi olacaktır. Bu anlayış içinde sadece gençlerin değil, mevcut işgücünün de bilgi ve iletişim teknolojileri becerilerinin geliştirilmesi zaruridir".*

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Karma KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.4.2. Siber Güvenliğe Ait Bulgular

5.7.4.2.1. Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı

Araştırmada ortaya çıkan bulgulara göre, raporlarda siber güvenlik ile ilgili toplamda 137 adet politika önermesi yer almaktadır. Söz konusu politika önermelerinin 32'si Rasyonel, 45'i Yorumsamacı, 60'ı ise Karma Kamu Politikası analiz yaklaşımı içerisinde yer almıştır.

Tablo 40: Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı (Raporlar)

Bu politika önermelerinin hangi karar verme modelleri içerisinde yer aldığı ise aşağıdaki tablolarda, her bir kamu politikası analizi yaklaşımı için ayrı ayrı gösterilmiştir.

5.7.4.2.2. Karar Verme Modellerine Göre Politika Önerme Dağılımı

5.7.4.2.2.1. Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Rasyonel Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Basamaklar Karar Verme Modelinde 25, Çoklu Akımlar Karar Verme Modelinde 2, Çöp Kutusu Karar Verme Modelinde 3 ve Politika Formülasyonu Karar Verme Modelinde 2 politika önermesi belirlenmiştir.

Tablo 41: Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Raporlar)

Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Basamaklar Karar Verme Yöntemi

> *"Hazırlanacak olan yeni Bilgi Toplumu Stratejisi ve Eylem Planı, bilişim sektörünün sürdürülebilir kalkınmaya katkısını azamiye çıkarma ve siber güvenliği sağlama işlevi görmelidir. Anılan Strateji Belgesinin hazırlanmasında TBMM Bilişim ve İnternet Komisyonu'nun işbu Raporundaki bulguları ve önerileri dikkate alınmalıdır"*

> *"Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı ile kurulan Siber Güvenlik Kurulunca, ivedilikle ulusal siber güvenlik stratejisi ve eylem planı oluşturulmalı; planın uygulama sürecine ilişkin sorumlu kurum/kuruluşlar açıkça belirlenmeli ve uygulama süreci periyodik olarak Kurul'a raporlanmalıdır"*

> *"İnsan Kaynakları Çalışmaları Siber güvenliğin sağlanması için gerçekleştirilecek insan kaynakları çalışmalarında personel istihdamı ve eğitim önemli yer tutmaktadır. Bu kapsamda, öncelikle yedekliliği sağlayacak şekilde yetişmiş personel istihdam edilmeli, sistem yöneticilerine işlettikleri sisteme hâkim olmalarını sağlayacak eğitimler*

planlanmalı, devamında ise bilgi güvenliği konusunda çalışacak uzman personel (mümkünse ayrı bir birim olacak şekilde) için bilgi güvenliği uzmanlık eğitimleri planlanmalıdır. İnsan kaynakları çalışmaları siber güvenliği sadece teknik bir olgu olarak görmemeli, siber güvenlik için gerçekleştirilecek eğitimlerde tüm bilgi sistemi kullanıcıları için düzenli bilinçlendirme çalışmaları yapılmalıdır".

Çoklu Akımlar Karar Verme Modeli

"Savunma Sanayi Müsteşarlığı ile birlikte yürütülen projede Teşkilatımızın Bilgi Teknolojileri kaynaklarının, iç ve dış siber tehditlere karşı korunması amaçlanmaktadır. Bilgi Güvenliği Projesi ile kurulacak olan Zararlı Yazılım Laboratuvarı sayesinde adli süreçlerin kısalması ve bağlı il birimlerimize zararlı yazılım inceleme yeteneği kazandırılması planlanmaktadır. Aynı zamanda kurulması planlanan Sosyal Medya Analiz Sistemi ve Açık Kaynak İstihbarat Sistemi ile de sosyal medya üzenden işlenen suçlar ile mücadele kapasitemiz artırılacak, önleme faaliyetlerimiz kapsamında bilgi toplama yeteneklerimiz artırılacak, takip etmekte zorlandığımız (deepweb, darknet) platformlardan bilgi alma imkânlarına kavuşulacaktır"

"Bilişim sektöründe donanım ve yazılım alanında yatırımcılara pazar alanlarının oluşturulması, üretilen ürünlere devlet tarafından belli miktarlarda alım garantisi verilmesi ve bu konuda üreticiyi destekleme esnasında koşullar konularak kuralların belirlenmesi".

Çöp Kutusu Karar Verme Modeli

"Psikolojik, göz bozukluğu gibi fiziksel rahatsızlıklara da neden olmakta zaman kaybını da beraberinde getirmektedir. Bir diğer olumsuz tarafı da internet oyunlarından sanal para alabilmek maksadı güdülerek maddi kayıplara neden olmaktadır. Bu olumsuzlukların asgariye indirilmesi konusunda uluslararası işbirliğine ihtiyaç duyulmaktadır"

"Yurt dışı kaynaklı sanal oyun pazarı ve oyun üretimi nedeniyle, yurt dışına çıkan trafiğin ve pazar gelirlerinin yurt içinde tutulabilmesini, bu gelirlerin vergilendirilebilmesini, çocukların ve gençlerin ruhsal ve ahlaki gelişimlerini olumsuz yönde etkilemeyecek oyunların üretimini teminen,

Türkiye'de üretilecek sanal oyunlara yönelik vergisel kolaylıklar da dâhil gereken kamusal desteğin sağlanması"

"Bulut bilişim hizmetinde, hizmet alıcıya ait kişisel verilerin yetkisiz kişilerce ele geçirilmesi, güvensiz veya hatalı şekilde silinmesi, değiştirilmesi, ifşa edilmesi, çıkar amaçlı kullanılması gibi sorunlarla karşılaşılmasının engellenmesi gerekmektedir. Bu güçlük ise, kişisel verilerin korunmasına ilişkin sağlam bir yasal çerçevenin oluşturulması ile bertaraf edilebilecektir".

Politika Formülasyonu Karar Verme Modeli

"2010 yılında TÜİK'in yapmış olduğu bir araştırmaya göre ülkemizde İnternet kullananların 72,8'i e-posta alıp gönderiyor, %22,6'sı seyahat, konaklama ve bilet satın alma gibi işlemler yapıyor, %10,2'si iş başvurusu yapma amacıyla bilgilerini İnternet ortamında paylaşıyor, %16,8'i İnternet bankacılığını kullanıyor, %4,1'i mal veya hizmet satın alma işlemi yapıyor. Görüldüğü gibi bu işlemlerin hepsinde kişisel verilerimizin kaybolması, çalınması ya da kötü amaçla kullanılmasını doğrudan etkileyen birçok neden bulunmaktadır. Özellikle de bu tür güvenlik problemlerinin ana merkezini İnternet cafe'ler oluşturmaktadır. Evde ebeveynlerine yakalanma korkusu yaşayan çocuklar, IP adresinin bilinmesini istemeyen hacker'lar yasadışı ve işlemler için İnternet cafeleri tercih etmektedirler. Ayrıca, oyun salonlarında bolca vakit geçiren çocuklar ve gençlerimizin bu bağımlılığa kendilerini kaptırmaları dolayısıyla sağlık problemleriyle karşılaşmaktadırlar"

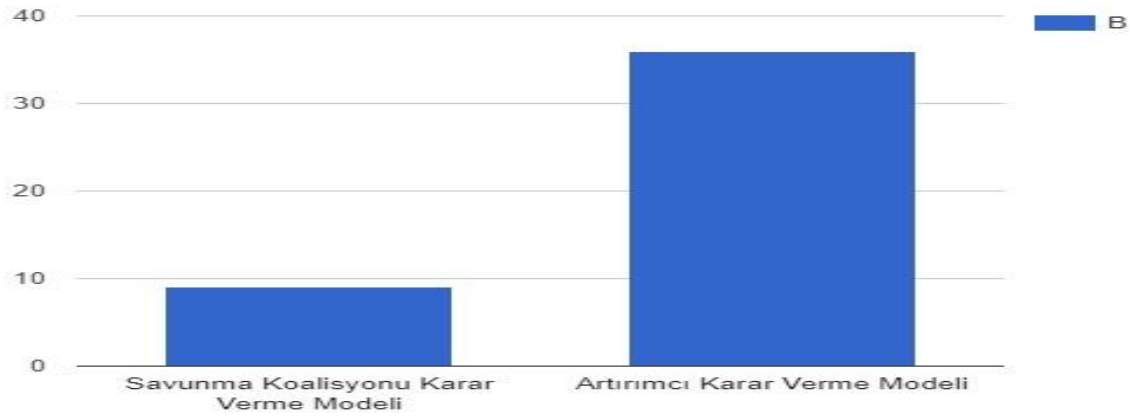
"Yazılımların, anılan kriterleri sağladıklarını doğrulayacak mekanizmaların geliştirilmesi, ulusal ağlarda dolaşan zararlı yazılımlar ve bulaştıkları sistemlerde yaptıkları etkilerin belirlenmesi, bu zararlı yazılımlara karşı uygulanacak korunma önlemlerinin geliştirilmesi".

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Rasyonel KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.4.2.2.2. Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Yorumsamacı Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Artırımcı Karar Verme Modelinde 36, Savunma Koalisyonu Karar Verme Modelinde 9 politika önermesi belirlenmiştir.

Tablo 42: Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Raporlar)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Savunma Koalisyonu Karar Verme Modeli

> *"Türkiye kaynaklı arama motoru, sosyal paylaşım siteleri, e-posta sağlayıcıların yaygınlaştırılmasının sağlanmasını teminen, söz konusu faaliyetlerin teşvik edilmesi ve vergisel kolaylıklar da dâhil gereken kamusal desteğin sağlanması"*

> *"Ülkenin yararı için büyük önem taşıyan bilgi toplumuna giden yolun tıkanmaması, ülke içinde dijital uçurumun derinleştirilmemesi gerekir. Yapılacak hukuki düzenlemelerle, bilgi toplumuna giden yolu geliştirici ve teşvik edici bir ortamın yaratılması için çaba gösterilmelidir. Asıl olan*

uluslararası sınırlara bakılmaksızın bilgiye ulaşılması, elde edilmesi, elde edilen veya oluşturulan bilginin başkalarına ulaştırılması sürecinde kamu makamlarının müdahale ve sınırlandırmalarının minimum düzeye indirilmesidir. Bilişim ve iletişim teknolojileri alanındaki hukuksal düzenlemeler, ülkeyi bilgi toplumuna taşıyacak seferberliğe katkıda bulunmalı ve insanların, ulusların gelişime açık bir hukuksal koruma sağlayan hukuk yoluyla temel hak ve özgürlüklerin korunduğu bir zemin yaratmalıdır. Bu çerçeveye, dijital bölünmenin önüne geçecek, teknolojiyi ülkenin her yerine yaymak için teknoloji erişimini kolaylaştıracak, ucuzlatacak ve herkes için ulaşılabilir kılacak teşvik kararları, özelleştirme mevzuatı, kamusal teknoloji erişimiyle ilgili düzenlemeler vb. dâhildir"

"Ülkenin bilgi toplumuna dönüşmesi, bilişim ve iletişim teknolojilerinin etkin bir biçimde kullanımıyla kamu yönetiminde şeffaflığın ve katılımın sağlanması ve yargı sürecinin şeffaf ve adaletli bir biçimde işleyebilmesi için, temel insan hak ve özgürlüğü olarak kabul edilen "Kamu Bilgilerine Erişim Özgürlüğü", açık ve net bir şekilde anayasa ile teminat altına alınmalı ve ayrıca özel bir bilgi edinme hak ve özgürlüğü yasası çıkarılmalıdır".

Artırımcı Karar Verme Modeli

"Yerli içeriğin yaygınlaştırılmasını teminen, işletmecilerin özel iletişim vergisi, idari ücret ve evrensel hizmet gibi mali yükümlülüklerinin elektronik haberleşme hizmetlerinden elde ettikleri gelirleriyle sınırlandırılması, içerik, ürün satışı, e-ticaret, mobil ödeme ve katma değerli servis gelirlerinin ise söz konusu mali yükümlülüklerin ve idari para cezalarının matrahına dahil edilmemesi"

"Faaliyetleri tüm kamu sektörünü etkileyen Maliye Bakanlığı gibi bazı kurumlarda her bir ana hizmet biriminin ayrı bilişim birimleri bulunmaktadır. Mükerrer yatırımlar yapılmamasını ve ciddi siber risklere yol açılmamasını teminen, söz konusu birimler arasında eşgüdüm sağlanmalıdır"

"Kurum İçi ve Kurumlar Arası Koordinasyon Son olarak, yaşanan bilgi güvenliği olaylarının çoğuna kurumların tek başına müdahale etmesi ya da kurum içindeki bilgi işlem biriminin tek başına çözüm üretmesi mümkün olmamaktadır. Siber güvenlik tehditleriyle mücadele edebilmek için gerek kurum içi (bilgi işlem birimi, hukuk birimi, iletişim birimi vs.) gerekse kurum dışı paydaşlarla iletişim arttırılmalı ve gerekli

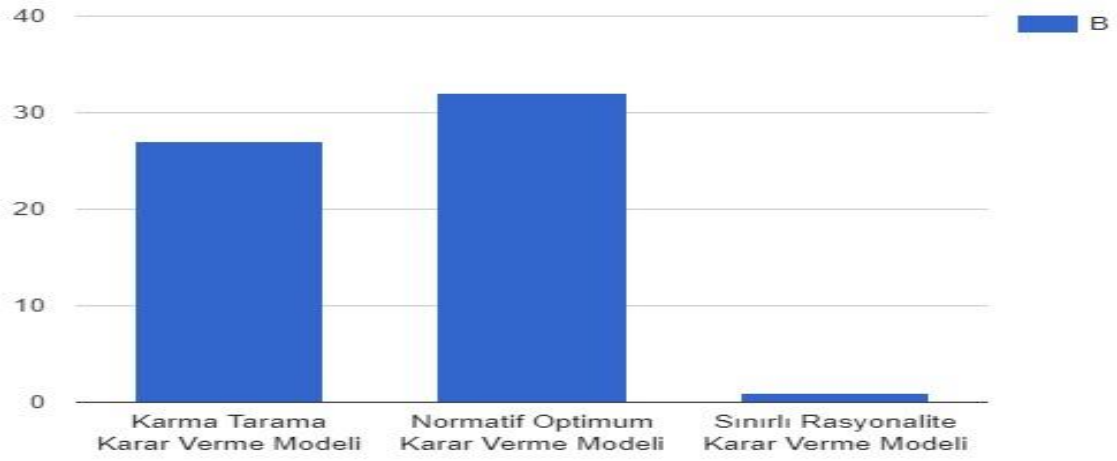
koordinasyon sağlanmalıdır".

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Yorumsamacı KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.4.2.2.3. Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Karma Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Karma Tarama Karar Verme Modelinde 27, Normatif Optimum Karar Verme Modelinde 32, Karar Vermede Sınırlı Rasyonalitede 1 politika önermesi belirlenmiştir.

Tablo 43: Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Raporlar)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Karma Tarama Karar Verme Modeli

> *"Siber güvenlik alanında çalışan grup ise bu alanı "yeterli gelişmenin olmadığı bir alan olarak belirtilmiş olup, bu konuda hızlı bir yapılanma ve mevzuat oluşumuna ihtiyaç duyulduğunu" belirtmiştir. Devlet güvenliği açısından "düzenlemelerin Avrupa'daki gibi STK'lar aracılığı ile*

yapılmasının, bu konuda esnek ve kişiye özelleştirilmiş filtre teknolojisi geliştirilmesinin ve kişilerin bilgisayar okuryazarlığı bağlamındaki bilinç düzeyinin arttırılmasının" önemi üzerinde de bir mutabakat sağlandığı görülmüştür"

"Kamu kurumlarının bilişim sistemleri düzenli olarak bağımsız dış denetime tabi tutulmalıdır"

"Bilgi sistemlerinin güvenlik testlerini yapan firmaların standardizasyonu ve sertifikasyonu sağlanacaktır. Kamu ve özel sektör kurumlarının kullanabileceği, belirlenmiş minimum güvenlik kriterlerini sağlayan açık kaynak kodlu mevcut güvenlik ürünleri hakkında bilgilendirme yapılacak, kılavuzlar yayınlanacak, açık kaynak kodlu yeni ürünlerin geliştirilmesi için platformlar oluşturulacaktır".

Normatif Optimum Karar Verme Modeli

"Bilişim Ajansı Kurulması Sektörün dinamizmine uygun bir şekilde, gerekli ihtiyaçlara hızlı reaksiyon verebilecek, uluslararası kabul görmüş kurumsal yönetişim ilkelerine tam uygun, Başbakana doğrudan bağlı, tüzel kişiliği haiz bir Bilişim Ajansı kurulması önerilmektedir"

"Ulusal siber güvenlik altyapısının güçlendirilmesini teminen, kamu kurumlarında yaşanabilecek bilişim güvenliği olaylarına müdahalede bulunabilmek amacıyla bilgisayar olaylarına müdahale ekiplerinin kurulması"

"Savaş halinde düşman ülke bilgi sistemlerini hedef alacak siber saldırıların Silahlı Kuvvetler bünyesinde teşkil edilecek siber komutanlık birimlerince yapılması ve bu amaçla gereken altyapının kurulması".

Sınırlı Rasyonalite

"Sorun Bilgi Teknolojilerinin kendisi değil bunların nasıl kullanıldığıdır. Bütün bu konuların araştırılmasıyla ilgili olarak işin ceza hukuku boyutu, müeyyideler boyutu, eğitim boyutu, psikolojik boyutu, teknolojik boyutu incelenmeli ve bunların getireceği sıkıntıların, alınacak tedbirlerin bir devlet politikası hâline dönüşebilmesi bakımından gündelik yaşamın vazgeçilmez bir öğesi olan Bilgi Teknolojilerinin daha geniş kapsamda imkânlarının ve risklerinin araştırılması, bu teknolojilerinin daha faydalı

bir biçimde kullandırılmasının sağlanması ve konu ile ilgili gerekli bilgilendirmenin yapılarak doğru bilgiye kısa zamanda ulaşmanın altyapısının oluşturulması gerekmektedir".

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Karma KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.5. Hukuki Belgelerden Elde Edilen Bulgular

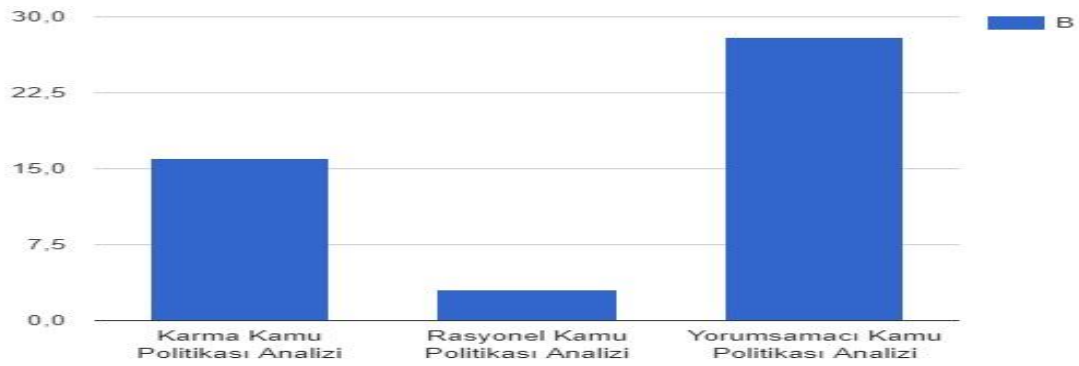
Bu başlık altında, Türkiye'nin siber güvenlikle ilgili hukuki belgelerinden elde edilen bulgular, siber güvenlik ve kritik altyapılar olmak üzere iki grup halinde sunulmuştur.

5.7.5.1. Kritik Altyapılara İlişkin Bulgular

5.7.5.1.1. Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı

Araştırmada ortaya çıkan bulgulara göre, hukuki belgelerde kritik altyapılar ile ilgili toplamda 47 adet politika önermesi yer almaktadır. Söz konusu politika önermelerinin 3'ü Rasyonel, 28'i Yorumsamacı, 16'sı ise Karma Kamu Politikası analiz yaklaşımı içerisinde yer almıştır.

Tablo 44: Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı (Hukuki Belgeler)



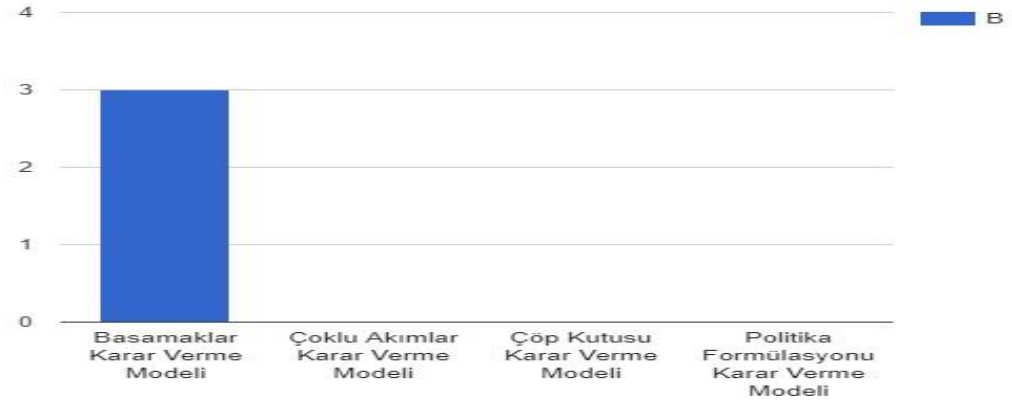
Bu politika önermelerinin hangi karar verme modelleri içerisinde yer aldığı ise aşağıdaki tablolarda, her bir kamu politikası analizi yaklaşımı için ayrı ayrı gösterilmiştir.

5.7.5.1.2. Karar Verme Modellerine Göre Politika Önerme Dağılımı

5.7.5.1.2.1. Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Rasyonel Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, yalnızca Basamaklar Karar Verme Modelinde 3, politika önermesi belirlenmiştir.

Tablo 45: Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Hukuki Belgeler)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Basamaklar Karar Verme Modeli

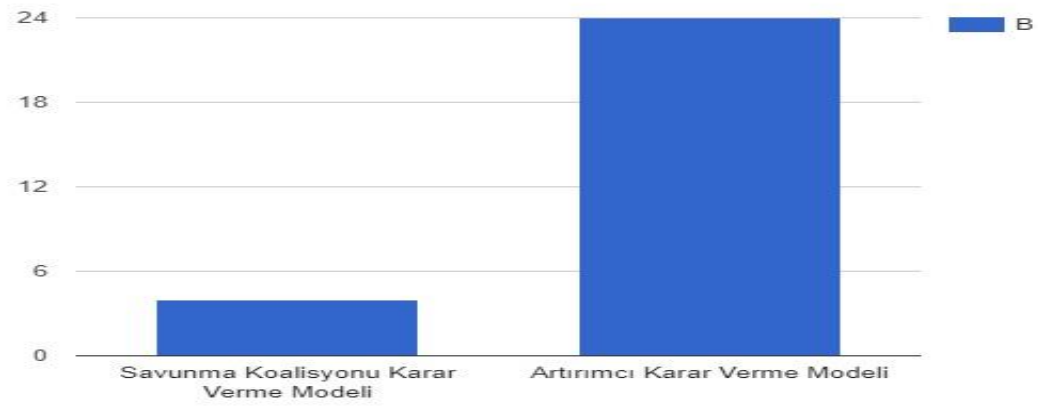
> *"Elektronik haberleşme sektörüne yönelik pazar analizleri yapmak, ilgili pazarı ve ilgili pazarda etkin piyasa gücüne sahip işletmeci veya işletmecileri belirlemek"*
>
> *"Bu Kanunun 46'ncı maddesinde belirtilen ücretlerle ilgili olarak terkin de dâhil olmak üzere her türlü usul ve esasları belirlemek, Kurumun yıllık bütçesini, gelir-gider kesin hesabını, yıllık çalışma programını onamak, gerekirse bütçede hesaplar arasında aktarma yapmak veya gelir fazlasını mevzuat çerçevesinde genel bütçeye devretmek"*
>
> *"Ara bağlantı ve ulusal dolaşım da dahil erişim ile ilgili uygulanacak usul ve esasları belirlemek ve mevzuatın öngördüğü düzenlemeleri yapmak, elektronik haberleşme sağlanması amacıyla imzalanan anlaşmaların rekabeti kısıtlayan, mevzuata ve/veya tüketici menfaatlerine aykırı hükümler içermemesi amacıyla mevzuatın öngördüğü tedbirleri almak*".

Yukarıda örnek olarak gösterilen politika önermeleri yorumlanarak Rasyonel KPA içerisinde konumlandırılan ilgili karar verme yaklaşımı içerisinde gruplandırılmıştır.

5.7.5.1.2.2. Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Yorumsamacı Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Artırımcı Karar ver Modelinde 24, Savunma Koalisyonu Karar Verme Modelinde 4 politika önermesi belirlenmiştir.

Tablo 46: Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Hukuki Belgeler)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Artırımcı Karar Verme Modeli,

> *"Herkesin, makul bir ücret karşılığında elektronik haberleşme şebeke ve hizmetlerinden yararlanmasını sağlayacak uygulamaların teşvik edilmesi"*
>
> *"Elektronik haberleşme sektöründe; rekabeti tesis etmeye ve korumaya, rekabeti engelleyici, bozucu veya kısıtlayıcı uygulamaların giderilmesine yönelik düzenlemeleri yapmak, bu amaçla ilgili pazarlarda etkin piyasa gücüne sahip işletmecilere ve gerekli hallerde diğer işletmecilere yükümlülükler getirmek ve mevzuatın öngördüğü tedbirleri almak"*

“Elektronik haberleşmeyle ilgili olarak, işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak, Bakanlık tarafından elektronik haberleşme sektörüne yönelik strateji ve politikaların belirlenmesinde ihtiyaç duyulanları, talebi üzerine Bakanlığa iletmek”.

Savunma Koalisyonu Modeli

“Elektronik haberleşme cihaz ve sistemlerinin kurulması, kullanılması ve işletilmesinde insan sağlığı, can ve mal güvenliği, çevre ve tüketicinin korunması açısından asgarî uluslararası normların dikkate alınması”

“Teknolojik yeniliklerin kullanılması da dâhil olmak üzere özürlü, yaşlı ve sosyal açıdan korunmaya muhtaç diğer kesimlerin özel ihtiyaçlarının dikkate alınması”

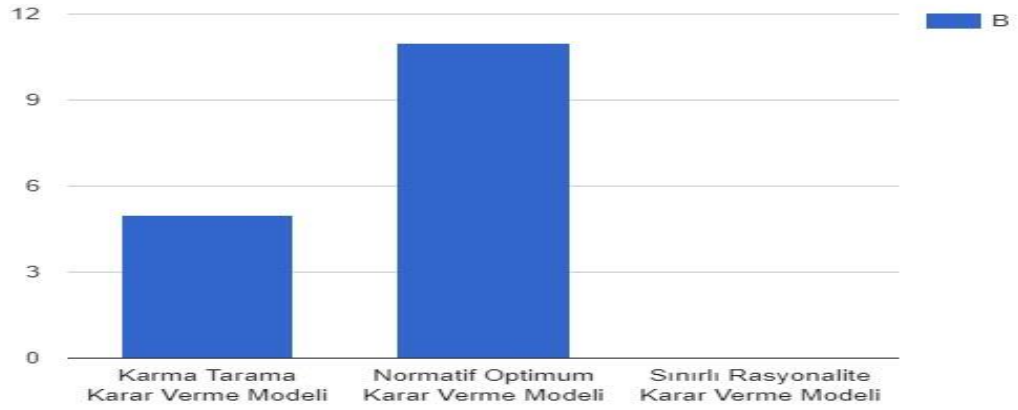
“Elektronik haberleşme cihaz ve sistemlerinin kurulması, kullanılması ve işletilmesinde insan sağlığı, can ve mal güvenliği, çevre ve tüketicinin korunması açısından asgarî uluslararası normların dikkate alınması”.

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Yorumsamacı KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.5.1.2.3. Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Karma Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Karma Tarama Karar Verme Modelinde 5, Normatif Optimum Karar Verme Modelinde 11 politika önermesi belirlenirken, Karar Vermede Sınırlı Rasyonalite grubunda hiçbir politika önermesi belirlenmemiştir.

Tablo 47: Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı(Hukuki Belgeler)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Karma Tarama Karar Verme Modeli

> *"Aksini gerektiren objektif nedenler bulunmadıkça veya toplumdaki ihtiyaç sahibi kesimlere özel, kapsamı açık ve sınırları belirlenmiş kolaylıklar sağlanması halleri dışında, eşit şartlardaki aboneler, kullanıcılar ve işletmeciler arasında ayrım gözetilmemesi ve hizmetlerin benzer konumdaki kişiler tarafından eşit şartlarla ulaşılabilir olması"*

> *"İşletmecilerin ticari sırları ile kamuoyuna açıklanabilecek bilgilerinin kapsamını belirlemek, işletmecilerin ticari sırları ile yatırım ve iş planlarının gizliliğini korumak ve bunları adli makamların talepleri dışında muhafaza etmek"*

> *"İlgili kanun hükümleri dahilinde, evrensel hizmetlere ilişkin hizmet kalitesi ve standartları da dahil olmak üzere, gerektiğinde her türlü elektronik haberleşme hizmetine yönelik hizmet kalitesi ve standartlarını belirlemek, denetlemek, denetlettirmek ve buna ilişkin usul ve esasları belirlemek".*

Normatif Optimum Karar Verme Modeli

> *“Yerel ağa ayrıştırılmış erişim ve veri akış erişimini de içerecek şekilde elektronik haberleşme şebekesi bileşenlerine ve ilgili tesislerine her türlü yöntemle erişim”*
>
> *“Teknolojik yeniliklerin uygulanması ile araştırma-geliştirme faaliyet ve yatırımlarının teşvik edilmesi”*
>
> *“Ulusal dolaşım da dahil olmak üzere sabit ve mobil şebekelere erişim”.*

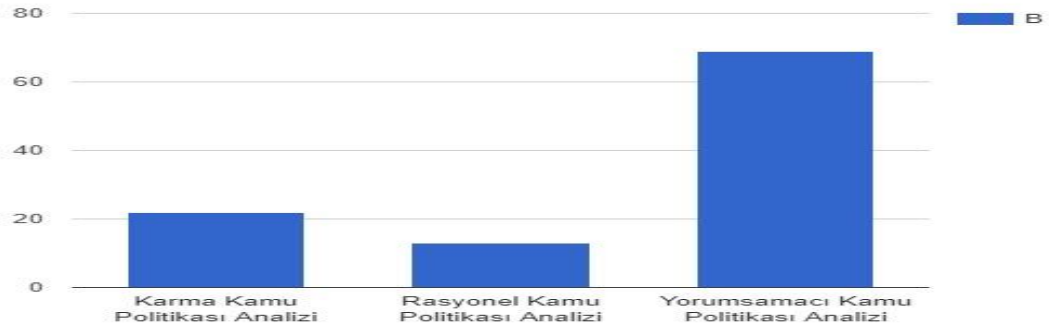
Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Karma KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.5.2. Siber Güvenliğe Ait Bulgular

5.7.5.2.1. Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı

Araştırmada ortaya çıkan bulgulara göre, ilgili hukuki belgelerde siber güvenlik ile ilgili toplamda 107 adet politika önermesi yer almaktadır. Söz konusu politika önermelerinin 13’ü Rasyonel, 69’u Yorumsamacı, 22’si ise Karma Kamu Politikası analiz yaklaşımı içerisinde yer almıştır.

Tablo 48: Kamu Politikası Analiz Yaklaşımlarına Göre Politika Önerme Dağılımı (Hukuki Belgeler)



Bu politika önermelerinin hangi karar verme modelleri içerisinde yer aldığı ise aşağıdaki tablolarda, her bir kamu politikası analizi yaklaşımı için ayrı ayrı gösterilmiştir.

5.7.5.2.2. Karar Verme Modellerine Göre Politika Önerme Dağılımı

5.7.5.2.2.1. Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Rasyonel Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Basamaklar Karar Verme Modelinde 6, Çoklu Akımlar Karar Verme Modelinde 0, Çöp Kutusu Karar Verme Modelinde 0 ve Politika Formülasyonu Karar Verme Modelinde 7 politika önermesi belirlenmiştir.

Tablo 49: Rasyonel KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Hukuki Belgeler)

Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Basamaklar Karar Verme Yöntemi

> *"Bu Kanunun amacı; ulusal güvenliği ilgilendiren bilgilerin korunması, Devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, kısa ve uzun dönemli planların hazırlanması, kriter ve standartlarının saptanması, ihracat ve ithalat izinlerinin ve sertifikalarının verilmesi, bilgi sistemlerinin teknolojiye uyumunun sağlanması, uygulamanın takip ve denetimi kamu ve özel kurum ve kuruluşların arasında koordinasyonun sağlanması amacıyla bir teşkilatın kurulması ve görevlerine ilişkin esas ve usulleri düzenlemektir"*

> *"Telekomünikasyon ve Bilgi sistemleri ortamındaki değişimlere uyum sağlayacak Ulusal bilgi güvenliği politikasının oluşturulması için gerekli verileri hazırlamak, prensipleri belirlemek"*

> *"Ulusal Bilgi güvenliği ile ilgili olarak görev alanına ilişkin planlama ve programlama faaliyetlerinde bulunmak, gerekli mevzuatı düzenlemek".*

Politika Formülasyonu Karar Verme Modeli

> *"Ulusal güvenliği ilgilendiren bilgiye işlem yapacak donanım ve yazılım ihtiyaçlarına ait güvenlik değerlendirmesini yapmak ve değerlendirilmiş ürün listelerini hazırlamak ve yayımlamak"*

“İletişim ortamları, donanım ve ağlar için tehdidi ve zafiyeti dikkate alarak risk analizleri yapmak ve risk yönetim usullerini belirlemek, risk analizleri sonucunda belirlenmiş koruyucu tedbirleri uygulamaya koymak”

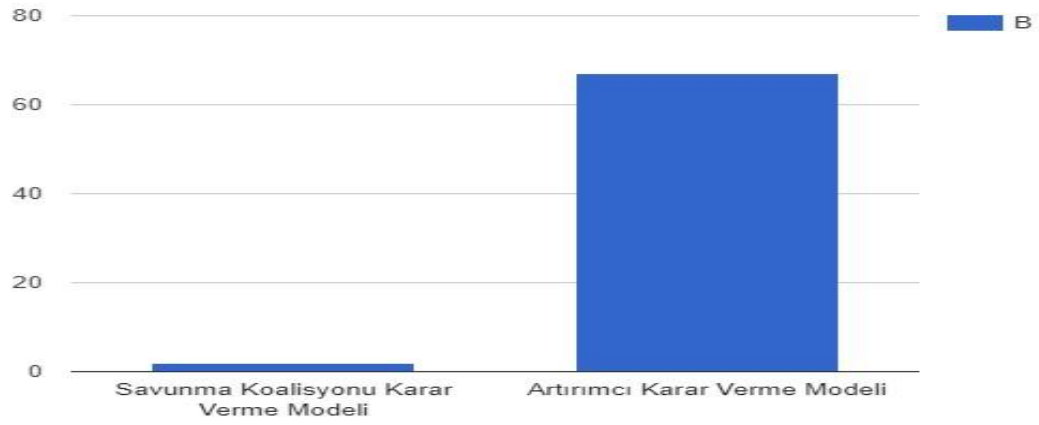
“Mevcut ve tasarlanan iletişim ortamları, donanım ve ağlar için tehdidi ve zafiyeti dikkate alarak risk analizleri yapmak”.

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Rasyonel KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.5.2.2.2. Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Rasyonel Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Artırımcı Karar Verme Modelinde 67, Savunma Koalisyonu Karar Verme Modelinde 2 politika önermesi belirlenmiştir.

Tablo 50: Yorumsamacı KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı (Hukuki Belgeler)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Savunma Koalisyonu Karar Verme Modeli

> *"Ulusal Siber Güvenlik konusunda yapılacak çalışmalar sürecinde, mümkün olan tüm alanlarda milli çözümler geliştirilmesi, yazılım ve donanım altyapılarında azami ölçüde milli kaynakların kullanılması esastır"*
>
> *"Ulusal Siber Güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretilmesini teşvik etmek, kullanımını sağlamak".*

Artırımcı Karar Verme Modeli

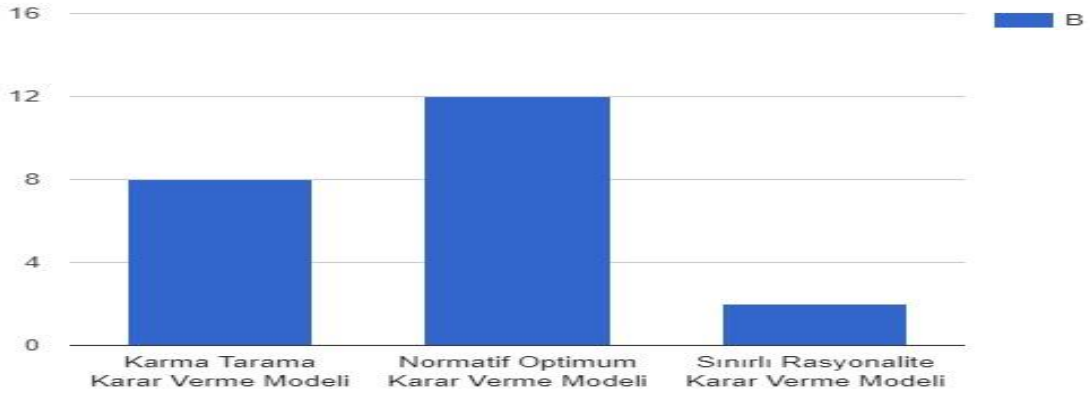
> *"Telsiz haberleşme sistemleri üzerinden kriptolu haberleşme yapmaya Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı, Milli İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Dışişleri Bakanlığı yetkilidir. Ayrıca yukarıda belirtilen kurumlara ait olanlar dışında kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapma usul ve esasları Kurum tarafından belirlenir".*

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Yorumsamacı KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.7.5.2.2.3. Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı

Politika önermelerinin Karma Kamu Politikası Analizi yaklaşımları içerisinde yer alan karar verme modellerine göre dağılımında, Karma Tarama Karar Verme Modelinde 8, Normatif Optimum Karar Verme Modelinde 12, Karar Vermede Sınırlı Rasyonalitede2 politika önermesi belirlenmiştir.

Tablo 51: Karma KPA Karar Verme Modellerine Göre Politika Önerme Dağılımı(Hukuki Belgeler)



Politika önermelerinin metin halleri ise şu şekilde sıralanmıştır:

Karma Tarama Karar Verme Modeli

> "Ulusal bilgi güvenliğine yönelik tehdidi değerlendirmek, ulusal bilgi güvenliği siyasetinin tayini, tespiti ve uygulamasıyla ilgili kararları almak ve kuruma bu konuda direktif vermek"
>
> "Ulusal bilgi güvenliği ile ilgili uluslararası mevzuat ve teknolojideki gelişmeleri takip etmek"
>
> "Ulusal bilgi Güvenliği ihlallerine karşı alınacak tedbirleri belirlemek, ihlallere karşı gerekli tedbirleri almak ve ilgili makamlarla koordineli olarak uygulanmasını sağlamak".

Normatif Optimum Karar Verme Modeli

> *"İşletmeciler, elektronik haberleşme sistemleri üzerinden millî güvenlikle ve 5397 ve 5651 sayılı kanunlar ve ilgili diğer kanunlarda getirilen düzenlemelerle ilgili taleplerin karşılanmasına yönelik teknik altyapıyı, elektronik haberleşme sistemini hizmete sunmadan önce kurmakla yükümlüdür. Halen elektronik haberleşme hizmeti sunan işletmeciler de; söz konusu teknik altyapıyı, Kurum tarafından belirlenecek süre içerisinde aynı şartlarla ve tüm harcamaları kendilerine ait olmak üzere kurmakla yükümlüdürler"*

“İletişim ortamları, şebeke, yazılımlara ait güvenlik sistemleri ile ilgili denetleme usul ve kriterlerini belirlemek, geliştirmek, denetleme yapılmasını sağlamak, gerektiğinde denetlemek ve denetleme raporlarını değerlendirmek”

“Ulusal bilgi teknolojileri ve iletişim altyapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik altyapılan belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik çalışmaları yapmak”.

Sınırlı Rasyonalite

“Kurum, spektrum izleme ve denetleme faaliyetlerinde kullandığı her türlü araç, cihaz ve sistemler ile tesisler için emniyet ve muhafaza tedbirleri amacıyla gerek görmesi halinde her türlü riske karşı sigorta yaptırabilir”

“Güvenlik hassasiyeti gösteren personel, yazılım, donanım, kripto, iletişim ortamlarını ve iletişim ağlarını her türlü tehdit kaynağına karşı maliyet etkin tedbirlerle koruma altına alınmasını sağlamak, bu tedbirleri uygulamaya sokmak”.

Yukarıda örnek olarak gösterilen politika önermeleri ve bu doğrultuda seçilen diğer politika önermeleri yorumlanarak Karma KPA içerisinde konumlandırılan ilgili karar verme yaklaşımları içerisinde gruplandırılmıştır.

5.8. BULGULARIN DEĞERLENDİRİLMESİ

Araştırmada kapsamında incelenen dokümanlardan elde edilen bulgular bu başlık altında değerlendirilmiştir. Değerlendirmeler yapılırken her belge türü kritik altyapılara ilişkin değerlendirmeler ve siber güvenliğe ilişkin değerlendirmeler şeklinde ikişer alt başlıkta verilmiştir.

5.8.1. Strateji Belgelerindeki Kamu Politikası Önermeleri Üzerine Değerlendirmeler

Araştırmada ele alınan siber güvenlik strateji belgelerinde hem kritik altyapılar üzerine hem de siber güvenlik üzerine yapılmış çok sayıda politika önermesi belirlenmiştir. Çalışmanın ilerleyen kısmında, araştırmanın bulgularına ilişkin değerlendirmelere kritik altyapılar ve siber güvenlik olmak üzere ayrı başlıklar halinde yer verilmiştir.

5.8.1.1. Strateji Belgelerindeki Kritik Altyapı Politika Önermeleri Üzerine Değerlendirmeler

Araştırmada ele alınan siber güvenlik strateji belgelerinde hem kritik altyapılar üzerine hem de siber güvenlik üzerine yapılmış çok sayıda politika önermesine rastlanmıştır. Özellikle kritik altyapılara ilişkin politika önermeleri strateji planlarından sadece bilgi toplumu stratejisi belgelerinde yer almıştır. Siber güvenlik strateji ve eylem planları olarak isimlendirilen belgelerde kritik altyapılara ilişkin politika önermelerine rastlanmamıştır. Bunun nedeninin belgelerin kapsamıyla alakalı olduğu düşünülmektedir.

Bilgi toplumu strateji belgeleri konu kapsamıyla, siber güvenlik, iletişim, internet teknolojileri vb. birçok konuyu içerisine alan belgelerdir. Zira bunu belgelerin sayfa sayıları temelindeki uzunlukları bağlamında görmek de mümkündür. Bilgi toplumu strateji belgelerinden 2006-2010 yıllarını kapsayan belgenin sayfa sayısı 49 iken, 2015-2018'i kapsayan belgenin sayfa sayısı 168'dir. Siber güvenlik strateji belgelerine bakıldığında ise 2013-2014 yıllarını kapsayan siber güvenlik stratejisi ve eylem planı belgesinin sayfa sayısı 46 iken 2016-2019 yıllarını kapsayan siber güvenlik stratejisinin sayfa sayısı 17'dir. Diğer yandan siber güvenlik konusunun Türkiye'de henüz gündeme gelen bir konu olması dolayısıyla ilgili strateji belgeleri ve eylem planlarının kapsamlarının diğer belgelere göre daha dar olması doğal

karşılanmaktadır. Belgelerin kapsamlarının ilerleyen zamanlarda genişleyip genişlemeyeceği ise merak konusudur.

Belgelerde kritik altyapılara ilişkin politika önermelerinin Rasyonel, Yorumsamacı ve Karma Kamu Politikası Analizi yaklaşımlarının tümüne neredeyse eşit dağıldığı gözlemlenmiştir. Yer verilen politika önermelerinin çok büyük bir oranı kritik altyapılardan "iletişim" üzerinde yoğunlaşmıştır. Belgelerin bilgi toplumu ve siber güvenlik odaklı belgeler olduğu düşünüldüğünde, söz konusu politika önermelerinin bu kritik altyapı üzerinde yoğunlaşmış olması normaldir.

Kritik altyapılar ile ilgili Rasyonel Kamu Politikası Analizi yaklaşımı çerçevesinde yer alan politika önermelerine bakıldığında, bunların büyük oranda Basamaklar modeli içerisinde yer aldığı tespit edilmiştir. Söz konusu politika önermeleri daha çok kritik altyapılar üzerine üretilen politikaların etki değerlendirmelerinin yapılması, politikaların sonuçlarının nicel olarak ölçülmesi, politika uygulama süreçlerinin takip edilmesi üzerinedir. Bilgi toplumu ve dolaylı olarak da siber güvenlik üzerine üretilecek politikaların potansiyel itibarı ile yenilikçi politikalar olması sebebi ile belgelerde geçen rasyonel yaklaşımlı politika önermeleri, üretilecek yenilikçi ve karma politikalarının takibi üzerine kurulması doğal karşılanmaktadır. Bu politikaların kayda değer bir kısmı akıllı kentler üzerine oluşturulan politikalardır.

Belgelerde yer alan politika önermeleri, basmaklar modelinden sonra en fazla Çöp Kutusu Karar Verme Modeli içerisinde yer almıştır. Bu politika önermeleri, daha önceden soru olarak belirlenmiş olan durumların, değişen teknoloji ile birlikte ortaya çıkan yeni çözümlerle giderilmesini öngören politika önermeleridir. Önermelerde etkin rekabet, erişim maliyetleri, teknolojik gelişmeler, hız ve kalite unsurları gibi etkenler yeniden değerlendirilerek, daha çok hizmet sektörünün içerdiği eski sorunlara çözüm aranmıştır. Bilgi toplumunda, kamu hizmetlerinin daha etkin, verimli ve katılımcı bir şekilde sunulması, e-devlet uygulamalarının başlaması ve geliştirilmesi gibi altı çizilen konular, Türkiye'nin siber güvenlik

politikalarının kamu hizmetleri üzerinde iyileştirme amacına hizmet etmek üzere tasarlandığını göstermektedir.

Yorumsamacı Kamu Politikası Analizi Yaklaşımında, kritik altyapılar için ortaya konulan politika önermelerinin neredeyse hepsi Artırımcı Karar Verme Modeli içerisinde yer almıştır. Bu politika önermelerinde bilgi toplumuna geçiş sürecinde sosyal ve kültürel yapıların etkiye uğrayacağı vurgulanmaktadır. Bu süreçte vatandaşların, farkındalık artırımı, eğitim gibi yöntemlerle sürece uyum sağlamalarını kolaylaştıracak politikalara yer verilmiştir. Bilgi toplumu ile birlikte vatandaşın yönetime katılımının artırılması, idare ve özel sektörce elektronik ortamda verilen hizmetlerin yaygınlaştırılması, fiber erişim altyapılarının yaygınlaştırılması, üniversitelerde bilgi teknolojilerine ilişkin projelerin daha çok desteklenmesi gibi önceden üretilmiş ve uygulanmaya devam eden politikaların üzerine eklemlenmiş politikalar da belgelerde yer alan Artırımcı modele örnek olabilecek diğer politikalardır.

Karma Kamu Politikası Analizi içerisinde yer alan politika önermelerinin de karar verme modellerinden Normatif Optimum ve Karma Tarama Karar Verme Modeli içerisinde eşit dağıldığı gözlemlenmiştir. Normatif Optimum model, yenilikçi ve yaratıcı politika alternatiflerinin ortaya konulması, minimal risk stratejisi ya da yenilik stratejisinin tercih edilmesi konusunda alternatiflerin ve kararların ortaya çıkaracağı sonuçların tahmin edilmesi, deneyimlerden öğrenme, öncülük ve yaratıcılığın uyarımı, personelin geliştirilmesi ve entelektüel çabanın teşvik edilmesi gibi özelliklere sahiptir. Türkiye'de ve dahi dünyada bilgi toplumu çağına geçiş de bu özelliklere sahip kamu politikalarını barındırmalıdır. Bilgi toplumuna dönüşüm ile birlikte bilgiye erişim ve bilginin kullanımı alternatifleri çoğalmış, ülkeler de bu alternatifleri yakalamak için iletişim altyapılarını geliştirmiş ve yenilemişlerdir. Türkiye'nin de bilgi toplumuna geçişte, strateji belgelerinde yer verdiği politika önermelerinde, yenilikçi kararları üretme potansiyeli taşıyan bu karar verme modelini kullanmış olması olumlu karşılanmaktadır**.**

Karma Tarama modelin Normatif Optimum modelden farklılaşan kısmı, değişken bir ortamda üretilecek olan politikalara karşı daha geniş açılı duruşu ve Normatif Optimum modele göre daha az radikal politikaları içermesidir. Strateji belgelerindeki politika önermelerine bu yaklaşım, elde altyapıların geliştirilmesi, bulunan yeni sistemlere eldeki sistemlerin entegre edilmesi şeklinde yansımıştır. Modelin de vurguladığı üzere, belgelerde kritik altyapılarda entegrasyon sağlamaya yönelik diğer ülke örneklerinin araştırılması, yeni altyapıların teknik anlamda araştırılması ve yeniden analiz edilmesine dair politika önermelerine yer verilmiştir. Bu yönüyle politika önermeleri, Türkiye'nin mevcut altyapılarının gelişen ve yenilenen altyapılara uyumlandırılması ülkeye bilgi toplumuna geçişte pozitif yönde bir ivme kazandırılması amaçlanmaktadır.

Strateji belgelerinde, kritik altyapılar ile ilgili politika önermelerinin kamu politikası analizi yaklaşımları çerçevesindeki mahiyetine genel olarak bakıldığında, önermelerin Karma, Rasyonel, ve Yorumsamacı Kamu Politikası Analizi yaklaşımları arasında eşit yoğunlaştığını görmek şaşırtıcı karşılanmamıştır. Zira Türkiye, bilgi toplumu kavramı konusuna yeni bir ülke olsa da, ülkede bilgi ve iletişim kanalları, internet teknolojileri gibi altyapılara önceden sahip olan bir ülkedir. Bu durumda Türkiye'nin, mevcutta var olan altyapılarını geliştirmek ve yeni teknolojileri yakalamak, var olmayan altyapılarını ve yenilikçi mekanizmalarını kurmak üzere Karma; verimlilik ve olumlu yönde etki artışlarını sağlamak, bu yönde planlar yapmak, eski sorunlarına yeni teknolojilerle çözüm bulmak adına Rasyonel ve süre gelen politikalarını, ortaya çıkan yeni sorunlara göre ilave politikalarla destekleyerek çözmeyi amaçlayan ve bunları yaparken kültür, sosyal fayda, kamu yararı gibi değerleri de göz önünde bulunduran Yorumsamacı Kamu Politikası Analizi yaklaşım ve yöntemlerini eşit ağırlıkta kullandığı söylenebilecektir.

5.8.1.2. Strateji Belgelerindeki Siber Güvenlik Politika Önermeleri Üzerine Değerlendirmeler

Ele alınan strateji belgelerinin tümünde siber güvenlik ile ilgili politika önermelerine yer verilmiştir. Yer verilen politika önermeleri büyük ölçüde Karma ve Yorumsamacı Kamu Politikası Analizi Yaklaşımı içerisinde yer alırken, Rasyonel Kamu Politikası Analizi Yaklaşımı içerisinde yer alan az sayıda politika önermesi belirlenmiştir. Bu genel tabloya ilk bakışta durumun Türkiye'nin sahip olduğu sınırlı siber güvenlik politikası altyapısını yansıttığı söylenebilir. Zira yer verilen politika önermelerinin ağırlıklı oranda Karma ve Yorumsamacı yaklaşım içerisinde yer almaları, önermelerin yeni bir yapıyı kurmak, olan bir yapıyı ortaya çıkan yenilikler doğrultusunda geliştirmek üzere ya da süre gelen politikalar üzerine ek politikalar yaparak sürdürmek üzere oluşturulduğu anlaşılmaktadır**.** Rasyonel yaklaşım içerisinde yer alan politika önermelerinin az sayıda olması ise bu alanda üretilecek planlı, nicel verilere dayanan, fayda maliyet analizlerini, etki ve uygulama değerlendirmelerini, ölçümlerini içeren politikaların da az olduğunu göstermektedir.

Strateji belgelerinde Karma Kamu Politikası Analizi Yaklaşımı içerisinde yer alan politika önermelerinin önemli bir kısmı Normatif Optimum Karar Verme Modeli içerisinde yer almıştır. Bu bulgu, Türkiye'nin siber güvenlik politikalarının önemli bir kısmının temelden inşa edilmeye başlandığını göstermektedir. Temelden inşa edilen politikalar veri ve bilgi yönetimi, veri toplama ve saklama, siber suçlara karşı oluşturulacak hukuki düzenlemeler, Bilim Vadisinin kurulması, siber güvenlik üzerine eğitim programlarının oluşturulması, siber güvenlik ile ilgili devlet organlarının oluşturulması ve siber güvenlik ile ilgili uzmanların yetiştirilmesi konularına dayanmaktadır. Karma Tarama model içerisinde yer alan politikalar ise mevcut altyapıların eksikliklerinin giderilmesine, bu altyapıların geliştirilerek yeni ortam ve şartlara uygun hale getirilmesine ve Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı etkin şekilde uygulanacak, teknolojik eğilimler ve ihtiyaçlar doğrultusunda güncellenmesine dayanmaktadır. Araştırma bulgularında Karar

Vermede Sınırlı Rasyonalite çerçevesine giren siber güvenlik politika önermelerine rastlanması dikkat çekici bulunmuştur. Zira araştırmanın genel bulgularına bakıldığında bu çerçevede çok az sayıda politika önermesine rastlanmıştır. Strateji belgelerinde bu yönde bir bulguya rastlanmasının nedeninin Türkiye'nin siber güvenlik konusuna yeni bir ülke olması dolayısıyla politika üreticiler açısından var olan belirsizlik durumudur. Oluşturulan strateji belgeleri henüz yeni üretilen siber güvenlik politikasının birer ürünü olmakla birlikte, bu alandaki ulusal entelektüel sermaye de henüz gelişmemiştir. Bu yüzden hem karar verme açısından hem de siber güvenliğin sağlanmasına yönelik atılacak adımlar açısından belirsizlik ortamı var olup, karar vericilerin bu alandaki teknik arka planları yeterince kapsamlı değildir.

Strateji belgelerinde yer alan politika önermelerinin yoğunlaştığı bir diğer yaklaşım ise Yorumsamacı Kamu Politikası Analizi Yaklaşımıdır. Bulgular doğrultusunda altı çizilmesi gereken bir husus ise bu yaklaşım altında yer alan Savunma Koalisyonu Karar Verme Modeli içerisinde yer alan politika önermeleri sayısının da azımsanmayacak nitelikte olmasıdır. Belgelerde bu yönde politika önermelerine yer verilmesinin nedeninin öncelikle yeni kurulacak siber güvenlikle ilgili altyapılarla ilgili politika önermelerinde sıkça rastlanan "yerli ve milli olma" vurgusudur. Modelin temel argümanlarından olan "verilen belirli bir resmi yapıda, değişen sosyo-ekonomik bir çevrede, farklı değer ve çıkarlara sahip grupların bir güç mücadelesi" durumu burada ulusal bir boyutta gözlemlenmektedir. Ulusal çıkarların yanı sıra kişisel verilerin korunması, özel hayatın gizliliği, şeffaflık, hesap verilebilirlik, etik ve ifade özgürlüğü gibi değerler de kamu politikası önermelerinde göze çarpmaktadır. Politika önermelerinde kritik altyapıların güvenliğinin sağlanması için, özel sektörle, karar mekanizmalarına katılımı da içeren işbirliklerinin de altı çizilmektedir. Yaklaşım çerçevesinde politika önermelerinin ağırlıklı bir kısmı yine Artırımcı Karar Verme Modeli içerisinde yer almıştır. Buradaki yoğunlaşmanın, oluşturulmak istenen siber güvenlik stratejilerinde, konu ile ilgili olabilecek mevcut devlet

kurumlarının görev ve sorumluluk alanlarını genişletmek üzere uygulanan artırımcı politikalardan ileri geldiği gözlemlenmiştir.

Yukarıda vurgulanan noktaları destekler şekilde araştırma bulguları, strateji belgelerinde Rasyonel Kamu Politikası Analizi içerisine giren siber güvenlik politika önermelerinin çok az sayıda olduğunu göstermektedir. Bu önermelerde ise genel olarak Basmaklar Karar Verme Modeli kullanımı yoğunluğu gözlemlenirken, adalet hizmetleri, e-dönüşüm, sektör yapılanması, risk yönetimi, Ulusal Risk Değerlendirmesi Siber saldırılara karşı koymak için Siber Saldırı Eylem Planları hazırlanması gibi konularda sürece dayalı ve eldeki tüm verilerin analize tabi tutulması hususunun ön planda olduğu bir politika üretimine başvurulduğu anlaşılmıştır. Çöp Kutusu modelde, eski sorunlara karşı yeni gelişen teknoloji ile çözüm aranırken, Politika Formülasyonu modelinde ise politikalar risk-fayda-maliyet-zarar unsurları arasında formüle edilmeye çabalanmıştır. Araştırma bulguları doğrultusunda, büyük oranda yeni altyapıların oluşturulacağı, bilgisel ve deneyimsel kapasitenin az, belirsizliğin hâkim olduğu siber güvenlik konusunda Rasyonel Kamu Politikası Analizi Yaklaşımı ile oluşturulmuş politika önermelerinin sayısının az olması beklenen bir sonuçtur.

Yukarıda bahsi geçen konu ve değerlendirmeler genel olarak özetlendiğinde, Türkiye'nin siber güvenlik ile ilgili resmi strateji belgelerinde yer verilen politika önermelerinin yoğun olarak Karma ve Yorumsamacı Kamu Politikası Analizi Yaklaşımları etrafında şekillendiği söylenebilecektir. Bunun yanında az sayıda da olsa, özellikle adalet hizmetleri, e-dönüşüm, sektör yapılanması, risk yönetimi, Ulusal Risk Değerlendirmesi Siber saldırılara karşı koymak için Siber Saldırı Eylem Planları hazırlanması gibi nicel yöntemlere ihtiyaç duyan politikalarda, Rasyonel Kamu Politikası Analizi yaklaşımına başvurulmaktadır. Türkiye'nin siber güvenlik konusundaki mevcut durumu, ülke dinamikleri, içinde bulunulan ve durağan olmayan siber ortam göz önüne alındığında, araştırmanın bulguları doğrultusunda

ortaya çıkan, ülkenin siber güvenlik politikası eğilimlerinin birbiri arasında tutarlı olduğu sonucuna ulaşılabilecektir.

5.8.2. Kalkınma Planlarındaki Kamu Politikası Önermeleri Üzerine Değerlendirmeler

Araştırmada ele alınan kalkınma planlarında kritik altyapılar üzerine çok sayıda politika önermesi belirlenirken, siber güvenlik ile ilgili sadece 3 politika önermesine yer verilmiştir. Çalışmanın ilerleyen kısmında, araştırmanın bulgularına ilişkin değerlendirmelere kritik altyapılar ve siber güvenlik olmak üzere ayrı başlıklar halinde yer verilmiştir.

5.8.2.1. Kalkınma Planlarındaki Kritik Altyapı Politika Önermeleri Üzerine Değerlendirmeler

Araştırmada Türkiye'nin içinde bulunulan döneme kadar olan tüm kalkınma planları ele alınmıştır. Bu kalkınma planlarının tümünde kritik altyapılara ilişkinin politika önermelerine yer verilmiştir. Politika önermelerinin kamu politikası analizi yaklaşımları içerisinde nerdeyse eşit bir şekilde dağılmış olduğu belirlenmiştir. Diğer yandan önermelerin, yer aldıkları kamu politikası analizi yaklaşımının altında sınıflanan karar verme modelleri arasındaki dağılımların kayda değer oranlarda farklılaştığı gözlemlenmiştir. En çok politika önermesine yer verilen kritik altyapılar sırasıyla enerji, su ve gıdadır.

Kritik altyapılar ile ilgili Rasyonel Kamu Politikası Analizi Yaklaşımı çerçevesinde yer alan politika önermelerine bakıldığında, bunların büyük oranda ve eşit şekilde Basamaklar ve Politika Formülasyon Karar Verme Modelleri içerisinde yer aldığı saptanmıştır. Basamaklar modeli içerisinde yer alan politika önermelerinin özellikle son üç (8'inci, 9'uncu ve 10'uncu) kalkınma planında yoğunlaştığı görülürken, Politika Formülasyon modeli içerisinde yer alan politika önermelerinin özellikle

7’inci, 8’inci ve 10’uncu kalkınma planında yoğunlaştığı görülmüştür. Genel olarak Rasyonel yaklaşım içerisinde yer alan politika önermelerinin ise 4’üncü, 8’inci ve 10’uncu kalkınma planları üzerinde yoğunlaştığı görülmektedir. Söz konusu bulgulardan net bir çıkarım yapılamayacak olsa da, Türkiye’nin kalkınma planlarında, kritik altyapılara ilişkin Rasyonel yaklaşım içerisinde yer alan politika önermelerinin özellikle son üç kalkınma planında daha çok yoğunlaştığı gözlemlenmiştir.

Basamaklar modeli içerisinde yoğunlaşan politika önermelerinin önemli bir kısmında politikaların üretilme sürecinde uygulanacak olan kritik altyapılara ilişkin politikalarda uygulanacak mastır planlar, planlar, programlar, ölçme ve değerlendirme süreçlerine vurgu yapılmıştır. Diğer yandan kritik altyapılarla ilgili çok sayıda politika da basamaklara ayrılarak ortaya konmuştur. Kritik altyapılara ilişkin bu yönde ortaya konulan politika önermelerinin genel görünüm itibarı ile daha sistemli ve sağlam temelli olarak tasarlandığı izlenimine sahip olunmuştur. Politika önermelerinin yoğunlaştığı diğer bir rasyonel karar verme modeli Politika Formülasyon Karar Verme Modelidir. Planlarda, modelde vurgulandığı üzere kamu politikasının öznesi olan problemlerin çözülebilme, bölünebilme, parasallaştırılabilme özelliklerinden yararlanılarak, verimlilik artışları, parasal değerler, iyileştirilen oranlar gibi nicel verilerle desteklenen politika önermelerinde bulunulmuştur. Bu yönüyle planlarda yer verilen politika önermelerinin amaçlarının ve hedeflerinin net bir şekilde ortaya konulduğu gözlemlenmiştir.

Planlarda yer alan kamu politikası önermelerinin en büyük kısmı Yorumsamacı Kamu Politikası Analizi Yaklaşımı içerisinde yer almıştır. Bu politika önermelerinin yaklaşım %75’i ise yaklaşım içerisindeki Artırımcı Karar Verme Modeli içerisinde bulunmaktadır. Kalkınma planlarının genel olarak ülkenin tüm altyapılarını kapsadığı düşünüldüğünde, bu belgelerde yerleşik kritik altyapıların geliştirilmesine yönelik politikaların yoğunlukta olacağı kuvvetle muhtemeldir. Dolayısıyla belgelerde yer alan kamu politikası önermelerinin büyük çoğunluğunun Artırımcı

Karar Verme Modeli içerisinde yer alması normal karşılanmıştır. Diğer yandan kritik altyapılara ilişkin “millileşme, yerli kaynakların kullanılması, yerlileşme, milli ve kültürel birlik değerleri” vurguları da Yorumsamacı Kamu Politikası Analizi Yaklaşımı içerisinde yer alan Savunma Koalisyonu Karar Verme Modelinde yer alan politika önermelerinin sayısını artırmıştır. Söz konusu politika önermeleri daha çok enerji kaynaklarının faaliyete geçirilmesi ve kullanılması konularında ortaya konulmuştur. Diğer yandan siber güvenlik strateji belgelerindeki siber güvenlik politika önermelerinde yer verilen tek kritik altyapı olan iletişim de kalkınma planlarında politika önerme sayısı anlamında kayda değer şekilde kendine yer bulmuştur.

Kalkınma planlarında, Karma Kamu Politikası Analizi Yaklaşımı kapsamında oluşturulmuş politika önermelerine neredeyse Yorumsamacı yaklaşımda olduğu kadar çok yer verilmiştir. Bu yaklaşım içerisinde sınıflandırılan karar verme modellerinden en çok Karma Tarama Karar Verme Modelinin izleri politika önermelerinde gözlemlenmiştir. Bu durumun nedeni elde var olan kritik altyapıların, bir politika önermesinde geçen ifadeyle “konudaki en gelişmiş teknolojiler uygulanarak, ülke çıkarları doğrultusunda, değerlendirilmesi” şeklinde değişen koşullara uyumlandırılması çabasıdır. Yaklaşım içerisinde yer alan ve “yenilikçilik, yaratıcılık, deneyim ve uzmanlaşma” ilkeleri doğrultusunda politika oluşturmayı hedefleyen Normatif Optimum Karar Verme Modeli içerisinde yer alan kamu politikası önermeleri de bir hayli fazladır. Önermeler, özellikle nükleer enerjiye geçiş, iletişim ile enerji alanında teknik uzmanların yetişmesi ile yeni altyapı sistem ve tesislerinin kurulmasına yöneliktir. Bu yöndeki kritik altyapı politika önermelerinin Türkiye’nin kalkınma planlarında bir hayli fazla olması durumunun Dror’un (1967) belirttiği “Normatif Optimum Karar Verme Modelini daha çok gelişmekte olan ülkelerdeki politika üretim süreçlerinde kullanılır” temalı fikrini desteklediği söylenebilecektir. Son olarak, bankacılık ve finans ile iklim değişikliği akabinde içecek su temini politikaları, planlamalarda vurgulanan belirsiz ortam ve sınırlı

rasyonel bilgiler vurguları dolayısıyla Karar Vermede Sınırlı Rasyonalite altında gruplanmışlardır.

Kalkınma planlarındaki politika önermelerinin genel tablosuna bakıldığında, belgelerin kapsamlı belgeler olması dolayısıyla her türlü yaklaşım ve karar verme modelinden çok sayıda örnekler içerdikleri gözlemlenmiştir. Bunun yanında, politika önermelerinin yoğunluklarının kamu politikası analizi yaklaşımlarına neredeyse eşit yoğunlukta dağılması ise dikkat çekici bulunmuştur.

5.8.2.2. Kalkınma Planlarındaki Siber Güvenlik Politika Önermeleri Üzerine Değerlendirmeler

Araştırma kapsamında incelenen Türkiye'nin kalkınma planlarının tümünde, güvenlik konusuna yapılan kodlamalar ulusal güvenlik ve özellikle sosyal güvenlik üzerinde yoğunlaşmıştır. Bu kodlamalardan çıkarılan politika önermelerinden yalnızca 3'ünün siber güvenliğe ilişkin olduğu tespit edilmiştir. Bu politika önermelerinden 2'si ise siber güvenliği "bilgi güvenliği" ve "ulusal bilgi güvenliği" olarak dolaylı şekilde yansıtmaktadır. Söz konusu önermelerin tümü Yorumsamacı Kamu Politikası Analizi Yaklaşımı içerisinde yer alan bir karar verme modeli olan Artırımcı Karar Verme Modeli içerisinde konumlandırılmıştır. Önermelerde "etkin mücadele, siber suçlara ait hukuki altyapının tamamlanması" gibi artırımcı politika vurguları yapılmıştır.

5.8.3. Raporlardaki Kamu Politikası Önermeleri Üzerine Değerlendirmeler

Araştırmada ele alınan meclis araştırma ve Emniyet Genel Müdürlüğü raporlarında hem kritik altyapılar üzerine hem de siber güvenlik üzerine yapılmış çok sayıda politika önermesi belirlenmiştir. Çalışmanın ilerleyen kısmında, araştırmanın

bulgularına ilişkin değerlendirmelere kritik altyapılar ve siber güvenlik olmak üzere ayrı başlıklar halinde yer verilmiştir.

5.8.3.1. Raporlardaki Kritik Altyapı Politika Önermeleri Üzerine Değerlendirmeler

Siber güvenlik sağlanamadığı takdirde oluşabilecek problemler, ülkenin kritik altyapılarını koruma ve geliştirmeye dair politika üretme ihtiyacını beraberinde getirmiştir. Bu nedenle araştırma kapsamında ele alınan belge, rapor vb. yazınlarda siber güvenliğe dair geliştirilen önermeler olduğu kadar, ülkenin kritik altyapılarının güvenliği adına geliştirilen politika önermeleri de dikkatle incelenmiştir. Meclis araştırma komisyonunun, ülkenin ihtiyaçlarını göz önüne alan önermeler sunduğu düşünülerek kritik altyapılara dair politika önermeleri analiz edilmiştir. Yorumsamacı Kamu Politikası Analizi başlığı altında yer alan önermelerin, Karma Analiz yönteminden iki kat daha fazla politika önermesi içerdiği saptanmıştır. Rasyonel Kamu Politikası Analizi ve içinde barındırdığı modellerin içerdiği önermeler ise sayıca diğer iki analiz yönteminin arasında yer almaktadır.

Kritik altyapılar ile ilgili Rasyonel Kamu Politikası Analizi yaklaşımı çerçevesinde yer alan politika önermelerine bakıldığında, bunların büyük oranda Politika Formülasyonu Modeli içerisinde yer aldığı görülmektedir. Meclis komisyonunun kritik altyapılarla ilgili problemlere çözüm odaklı yaklaştığı, sorunu daha küçük parçalara bölerek ve sorunun etki alanını iyi hesaplayarak politika önermesi ürettiği tespiti yapılabilecektir. Modelden seçilen politika önermesine bakıldığında “Elektronik haberleşme sektöründe uygulanan vergiler Avrupa Birliği’ne uyum sürecinde yürütülen müzakerelerde ve ilerleme raporlarında eleştirilmektedir. Bu açıdan, elektronik haberleşme sektöründeki dolaylı vergi yükünün Avrupa Birliği ortalamasına çekilmek suretiyle hafifletilmesi ve Avrupa Birliği müktesebatıyla uyumun sağlanması hedefine ulaşılmalıdır” ifadesi, sorunun parasallaştırılarak çözüme kavuşturulmasına dair bir çaba görülmektedir. Politika formülasyonu

modelinden sonra en çok önerme içeren başlığın Çoklu Akımlar Modeli olduğu görülmektedir. Bunun nedeni olarak kriz seviyesine gelerek medyanın etkisiyle gündeme taşınan sorunlar ve bu sorunların politikaya yön veren çeşitli aktörlerce çözüme kavuşturulmak üzere oluşacak fırsat pencerelerinin yakalanması çabası gösterilebilir. Çöp kutusu ve basamaklar modeli ise içerisinde en az önerme bulunan modeller olarak kayda geçmiştir ve bu sebeple barındırdıkları politika önermeleri hakkında kapsamlı bir yorum yapılamamaktadır.

Raporlar doğrultusunda ortaya çıkan politika önermeleri en çok Yorumsamacı Kamu Politikası Analizi başlığında yer almaktadır. Özellikle bilişim sektöründe rekabeti teşvik etme, istihdam yaratma kapasitesini geliştirme ve işletmelere AR-GE desteğini arttırma gibi politikalara bakıldığında, sayıca daha fazla önermenin Artırımcı Model içerisinde konumlandırılması uygun görülmüştür. İletişim ve haberleşme sektörüne dair kritik altyapı önermelerini görece daha fazla barındıran raporlara göre, yine bilişim sektöründe yerli üretimi teşvik eden ve bu doğrultuda yerli üreticiye de kolaylık sağlayan politikalar Savunma koalisyonu modeli kapsamına dâhil edilmiştir. Yorumsamacı Kamu Politikası Analizi kapsamına giren politika önermelerine bakıldığında, ülkece siber güvenliği sağlamak adına desteklenen altyapı çalışmaları sırasında milli değerlerin elden bırakılmadığı ve önceden üretilmiş politikalara eklemeler yapılarak eldeki çözüm önerisinin geliştirilmeye uğraşıldığı söylenebilecektir.
Karma Politika Analizi raporlardan çıkan önermelerin sayıca en az konumlandırıldığı analiz yöntemi olarak kayda geçmiştir. Sınırlı Rasyonalite modeli ile yalnızca bir adet politika önermesi eşleştirilirken, Karma Tarama ve Normatif Optimum modelleri, aralarında bir politika önermesi fark barındıracak şekilde ön sıralarda yer almışlardır.
Ulusal siber güvenlik ekiplerinin tesisi ve organizasyon yapısının belirlenmesine, bilişim yatırımları için fayda-maliyet, fizibilite, etki analizi gibi çalışmaların genel kabul görmüş standartlara uygun gerçekleştirilmesine ve teknoloji kullanım

kültürünü anahtar yetkinlik olarak kabul eden bir eğitim reformuna gidilmesine yönelik politikalar; değişken bir ortamda üretilecek olan politikalara karşı daha geniş açılı bir duruşu içerisinde barındırırken, aynı zamanda yenilikçi kararları üretme potansiyelini ve personelin geliştirilerek entelektüel çabanın teşvik edilmesini elden bırakmamaktadır. Sınırlı Rasyonalite modeli içerisinde yalnızca bir politika önermesinin konumlandırılması, meclis araştırma komisyonunun kritik altyapıların meydana getirdiği veya getirebileceği problemlere yönelik tavrının belirsiz olmadığını, tatmin edici seçimden çok doğru seçim olarak nitelendirilen politika anlayışı ile hareket ettiğini göstermektedir.

5.8.3.2. Raporlardaki Siber Güvenlik Politika Önermeleri Üzerine Değerlendirmeler

İnceleme kapsamına alınan tüm raporlarda siber güvenlik kavramını bünyesinde barındıran politika önermelerine yer verildiği görülmektedir. İlgili politika önermelerinin kamu politikası analizi yaklaşımları içerisindeki sayısal değerleri incelendiğinde ise, en az politika önermesinin Rasyonel Kamu Politikası Analizi başlığında konumlandığı belirlenmiştir. Karma Politika Analizi ve Yorumsamacı Politika Analizi ise bünyesinde Rasyonel Analiz yöntemine göre nispeten daha çok politika barındırmaktadır. Fayda maliyet analizine dayanan, nicel verilerin öne çıktığı, etki ve uygulama değerlendirmelerini içerisinde barındıran Rasyonel Kamu Politikası Yaklaşımının meclis araştırma komisyonu ve emniyet genel müdürlüğü raporlarında görece daha az olması, ilgili raporlarındaki çıkarsamaların ve politika önermelerinin rasyonel bir yaklaşımdan çok değer odaklı gelişme sürecinin bir parçası olduğunu göstermektedir. Siber güvenlik gibi ülkece diğer politikalara nazaran daha yeni karşılaşılan bir kavramın, beraberinde getirdiği güvenlik sorunlarını çözmeye yönelik bakış açısının, yeni bir yapı kurmak ya da hali hazırdaki uygulamaları yeni bakış açılarıyla revize etmek üzere şekillendiği, araştırma sonucunda ortaya çıkmaktadır.
Raporlar incelendiğinde, Karma Kamu Politikası Analizi Yaklaşımı içerisinde yer

alan politika önermelerinin önemli bir kısmının Normatif Optimum Karar Verme Modeli içerisinde konumlandığı görülmektedir. Siber güvenlik alanında çalışan ve politika üreten devlet organlarının kurulması, hali hazırda var olan kurumların uzmanlaşmaya yönelik adımlar atması, siber suçlarla daha etkili mücadele etmek adına kullanılması teşvik edilen yeni teknolojiler vb. vurgular, normatif optimum karar verme modeli içinde yer alan politika önermelerinin temelini oluşturmaktadır. Raporlarda yer alan ve Karma Tarama Karar Verme Modeli içinde konumlandırılan politika önermelerinde ise, politika üretim sürecine doğrudan veya dolaylı olarak etki eden tüm aktörlerin, değişen şartlara ayak uydurmak adına yenilikleri yakından takip etmesinin önemine vurgu yapılmaktadır. Karar Vermede Sınırlı Rasyonalite Modelinde yalnızca bir politika önermesinin yer alması dikkat çekmektedir. Türkiye'nin yeni tanıştığı siber güvenlik konusu hakkında üretilecek politika önermelerinin, temelinde belirsizlik durumunu barındıran Sınırlı Rasyonalite Modeli çerçevesinde daha sık yer alması tahmin edilebilir bir durum olarak değerlendirilmektedir ancak raporlara göz atıldığında yalnızca bir politika önermesinin bu model içerisinde konumlandığı göze çarpmaktadır. Bunun sonucunda Türkiye'nin siber güvenlik kavramı ile yeni tanışmasına rağmen, belirsizlik aşamasını geçerek yenilikçi adımlar atmaya başladığı söylenebilecektir.

Raporlarda yer alan politika önermelerinin yoğunlaştığı bir diğer yaklaşım ise Yorumsamacı Kamu Politikası Analizi Yaklaşımıdır. Bu yaklaşım içerisinde yer alan Artırımcı Karar Verme Modeli içerisine yerleştirilen politika önermeleri ise azımsanamayacak kadar çoktur. Siber suçlarla mücadele kapasitesini yükseltme, hali hazırdaki ilgili devlet kurumlarının uygulamalarına daha etkili devam edebilmeleri adına düzenlemeler yapma, bilişim güvenliğini sağlamaya yönelik altyapı çalışmalarını hızlandırma gibi artırımcı kararlar bu modelin içerisinde yer alabilecektir. Yaklaşımın içerisinde yer alan bir diğer model ise Savunma Koalisyonu Modelidir. Politika oluşturma sürecini ülkenin değer yargılarıyla, sosyal yapısıyla, inançlarıyla ve ideolojileriyle harmanlayan bu model kapsamında

kategorize edilen politika önermelerine bakıldığında “yerli içeriğin üretimi” veya “halk katılımı” gibi olguların ön plana çıktığı görülmektedir.

Araştırma sonunda elde edilen verilere dayanarak, sayıca en az politika önermesine sahip olan yaklaşımın Rasyonel Kamu Politikası Analizi yaklaşımı olduğu belirlenmiştir. “Kamu kurumlarına, kurum bazında özelleştirilmiş test ve denetim prosedürleri kullanılarak, düzenli aralıklarla güvenlik test ve denetimlerinin gerçekleştirilmesi” gibi rasyonel ve ampirik verilere dayanan politika önermeleri, ilgili yaklaşımın Basamaklar Modeli başlığı altında yer bulmuştur. Bu model altında sayıca daha fazla politika önermesinin yer alması, meclis raporlarının hazırlanma sürecinde ihtiyaçlara nokta atışı çözüm önerisi düşünülmesi ve buna yönelik planlamalar yapılmasına, çözüm önerilerinin belirli bir rasyonel sürece dayandırılmasına ve konuyla ilgili kapsamlı bir metodoloji kurulmasına örnek teşkil etmektedir. Çöp Kutusu Karar Verme Modeli, Politika Formülasyonu ve Çoklu Akımlar Modeli ise sayıca en az politika önermesi içeren modeller arasına girmiştir. Bu nedenle bahsi geçen üç modelden anlamlı ve kapsamlı bir sonuç çıkarılamamaktadır.

Yukarıda bahsi geçen konular dahilinde, Raporlardaki siber güvenlik politika önermelerinin en çok Karma ve Yorumsamacı Kamu Politikası Analizi Yaklaşımları içerisinde yer aldığı görülmektedir. İlgili modellerin içerisinde yer alan kamu politikası önermelerinin, meclis komisyonunca değer odaklı ve uzmanlaşmanın teşvik edildiği bir bakış açısıyla ele alındığını söylemek yanlış olmayacaktır. Politika üretimine ihtiyaç duyan sorunların içerisinde görece daha yeni olan siber güvenlik kavramı, beraberinde getirdiği güvenlik açığı ve bu açığın giderilmesine duyulan ihtiyaç; izlenen politikaları yenilikçi ve yaratıcı olmaya, değişen şartlara ayak uydurmaya ve tüm bunları ülkenin ideolojisini ve sosyal yapısını göz artı etmeden uygulamaya geçirmeye teşvik etmiştir. Bunun yanında sayıca az da olsa performans izleme, kurumlar arası çalışmaları koordine ve analiz etme, siber

güvenlik strateji ve eylem planı oluşturma gibi çalışmalarda karar vericilerin Rasyonel Kamu Politikası Analizine başvurdukları gözlemlenmiştir.

5.8.4. Hükümet Programlarındaki Kamu Politikası Önermeleri Üzerine Değerlendirmeler

Araştırmada ele alınan hükümet programlarının tümünde kritik altyapılar üzerine yapılmış çok sayıda politika önermesi belirlenmiştir. Bu politika önermelerinin sayısının en çok 61. Hükümet döneminde arttığı saptanmıştır. Diğer yandan, programların hiçbirinde siber güvenliğe ilişkin doğrudan politika önermelerine yer verilmemiştir. Araştırmada güvenlikle ilgili yapılan kodlamalardan çıkan politika önermelerinin tümü milli güvenlik ve bölgesel güvenlik konularında oluşturulmuş kamu politikası önermeleridir. Çalışmanın ilerleyen kısmında, araştırmanın bulgularına ilişkin değerlendirmelere kritik altyapılar ve güvenlik olmak üzere ayrı başlıklar halinde yer verilmiştir.

5.8.4.1. Hükümet Programlarındaki Kritik Altyapı Politika Önermeleri Üzerine Değerlendirmeler

Araştırmada ele alınan hükümet programlarında yer verilen politika önermelerine bakıldığında, kamu politikası analizi yaklaşımları altında kümelenme yoğunluğu yönünden çok anlamlı farklılaşmalar görülmemiştir. Politika önermelerinin sayı yönünden daha çok Rasyonel ve Yorumsamacı Kamu Politikası Analizi Yaklaşımı içerisinde konumlandığı tespit edilirken, Karma Kamu Politikası Analizi Yaklaşımı içerisinde konumlanan politika önermelerinin sayısı da azımsanmayacak niteliktedir.

Hükümet programlarında yer alan ve Rasyonel Kamu Politikası Analizi Yaklaşımı içerisinde konumlandırılan politika önermelerinin büyük bir kısmı, araştırmada incelenen diğer belgelerde olanın aksine Politika Formülasyonu Karar Verme

modeli içerisinde yer almıştır. Önermelerde modelin ortaya koyduğu, politika konusu problemlerin sınıflandırılmasına yönelik pek çok ize rastlanmıştır. Bunun yanı sıra önermelerin bir kısmında uygulanması öngörülen politikalarda yine modelde yer aldığı üzere "ölçek" unsuruna vurgu yapılmıştır. Politika önermelerinde ana plan ve program yapma eğilimi de gözlemlenmiş ve bu da basamaklar modeli içerisinde yer alan önerme sayısını artırmıştır. Ülkenin jeostratejik konumunun güçlendirilmesi, Orta-Asya ve Kafkasya ülkeleri ile ilişkilerde birleştirici bir unsur olma, enerji geçişinde merkezileşme gibi fırsat pencerelerini kollayan ve değerlendiren politika önermeleri de programlarda geçmektedir. Çoklu Akımlar Karar Verme Modeli içerisinde yer alan söz konusu önermelerin dışında programda, yatırımcıların önündeki engeller, enerji ücretlerinin fazlalığı, enflasyon gibi önceden de bulunan sorunlara yeni politikalarla çözüm arayan ve Çöp Kutusu Karar Verme Modeli içerisinde konumlanan önermeler de yer almıştır.

Hükümet Programlarının incelenmesi sonucunda elde edilen politika önermelerinin en az Karma Kamu Politikası Analizi yaklaşımı içerisinde yer aldığı gözlemlenmiştir. İçeriklerine göre kodlanan önermelerinin yarısı ise Normatif Optimum Model başlığına dahil edilmiştir. "Yeni bilgi ve iletişim teknolojilerinden yararlanılarak, kamu kuruluşlarının hizmet ve işlemleri halka duyurulacak, yönetimde şeffaflık sağlanacaktır" "Kamuda 'kâğıtsız ofis' dönemini başlatacak ve yazışmaların elektronik ortamda gerçekleştirilmesini yaygınlaştıracağız" gibi politika önermelerinin ve stratejik hedeflerin arasından örnek olarak seçilen bu iki söylem incelendiğinde, sıfırdan oluşturulan, öncülük ve yaratıcılığın teşvik edildiği ve oluşan yeni durumlara yönelik çözüm arayışı sunan nitelikte bir yaklaşımın ön plana çıktığı görülmektedir. Bu nedenle ilgili söylemler ve benzeri politika önermeleri Normatif Optimum Model başlığı altında konumlandırılmıştır. Yenilikten ziyade değişen şartlara uyum sağlamaya yönelik ve mevcut kurumların iyileştirilmesine odaklanan politika önermelerine ise Normatif Optimum modele

göre daha az radikal kararları bünyesine dahil etmeleri bakımından Karma Tarama Model içerisinde yer verilmiştir. İçerisinde sayıca en az politika önermesini barındıran model Sınırlı Rasyonalite Modeli olmuştur. Enerji sektöründeki ve vadeli döviz piyasalarının oluşturulmasındaki belirsizlik durumunun çözümüne yönelik ortaya konulan politika önermeleri bu başlık altında yer almıştır.

Politika önermelerinin en yoğun şekilde toplandığı Yorumsamacı Kamu Politikası Analizi Yaklaşımında, kritik altyapılar için ortaya konulan politika önermelerinin neredeyse hepsi Artırımcı Karar Verme Modeli içerisinde yer almıştır. Önceden kararı alınan termik santral ve hidroelektrik santrallerinin yapımının tamamlanması, kentsel dönüşüm projesi adı altında ulaşım ağlarının yeniden düzenlenmesi gibi sonuçları önceden kestirilebilecek ve hali hazırda olanı revize eden politikalar Artırımcı Modele örnek olabilecektir. Hükümet raporlarında yer alan politika önermelerinin çoğunun bu model başlığı altında değerlendirilmesinde, ilgili aktörlerin politika önermelerini yenilikçi bir temelden ziyade marjinal fayda sağlamaya ve olanı geliştirmeye yönelik atılımlarla geliştirmesinin etkisi olmuştur. Sayıca Artırımcı Modele göre daha az olan ve ulusal çıkarları korumaya yönelik, halk katılımını destekleyen, enerji üretiminde yerli kaynak kullanımını teşvik eden ve şeffaflığı rekabetçi bir anlayışla harmanlayan politikalar ise Savunma Koalisyonu Modeli içerisinde yer almıştır.

Araştırmada ele alınan hükümet programlarında yer verilen politika önermelerinin geneline bakıldığında, diğer belgelerden farklı olarak en çok göze çarpan husus şüphesiz ki Savunma Koalisyonu Karar Verme Modeli içerisinde konumlanan politika önermelerinin fazlalaşması olmuştur. Bunun bir yansıması olarak ve belgelerin niteliği gereği, bir nevi meclise, dolayısıyla topluma sesleniş ve politika beyan ve vaadi belgeleri olmaları dolayısıyla toplumsal, ulusal ve kültürel değerlerin ön planda tutulması normal karşılanabilecektir. Diğer yandan ilgi çekici bir nokta da, hükümet programlarında siber güvenlik ile ilgili belirlenen politika önermelerinde, Yorumsamacı Kamu Politikası Analizi Yaklaşımı içerisinde yer alan

Savunma Koalisyonu Karar Verme Modeline daha çok başvurulurken, kritik altyapılar ile ilgili belirlenen politika önermelerinde yine aynı yaklaşım içerisinde yer alan Artırımcı Karar Verme Modeline başvurulmuştur.

5.8.4.2. Hükümet Programlarındaki Siber Güvenlik Politika Önermeleri Üzerine Değerlendirmeler

Hükümet programlarında siber güvenlikle doğrudan ilişkili ya da bu kavramı barındıran politika önermelerine yer verilmediği tespit edilmiştir. Güvenlik konusu içerisinde oluşturulan politika önermelerinin büyük çoğunluğu milli güvenlik, bölgesel güvenlik ve terörle ilgili politika önermeleridir. Siber güvenlik ile ilgili sayılabilecek en önemli politika önermesi “SELSAN tarafından 100 milyon doların üzerinde bir yatırımla Gölbaşı'nda radar ve elektronik harp tasarım ve üretim merkezi kurulacak” önermesi olup, bu önerme de siber güvenlik için politika transferi potansiyeli taşıması dolayısıyla ele alınmıştır. Önerme, Yorumsamacı Kamu Politikası Analizi Yaklaşımlarından Artırımcı Karar Verme Modeli içerisinde konumlandırılmıştır. Diğer yandan temel politika olarak vurgulanan “özgürlük için güvenlik” ilkesi de bu kapsamda düşünülebilecektir. Güvenlik konusunda oluşturulmuş politika önermelerinin genelinde ortaya çıkan dikkat çekici başka bir durum, araştırmanın tümünde içinde konumlanan politika önermesi sayısı bakımından en zayıf karar verme modeli olarak belirlenen Savunma Koalisyonu Modelinin burada en güçlü çıkmasıdır. Bunun nedeninin “millileştirme, yerlileştirme, özgürlük” gibi değer vurgularının politika önermelerinde sıkça yer alması olduğu anlaşılmıştır. Politika önermeleri arasında güvenliğe ilişkin yeni altyapı ve merkezlerin kurulmasına ve elde olanların ortaya çıkan yeni gelişmeler çerçevesinde revize edilmesine dair, Normatif Optimum ve Karma Tarama Karar Verme Modelleri içerisinde yer alan önermelere de rastlanmıştır. Sonuç olarak hükümet raporlarında, kamu politikası analizi yaklaşımları çerçevesinde değerlendirilebilecek siber güvenlik politika önermelerine yer verilmemiştir. Bu

sonuç aynı zamanda siber güvenlik politikası üretiminin Türkiye'de yeterince kurumsallaşmadığını göstermektedir.

5.8.5. Siber Güvenlik İle İlgili Hukuki Belgelerdeki Kamu Politikası Önermeleri Üzerine Değerlendirmeler

Araştırmada ele alınan siber güvenlik ile ilgili hukuk belgelerinde hem kritik altyapılar üzerine hem de siber güvenlik üzerine yapılmış politika önermeleri belirlenmiştir. Çalışmanın ilerleyen kısmında, araştırmanın bulgularına ilişkin değerlendirmelere kritik altyapılar ve siber güvenlik olmak üzere ayrı başlıklar halinde yer verilmiştir.

5.8.5.1. Siber Güvenlik İle İlgili Hukuki Belgelerdeki Kritik Altyapı Politika Önermeleri Üzerine Değerlendirmeler

Araştırmada ele alınan siber güvenlik ile ilgili hukuki belgelerde hem kritik altyapılar üzerine hem de siber güvenlik üzerine yapılmış politika önermelerine rastlanmıştır. Belgelerde, kritik altyapılara ilişkin politika önermelerinin tümü iletişim altyapısı üzerinde tespit edilmiştir. Bunun nedeni ele alınan siber güvenlik ile ilgili hukuki belgelerin Elektronik Haberleşme Kanununu da içermesidir. Doküman analizi sonucunda elde edilen 47 adet kritik altyapı politika önermesinin tümü bu belgede yer almıştır.

Belgede yer alan kritik altyapıya ilişkin politika önermelerinin büyük çoğunluğu (28 adet) Yorumsamacı Kamu Politikası Analizi Yaklaşımı içerisinde yer alırken, Rasyonel Kamu Politikası Analizi Yaklaşımı içerisinde yer alan yalnızca 3 adet politika belirlenmiştir. Karma Kamu Politikası Analizi Yaklaşımı içerisinde yer alan politika önermelerinin sayısı ise 16'dır. Hukuki belgelerin yorumsamacı doğası gereği, belgede yer alan kritik altyapılara ilişkin politika önermelerinin yoğunluklu

olarak kamu politikası analizi yaklaşımlarından Yorumsamacı Yaklaşım içerisinde yer alması doğal bir sonuç olarak düşünülmektedir.

Rasyonel Kamu Politikası Analizi Yaklaşımı içerisine alınan 3 adet politika önermesinin tümü Basamaklar Karar Verme Modeli temelinde oluşturulmuştur. Bu politika önermelerindeki temel vurgular pazar analizleri, düzenlemelere yönelik usul ve esasların belirlenmesi gibi konuları kapsamaktadır. Politika önermelerinin sayıca çok az olmasından dolayı burada anlamlı bir farklılaşma görülmemiş ve değerlendirilmemiştir.

Belgede, Yorumsamacı Yaklaşım içerisinde yer alan ve Artırımcı Karar Verme Modeli içerisinde konumlandırılan politika önermeleri altyapılara ilişkin “tedbirler almak, öncelikler vermek, teşviklerde bulunmak, düzenlemeler yapmak” gibi artırımcı vurguları içermektedir. Yaklaşım içerisinde yer alan diğer politika önermeleri insan sağlığı, can ve mal güvenliği, çevre ve tüketicinin korunması üzere özürlü, yaşlı ve sosyal açıdan korunmaya muhtaç diğer kesimlerin özel ihtiyaçlarının dikkate alınması, kamu sağlığını tehdidin önlenmesi gibi ilke ve değer yönelimli önermeler olarak Savuma Koalisyonu Modeli içerisine konumlandırılmıştır. 47 adet politika önermesinden yalnızca 4’ünün bu modelde konumlandırılması, belgede yer alan kanunların değer odaklılığının düşük olduğunu göstermektedir. Göze çarpan başka bir husus ise iletişime ait Yorumsamacı politika önermelerinde, siber güvenlik ile bağlantı kuran vurgulara rastlanmamış olunmasıdır.

Karma Kamu Politikası Yaklaşımı içerisinde gruplanmış politika önermelerine bakıldığında, söz konusu önermelerin en çok Normatif Optimum Karar Verme Modeli içerisinde gruplandığı gözlemlenmiştir. Önermeler, yenilikçi teknolojileri yakalamak ve iletişim haberleşme altyapılarına erişim yöntemlerinin optimizasyonuna dayanmaktadır. Karma Tarama Karar Verme Modeli içerisinde yer alan politika önermeleri ise elektronik haberleşme sektöründeki gelişmeleri

takip etmek, sektörün gelişimini teşvik etmek amacıyla gerekli araştırmaları yapmak, elektronik haberleşme sektörü ile ilgili uluslararası birlik ve kuruluşların çalışmalarına katılmak gibi modelde de vurgulanan “gelişen şartlara uyum sağlanması” üzerine yapılan önermelerdir. Bu önermelerden anlaşılacağı üzere Türkiye’nin ilgili hukuki düzenlemeleri de siber güvenlikle birincil derecede bağlantılı olan iletişim kritik altyapısını geliştirme politikası izlemektedir.

Hukuki belgelerin kritik altyapılar ile ilgili politika önermelerinin kamu politikası analizi yaklaşımları çerçevesindeki mahiyetine genel olarak bakıldığında, önermelerin Karma, Rasyonel, ve Yorumsamacı Kamu Politikası Analizi yaklaşımları arasında eşit yoğunlaşmadığı, yoğunluğun özellikle Yorumsamacı yaklaşım üzerinde oluştuğu görülmüştür. Hukuki belgelerde yer alan kanunların yorumsamacı doğası göz önüne alındığında böyle bir sonuç doğal karşılanmıştır. Politika önermelerinin genel olarak eldeki altyapıların gelişen ve değişen teknolojilere uyum sağlamak üzere tasarlanmış olması ise Türkiye’nin siber güvenlik politikaları adına olumlu bulunurken, siber güvenliğe ilişkin yenilikçi ve yerli altyapıların tesisi için Savunma Koalisyonu, Normatif Optimum ve Karma Tarama Modellerde tasarlanmış yenilikçi politikaların artırılması gerektiği düşünülmektedir.

5.8.5.2. Siber Güvenlik İle İlgili Hukuki Belgelerdeki Siber Güvenlik Politika Önermeleri Üzerine Değerlendirmeler

Ele alınan hukuki belgelerinin tümünde siber güvenlik ile ilgili politika önermelerine yer verilmiştir. Yer verilen politika önermelerinin büyük ölçüde Yorumsamacı Kamu Politikası Analizi Yaklaşımı içerisinde yer alırken, Rasyonel Kamu Politikası Analizi Yaklaşımı ve Karma Kamu Politikası Analizi Yaklaşımı içerisinde yer alan az sayıda politika önermesi belirlenmiştir (her biri Yorumsamacı yaklaşımın yaklaşık %25’i oranında). Bu genel tabloya bakıldığında, yine yukarıdaki “hukuki belgelerin

yorumsamacı doğası" yorumu yanında, ele alınan diğer iki hukuki belgenin direkt olarak siber güvenliği konu almasının etkili olduğu düşünülmektedir.

Genel kanaati destekleyen bir şekilde Yorumsamacı yaklaşım içerisinde yer alan politika önermelerinin 2'si dışında tümü Artırımcı Karar Verme Modeli içerisinde konumlanmıştır. 2 politika önermesinde ise ulusal siber güvenlik konusunda yapılacak çalışmalar sürecinde, mümkün olan tüm alanlarda milli çözümler geliştirilmesi, yazılım ve donanım altyapılarında azami ölçüde milli kaynakların kullanılması, ulusal siber güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretilmesini teşvik etmek, kullanımının sağlanması gibi konuları içermektedir. Siber güvenliğin sağlanmasına yönelik politikaları destekleyecek şekilde bu yönde oluşturulacak hukuki düzenlemelerin ve politika önermelerinin artması gerekmektedir.

Belgelerde, Karma Kamu Politikası Analizi Yaklaşımı içerisinde konumlandırılan politika önermelerinin çoğunluğu Normatif Optimum Karar Verme Modeli içerisinde yer almıştır. Önermelerin ikinci olarak en fazla yoğunlaştığı model ise Karma Tarama Karar Verme Modelidir. Normatif Optimum modelde yer alan kamu politikası önermelerinde, çağının gerektirdiği çağdaş güvenlik tedbirlerinin oluşturulması, ulusal bilgi güvenliğine ilişkin konularda altyapı temini modelinin oluşturulması gibi yenilikçi politika önermelerine yer verilirken aynı zamanda kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini gibi uzmanlaşmaya yönelik vurgular da yer almaktadır. Karma Tarama modelde yer alan önermelerde ise ulusal bilgi güvenliğine karşı yurt içi ve yurt dışı tehdidin tespit edilmesini sağlamak, ulusal bilgi güvenliği ile ilgili uluslararası mevzuat ve teknolojideki gelişmeleri takip etmek gibi teknolojik gelişmelere bağlı olarak değişen siber güvenlik çevresine uyum sağlamaya yönelik tarama politikalara daha fazla yer verilmiştir.

Hukuki belgelerde, Rasyonel Kamu Politikası Analizi Yaklaşımı çerçevesinde konumlandırılan politika önermelerinin tümü Basamaklar ve Politika Formülasyonu Karar Verme Modeli arasında neredeyse eşit şekilde dağılmıştır. Bu yaklaşım altında Çöp Kutusu ve Çoklu Akımlar Modelleri içerisinde hiçbir politika önemesi bulunmaması, hukuki belgelerde yer alan rasyonel politikaların daha çok problemlerin formülize edilerek, sistematik süreçler dâhilinde ve nicel verilere dayanılarak yapıldığını ortaya koymaktadır. Önermelerde, ulusal bilgi güvenliği risk yönetimi ve değerlendirmesi Ulusal Bilgi güvenliği ile ilgili olarak görev alanına ilişkin planlama ve programlama faaliyetlerinde bulunmak, risk analizleri ve risk azaltma planları yapmak, internet teknolojileri yapısına karşı iç ve dış tehdidi teşhis etmek, tanımlamak gibi konulara ağırlık verilmesi bu görüşü desteklemektedir. Diğer yandan bu politika önermelerinin sayısının çok sınırlı olması, Türkiye'nin siber güvenlik politikaları üzerinde planlı yaklaşımların etkisinin yetersiz olduğu görüşünü ortaya çıkarmaktadır.

Bahsi geçen konu ve değerlendirmeler genel olarak ele alındığında, Türkiye'nin siber güvenlik ile ilgili olan hukuki belgelerde yer verilen politika önermelerinin yoğun olarak Yorumsamacı Kamu Politikası Analizi Yaklaşımı etrafında şekillendiği söylenebilecektir. Bunun yanında, siber güvenliğe ilişkin eldeki altyapıların geliştirilmesi ve yeni gelişen teknolojilere uyumlaştırılması için özellikle Karma Kamu Politikası Analizi Yaklaşımı içerisinde yer alan politika önermelerine de belgelerde azımsanmayacak sayıda yer verildiği tespit edilmiştir. Belgelerde yer verilen Rasyonel Kamu Politikası Analizi Yaklaşımı içerisinde yer alan ve genel olarak politikaların daha çok problemlerin formülize edilerek, sistematik süreçler dâhilinde ve nicel verilere dayanılarak oluşturulmasıyla elde edilen politika önermelerinin sayısının sınırlılığı ise hukuki belgelerin yorumsamacı doğasıyla ilişkilendirilmiştir. Bu belgelerde eksikliği göze çarpan rasyonel politika önermelerinin Türkiye'nin siber güvenlik politikasını belirleyen ve belirten diğer

belgelerde yoğunlaştığı ve söz konusu eksikliğin bu belgelerle giderilmeye çabalandığı kanısına ulaşılmıştır.

SONUÇ VE ÖNERİLER

Bu çalışma, kamu politikası analizi yaklaşımlarını ve bu yaklaşımlar içerisinde yer alan karar verme modellerini derinlemesine bir şekilde ele alarak, Türkiye'nin siber güvenlik ve onunla bağlantılı olarak kritik altyapılarla ilgili politikalarını belirleyen resmi belgelerde uyguladığı ya da uygulamayı öngördüğü politikaları bu yaklaşım ve modeller çerçevesinde analiz etmiştir. Bunun yanında siber güvenlik ve siber güvenlik politikaları ile ilgili bir örnek olay ve belirli bir yaklaşım çerçevesinde ele alınan 5 ülke incelemesine yer vermiştir. Çalışmanın beşinci bölümünde yapılan nitel araştırma, ele alınan resmi belgelere dâhil edilmiş politika önermelerinin ilk bölümde ele alınan ve araştırmacı tarafından sınıflandırılan kamu politikası yaklaşım ve modellerinin hangisinin sınırlarına girdiğini belirlemektedir. Böylece çalışma, Türkiye'de hangi politika önermeleri yapılırken hangi yaklaşım ve modellerin (kasten ya da farkında olmadan) ne yoğunlukta içerildiğinin altını çizerek hangilerinin eksik kaldığını tespit etmiş ve Türkiye'nin siber güvenlik ve onunla doğrudan bağlantılı kritik altyapılar konusunda ürettiği ve belirlediği politikaların bu yaklaşım ve modeller çerçevesindeki yönelimlerini ortaya koymuştur. Çalışmada siber güvenliğin devlet (idari) boyutuna odaklanılmıştır. Tüm bu adımlar doğrultusunda, belirlenen araştırma sorularına karşı çalışmanın ortaya koyduğu sonuçları şu şekilde sıralamak mümkündür:

Siber Güvenliğin Önemine İlişkin Sonuçlar

- Siber güvenlik, bireysel, kitlesel, bölgesel ya da ulusal ve dahi uluslararası anlamda güvenliği ifade etmekte olup, bu yönüyle son yıllarda hem bir vatandaş olarak bireyin hem de bireyin güvenliğinden sorumlu olan ve bir politika üreticisi, uygulayıcısı olarak devletin yaşam alanına giren bir konu haline gelmiştir.

- Çalışmada siber güvenliğin kritik altyapıların güvenliği için hayatî önemini kavramak adına ele alınan örnek olay Stuxnet, siber güvenlik ve siber savaş alanına yeni bir boyut kazandırmıştır. Bu olay, siber güvenlik ile ulusal güvenliğin, siber savaş ile fiziki savaşın arasındaki siber olguların daha tehlikesiz ve önemsiz olarak algılanmasına neden olan sınırları kaldırmış, siber güvenliğin önemini özellikle devletler açısından kalıcı bir şekilde gün yüzüne çıkarmıştır.

- Türkiye'de kritik altyapıların korunmasına yönelik bir algı oluşmaya başlamıştır. Bu bağlamda ülkede siber güvenliğe ilişkin hukuki düzenlemeler yapılmış, strateji belgeleri oluşturulmuş, yeni devlet birimleri kurulmuş, bu birimler ve kurumlar siber güvenlik konusunda çalışmalar yapmaya (çalıştaylar, eğitimler, yayınlar, projeler vb.) başlamışlardır.

Ülkelerin Siber Güvenlik Politikalarına İlişkin Sonuçlar

- ABD'nin siber güvenliğe yönelik farkındalığı henüz 2000'li yılların başlangıcına dayanmaktadır. Diğer yandan ülkenin siber güvenlik ile ilgili olarak 2015 yılında yayınlanan strateji belgesinde gelinen noktaya bakıldığında, bu zaman aralığında çıkarılan diğer belgelere karşın somut adımların daha çok son dönemde atıldığı ve bu farkındalığın halen gelişmekte olduğu gözlemlenmiştir. Bu durum Türkiye açısından ele alındığında, siber güvenlik konusuna yönelik olarak yapılan çalışmalar ve gelişmeler için henüz çok geç kalınmadığı, kritik altyapıların yerlileştirilmesi, yerli bilişim uzmanlarının yetiştirilmesi gibi yapısal reformlar ve yerinde politikaların uygulanarak orta ve uzun vadede siber güvenlik altyapılarının oluşturulmasında, kalkan treni yakalamanın mümkün olabileceği kanısına ulaşılmıştır.

- Rusya'nın siber güvenlik politikası oluşturma sürecinin savunmacı anlayışla temellendiği, fakat gelişim sürecinde saldırıya saldırı politikasıyla güvenlik anlayışını geliştirerek bu politika anlayışıyla ele alınan diğer ülkelerden farklılaştığı tespit edilmiştir.

- Çin'in siber güvenlik stratejisi daha çok saldırı odaklı olarak tanımlanmıştır. Fakat bu yönde genel geçer bir tanımın yanlış olacağı düşünülmektedir. Çin, diğer ülkelerden ayrı olarak kendi milli siber ağlarını kullanarak ve uluslararası platformlarda aygın bir şekilde kullanılan birçok ağı kullanmayı yasaklayarak ya da kullanımına sınırlar getirerek aslında en güçlü savunma mekanizmasını geliştirmiştir. Bu yönde izlenen bir politika ülkeyi somut savunma mekanizmaları kurmasa da, ülkeyi siber güvenlik konusunda batı ülkelerine nazaran daha güvenlikli bir hale getirmektedir.

- İran'ın siber güvenlik politikası, özellikle ülkenin kendi Proxy ağlarını kurması yönünden Çin'in milli siber altyapı politikasına benzer bir özellik taşımaktadır. Bu girişim ve teşviklerin Çin'de olduğu gibi kendi operatör ve servis sağlayıcılarını oluşturma, kendi yazılımlarını geliştirme ve kendi siber donanımlarını üretme safhasından çok geride olduğu tespit edilmiştir. Bir diğer politika olarak devletin siber güvenliğe ilişkin insan kaynağını hem kamu hem de kamu dışı sektörden oluşturmasına ve bunlara destek vermesine dayanan politika da yine Çin'in politikası ile benzerlik gösterirken, Çin'de bu politikanın; ülkenin kendi yazılım ve donanım firmalarının sektörde gelişmek ve bağımsızlaşmak adına yaptığı hamlelerle, daha sistematik ve kurumsal bir şekilde geliştiği görülmektedir.

- Kuzey Kore'nin siber güvenlik politikasının ele alınan ülkelerden daha çok Çin ile benzerlik gösterdiği ve dahi bu konuda Çin'i taban aldığı belirlenmiştir. Yine de ülkenin küresel arenada, her yönüyle dışarı kapalı bir ülke olması dolayısıyla her türlü kurumsal kapasitesinin olduğu gibi siber kapasitesinin de

durumu diğer ülkeler açısından gizemini korumaktadır. Ülkede Operatör yazılım olarak (Windows yerine) ülkenin kendi geliştirdiği Bulguenbyol kullanılmaktadır. Yardımcı yazılımlar ve paket programlar yine milli olarak geliştirilmektedir. Donanımlar ise Çin'den ithal edilmekte ve sınırlı sayıda satın alınmaktadır.

- İsrail'de siber güvenlik halk ve devletin ortak konusu ve sorumluluğu olarak görülmektedir. Devletin siber güvenlik politikasında, operasyonel fonksiyonlarda ordusu altyapısal fonksiyonlarda ise özel sektörü ön plana çıkmaktadır.

- Almanya, devletler arasında siber güvenlik politikalarını kurumsal anlamda en sistematik olarak geliştiren ülke olarak belirlenmiştir.

- Devletler kritik altyapıların korunmasına ve siber güvenliğin artırılarak güvenlik açıklarının azaltılmasına yönelik olarak daha merkezi ve katı kurallar koymak üzere adımlar atmayı planlarken, bireyler ise kendi özgürlüklerine yönelik olarak siber uzaydaki hareket alanlarını en serbest şekilde muhafaza etmek istemektedir. Bu çatışmadan bir ikilem doğmaktadır. Bu ikilemde, uluslararası şirketler de liberal görüşün etkisiyle, bireylerin tutumundan yana taraf almaktadır. Devletler açısından, siber uzayda bireylere ve firmalara (özellikle yazılım firmalarına) sunulan serbesti, aynı zamanda ulusal siber güvenlik açısından genişleyen güvenlik açıklarını da beraberinde getirmektedir. Bu ikilemin çözümü, geniş kapsamlı tanımları ve birbirine bağımlı değişkenleri içeren, bireysel ve ulusal güvenlik önceliklerini belirleyerek bir uzlaşma temelinde oluşturulacak olan siber güvenlik politikasıdır.

Türkiye'nin Siber Güvenlik Politikalarına İlişkin Sonuçlar

- Kalkınma planlarındaki politika önermelerinden yalnızca 3'ünün siber güvenliğe ilişkin olduğunun tespit edilmesi ve kalkınma planlarına benzer şekilde hükümet programlarında siber güvenliğe ilişkin politika önermelerinin bulunmaması, Türkiye'de siber güvenliğin henüz bir makro politika olarak görülmediğini göstermektedir.

- Kalkınma planlarında, kritik altyapı politika önermelerinin en yoğun şekilde yöneldiği yaklaşım Karma Kamu Politikası Analizi Yaklaşımıdır. Yaklaşım içerisinde yer alan ve "yenilikçilik, yaratıcılık, deneyim, uzmanlaşma" ilkeleri doğrultusunda politika oluşturmayı hedefleyen Normatif Optimum Karar Verme Modeli içerisinde yer alan kamu politikası önermeleri de bir hayli fazladır. Önermeler, özellikle nükleer enerjiye geçiş, iletişim ile enerji alanında teknik uzmanların yetişmesi ile yeni altyapı sistem ve tesislerinin kurulmasına yönelik olduğu tespit edilmiştir.

- Strateji Belgelerindeki kritik altyapı politika önermelerinin daha çok Karma Kamu Politikası Analizi ve Rasyonel Kamu Politikası Analizi kapsamında, Normatif Optimum Model ve Basamaklar Modeli içerisinde yer almasının sebebi, uygulanacak politikaların daha çok yenliğe dayalı olması, var olmayan altyapıları oluşturmasına yönelik olması ve bu politikaların belirli süreçler içerisinde gerçekleştirilmesine dayanmasıdır.

- Strateji belgelerinde, kritik altyapılar ile ilgili politika önermelerinin kamu politikası analizi yaklaşımları çerçevesindeki mahiyetine genel olarak bakıldığında, Türkiye'nin, mevcutta var olan altyapılarını geliştirmek ve yeni teknolojileri yakalamak, var olmayan altyapılarını ve yenilikçi mekanizmalarını kurmak üzere Karma; verimlilik ve olumlu yönde etki artışlarını sağlamak, bu yönde planlar yapmak, eski sorunlarına yeni teknolojilerle çözüm bulmak

adına rasyonel ve süre gelen politikalarını, ortaya çıkan yeni sorunlara göre ilave politikalarla destekleyerek çözmeyi amaçlayan ve bunları yaparken kültür, sosyal fayda, kamu yararı gibi değerleri de göz önünde bulunduran Yorumsamacı Kamu Politikası Analizi yaklaşım ve yöntemlerini eşit ağırlıkta dağılım gösterdiği tespit edilmiştir.

- Araştırmada ele alınan strateji belgelerinde geçen siber güvenliğe ilişkin politika önermeleri büyük ölçüde Karma ve Yorumsamacı Kamu Politikası Analizi Yaklaşımı içerisinde yer alırken, Rasyonel Kamu Politikası Analizi Yaklaşımı içerisinde yer alan az sayıda politika önermesi belirlenmiştir. Bu genel tabloya ilk bakışta durumun Türkiye'nin sahip olduğu sınırlı siber güvenlik politikası altyapısını yansıttığı söylenebilir. Zira yer verilen politika önermelerinin ağırlıklı oranda Karma ve Yorumsamacı yaklaşım içerisinde yer almaları, önermelerin yeni bir yapıyı kurmak, olan bir yapıyı ortaya çıkan yenilikler doğrultusunda revize etmek üzere ya da süre gelen politikalar üzerine ek politikalar yaparak sürdürmek üzere oluşturulduğu anlaşılmıştır. Bunun yanında az sayıda da olsa, özellikle adalet hizmetleri, e-dönüşüm, sektör yapılanması, risk yönetimi, Ulusal Risk Değerlendirmesi Siber saldırılara karşı koymak için Siber Saldırı Eylem Planları hazırlanması gibi nicel yöntemlere ihtiyaç duyan politikalarda, Rasyonel Kamu Politikası Analizi yaklaşımına başvurulmuştur. Türkiye'nin siber güvenlik konusundaki mevcut durumu, ülke dinamikleri, içinde bulunulan ve stabil olmayan siber ortam göz önüne alındığında, araştırmanın bulguları doğrultusunda ortaya çıkan, ülkenin siber güvenlik politikası eğilimlerinin birbiri arasında tutarlı olduğu sonucuna ulaşılmıştır.

- Araştırmada ele alınan strateji belgelerinden çıkarılan yargıya göre Türkiye'de hem karar verme açısından hem de siber güvenliğin sağlanmasına yönelik atılacak adımlar açısından bir belirsizlik ortamı var olduğu görülmüş, karar vericilerin bu alandaki teknik bilgilerinin yeterince kapsamlı olmadığı ve

bu konuda diğer ülke uygulamalarına ilişkin raporlar oluşturma gibi araştırmalara yöneldikleri tespit edilmiştir.

- Raporlardaki siber güvenlik politika önermelerinin en çok Karma ve Yorumsamacı Kamu Politikası Analizi Yaklaşımları içerisinde yer aldığı görülmüştür. İlgili modellerin içerisinde yer alan kamu politikası önermeleri, meclis komisyonunca değer odaklı ve uzmanlaşmanın teşvik edildiği bir bakış açısıyla ele alınmıştır. Politika üretimine ihtiyaç duyan sorunların içerisinde görece daha yeni olan siber güvenlik kavramı, beraberinde getirdiği güvenlik açığı ve bu açığın giderilmesine duyulan ihtiyaç; izlenen politikaları yenilikçi ve yaratıcı olmaya, değişen şartlara ayak uydurmaya ve tüm bunları ülkenin ideolojisini ve sosyal yapısını göz artı etmeden uygulamaya geçirmeye teşvik etmiştir.

- Araştırmada, komisyon raporlarındaki kritik altyapılara ilişkin üretilen politika önermelerinin en az Karma Politika Analizi yaklaşımı içerisinde konumlandırıldığı saptanırken, siber güvenlik politika önermelerinin en fazla yer aldığı başlığın yine Karma Politika Analizi yaklaşımı olduğu göze çarpmıştır. Bunun sonucunda meclis araştırma komisyonunca oluşturulan siber güvenliğe dair politika önermelerinin mevcutta var olan altyapıları geliştirmek, var olmayan altyapıları kurmak ve yeni teknolojileri yakalamak adına geliştirildiği belirlenmiştir.

- Araştırmada ele alınan hükümet programlarında yer verilen kritik altyapı politika önermelerinde diğer belgelerden farklı olarak Savunma Koalisyonu Karar Verme Modeli içerisinde konumlanan politika önermelerinin fazlalaştığı tespit edilmiştir. Kritik altyapılara ilişkin politika önermelerinde, Yorumsamacı Kamu Politikası Analizi Yaklaşımı içerisinde yer alan Savunma Koalisyonu Karar Verme Modeline daha çok başvurulurken, kritik altyapılar ile ilgili

belirlenen politika önermelerinde yine aynı yaklaşım içerisinde yer alan Artırımcı Karar Verme Modeline başvurulmuştur.

- Araştırmanın genelinde içinde konumlanan politika önermesi sayısı bakımından en zayıf karar verme modeli olarak belirlenen Savunma Koalisyonu Modeli, hükümet programlarının güvenliğe ilişkin analizinde en güçlü karar verme modeli olarak tespit edilmiştir. Bunun nedeni, siber güvenliğin sağlanması konusunda, "kritik altyapıların yerlileştirilmesi, millileştirilmesi, ithal edilmemesi gibi" gibi savunucu değer vurgularının politika önermelerinde sıkça yer almasıdır.

- Türkiye'nin siber güvenlik ile ilgili olan hukuki belgelerde yer verilen siber güvenlik politika önermeleri yoğun olarak Yorumsamacı Kamu Politikası Analizi Yaklaşımı içerisinde yer almıştır. Rasyonel Kamu Politikası Analizi Yaklaşımı içerisinde yer alan siber güvenlik politika önermelerinin sayısının sınırlılığı ise hukuki belgelerin yorumsamacı doğasıyla ilişkilendirilmiştir.

Çalışma, bulguları ve analizleriyle her ne kadar çok sayıda ve geniş kapsamlı sonuca ulaşsa da, genel sonuç olarak Türkiye'nin siber güvenlik politikalarının, ülkenin alana yeni adapte olan bir ülke olması dolayısıyla Karma Kamu Politikası Analizi Yaklaşımı doğrultusunda "Normatif Optimum" ve "Karma Tarama" modelleri çerçevesinde oluştuğu; siber güvenlikle doğrudan ilgili olan eldeki kritik altyapılarının geliştirilmesi amacıyla da "Yorumsamacı Kamu Politikası Analizi" doğrultusunda "Artırımcı Karar Verme" modelleri üzerinde yoğunlaşarak şekillendiği söylenebilecektir. Ülkenin siber güvenlik nezdindeki mevcut durumu ve dinamikleri göz önüne alındığında, KPA yaklaşımları ve karar verme modelleri içerisindeki yönelimler doğal karşılanmıştır. Bunun yanında ileride üretilecek kamu politikalarında, kritik altyapıları geliştirmek ve yerlileştirmek için Artırımcı ve Savunma Koalisyonu Modellerinde; yeni altyapıların tesisi için ise Normatif

Optimum ve Karma Tarama Modellerinde tasarlanmış yenilikçi politikaların artırılması gerekmektedir.

Siber güvenlik konusunda Türkiye'de yapılan çalışmalar henüz başlangıç aşamasında olmakla birlikte ülkede konuya ilişkin algının, dünyada olduğu gibi hızlı bir şekilde arttığı görülmüştür. Bu yönde ülkede siber güvenliğe ilişkin hukuki altyapı oluşturulmaya başlanmış, kalkınma planlarında yer verilmese de konuya odaklı strateji ve eylem planları oluşturulmuş, politikalar doğrultusunda birimler kurulmuştur. Ancak bunların geliştirilmesi gerekmektedir. Söz konusu gelişim, teknik altyapının yanı sıra öncelikle siber güvenliğe ilişkin insan kaynağının yetiştirilmesi ve oluşturulması ile mümkün olabilecektir. Bunun için "bilişim uzmanı" yetiştirilmesine ve yetiştirilen bu uzmanların ise sürekli geliştirilmesine ihtiyaç vardır. Zira ülkenin siber güvenlik konusunda birincil ihtiyacı olarak düşünülen "yerli ve milli" altyapıların inşası için "yerli ve milli bilişim uzmanları" gerekmektedir. Bunun sağlanabilmesi için de siber güvenlik eğitimi konusuna önem vermek gerekmektedir. Yapılan çalışmada ele alınan belgelerde, siber güvenliğin yükseköğretim düzeyindeki eğitim ve öğretim kapasitesinin artırılmasına ilişkin politikalar yer alırken, ilk ve ortaöğretim seviyesinde eğitim uygulamalarına ilişkin politikalara rastlanmamıştır. Hem bahsi geçen bilişim uzmanlarının yetiştirilmesinde eğitim altyapısının güçlendirilmesi hem de bireylerin siber güvenliklerinin sağlanmasının aynı zamanda ülkenin siber güvenliğinin sağlanmasının şartı olması temelinde, bireylere henüz erken yaşlardan itibaren siber güvenlik eğitimleri verilmelidir.

Kalkınma planlarında siber güvenliğe değinilmemesi endişe vericidir. Bu bağlamda, yeni dönem için hazırlanacak olan kalkınma planında bu eksiğin giderilmesi ve siber güvenlik ile siber güvenlik-kritik altyapılar bağlantısı üzerine özellikle Normatif Optimum ve Karma Tarama Karar Verme Modelleri çerçevesinde üretilmiş yenilikçi, geniş açılı, yaratıcı ve uzmanlaşmaya yönelik politika önermelerine yer verilmesi, bu önermelerin de mümkün olan en kısa sürede bir politika olarak

uygulamaya geçirilmesi gerekmektedir. Bunun yanında, Türkiye'nin siber güvenlik konusunda, bir uzlaşı temelinde oluşturulmuş, bireyleri, özel şirketleri, devlet kurumlarını bir taraf olarak içeren, tüm taraflar açısından bağlayıcı, ülkenin dinamiklerini göz önünde bulundurarak ülkeye özgün tasarlanmış yerli ve milli olan uzun vadeli bir strateji belgesine ihtiyacı vardır. Ayrıca, hem söz konusu stratejinin üretilmesinde gerekli zemini sağlayacak hem de siber güvenlik konusunda yine bireylere, özel şirketlere, devlet kurumlarına geniş kapsamlı rehberlik edecek nitelik ve donanımda, siyaset üstü kurum ya da kurumlar oluşturulmalıdır.

Siber güvenlik konusu, ülkeler açısından önemli bir hale gelmekle birlikte çeşitli bilim dalları arasında da bir çalışma konusu olarak popüler bir hale gelmiştir. Türkiye'de de bu etkiyi görmek mümkündür. Çalışmada yapılan araştırmaya göre, ülkede 5 yıldır siber güvenlik konusuna ilişkin lisansüstü tezler yazılmaktadır. Bu tezler, hem sosyal bilimler hem de fen bilimleri alanlarında yer alan çeşitli anabilim dalları kapsamında yazılmıştır. Siber güvenliği konu alan bu tezlerin yazıldığı anabilim dallarının bu denli farklılaşmasının yanı sıra tezlerin tümünün sosyal bilimler konularına odaklı yazıldığı göze çarpmaktadır. Gelecekte, özellikle bilgisayar mühendisliği kapsamında yazılacak siber güvenlik tezlerinin daha teknik ve somut çözümler ya da ürünler ortaya koyan, Türkiye'nin siber güvenliğe ilişkin altyapılarına katkı sağlayacak tezler olması yararlı olacaktır.

KAYNAKÇA

Akdoğan, A. A. (2011). Türkiye'de Kamu Politikası Disiplininin Tarihsel İzleri. iç. Kartal, F. (der). *Türkiye'de Kamu Yönetimi ve Kamu Politikaları*. TODAİE: 75-99.

Akyıldız, M. A. (2013). *Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar İle Değerlendirilmesi*. Yayınlanmamış Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Isparta: Süleyman Demirel Üniversitesi.

Albrechts, L., ve Mandelbaum, S. (2007). *The Network Society: A New Context for Planning*. Routledge.

Aljazeera. (2014). Anonymous'tan İsrail'e Siber Saldırı. 22.11.2017 tarihinde: http://www.aljazeera.com.tr/haber/anonymoustan-israile-siber-saldiri adresinden alınmıştır.

Altunok, M. ve Metin, H. (2003). Karşılaştırmalı Bir Yaklaşımla Karar Verme Modelleri. *Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 2(7): 93-104.

Anderson, J. E. (2003). *Public Policymaking: An Introduction*. Boston: Houghton.

Andreasson, K. (2012). *Cybersecurity: Public Sector Threats and Responses*. CRC Press.

Andrews, C. J. (2007). Rationality in Policy Decision Making. iç. Fischer, F., Miller, Gerald, J. ve Sidney, Mara, S. (der). *Handbook of Public Policy Analysis*. CRC Press, pp.161-171.

Angelov, A. (2002). Actors and Institutions in The Policy Process: Theoretical Frameworks and Empirical Example / The Case Of Germany, Italy, US and Grate Britain Association for Studies in Public Economics. The *Fifth International Conference On "Public Sector Transition",* 24- 25 May 2002, St. Petersburg.

Aydın, F. (2012). *Türkiye'nin Ulusal Korunmasında Siber Güvenlik*. Yayınlanmamış Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Ankara: Çankaya Üniversitesi.

Aytekin, A. (2015). *Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi*. Yayınlanmamış Yüksek Lisans Tezi, Bilişim Enstitüsü, Ankara: Gazi Üniversitesi.

Babaoğlu, C. (2017). Kamu Politikası Analizine Yönelik Kavramsal ve Kuramsal Bir Çerçeve. *Yönetim Bilimleri Dergisi*, 15(30): 511-532.

Bakioğlu, A. ve Demiral, S. (2013). Okul Yöneticilerinin Belirsizlik Durumlarını Algılama ve Karar Verme Tarzları. *Eğitim Bilimleri Dergisi*, (38): 9-35.

Balcı, A. (2001). *Sosyal Bilimlerde Araştırma; Yöntem, Teknik ve İlkeler*. Ankara: Pagem Yayınevi.

Barros, G. (2010). Herbert A. Simon and The Concept of Rationality: Boundaries and Procedures. *Brazilian Journal of Political Economy*, 30-3(119): 455-472.

Baybutt, P. (2004). Cyber Security Risk Analysis for Process Control Systems Using Rings of Protection Analysis (ROPA). *Process Safety Progress*, 23(4): 284-291.

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

Baylon, C. (2017). Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare. iç. Taddeo, M. ve Glorioso, L. (der), *Ethics and Policies for Cyber Operations*. Springer: 213-229.

Bayuk, J. L., Healey, J. Rohmeyer P., Sachs, M. H., Schmidt J. ve Weiss, J. (2012). *Cyber Security Policy Guidebook*. Wiley Publishing.

Bazeley, P. ve Richards, L. (2000). *The Nvivo Qualitative Project Book*. London: Sage.

BBC. (2017). Çin'den Kuzey Kore ile ABD ve Güney Kore'ye Karşılıklı Çağrı. 02.05.2017 tarihinde: http://www.bbc.com/turkce/haberler-dunya-39202489 adresinden alınmıştır.

Bearne, S., Oliker, O., O'Brien, K. A. ve Rathmell, A. (2005). *National Security Decision-Making Structures and Security Sector Reform*. RAND Europe.

Bell, D. (1973). *The Coming of Post-Industrial Society. A Venture in Social Forecasting*. New York: Basic Books.

Bello, F. (2011). Public Policy Implication on National Security. 08.04.2017 tarihinde: http://nials-nigeria.org/pub/lFATIMABELLO.pdfn adresinden alınmıştır.

Bensghir, T. K. (2002). Türkiye'de Yönetim Bilişim Sistemleri Disiplininin Gelişimi Üzerine Düşünceler. *Amme İdaresi Dergisi*, 35(1): 77-103.

Berg, L. B. (2001). *Qualitative Research Methods for the Social Sciences*. Boston: Allyn and Bacon.

Bertalanffy, L. (1968). General System Theory: Foundations, Development, Applications. NY: George Braziller.

Bıçakçı, S., Ergun, F. D. ve Çelikpala, M. (2016). Türkiye'de Siber Güvenlik. Ülgen, S. ve Kim, G. (ed.), *Türkiye'de Siber Güvenlik ve Nükleer Enerji. Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM)*, İstanbul: İmak Basın Yayın: 28-73.

Birdişli, F. (2011). Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri. *Sosyal Bilimler Enstitüsü Dergisi*, 31(2): 149-169.

Birkland, T.A. (2010). *An Introduction to the Policy Process: Theories, Concepts, and Models of Public Policy Making*. M E Sharpe Inc., NY.

Booth, K. (1991). Security and Emancipation. *Review of International Studies*, 17(4): 313-326.

Booth, K. (2007). *Theory of World Security*. UK: Cambridge University Press.

Borah, C. K. (2015). Cyber war: The Next Threat to National Security and What to do About It? by Richard A. Clarke and Robert K. Knake. *Strategic Analysis*, (39)4: 458-460.

Breene, K. (2016). There Are Now Five Countries Considered to be Cyberwar Superpowers. 27.03.2017 tarihinde: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/ adresinden alınmıştır.

BTK (2010). *Kritik Altyapıların Korunması.* Ankara: Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı.

BTK (2017). Siber Güvenlik Kurumu. 20.09.2017 tarihinde: https://www.btk.gov.tr/tr-TR/Sayfalar/SG-SIBER-GUVENLIK-KURULU adresinden alınmıştır.

BTSEP (2015). *2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı*. Ankara: T.C. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi.

BTİK (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*. Ankara: Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı

Bucala, P. (2015). Iranian Cyber Strategy: A View from the Iranian Military. 30.04.2017 tarihinde: https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military adresinden alınmıştır.

Buchanan, J. M., (1984). Politics without Romance: A Sketch of Positive Public Choice Theory and Its Normative Implications. Ed: J.M. Bunchanan ve R. D. Tollison. *The Theory of PublicChoice II. United States of America*. The University of Michigan Press. 11-23.

BVP (2017). Israel Cybersecurity Landscape. 22.11.2017 tarihinde: https://www.bvp.com/sites/default/files/files/strategy-resource/Israel%20Cybersecurity%20Landscape%20January%202017.pdf adresinden alınmıştır.

Castells, M. (1999). *Critical Education in the New Information Age.* Rowman ve Littlefield.

Castells, M. (2004). *The network society: A Cross-Cultural Perspective.* North Hampton, MA: Edgar Elgar.

Cavelty, M. D. (2014). Breaking the Cyber-security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, 20(3): 701-715.

Chang, E. S., Jain, A. K., Slade, D. M. ve Tsao, S. L. (1999). Managing Cyber Security Vulnerabilities in Large Networks. *Bell Labs Technical Journal*, 252-272.

Chen, T. M. ve Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*, 44(4): 91–93.

CII. (1986). Comprint 85: Computer Aided Technologies. *Computers in Industry*, 7(5): 461-474.

CISCO (2017). Australian Government Cyber Security Review. 17.02.2017 tarihinde: http://www.cisco.com/c/dam/global/en_au/assets/pdf/cisco-cybersecurity-response.pdf adresinden alınmıştır.

Cilluffo, F. J. (2013). *Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure.* Washington D.C.: Homeland Security Policy Institute.

Clark, D., Berson, T., and Lin, H. S., (2014). *At the Nexus of Cybersecurity and Public Policy. Computer Science and Telecommunications Board*. National Research Council, Washington DC: The National Academies Press.

Clarke, R. A. ve Robert, K. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Harper Collins.

Cochran, C. E., Meyer, L. C, Carr, T. R. ve Cayer, N. J. (2009). *American Public Policy: An Introduction*. Wadsworth Cengage Learning, Boston.

Cohen, M. D. and J. G. March, and J. P. Olsen(1972), A Garbage Can Model of Organizational Choice. *Administrative Science Quarterly*, 17, 1—2.

Collier, Z. A., Linkov, I. ve Lambert, J. H. (2013). Four Domains of Cybersecurity: A Risk-Based Systems Approach to Cyber Decisions. *Environment Systems and Decisions*, (33): 469–470.

Collins, S. ve McCombie, S. (2012). Stuxnet: The Emergence of a New Cyber Weapon and Its Implications. *Journal of Policing, Intelligence and Counter Terrorism*, 7(1): 80-91.

Cooper, R. ve G. Burrell, (1988), Modernism, Postmodernism and Organizational Analysis. *Organization Studies*, 9(1): 91-112.

COV (2017). *China Passes New Cybersecurity Law*, 27.07.2017 tarihinde: https://www.cov.com/-/media/files/corporate/publications/2016/11/china_passes_new_cybersecurity_law.pdf adresinden alınmıştır.

CRS (2017). *North Korean Cyber Capabilities: In Brief.* USA: Congressional Research Service.

Çalı, H. H. (2012). Aile İçi Şiddet: Bir Kamu Politikası Analizi. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 16(2): 1-25.

Çelik, A. (1998). Bilgi Toplumu Üzerine Bazı Notlar. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi,* (15)1: 53–59.

Çeliktaş, B. (2016). *Siber Güvenlik Kavramının Gelişimi Ve Türkiye Özelinde Bir Değerlendirme*. Yayınlanmamış Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, Trabzon: Karadeniz Teknik Üniversitesi.

Çevik, H. H. (1998). Kamu Politikaları Analizi Çalışmaları Üzerine Türkiye Açısından Bir Değerlendirme. *Amme İdaresi Dergisi*, 31(2): 103-112.

Çorbacıoğlu, S. (2008). Kamu Politikası Analizinde Görünmez Üniversite: Altı Bilim Adamı Arasındaki Bilişsel ve Sosyal Ağ. *Amme İdaresi Dergi*si, 41(4): 23-48.

Daft, R. L. (2008). *Organization Theory and Design*. USA: South-Western Cengage Learning.

Davis, L. E. (2003). *Globalization's Security Implications*, RAND, 1-8. 05.04.2017 tarihinde: https://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP245.pdf adresinden alınmıştır.

Dicle, İ. A. ve Dicle, Ü. (1969). Sistem Kuramı ve Toplumsal Örgütlere Uygulanışı. *Amme İdaresi Dergisi*, (2): 86-98.

Dissanayake, B. S. (2014). North Korea's National Security Strategy and Its Impact on Development. *Journal of Social Sciences – Sri Lanka*, 214-225.

DOD (2011). *Department of Defense Strategy for Operating in Cyberspace*. Department of Defense, 17.04.2017 tarihinde: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf adresinden alınmıştır.

DOD (2012b). *Military and Security Developments Involving the Democratic People's Republic of Korea*. USA: Department of Defence.

DOD (2013). *DoD Strategy for Defending Networks, Systems, and Data.* Department of Defense, 18.04.2017 tarihinde:

http://iac.dtic.mil/csiac/download/DDNSD_Public_Releasable_11132014.pdf adresinden alınmıştır.

DOD (2015). *The DOD Cyber Strategy*. Washington: The Departmen of Defense, 19.07.2017 tarihinde: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf adresinden alınmıştır.

Doğançay, G. (t.y.). *Kamu Kurumlarında Siber Savunma Konsepti*, 20.03.2017 tarihinde: http://www.tkhk.gov.tr/Dosyalar/ccd23a7e99084fae98b21271a8a5e223.pdf adresinden alınmıştır.

Doyle, R. B. (2007). " The U.S. National Security Strategy: Policy, Process, Problems", *Public Administration Review*, 624-629.

DPT (1963). *1. Kalkınma Planı*. Ankara: Devlet Planlama Teşkilatı.

DPT (1968). *2. Kalkınma Planı*. Ankara: Devlet Planlama Teşkilatı.

DPT (1973). *3. Kalkınma Planı*. Ankara: Devlet Planlama Teşkilatı.

DPT (1979). *4. Kalkınma Planı*. Ankara: Devlet Planlama Teşkilatı.

DPT (1985). *5. Kalkınma Planı*. Ankara: Devlet Planlama Teşkilatı.

DPT (1990). *6. Kalkınma Planı*. Ankara: Devlet Planlama Teşkilatı.

DPT (1996). *7. Kalkınma Planı*. Ankara: Devlet Planlama Teşkilatı.

DPT (2001). *8. Kalkınma Planı*. Ankara: Devlet Planlama Teşkilatı.

DPT (2006). *Bilgi Toplumu Stratejisi.* Ankara: Devlet Planlama Teşkilatı.

DPT (2007). *9. Kalkınma Planı.* Ankara: Devlet Planlama Teşkilatı.

Dror, Y. (1964). Muddling Through-"Science" or Inertia?. *Public Administration Review*, 24(3): 153-157.

Dror, Y. (1967). Policy Analysts: A New Professional Role in Government Service. *Public Administration Review*, (27): 197-203.

Dror, Y. (1968). *Public Policymaking Reexamined.* Pennsylvania: Chandler Publishing.

DSB (2017). *Task Force on Cyber Deterrence*. Washington D.C.: Department of Defense, Defense Science Board.

DTCC (2014). *Cyber Risk-A Global Systemic Threat*. DTCC. 25.03.2017 tarihinde: http://dtcc.com/~/media/Files/Downloads/issues/risk/Systemic_Risk_Summary_Report.ashx adresinden alınmıştır.

Dye, T. R. (1972). *Understanding Public Policy*. New Jersey: Prentice.

Easton, D. (1957). An Approach to the Analysis of Political Systems. *World Politics*, 9(3): 383-400.

Easton, D. (1965). *A Framework for Political Analysis*. London: Prentice Hall Int..

EGM (2016). *Emniyet Genel Müdürlüğü Faaliyet Raporu*. Ankara: T.C. İç İşleri Bakanlığı.

EHK (2008). *Elektronik Haberleşme Kanunu*. T.C. Resmi Gazete.

Eisenstadt, M. (2016). Iran's Lengthening Cyber Shadow. *The Washington Institute for Near East Policy*, 34: 1-20.

Enserink, B., Joop, F. M. K. ve Mayer, I. S. (2013). A Policy Sciences View on Policy Analysis, iç. W. A. H. ve Walker, W. E. (der). *Public Policy Analysis*. Thissen, Springer.pp.11-40.

Erat, V. ve Kaçer, F. (2014). Siyasal Yapım Sürecinde Müzakereci Yaklaşımlar. *Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 1(4): 57-75.

Ercan, M. (2015). *Kritik Altyapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri.* Yayınlanmamış Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, Gebze: Gebze Teknik Üniversitesi.

Erickson, J. (2008). *Hacking: The Art of Exploitation*. San Francisco: No Starch Press.

Erol, S. E. (2016). *Siber Güvenlik Farkındalığı İçin Yetenek Tabanlı Dinamik Model.* Yayınlanmamış Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi, Fen Bilimleri Enstitüsü.

ETK (2004). *Electronic Commerce Law of the Islamic Republic of Iran*. 01.05.2017 tarihinde: http://en.iccima.ir/images/stories/DATA/LAW/Tejarat%20Electronic.pdf adresinden alınmıştır.

Etzioni, A. (1967). Mixed-Scanning: A 'Third' Approach to Decision-Making. *Public Administration Review*, 27(5): 385-392.

EUC (2012). *Special Eurobarometer 390: Cyber Security*. European Comission, 21.03.2017 tarihinde:

http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf adresinden alınmıştır.

Eyestone, R. (1971). *The Threads of Public Policy: A study in Policy Leadership*, Indianapolis.

Farwell, J. P. ve Rohozinski, R. (2011). Stuxnet and the Future of Cyber War, Survival. *Global Politics and Strategy*, 53(1): 23-40.

Fei, G. (2011). China's Cybersecurity Challenges and Foreign Policy. *Georgetown Journal of International Affairs*, 2011: 185-190.

Fidler, D. P. (2011). Was Stuxnet an Act of War? Decoding a Cyberattack*. IEEE Security and Privacy*, 9(4): 56–59.

Filiz, S. (2013). *Siber Güvenlikte Biyometrik Sistemler Ve Yüz Tanıma*. Yayınlanmamış Yüksek Lisans Tezi, Bilişim Enstitüsü, Ankara: Gazi Üniversitesi.

Fischer, F., Miller, G. J. ve Sidney, M. S. (2007). *Handbook of Public Policy Analysis*. CRC Press.

Flanagan, S. J., Frost, E. L. ve Kugler, R. L. (2001). *Challenges of the Global Century Report of the Project on Globalization and National Security.* Washington: Institute for National Strategic Studies National Defense University.

Forbes. (2017). 6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry. 22.11.2017 tarhinde: https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-

a-cybersecurity-powerhouse-leading-the-82-billion-industry/#73536b7c420a adresinden alınmıştır.

Fovino, I. N., Masera, M. ve Cian, A. D. (2009). Integrating Cyber Attacks within Fault Trees*. Reliability Engineering and System Safety*, (94): 1394–1402.

GCHQ (2012). *10 Steps to Cyber Security*. UK: Crown.

Geers, K. (2010). The Challenge of Cyber Attack Deterrence. *Computer Law ve Security Review,* (26): 298-303.

Genge, B., Haller, P. ve Kiss, I. (2015). Cyber-Security-Aware Network Design of Industrial Control Systems. *IEEE Systems Journal*, 1-12.

Genge, B., Siaterlis, C., Fovino, I. N. ve Masera, M. (2012). A Cyber-Physical Experimentation Environment for the Security Analysis of Networked Industrial Control Systems. *Computers and Electrical Engineering*, (38): 1146–1161.

Gibney, A. ve Shmuger, M. (2016). *Zero Days (Stuxnet)*. [Film]. Magnolia Pictures.

Gierow, H. J. (2015). Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses. Mercator Institute for China Studies, (22): 1-10.

Giles, K. (2012). *Russia's Public Stance on Cyberspace Issues*. 4th International Conference on Cyber Conflict, Tailinn: NATO CCD COE Publications.

Giles, K. (2013). *Internet Use and Cyber Security in Russia*. Russian Analytical Digest No: 134, 24.04.2017 tarihinde: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/RAD-134-2-4.pdf adresinden alınmıştır.

Gohlert, E. W. (1974). National Security Policy Formation in Comparative Perspective. *Policy Studies Journal*, 3(2): 174-177.

Goodin, R. E., Rein, M. ve Moran, M. (2006). The Public and Its Policies. iç. Moran, M., Rein, M. ve Goodin, R. (der). *The Oxford Handbook of Public Policy*. Oxford University Press: 3-35.

Göçoğlu, V. (2014). *Postmodernizm Yansımalarının Çeşitli Alanlar Üzerinden Incelenmesi*. 17.12.2016 tarihinde: https://www.academia.edu/10411248/Postmodernizmin_%C3%A7e%C5%9Fitli_alanlardaki_yans%C4%B1malar%C4%B1_%C3%BCzerine_bir_deneme._Volkan_G%C3%B6%C3%A7o%C4%9Flu adresinden alınmıştır.

Göçoğlu, V. (2014). *Kamu Politikası ve Sosyal Medya İlişkisi*. Yayınlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü.

Gül, H. (2015). Kamu Politikası Analizi, Yöntemleri ve Teknikleri. *Yasama Dergisi*, (29): 5-31.

Güngör, M. (2015). *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma.* Uzmanlık Tezi. Ankara: Bilgi Toplumu Dairesi Başkanlığı.

Güntay, V. (2016). *Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Kuramı (Micro-CAT)*. Yayınlanmamış Doktora Tezi, Trabzon: Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü.

Gürakar, H. T. (t.y.). *Bir Toplumsal Hareketin Anatomisi: İran Yeşil Hareketi*. 30.04.2017 tarihinde: https://www.academia.edu/7396178/B%C4%B0R_TOPLUMSAL_HAREKET%C4%B0N_ANATOM%C4%B0S%C4%B0_%C4%B0RAN_YE%C5%9E%C4%B0L_HAREKET%C4%B0 adresinden alınmıştır.

Gürbüz, S. ve Sahin, F. (2014). *Sosyal Bilimlerde Araştırma Yöntemleri*. Ankara: Seçkin Yayıncılık.

Güriz, A. (2011). *Feminizm Postmodernizm ve Hukuk*. Phoenix Yayınları.

Hagestad, W. (2013). *Comparative Study: Iran, Russia ve PRC Cyber War*. RSA Confrerence.

Hampton, G. (2009). Narrative Policy Analysis and the Integration of Public Involvement in Decision Making. *Policy Sci*, (42): 227-242.

Hare, F. B. (2009). Private Sector Contributions to National Cyber Security: A Preliminary Analysis. *Journal of Homeland Security and Emergency Management*, 6(1): 1-20.

Harold, S. W., Libicki, M. C. ve Cevallos, A. S. (2016). *Getting to Yes with China in Cyberspace.* CA: RAND Corporation.

Heclo, H. (1978). Issue Networks and the Executive Establishment. iç. A. King (ed.). *The New American Political System*. Washington: AEI Press: 87–124.

Herbolzheimer, C. (2016). *Go to Cyber Extremes: What to do When Digitalization Goes Wrong*. iç. MMC Cyber Handbook: 13-14, 25.02.2017 tarihinde: https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/MMC-Cyber-Handbook_2016-web-final.pdf adresinden alınmıştır.

Heymann, P. B. (2008). *Living The Policy Process*. Oxford University Press.

Hill, J. M. (2005). *The Public Policy Process*. Pearson Longman.

Hill, M. ve Hupe, P. (2009). *Implementing Public Policy*. Sage Publication.

Hill, M. (1997).*The Policy Process: A Reader*. London: PrenticeHall.

Hoppe, R. (1999). Policy Analysis, Science And Politics: From 'Speaking Truth To Power' To 'Making Sense Together. *Science and Public Policy*, 26(3), 201-210.

Hoşsucu, A. G. (2015). *Siber Güvenlik Alanında Yapısal Ve Düz Metinden Anlamsal Konsept Çıkarımı*. Yayınlanmamış Yüksek Lisans Tezi, Enformatik Enstitüsü, Ankara: Orta Doğu Teknik Üniversitesi.

Housen-Couriel, D. (2017). *National Cyber Security Organisation: ISRAEL*. Tallinn: NATO Cooperative Cyber Defence of Excellence.

HP (2014). *Profiling an enigma: The mystery of North Korea's Cyber Threat Landscape*. HP Security Briefing Episode 16.

Huang, R. (2002). On the Nature of Public Policy. *Chinese Public Administration Review*, 1(3-4): 275-282.

Immergut, M. E. (2011). Democratic Theory and Policy Analysis: Four Models of "Policy, Politics and Choice", Zeitschrift für Public Policy. *Recht und Management Hef*, (1): 69-86.

ISS (2017). *Basic Principles for Sate Policy of the Russian Federation in the Field of International Information Security to 2020*. 23.04.2017 tarihinde: https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf adresinden alınmıştır.

ITU (2015). *Iran Country Syber Security Profile*. 22.08.2017 tarihinde: https://www.itu.int/net4/itu-d/.../CountryProfileReport.aspx? adresinden alınmıştır.

Jann, W. ve Wegrich, K. (2007). Theories of the Public Cycle. iç. Fischer, F., Miller, G. J. and Sidney, M. S*. Handbook of Public Policy Analysis: Theory, Politics, and Methods*. CRC Press.

Jenkins, R. (1997). *Rethinking Ethnicity: Arguments and Explorations*. SAGE Publications.

Jenkins, R. (2013). Is Stuxnet Physical? Does It Matter?. *Journal of Military Ethics*, 12(1): 68-79.

Jenkins, W. I. (1978). *Policy Analysis: A Political And Organisational Perspective*. Martin Robertson, London.

Jones, K. S. (1991). The Role of Artificial Intelligence in Information Retrieval. *Journal of the American Society For Information Science*, 42(8): 558-585.

Jones, O. (1977). *An Introduction to the Study of Public Policy*. Duxbury Press.

Kademi, A. M. (2014). *Milli Siber Güvenlik Stratejisi: Nijerya İçin Bir Model*. Yayınlanmamış Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, İzmir: Yaşar Üniversitesi.

Kademi, A. M. (2014). *Milli Siber Güvenlik Stratejisi: Nijerya İçin Bir Model*. Yayınlanmamış Yüksek Lisans Tezi, İzmir: Yaşar Üniversitesi, Fen Bilimleri Enstitüsü.

Kara, M. (2013). *Siber Saldırılar-Siber Savaşlar ve Etkileri*. Yayınlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü.

Karabacak, B., Yıldırım, S. Ö. ve Baykal, N. (2016). A Vulnerability-Driven Cyber Security Maturity Model for Measuring National Critical Infrastructure

Protection Preparedness. *International Journal of Critical Infrastructure Protection*, (15): 47-59.

Karnouskos, S. (2013). *Stuxnet Worm Impact on Industrial Cyber-Physical System Security*. 12.04.2017 tarihinde: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.259.7495&rep=rep1&type=pdf adresinden alınmıştır.

Kasapoğlu, C. (2017). *Siber Güvenlik: Beşinci Boyutu Anlamak*. İstanbul: EDAM Siber Politikalar Kagitlari Serisi.

Kay, S. (2004). Globalization, Power, and Security. *Security Dialogue*, 35(1): 9–25.

KB (2013). *10. Kalkınma Planı.* Ankara: T.C. Kalkınma Bakanlığı.

KB (2015). *Bilgi Toplumu Stratejisi ve Eylem Planı*. Ankara: T.C. Kalkınma Bakanlığı.

Kenney, M. (2015). Cyber-Terrorism in a Post-Stuxnet World. *Orbis*, 59(1): 111-128.

Kıratlı, O. S. (2016). Avrupa Dış İlişkiler ve Güvenlik Politikası ve Üç Büyükler: Almanya, Fransa ve İngiltere. *Akademik İncelemeler Dergisi*, 11(1): 207-224.

Kingdon, J. W. (2014). *Agendas, Alternatives, and Public Policies*. Pearson Education Limited.

Kirshner, J. (2006). *Globalization and National Security*. NY: Routledge.

Klimburg, A. (2012). *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE Publication.

KMPG (2016). *Cyber Security in China. Management Consulting*. Cihna: KMPG.

KMPG (2016). *Cyber Security: Designin a Government-Bussiness Partnership in Australia*. 17.03.2017 tarihinde: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/cyber-security-business-government-partnership-2016.pdf adresinden alınmıştır.

Kobara, K. (2016). Cyber Physical Security for Industrial Control Systems and Iot. *IEICE Transactions on Information and Systems*, 99(4): 787-795.

Koçak A. ve Arun, Ö. (2006). İçerik Analizi Çalışmalarında Yöntem Sorunu. *Selçuk İletişim*, 4(3): 21-28**.**

Koik, Y. Ö. (2015). *Uluslararası İlişkilerde Siber Güvenlik Algısı Ve Ulus Devletin Değişen Stratejisi*. Yayınlanmamış Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, Adana: Çukuroava Üniversitesi.

Korff, D. (t.y.). *Cyber Security Definitions*. UK: Associate of the Oxford Martin School of the University of Oxford's Global Cybersecurity Capacity Centre.

Köseoğlu, Ö. (2013). Kamu Politikası Sürecinde Karar Verme Modelleri. iç. (der) Yıldız, M., Sobacı, M. Z. *Kamu Politikası Kuram ve Uygulama*. Ankara: Adres Yayınları: 244-265.

Kritzinger, E. ve Solms, S. H. (2010). Cyber Security for Home Users: A New Way of Protection Through Awareness Enforcemen. *Computers & Security*, (29): 840-847.

Kshetri, N. (2016). *The Quest to Cyber Superiority*. Switzerland: Springer.

Kurnaz, İ. (2016). *21. Yüzyılda Ortodoks Güvenlik Paradigmasının Aşınımı: Uluslararası İlişkilerde Siber Güvenlik*. Yayınlanmamış Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, Konya: Selçuk Üniversitesi.

Kushner, D. (2013). *The Real Story of Stuxnet*. IEEE Spectrum. 11.04.2017 tarihinde: http://spectrum.ieee.org/telecom/security/the-realstory-of-stuxnet adresinden alınmıştır.

Küçükaydın, D. (2016). *Amerika Birleşik Devletleri'nin Ulusal Ve Uluslararası Siber Güvenlik Stratejileri: Güvenlikleştirme Hareketi*. Yayınlanmamış Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, Ankara: Orta Doğu Teknik Üniversitesi.

Küçüksillle, E. U., Genç, S. ve Karabulut Y. E. (2013). *Dünyada Siber Güvenlik Stratejileri ve Bir Siber Güvenlik Stratejisinin Oluşumu.* Elazığ: 1st. International Symposium on Digital Forensic and Security.

Lakeman, R. (2008). Qualitative Data Analysis with NVivo. *Journal of Psychiatric and Mental Health Nursing*, 15(10): 868-868.

Lantis, S. J. (2002). Strategic Culture and National Security Policy. *International Studies Review*, 4(3): 87-113.

Larkin, P.J. 2012. John Kingdon’s “Three Streams” Theory and the Antiterrorism and Effective Death Penalty Act of 1996. *Journal of Law and Politics*, 28 (25): 25-50.

Lasswell, H. (1951). The Immediate Future of Research Policy and Method in Political Science. *American Political Science Review*, (45): 133–142.

Lasswell, H. D. (1956). *The Decision Process*. Md.: Bureau of Governmental Research, University of Maryland.

Lasswell, H. D. (1971). *A Pre-View of Policy Sciences*. New York: American Elseiver Publication.

Lax, S. (2001). *Access Denied in the Information Age*. New York: Palgrave Macmillan.

Lehman, J. ve Willett, T. D. (1986). National Security and Industrial Policy: The Need For a Public Choice Perspective*. Contemporary Policy Issues*, (7): 36-47.

Lejano, R. P. (2013). Postpositivism And The Policy Process. iç. Jr, Araral, E., Fritzen, S., Howlett, M., Ramesh, M. ve Wu, X. (der). *Routledge Handbook of Public Policy*. Routledge, pp.98-112.

Leoveanu, A. C. (2013). Rationalist Model in Public Decision Making. *Journal of Public Administration, Finance and Law*, (4): 43-54.

Lewis, J. A. (2014). *Cybersecurity and Stability in the Gulf*. Gulf Analysis Paper. Center for Strategic & Inernational Studies.

Lieberthal, K. ve Singer, P. W. (2012). *Cybersecurity and U.S*. - China Relations. Brookings.

Lin, H. (2012). Why Computer Scientists Should Care About Cyber Conflict and U.S. National Security Policy. *Communications of the ACM*, 55(6): 41-43.

Lindblom, C. (1959). The Science of "Muddling Through". *Public Administration Review*, 19(2): 79-88.

Lindh, M. ve Nolin, J. (2016). Information We Collect: Surveillance and Privacy in the Implementation of Google Apps for Education. *European Educational Research Journal*, : 1-20.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3): 365-404.

Lindsay, J. R. (2015). The Impact of China on Cybersecurity. *International Security*, 39(3): 7-47.

Lipsky, M. (1980). *Street-Level Bureaucracy: Dilemmas of the Individual in Public Services*. New York: Russell Sage.

Lowi, T. J. (1972). Four Systems of Policy, Politics, and Choice. *Public Administration Review*, 32(4): 298-310.

Lu, M. (2014). *Types of Cyber Attacks*. Trustworthy Cyber Infrastructure For The Power Grid. 18.03.2017 tarihinde: https://tcipg.org/sites/default/files/rgroup/tcipg-reading-group-fall_2014_09-12.pdf adresinden alınmıştır.

Lynne, J. (2006). Software and Method: Reflections on Teaching and Using QSR NVivo in Doctoral Research. *International Journal of Social Research Methodology*, 9(5): 379-391.

Lyotard, J. F. (1994).*The Postmodern Condition: A Report on Knowledge*. Manchester: Manchester University Press.

Mansourov, A. (2014). North Korea's Cyber Warfare and Challenges for the U.S. - ROK Alliance. *Korea Economic Institute of America, Academic Paper Series*: 1-17.

Matrosov, A., Rodionov, E., Harley, D. ve Malcho, J. (2010). *Stuxnet Under the Microscope*. eset, Tech. Rep., [Online]. 14.11.2016 tarihinde: http://www.eset.com/resources/white-papers/Stuxnet Under the Microscope.pdf adresinden alınmıştır.

Medvedev, S. A. (2015). *Offense-Defense Theory Analysis of Russian Cyber Capability*. Masters' Thesis, California: Naval Postgraduate School.

Morçöl, G. (2013). Karmaşıklık Kuramı ve Kamu Politikaları. iç. (der) Yıldız, M., Sobacı, M. Z. *Kamu Politikası Kuram ve Uygulama*. Ankara: Adres Yayınları: 88-113.

Mueller, P., ve Yadegari, B. (2012). *The Stuxnet Worm. University of Arizona, Department of Computer Science*. 22.02.2017 tarihinde: http://www. cs. arizona. edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report. Pdf adresinden alınmıştır.

NATO (2016). *Siber Saldırıların Tarihçesi*. 23.11.2016 tarihinde: http://www.nato.int/docu/review/2013/Cyber/timeline/TR/index.htm adresinden alınmıştır.

NS (2011). *Thanks, Stuxnet*. NewScientist.

O'Shea, K. (2003). *Cyber Attack Investigative Tools and Technologies*. in HTCIA, Institue for Security Technology Studies, Hanover, NH: Dartmouth College.

OAG (2017). *Cyber Exploitation Fact Sheet*. USA: State of California Department of Justice. 20.03.2017 tarihinde: https://oag.ca.gov/sites/all/files/agweb/pdfs/ce/cyber-exploitation-fact-sheet.pdf adresinden alınmıştır.

Orhan, G. (2013). Kamu Politikasına Yorumlamacı Yaklaşımlar. iç. (der) Yıldız, M., Sobacı, M. Z. *Kamu Politikası Kuram ve Uygulama*. Ankara: Adres Yayınları: 66-87.

Öğüt, H., Raghunathan, S. ve Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, 31(3): 497-512.

PA (2016). *Uluslararasi Kitlesel Göçler ve Türkiye'deki Suriyeliler Sonuç Raporu*. Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü Göç ve Sinir Güvenligi Arastirma Merkezi (GÖÇMER).

Park, J. M. (2015). *Finding Effecive Responses Against Cyber Attacks for Divided Nations*. Masters' Thesis, CA: Naval Postgraduate School.

Pernik, P. (2014). *Improving Cyber Security: NATO and the EU*. 09.0.2017 tarihinde: https://www.icds.ee/fileadmin/media/icds.ee/failid/Piret_Pernik_-_Improving_Cyber_Security.pdf adresinden alınmıştır.

Peters, B. G. (2005). The Problem of Policy Problems. *Journal of Comparative Policy Analysis: Research and Practice*, 7(4): 349-370.

Pfleeger, S. L. ve Caputo, D. D. (2012). Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Computers & Security*, (31): 597-611.

Politico. (2017). *German Cybersecurity Chief: Army Attacked Over 284,000 Times This Year*. 26.11.2017 tarihinde: http://www.politico.eu/article/german-cybersecurity-chief-army-attacked-over-284000-times-this-year/ adresinden alınmıştır.

Raska, M. (2015). *Confronting CyberSecurity Challenges: Israel's Evolving Cyber Defence Strategy*. Singapore: RSIS.

Raud, M. (2016). *China and Cyber: Attitudes, Strategies, Organisation*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Redd, S. B. ve Mintz, A. (2013). Policy Perspectives on National Security and Foreign Policy Decision Making. *Policy Studies Journal*, 41(S1): 11-37

Report. (2002). *Challenges For The Chemical Sciences In The 21st Century National Security & Homeland Defense*. Washington: The National Academies Press.

RFBGD. (2000). *Information Security Doctrine of the Russian Federation*. 22.04.2017 tarihinde: https://toinformistoinfluence.com/2016/12/19/information-security-doctrine-of-the-russian-federation-6-december-2016/ adresinden alınmıştır.

RNS (2015). *Russian National Security Strategy*. December 2015 – Full-text Translation. 21.04.2017 tarihinde: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf adresinden alınmıştır.

RN2444. (2015). Resolution: Advancing the National Preparedness for Cyber Security. 22.11.2017 tarihinde: https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202444%20-%20Advancing%20the%20National%20Preparedness%20for%20Cyber%20Security.pdf adresinden alınmıştır.

RN3611. (2011). Advancing National Cyberspace Capabilities. 22.11.2017 tarisinde: http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf adresinden alınmıştır.

Rochefort, D. A. ve Cobb, R. W. (1994). *The Politics of Problem Definition*. Lawrence, KS: University Press of Kansas.

Rollins, J. W. (2015). *U.S.–China Cyber Agreement*. 28.04.2017 tarihinde: https://fas.org/sgp/crs/row/IN10376.pdf adresinden alınmıştır.

RSG (t.y.). *Concept of the Russian Cyber Security Strategy*. 21.04.2017 tarihinde: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf adresinden alınmıştır.

Sabatier, P. (1991). Toward Better Theories of the Policy Process. *Political Science and Politics*, (24): 56-147.

Sabatier, P. A. (1987). Knowledge, Policy-Oriented Learning, and Policy Change: An Advocacy Coalition Framework. *Science Communication*, 8(4): 649-697.

Sadioğlu, U. ve Yıldız, M. (2007). Kamu Yönetimi ile Bilgi ve İletişim Teknolojileri: Bir Bibliyografik Analiz. *H.Ü. İktisadi ve Idari Bilimler Fakültesi Dergisi*, 25(2): 325-359.

Sallan, S. ve Boybeyi, S. (1994). Postmodernizm-Modernizm İkilemi. Araştırma. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Felsefe Bölümü Dergisi*, (15): 313-323.

Sanalp, S. (2016). Çeşitli Ülkelerde USOM ve SOME Yapılandırılması ve Türkiye Model Önerisi. Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Bilgi Üniversitesi.

Sancak, K. (2003). Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenliğin Dönüşümü. *Sosyal Bilimler Dergisi*, (6): 123-143.

Sarı, O. (2013). *Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik Ve Bilişim Sistemine Yönelik Suçlar*. Yayınlanmamış Yüksek Lisans Tezi, Stratejik Araştırmalar Enstitüsü, Ankara: Harp Akademileri Komutanlığı.

Schockenhoff, A. (t.y.). *A Security Strategy for Germany.* Berlin: ISPSW Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung.

Semiz, Ö. (2009). *Bir Kamu Politikası Analizi: Türkiye'de Korsanla Mücadele Odaklı Fikri Haklar Politikası.* Ankara Barosu Dergisi. 20.09.2016 tarihinde: http://www.ankarabarosu.org.tr/siteler/ankarabarosu/frmmakale/2009-4/1.pdf adresinden alınmıştır.

Sepulveda, P., Sanchez, F. ve Gomez, M. C. (2012). Content Analysis Research Method With Nvivo-6 Software In A Phd Thesis: An Approach To The Long-Term Psychological Effects On Chilean Ex-Prisoners Survivors Of Experiences Of Torture And Imprisonment. *Quality & Quantity*, 46(1): 379-390.

SGR (2012). *Siber Güvenlik Raporu*. Istanbul: Istanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü.

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance?. *Business Horizons*, (55): 349—356.

Shakarian, P., Shakarian, J. ve Ruef, A. (2013). *Introduction to Cyber-Warfare: A Multidisciplinary Approach.* Maryland Heights: Syngress Publishing.

Simmons, A. D. (2007). *Globalization and its Effect on National Security*. Forum on Public Policy. 04.01.2017 tarihinde: http://forumonpublicpolicy.com/archivespring07/simmons.pdf adresinden alınmıştır.

Simon, H. A. (1972). Theories of Bounded Rationality. *Decision and Organization*, 1(1): 161-176.

Simon, H. A. (1997). *Models of Bounded Rationality: Empirically Grounded Economic Reason*. Massachusetts: MIT Press.

Simon, H. (1957). *"A Behavioral Model of Rational Choice" in Models of Man, Social and Rational: Mathematical Essays on Rational Human Behavior in a Social Setting.* New York: Wiley.

Simonsen, J. (1994). *Herbert A. Simon: Administrative Behavior, How Organizations Can Be Understood in Terms of Decision Processes.* Computer Science. Roskilde University. 01.03.2017 tarihinde: http://jespersimonsen.dk/Downloads/Simon-introduction.pdf adresinden alınmıştır.

Smith, K. B. ve Larimer, C. W. (2009). *The Public Policy Theory Primer*. Boulder: Westview Press.

Snape, D. ve Spencer, L. (2003). The Foundations of Qualitative Research. in Ritchie, J. ve Lewis, J. (ed.). *Qualitative Research Practice*. SAGE Publications.

Spade, C. J. M. (2012). *Information As Power: China's Cyber Power and American's National Security.* U.S. Army War College.

Sputnik. (2017). *Çinli Yetkililerden Kuzey Kore'ye: Saldırılara Karşı Savunmak Zorunda Değiliz.* 02.05.2017 tarihinde: https://tr.sputniknews.com/asya/201704151028080224-cin-yetkililer-kuzey-kore-saldirilara-karsi-savunmak-zorunda-degiliz/ adresinden alınmıştır.

Stitilis, D., Pakutinskas, P. ve Malinauskaite, I. (2016). EU and NATO Cybersecurity Strategies and National Cyber Security Strategies: A Comparative Analysis. *Security Journal*.

Stoddart, K. (2016). UK Cyber Security and Critical National Infrastructure Protection. *International Affairs*, 92(5): 1079–1105.

Strauss, A. L. ve Corbin, J. M. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Sage Publications.

SÜ (t.y.). *Beşinci Bölüm: Kamu Politikası ve Gündem Oluşturma*. Sakarya Üniversitesi Ders İçeriği Yayını. 07.02.2017 tarihinde: http://content.lms.sabis.sakarya.edu.tr/Uploads/50656/33504/6._hafta_g%C3%BCndem_ders_notu.pdf adresinden alınmıştır.

Sutton, R. (1999). *The Policy Process: An Overview.* Overseas Development Institute,Chameleon Press Ltd, London.

Swaine, M. D. (2013). Chinese Views on Cybersecurity in Foreign Relations. *China Leadership Monitor*: 1-27.

Şahin, A. E. (2001). Eğitim Araştırmalarında Delphi Tekniğinin Kullanımı. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, (2): 215- 220.

Şahin, Y. (2017). *Brexit ve Trump Çağında AB Güvenlik ve Savunma Politikaları.* Istanbul: Iktisadi Kalkinma Vakfi.

Tabansky, L. ve Israel, I. B. (2015). *Cyber Security in Israel*. UK: Springer.

Tasçı, G., Altun, A. ve Soran, H. (2008). Biyoloji Öğretmen Adaylarının Öğrenme Stratejilerinin Belirlenmesi Üzerine Nitel Bir Çalışma. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, (35): 284-296.

Tatar, T. (2011). Sömürgecilik Ve Kızıl – Kara Katliam. *Sosyoloji Konferansları Dergisi (Istanbul Journal of Sociological Studies)*, (44): 195-220.

TBD (2015). *Siber Güvenlik ve kritik Altyapi Güvenligi Çalisma Grubu Nihai Raporu*. Ankara: Türkiye Bilisim Dernegi.

TBMM (2002). *Gül Hükümeti Programı.* 22.10.2017 tarihinde: https://www.tbmm.gov.tr/hukumetler/HP58.htm adresinden alınmıştır.

TBMM (2003). *I. Erdoğan Hükümeti Programı.* 22.10.2017 tarihinde: https://www.tbmm.gov.tr/hukumetler/HP59.htm adresinden alınmıştır.

TBMM (2007). *II. Erdoğan Hükümeti Programı.* 24.10.2017 tarihinde: https://www.tbmm.gov.tr/hukumetler/HP60.htm adresinden alınmıştır.

TBMM (2011). *III. Erdoğan Hükümeti Programı*. 24.10.2017 tarihinde: https://www.tbmm.gov.tr/hukumetler/HP61.htm adresinden alınmıştır.

TBMM (2012). *Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler ile İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyonu Raporu*. Ankara: TBMM.

TBMM (t.y). *Bilgi Güvenliği ve Bilişim Suçları Üçüncü Kısım*. Ankara: TBMM.

Techinasia. (2017). *China Now Has 731 Million Internet Users, 95% Access From Their Phones.* 27.04.2017 tarihinde https://www.techinasia.com/china-731-million-internet-users-end-2016 adresinden alınmıştır.

Tirrell, W. K. (2012). *United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment.* B.A. Thesis, Washington D.C: The George Washington University.

Tosun, A. (2015). *İnsan Zafiyetlerini İstismar Ederek Yapılan Sosyal Mühendislik, Saldırılarının Siber Güvenlik İle İlişkilendirilmesi: Türkiye Örneği.* Yayınlanmamış Yüksek Lisans Tezi, Enformatik Enstitüsü, Ankara: Orta Doğu Teknik Üniversitesi.

Tuluk, A. ve Seferoglu, S. (2016). *Ulusal ve Uluslararasi BIlgi Güvenligi Politikalarinin Analizi Üzerine Karsilastirmali Bir Inceleme.* KKTC: Uluslararasi Egitim Teknolojisinde Yeni Egilimler Konferansi.

Türker, M. (2015). *Finansal Güvenlik Sistemi Erken Uyarı Modeli: Türk Bankacılık Sektörü Üzerine Bir Uygulama ve Politika Önerileri.* İstanbul: Türkiye Bankalar Birliği, Yayın No: 313.

UBGKT (2002). *Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı. 18.05.2017 tarihinde:* http://www.kgm.adalet.gov.tr/Tasariasamalari/Uzerindecals/uzrencal.htm adresinden alınmıştır.

UBGMD (2017). *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi.* 17.07.2017 tarihinde: http://dergipark.gov.tr/ubgmd adresinden alınmıştır.

UBMGD (2017). *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*. 10.10.2017 tarihinde: http://dergipark.ulakbim.gov.tr/bgmd/ adresinden alınmıştır.

UDHB (2012). *Ulusal Siber Güvenlik Stratejisi.* Ankara: Bilgi Güvenliği Derneği.

UDHB (2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.* Ankara: T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı.

UDHB (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi.* Ankara: T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı.

Ulsch, M. (2014). *Cyber Threat! How to Manage the Growing Risk of Cyber Attacks*. NJ: Wiley.

USGÇYYKİK (2012). *Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar.* Ankara: T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı.

USOM (2017). *USOM Hakkında.* 19.10.2017 tarihinde: https://www.usom.gov.tr/hakkimizda.html adresinden alınmıştır.

Usta, A. (2013). Kamu Politikaları Analizine Kuramsal Bir Bakış. *Yasama Dergisi,* (24): 78-102.

Webster, F. (2014). *Theories of the Information Society.* Routledge.

WH (2003). *The National Strategy to Secure Cyberspace*. Washington: The White House. 17.04.2017 tarihinde: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf adresinden alınmıştır.

WHOPS (2014). *Fact Sheet: U.S.-EU Cyber Cooperation.* The White House Office of the Press Secretary. 17.04.2017 tarihinde: https://uk.usembassy.gov/fact-sheet-u-s-eu-cyber-cooperation/ adresinden alınmıştır.

WHOPS (2015). *Fact Sheet: U.S.-United Kingdom Cybersecurity Cooperation.* The White House Office of the Press Secretary. 17.04.2017 tarihinde: https://uk.usembassy.gov/fact-sheet-u-s-united-kingdom-cybersecurity-cooperation/ adresinden alınmıştır.

Whyte, C. (2016). Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea. *Comparative Strategy*, 35(2): 93-102.

Wiener, N. (1948). *Cybernetics, or Control and Communication in the Animal and the Machine*. Cambridge: MIT Press.

Wildavsky, A. (1979). *The Art and Craft of Policy Analysis.* UK: Palgrave Macmillan.

Wildavsky, A. (1980). *The Art and Craft of Policy Analysis*. Macmillian Press Ltd.

Wilson, J. Q. (1980). *The Politics of Regulation.* USA: Basic Books.

WP (2016). *White Paper on German Security Policy and The Future of the Bundeswehr.* Germany: The Federal Government.

Yadak, A. (2014). İsrail Güvenlik Politikası Ve Güvenlik Duvarının Filistin Halkına Etkileri. *21. Yüzyılda Eğitim ve Toplum*, 3(9): 163-175.

Yıldız, M. ve Sobacı, M. Z. (2013). Kamu Politikası ve Kamu Politikası Analizi. iç. Yıldız, M. ve Sobacı, M. Z. (der). *Kamu Politikası: Kuram ve Uygulama*. Ankara: Adres Yayınları: 16-42.

Yıldız, M. (2011). *Kamu Politikası.* Türkiye Bilimler Akademisi Açık Ders Malzemeleri. 29.12.2016 tarihinde: http://www.acikders.org.tr/course/view.php?id=66 adresinden alınmıştır.

Yılmaz, S. ve Sağıroğlu, Ş. (2013). Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı. Ankara: ISC: 323-331.

Yoon, S. ve Lim, K. (2013). North Korea's National Security Strategy and Its Implications for South Korea. *Asian Journal of Social Sciences & Humanities*, 2(2): 144-155.

Young, O. R. (2006). Choosing Governance Systems: A Plea For Comparative Research. in Moran, M., Rein, M. ve Goodin, R. E. (der). *The Oxford Handbook of Public Policy*. Oxford University Press: 844-857.

Yue, O. (2003). Cyber Security. *Technology in Society*, (25): 565–569.

Zerin, D. (2016). *Türkiye'de İnternet'in Yönetimi: Bir İktidar Stratejisi Olarak Siber Güvenlik.* Yayınlanmamış Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, İstanbul: Boğaziçi Üniversitesi.

Zhang, H., Cheng, P., Shi, L. ve Chen, J. (2016). Optimal Denial-of-Service Attack Policy against Wireless Industrial Control Systems. iç. Cheng, P., Zhang, H. ve Chen, J. (der). *Cyber Security For Industrial Control Systems*. CRC Press: 97-117.

Zhang, J., Porras, P., ve Ullrich, J. (2010). Gaussian Process Learning for Cyber Attack Early Warning. *Statistical Analysis and Data Mining*, (3): 56-68.

EKLER

EK-1 ARAŞTIRMADA UYGULANAN KODLAMA SİSTEMATİĞİNE DAİR ÖRNEK TABLO

ÜST KATEGORİ KODLAMASI (Politika Analizi Yaklaşımı)	Kod Tanımlamaları Örneği (Bağımsız Değişken)	Politika Önerisi Örneği(Bağımlı Değişken)
Rasyonel Politika Analizi Yaklaşımı	-Nicel Analiz -Süreçler -Fayda Maliyet -Kar Odaklılık	"Stratejinin genel koordinasyonu, politika belirlemede İcra Kuruluna müşavirlik, gerekli kaynakların tahsisi, bütünleşik e-devlet yapısının oluşumu için standartların ve uyum mekanizmalarının belirlenmesi, uygulamaların strateji hedeflerine uyumunun takibi, uygulama projelerinin yürütülmesinde kurumlara rehberlik, iletişim, ölçme, değerlendirme ve raporlama işlevlerini yerine getirecektir"
Yorumsamacı Politika Analizi Yaklaşımı	-Nitel Analiz -Değer Yorumsamaları -Kamu Yararı -Katılım ve Uzlaşı	"Yüksek Motivasyon ve Zengin İçerik: Vatandaşların bilgi ve iletişim teknolojilerini kullanma motivasyonlarını artırmak üzere; bu teknolojilerin günlük hayatta sağlayacağı faydalar konusunda bilinçlendirme çalışmaları yapılacak, kamu ve özel kesimin elektronik ortamda sunduğu hizmetler yaygınlaştırılacaktır"
Karma Politika Analizi Yaklaşımı	-Karma Analiz -Sınırlı Rasyonalite -Katılım ve Uzman Analizi -Kuram, Tecrübe ve Rasyonalite Yoğurumu	"Soğuk-donmuş zincirin geliştirilmesi ve teknolojisinin iyileştirilmesi ilgili araştırma, eğitim ve yatırım çalışmaları TÜBiTAK yapısında kurulacak Türk Soğuk Tekniği Enstitüsü'nce yönlendirilecektir"

ALT KATEGORİ KODLAMASI (Politikadaki Karar Verme Yaklaşımları-Bazı Örnekler)	Kod Tanımlamaları Örneği (Bağımsız Değişken)	Politika Önerisi Örneği(Bağımlı Değişken)
Basamaklar Modeli	- Kaynaklar, Sorunlar ve Stratejilerin Oluşturulması -En İyi Alternatif Politika Oluşturulması -Uygulama, Ölçme, Değerlendirme	"Stratejinin genel koordinasyonu, politika belirlemede İcra Kuruluna müşavirlik, gerekli kaynakların tahsisi, bütünleşik e-devlet yapısının oluşumu için standartların ve uyum mekanizmalarının belirlenmesi, uygulamaların strateji hedeflerine uyumunun takibi, uygulama projelerinin yürütülmesinde kurumlara rehberlik, iletişim, ölçme, değerlendirme ve raporlama işlevlerini yerine getirecektir"
Artırımcı Karar Verme Modeli	-Marjinal Fayda -Kök Problem -Basite İndirgeme -İlave Kararlar	"Yüksek Motivasyon ve Zengin İçerik: Vatandaşların bilgi ve iletişim teknolojilerini kullanma motivasyonlarını artırmak üzere; bu teknolojilerin günlük hayatta sağlayacağı faydalar konusunda bilinçlendirme çalışmaları yapılacak, kamu ve özel kesimin elektronik ortamda sunduğu hizmetler yaygınlaştırılacaktır"
Normatif Optümum Karar Verme Modeli	-Oluşan Yeni Durumlar -Yenilikçilik -Yaratıcılık -Beklentiler -Sezgisel Yargı -Uzmanlaşma	"Soğuk-donmuş zincirin geliştirilmesi ve teknolojisinin iyileştirilmesi ilgili araştırma, eğitim ve yatırım çalışmaları TÜBiTAK yapısında kurulacak Türk Soğuk Tekniği Enstitüsü'nce yönlendirilecektir"

EK-2 ETİK KURUL ONAY YA DA MUAFİYET

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TEZ ÇALIŞMASI ETİK KURUL İZİN MUAFİYETİ FORMU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 08/01/2018

Tez Başlığı / Konusu: **TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARININ KAMU POLİTİKASI ANALİZİ ÇERÇEVESİNDE DEĞERLENDİRİLMESİ**
Yukarıda başlığı/konusu gösterilen tez çalışmam:

1. İnsan ve hayvan üzerinde deney niteliği taşımamaktadır,
2. Biyolojik materyal (kan, idrar vb. biyolojik sıvılar ve numuneler) kullanılmasını gerektirmemektedir.
3. Beden bütünlüğüne müdahale içermemektedir.
4. Gözlemsel ve betimsel araştırma (anket, ölçek/skala çalışmaları, dosya taramaları, veri kaynakları taraması, sistem-model geliştirme çalışmaları) niteliğinde değildir.

Hacettepe Üniversitesi Etik Kurullar ve Komisyonlarının Yönergelerini inceledim ve bunlara göre tez çalışmamın yürütülebilmesi için herhangi bir Etik Kuruldan izin alınmasına gerek olmadığını; aksi durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

08/01/2018
Tarih ve İmza

Adı Soyadı:	Volkan GÖÇOĞLU
Öğrenci No:	N13249848
Anabilim Dalı:	Siyaset Bilimi ve Kamu Yönetimi
Programı:	Kamu Yönetimi Doktora
Statüsü:	☐ Y.Lisans ■ Doktora ☐ Bütünleşik Dr.

DANIŞMAN GÖRÜŞÜ VE ONAYI

Uygundur.

Prof. Dr. Mehmet Devrim Aydın
(Unvan, Ad Soyad, İmza)

Detaylı Bilgi: http://www.sosyalbilimler.hacettepe.edu.tr
Telefon: 0-312-2976860 **Faks:** 0-3122992147 E-**posta:** sosyalbilimler@hacettepe.edu.tr

EK-3 ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
DOKTORA TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 09/01/2018

Tez Başlığı / Konusu:
TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARININ KAMU POLİTİKASI ANALİZİ ÇERÇEVESİNDE DEĞERLENDİRİLMESİ

Yukarıda başlığı/konusu gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 316 sayfalık kısmına ilişkin, 09/01/2018 tarihinde tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 4 'tür.

Uygulanan filtrelemeler:
1- Kabul/Onay ve Bildirim sayfaları hariç,
2- Kaynakça hariç
3- Alıntılar hariç
4- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim. 09/01/2018

Tarih ve İmza

Adı Soyadı: Volkan Göçoğlu
Öğrenci No: N13249848
Anabilim Dalı: SİYASET BİLİMİ VE KAMU YÖNETİMİ
Programı: Kamu Yönetimi
Statüsü: ☐ Y.Lisans ■ Doktora ☐ Bütünleşik Dr.

DANIŞMAN ONAYI

UYGUNDUR.

Prof. Dr. Mehmet Devrim Aydın
(Unvan, Ad Soyad, İmza)